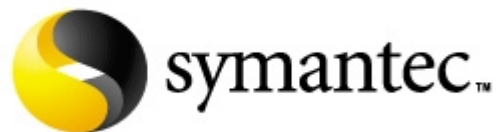


Security Assessment Report

*Network Vulnerabilities Detail Report
Grouped by Network Resource Name*

Report Generated by:	Symantec NetRecon 3.6
Licensed to:	Unknown
Serial Number:	Unknown
Machine Scanned from:	KENS-HPXE3 (10.1.1.71)
Scan Date:	5/16/2003
Scan Duration:	2 minutes, 2 seconds
Scan Objective:	Heavy scan
Resources Scanned:	Customize column order Customize column order
Resources Reported On:	All scanned network resources.

Copyright 2001, Unknown
Portions Copyright 2001, Symantec Corporation. All Rights Reserved.



Network Resource: **aqua.netrecon.com**

Resource Type: IP host, Windows NT 4.0, Windows Networking resource 4.0, Windows NT 4.0 Service Pack 3

Aliases: aqua, 10.1.3.1, 00:a0:d2:47:b9:23

of Unique Vulnerabilities: 36

Highest Risk Level Found:  98

Vulnerability Name: **auditing of rights not enabled**

Risk: 44

Vulnerability Description: NetRecon has discovered a Windows NT 4 computer that does not audit all user rights. Under this configuration, if a user has the right to back up files, that user can access all files on the computer, something that normally goes unaudited.

Vulnerability Solution: Enable auditing of rights to help ensure that users are using backup files properly.

Note: This setting may cause the audit log to fill very quickly. Typically only companies with very strict security policies will need to enable this setting.

To enable auditing of all user rights:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.

2. In the Open box, type Regedt32, and then click OK.

3. In the Registry Editor, navigate to and then select the following key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

4. From the Edit menu, choose Add Value.

5. In the Add Value dialog box specify the following, then click OK:
Value Name: FullPrivilegeAuditing
Data Type: REG_BINARY

6. In the Binary Editor dialog box, specify the following, then click OK:

Value: 01

Data Format: Hex

7. Exit the Registry Editor. Any changes take effect the next time Windows starts.

Additional Information: This information, as well as a great deal of other security-related

Vulnerability Name: **auditing of rights not enabled** (cont.)

Windows NT information, can be found in Microsoft Windows NT 4.0 Security, Audit, and Control, published by Microsoft Press.

See Common Vulnerabilities and Exposures CAN-1999-0575 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0575>

Details:

Vulnerability Name: **base system objects not audited**

Risk:  48

Vulnerability Description: NetRecon has discovered a Windows system that does not audit base objects. Base objects are kernel level processes, threads, and the like, that are used by the operating system and applications, but are not visible to users. If you believe your computer may have been compromised, for example, one way to verify this is to audit base objects, to determine that all processes used by the operating system are legitimate.

Vulnerability Solution: Turn on base object auditing.

Note: Auditing base objects can fill the audit log very quickly, making it more difficult to discover other security concerns. Enabling base auditing is recommended only when the highest-level security is desired, or when there is some specific need to audit all computer processes in great detail (to investigate the possibility of a system compromise, for example).

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. Choose Start, Programs, Administrative Tools (Common), User Manager.
2. In User Manager, select the username of the user that generally logs in to the computer, then choose Policies, Audit.
3. Select Audit These Events (if it is not already selected), and then select both the Success and Failure check boxes next to File and Object Access, then click OK.
4. Close the User Manager.
5. From the Start menu, click Run.
6. In the Open box, type Regedt32, and then click OK.

Vulnerability Name: **base system objects not audited**

(cont.)

7. In the Registry Editor, navigate to and then select the following key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

8. From the Edit menu, choose Add Value.

9. In the Add Value dialog box specify the following, then click OK:
Value Name: AuditBaseObjects
Data Type: REG_DWORD

10. In the DWORD Editor dialog box, specify the following, then click OK:
Data: 1

11. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: This and other security-related Windows NT information, can be found in Microsoft Windows NT 4.0 Security, Audit, and Control, published by Microsoft Press.

Links:

Details:Vulnerability Name: **base system objects not sufficiently protected**Risk:  48

Vulnerability Description: NetRecon has discovered a Windows computer that does not provide the C2 level of security for base system objects. Base objects are kernel level processes, threads, and the like, that are used by the operating system and applications, but are not visible to users.

Vulnerability Solution: To protect base system objects at the C2 level, add the following registry value:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.

2. In the Open box, type Regedt32, and then click OK.

3. In the Registry Editor, navigate to and then select the following key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

Vulnerability Name: **base system objects not sufficiently protected** (cont.)

4. From the Edit menu, choose Add Value.

5. In the Add Value dialog box specify the following, then click OK:
Value Name: ProtectionMode
Data Type: REG_DWORD

6. In the DWORD Editor dialog box, specify the following, then click OK:
Value: 1

7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: This and other security-related Windows NT information can be found in Microsoft Windows NT 4.0 Security, Audit, and Control, published by Microsoft Press.

Links:

Details:

Vulnerability Name: **connected to resource via Windows Networking**

Risk:  90

Vulnerability Description: NetRecon has successfully logged on to a network resource with user privileges.

NetRecon uses all known login name and password combinations to connect with each network resource it has discovered.

Many people mistakenly believe that only certain critical network resources need to have a high level of security. Attackers often try to gain access to weak links in a network, and then exploit trust relationships between network resources to access more secure resources.

Vulnerability Solution: To increase the difficulty of cracking or guessing passwords, enforce the use of secure passwords. Passwords should be a combination of letters, numbers, and punctuation. They should not correspond to words in any language, names of people, places, fictional characters, initials, dates, or similar things. They should not be common or simple sequences of letters, numbers, or characters such as abcde or 12345. Additionally, passwords should be changed regularly and should never be reused.

Additional Information:

Links:

Details:

Vulnerability Name: **connected to resource via Windows Networking** (cont.)

Share = \\10.1.3.1\IPC\$, Login Name = glennw, Password = f*e

Share = \\10.1.3.1\IPC\$, Login Name = willie, Password = k*1

Share = \\10.1.3.1\IPC\$, Login Name = administrator, Password =

Vulnerability Name: **DCOM enabled**

Risk: ■ 19

Vulnerability Description: NetRecon has discovered a Windows System that has DCOM (Distributed Component Object Model) enabled. DCOM allows programs to execute other programs remotely. If permissions are set incorrectly on the OLE registry key, an attacker can use DCOM to remotely execute a program on the computer.

Vulnerability Solution: Disable DCOM in the HKEY_LOCAL_MACHINE\Software\Microsoft\Ole registry key:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. On the Start menu, click Run.
2. On the Open box, type Regedt32, then click OK.
3. In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\Software\Microsoft\Ole key.
4. Double-click the EnableDCOM value name.
5. In the String Editor, change the Y to N and click OK.
6. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0658 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0658>

Details:

Vulnerability Name: **event auditing failure permitted**

Vulnerability Name: **event auditing failure permitted**

(cont.)

Risk:  45

Vulnerability Description: NetRecon has discovered a Windows system that does not shut down when the audit log is full or otherwise unavailable. With this setting, system events may go unaudited, making it much easier for attackers to try to a wider range of attacks.

Vulnerability Solution: Add the CrashOnAuditFail value to the registry to have the system shut down if the audit log is unavailable for any reason. After the system is shut down, the next time the system is started, only an administrator can log on to clear or archive the audit log. The administrator may need to reset the registry setting after clearing the audit logs.

Note: Typically only companies with very strict security policies will want to enable this setting, since it has the potential to disrupt work, especially when used in conjunction with security settings that cause the audit log to fill up more quickly.

To shut the system down when auditing fails:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, and then click OK.
3. In the Registry Editor, navigate to and then select the following key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
4. From the Edit menu, choose Add Value.
5. In the Add Value dialog box specify the following, then click OK:
Value Name: CrashOnAuditFail
Data Type: REG_DWORD
6. In the DWORD Editor dialog box, specify the following, then click OK:
Value: 1
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: This information, as well as a great deal of other security-related Windows NT information, can be found in Microsoft Windows NT 4.0 Security, Audit, and Control, published by Microsoft Press. See Common Vulnerabilities and Exposures CAN-1999-0575 (1)

Vulnerability Name: **event auditing failure permitted**

(cont.)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0575>**Details:**Vulnerability Name: **guest account can access application event log**Risk:  37

Vulnerability Description: NetRecon has discovered a network resource with a guest account that can view the application event log. The application event log records events reported by applications (typically application errors). An attacker could use the information in this log file to learn which applications run on a system and thus direct a more focused attack.

Vulnerability Solution: Add the RestrictGuestAccess value to the registry to restrict guest account access.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, and then click OK.
3. In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application key.
4. From the Edit menu, choose Add Value.
5. Enter the following values, and then click OK.
Value Name: RestrictGuestAccess
Data Type: REG_DWORD
6. In the DWORD Editor, type 1 in the Data field, and then click OK.
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: For more information about securing Event Log Viewing, see the following Microsoft article:
http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

Links: 1. http://www.microsoft.com/ntserver/security/exec/overview/Secure_

Vulnerability Name: **guest account can access application event log** (cont.)

NTInstall.asp

Details:Vulnerability Name: **guest account can access security event log**Risk:  45

Vulnerability Description: NetRecon has discovered a network resource with a Guest account that can view the Security Event Log. The Security log contains sensitive security-related information, such as logon/logoff and username information, that could be used by an attacker to gain access to this computer.

This vulnerability applies to Windows NT 4.0 Server and Workstation.

Vulnerability Solution: Add the RestrictGuestAccess value to the registry to restrict guest account access.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, and then click OK.
3. In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Security key.
4. From the Edit menu, choose Add Value.
5. Enter the following values, and then click OK.
Value Name: RestrictGuestAccess
Data Type: REG_DWORD
6. In the DWORD Editor, type 1 in the Data field, and then click OK.
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: For more information about securing Event Log Viewing, see the following Microsoft article:
http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

Vulnerability Name: **guest account can access security event log** (cont.)

Links: 1.
http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

Details:

Vulnerability Name: **guest account can access system event log**

Risk:  45

Vulnerability Description: NetRecon has discovered a network resource with a Guest account that can view the System Event Log. The system event log contains events logged by Windows system components, such as failed attempts to load a driver. An attacker could use this information to find out more about the operating system of this computer, which could help in designing a more focused attack.

Vulnerability Solution: Add the RestrictGuestAccess value to the registry to restrict Guest account access.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, and then click OK.
3. In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System key.
4. From the Edit menu, choose Add Value.
5. Enter the following values, and then click OK.
Value Name: RestrictGuestAccess
Data Type: REG_DWORD
6. In the DWORD Editor, type 1 in the Data field, and then click OK.
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: For more information about securing Event Log Viewing, see the following Microsoft article:
http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

Vulnerability Name: **guest account can access system event log** (cont.)

Links: 1.
http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

Details:

Vulnerability Name: **IP address found from name**

Risk: ■ 5

Vulnerability Description: NetRecon has successfully discovered the IP address of a network resource using its name.

If NetRecon discovers the names of any network resources (via Windows networking, for example), it attempts to obtain their IP address as well.

Finding the IP address of a network resource verifies that the resource exists. It also helps attackers identify TCP/IP networks to scan for further resources. Having an IP address also opens up the possibility of a wide range of TCP/IP information gathering (port scans, for example) and attacks.

Vulnerability Solution: Do not allow hosts outside your firewall to resolve internal IP addresses unless absolutely necessary. Public DNS should contain only public systems.

Additional Information:

Links:

Details:

Alias = 10.1.3.1

Vulnerability Name: **IP name obtained**


Risk: ■ 10

Vulnerability Description: NetRecon has discovered the IP name of a network resource.

System names often reveal something about the system. For example, servers sometimes have the word server in the name, systems are named after their users, etc. Systems with an IP address but no name are usually either old, unused systems (which can be attacked with less risk of notice) or protected systems (containing highly significant information).

Knowing system names can, therefore, help attackers focus their

Vulnerability Name: IP name obtained	(cont.)
attacks on key systems.	
Vulnerability Solution:	Do not allow hosts outside your firewall to resolve internal IP names or addresses unless absolutely necessary. Public DNS should contain only public systems.
Additional Information:	
Links:	
Details:	
Alias = aqua	
Alias = AQUA.netrecon.com	
Alias = AQUA	
Alias = aqua.netrecon.com	

Vulnerability Name: land attack (spoofed SYN) possible
Risk:  58
Vulnerability Description: NetRecon has discovered a network resource that may be susceptible to denial of service attacks. TCP/IP systems may be vulnerable to spoofed connection request (SYN) packets that use the system's own address as the source and destination IP address and the same source and destination ports, making a system believe it sent the packets to itself. This type of attack slows a system down as it tries to respond to itself. The attack is named land after widely-distributed source code files used to exploit this vulnerability. Note: NetRecon detects this vulnerability based on version information, which means that NetRecon reports it even if you have applied the solution, as long as the version number remains the same.
Vulnerability Solution: Check with your vendor for any patches that reduce the effectiveness of this attack. Microsoft has released a post-SP3 hotfix called teardrop2-fixto address this and several other TCP/IP problems. Apply this hotfix or Windows NT Service Pack 4 or greater. The hotfix can be downloaded from: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/ (1)
Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0016 (1)
Links: 1. ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/

Vulnerability Name: **land attack (spoofed SYN) possible**

(cont.)

2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0016>**Details:**Vulnerability Name: **LanManager authentication permitted**Risk:  48

Vulnerability Description: NetRecon has discovered a Windows system that permits LanManager authentication, which uses a weaker form of encryption than Windows NT authentication. Many systems permit this by default for compatibility with Windows 95 and NetWare clients. An attacker could potentially sniff and then crack the LanManager password hash.

Vulnerability Solution: To permit only Windows NT authentication, first apply the lm-fix hotfix, which is available at:
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/lm-fix/> (1)

After you have applied the hotfix, add the LMCompatibilityLevel value as follows:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, and then click OK.
3. In the Registry Editor, navigate to and then select the following key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
4. From the Edit menu, choose Add Value.
5. In the Add Value dialog box specify the following, then click OK:
Value Name: LMCompatibilityLevel
Data Type: REG_DWORD
6. In the DWORD Editor dialog box, specify the following, then click OK:
Value: 2
Radix: Hex
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Vulnerability Name: **LanManager authentication permitted** (cont.)

Additional Information: This information, as well as a great deal of other security-related Windows NT information, can be found in Microsoft Windows NT 4.0 Security, Audit, and Control, published by Microsoft Press.

Links: 1.
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/lm-fix/>

Details:

Vulnerability Name: **legal notice logon banner not enabled**

Risk: ■ 4

Vulnerability Description: NetRecon has discovered a Windows system that does not provide a legal notice during the logon process.

A legal notice can be used to warn anyone trying to log on to a computer of the company's legal policies regarding computer use, which can help strengthen the legal case in the event of misuse.

Example legal notice: Only individuals currently assigned an account on this computer by XYZCorp may access data on this computer. All information stored on this computer is the property of XYZCorp and is subject to all the protections accorded intellectual property.

Vulnerability Solution: Add a legal notice logon banner.

Note: Check with your legal department to determine the exact wording of such a notice.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.

2. In the Open box, type Regedt32, and then click OK.

3. In the Registry Editor, navigate to and then select the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

4. From the Edit menu, choose Add Value.

5. In the Add Value dialog box specify the following, then click OK:

Value Name: LegalNoticeText

Data Type: REG_SZ

Vulnerability Name: **legal notice logon banner not enabled**

(cont.)

6. In the String Editor dialog box, include the legal notice your company wants to use, then click OK.

7. From the Edit menu, choose Add Value.

8. In the Add Value dialog box specify the following, then click OK:
Value Name: LegalNoticeCaption
Data Type: REG_SZ

9. In the String Editor dialog box, include the text you'd like to appear in the title bar of the banner dialog box, then click OK.

10. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: This information, as well as a great deal of other security-related Windows NT information, can be found in Microsoft Windows NT 4.0 Security, Audit, and Control, published by Microsoft Press, and in the NT security document available at the following address:
http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp
See Common Vulnerabilities and Exposures CVE-1999-0590 (2)

Links: 1.

http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0590>

Details:Vulnerability Name: **local users can get admin access using getadmin**Risk:  43

Vulnerability Description: NetRecon has discovered a network resource running an older version of Windows that may be susceptible to an unauthorized access attack.

Windows NT 4.0 systems are vulnerable to an attack that exploits a kernel routine for allowing access to system processes (WinLogon in this case) to add any user to the administrators group. The attack is named getadmin after a widely-distributed source code file used to exploit this vulnerability.

Note: NetRecon detects this vulnerability based on version information, which means that NetRecon reports it even if you have applied the solution, as long as the version number remains the same.

Vulnerability Name: **local users can get admin access using getadmin** (cont.)

Vulnerability Solution: Microsoft has released a post-SP3 hotfix called getadmin-fix to address this problem. Apply the hotfix or Windows NT Service Pack 4 or greater. The hotfix can be downloaded from:
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/getadmin-fix/> (1)

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0496 (2)

Links: 1.

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/getadmin-fix/>
1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0496>

Details:

Vulnerability Name: **local users can install print drivers**

Risk:  42

Vulnerability Description: NetRecon has discovered a registry setting that allows anyone to install print drivers on this system. This setting (i.e., registry value) should be set to enable the system spooler to restrict the ability to install printer drivers to administrators and print operators (on the server) or power users (on the workstation).

Vulnerability Solution: Add the AddPrintDrivers value to the registry.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.

2. In the Open box, type Regedt32, and then click OK.

3. In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers key.

4. From the Edit menu, choose Add Value.

5. Enter the following values, and then click OK.

Value Name: AddPrintDrivers

Data Type: REG_DWORD

6. In the DWORD Editor, type 1 in the Data field, and then click OK.

7. Exit the Registry Editor. Changes take effect the next time

Vulnerability Name: **local users can install print drivers**

(cont.)

Windows starts.

Additional Information:

Links:

Details:Vulnerability Name: **logon dialog box allows system shutdown**Risk: ■ 3

Vulnerability Description: NetRecon has discovered a Windows system that allows a user to shutdown and reboot the system from the Login Information dialog box. Windows NT 4.0 systems display the shutdown button by default. If the system uses more than one operating system, an attacker could use this button to shutdown Windows NT and reboot into a less secure operating system.

Note: Where security precautions must be very strict, you should deny physical access to the system to prevent an attacker from turning the computer off and rebooting from a disk.

Vulnerability Solution: Disable the shutdown button on the Login Information dialog box:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. On the Start menu, Click Run.
2. In the Open box, type Regedt32, then click OK.
3. In the Registry Editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
4. Double-Click the ShutdownWithoutLogon value name. The String Editor dialog box appears.
5. In the String box, type 0.
6. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: For more information on this vulnerability, see Securing Microsoft Windows NT Installation at:
http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

Vulnerability Name: **logon dialog box allows system shutdown** (cont.)

See Common Vulnerabilities and Exposures CAN-1999-0593 (2)

- Links: 1. http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0593>

Details:

Vulnerability Name: **nbssession service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the nbssession service.

The nbssession service permits Server Message Block (SMB) communications between Windows network resources and many other kinds of network resources, including other Windows resources. The SMB protocol can be used to allow network resources with different operating systems to share files, printers, etc.

Some versions of Windows 95 are vulnerable to file access attacks using this service. For example, NetRecon tries to use this service to obtain .PWL files, which can often be decrypted to discover passwords and network resource names.

Vulnerability Solution: If it is not needed, disable this service. The nbssession service (also known as NetBEUI) is unique to Windows operating systems. An attacker who runs a simple port scan can infer what operating system you are using if the nbssession service is running. This is, in fact, one of the ways that NetRecon identifies operating systems.

Note: In some cases, turning this service off may prevent or hinder some network communications.

Additional Information:

Links:

Details:

Protocol = TCP, Port = 139, Service = nbssession

Vulnerability Name: **network access to CD-ROM possible**

Risk:  18

Vulnerability Description: NetRecon has discovered a Windows system that allows its

Vulnerability Name: **network access to CD-ROM possible** (cont.)

CD-ROM to be accessed from the network. Windows NT 3.51 and 4.0 systems allow CD-ROM drives to be shared on the network. If sensitive information is kept on a shared CD-ROM, an attacker could access the information on the CD-ROM.

Vulnerability Solution: In the Winlogon key of the Windows NT registry, enable the AllocateCDRoms value name. This setting prevents network users, including Administrators, from accessing the CD-ROM while you are logged in to the computer. You should remove the CD-ROM disk when finished because network users can still access the CD-ROM when you have logged out of the computer.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. On the Start menu, Click Run.
2. In the Open box, type Regedt32, then click OK.
3. In the Registry Editor, navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon.
4. In the Edit menu, click Add Value.
5. In the Add Value dialog box specify the following, then click OK:
Value Name: AllocateCDRoms
Data Type: REG_SZ
6. In the String Editor dialog box, specify the following, then click OK:
Value: 1
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: For more information on shared CD-ROM drives, refer to Knowledge Base Article Q172520 in the Microsoft Support Online Library at:
<http://support.microsoft.com/support/kb/articles/Q172/5/20.ASP> (1)
See also: Securing Microsoft Windows NT Installation at:
http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp
See Common Vulnerabilities and Exposures CVE-1999-0594 (3)

Links: 1. <http://support.microsoft.com/support/kb/articles/Q172/5/20.ASP>
2. http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

Vulnerability Name: **network access to CD-ROM possible**

(cont.)

3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0594>**Details:**Vulnerability Name: **network access to floppy disk drive possible**Risk: ■ 18

Vulnerability Description: NetRecon has discovered a Windows system that allows its Floppy disk drive to be accessed from the network. Windows NT 3.51 and 4.0 systems allow floppy disk drives to be shared on the network. If sensitive or proprietary information is kept on a shared disk drive, an attacker could access the information on the disk.

Vulnerability Solution: In the Winlogon key of the Windows NT registry, enable the AllocateFloppies value name. This setting prevents network users, including Administrators, from accessing the disk drive while you are logged in. Remove the floppy disk when finished because network users can still access the disk drive when you have logged out of the computer:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. On the Start menu, Click Run.
2. In the Open box, type Regedt32, and then click OK.
3. In the Registry Editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
4. In the Edit menu, click Add Value.
5. In the Add Value dialog box specify the following, then click OK:
Value Name: AllocateFloppies
Data Type: REG_SZ
6. In the String Editor dialog box, specify the following, then click OK:
Value: 1
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: For more information on shared floppy disk drives, refer to

Vulnerability Name: **network access to floppy disk drive possible** (cont.)

Knowledge Base Article Q172520 in the Microsoft Support Online Library at:

<http://support.microsoft.com/support/kb/articles/Q172/5/20.ASP> (1)

See also: Securing Microsoft Windows NT Installation at:

http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

See Common Vulnerabilities and Exposures CVE-1999-0594 (3)

Links: 1.

<http://support.microsoft.com/support/kb/articles/q172/5/20.asp?FR=0>

2.

http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0594>

Details:

Vulnerability Name: **network resource identified**

Risk: ■ 16

Vulnerability Description: NetRecon has obtained information that helps to identify a particular network resource. This information could include full or partial identification of the operating system, server types (SMB server, for example), whether a computer is an IP host, etc.

Once an attacker has identified a specific target, he or she can find and exploit weakness in that resource.

Vulnerability Solution: Using the data table in NetRecon, determine how the information was obtained. Either eliminate the service responsible or configure it to not give any clues that can help identify the network resource.

Additional Information:

Links:

Details:

Type = IP host

Type = Windows NT, Revision = 4.0

Type = Windows Networking resource

Type = Windows NT

Type = Windows Networking resource, Revision = 4.0

Type = Windows Networking resource

Type = Windows NT, Revision = 4.0 Service Pack 3

Vulnerability Name: **network resource identified**

(cont.)

Type = Windows NT

Type = IP host

Type = Windows NT, Revision = 4.0 Service Pack 3

Type = Windows NT

Type = IP host

Type = Windows Networking resource

Type = Windows Networking resource, Revision = 4.0

Type = Windows Networking resource

Type = Windows NT, Revision = 4.0

Type = Windows NT

Vulnerability Name: **newtear attack (corrupt UDP packet) possible**Risk:  70

Vulnerability Description: NetRecon has discovered an older version of Windows that may be susceptible to a malformed packet denial of service attack.

Windows NT 4.0 and Windows 95 systems are vulnerable to a denial of service attack that is a modified version of the teardrop attack. The attack sends IP fragments deliberately constructed to result in corrupt UDP datagrams when reassembled, which can crash a computer. Several slightly different versions of code to exploit this vulnerability have been created, including bonk, boink, and newtear.

Note: NetRecon detects this vulnerability based on version information, which means that NetRecon reports it even if you have applied the solution, as long as the version number remains the same.

Vulnerability Solution: Microsoft has released a post-SP3 hotfix for Windows NT 4.0 called teardrop2-fix to address this and several other TCP/IP problems. Apply this hotfix or Windows NT 4.0 Service Pack 4 or greater. The hotfix can be downloaded from:
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/> (1)

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0104 (2)

Links: 1.

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/>

2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0104>

Vulnerability Name: **newtear attack (corrupt UDP packet) possible** (cont.)**Details:**Vulnerability Name: **non-administrator job scheduling permitted**Risk:  43

Vulnerability Description: NetRecon has discovered a Windows network resource with a registry setting that permits an attacker to execute malicious applications using the schedule service. Scheduler, which is designed to make it easy to run programs at certain times, runs programs with the authority of the local system account.

For the greatest security, Microsoft recommends permitting only administrators to schedule jobs.

Vulnerability Solution: To restrict everyone but administrators from scheduling jobs, add the SubmitControl registry key, as follows:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, and then click OK.
3. In the Registry Editor, navigate to and then select the following key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
4. From the Edit menu, choose Add Value.
5. In the Add Value dialog box specify the following, then click OK:
Value Name: SubmitControl
Data Type: REG_DWORD
6. In the DWORD Editor dialog box, specify the following, then click OK:
Value: 0
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: This information, as well as a great deal of other security-related Windows NT information, can be found in Microsoft Windows NT 4.0 Security, Audit, and Control, published by Microsoft Press. See Common Vulnerabilities and Exposures CVE-1999-0839 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0839>

Vulnerability Name: **non-administrator job scheduling permitted** (cont.)**Details:**Vulnerability Name: **non-administrator remote registry access possible**Risk:  98

Vulnerability Description: NetRecon has discovered that any person or device that can access the system remotely can access and modify the registry. You can restrict remote access on Windows NT 3.51 with Service pack 4 or Windows NT version 4.0 systems.

Vulnerability Solution: To control remote access to the registry:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. On the Start menu, click Run.
2. In the Open box, type Regedt32, then click OK.
3. In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control key.
4. Choose Edit, Add Key (unless the SecurePipeServers key already exists, in which case skip to step 6).
5. Enter the following values:
Key Name: SecurePipeServers
Class: REG_SZ
6. Select the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers key.
7. On the Edit menu, click Add Key (unless the winreg key already exists, in which case skip to step 9).
8. Enter the following values:
Key Name: winreg
Class: REG_SZ
9. Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg key.

Vulnerability Name: **non-administrator remote registry access possible** (cont.)

10. On the Edit menu, click Add Value.

11. Enter the following values:

Value Name: Description

Data Type: REG_SZ

String: Registry Server

12. Select the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
\SecurePipeServers\winreg

13. Choose Security, Permissions. Remove any permissions
except:

Administrators: Full Control

Note: Any other permissions configuration, even if it meets your
security policy, will cause NetRecon to report this vulnerability.

14. Exit the Registry Editor. Changes take effect the next time
Windows starts.

Additional Information: Some services need remote access to the registry to function
correctly. For more information about bypassing the access
restrictions on the Winreg key, see the following Microsoft
Knowledge base article:
<http://support.microsoft.com/support/kb/articles/q153/1/83.asp?FR=0>
See Common Vulnerabilities and Exposures CAN-1999-0562 (2)

Links: 1.
<http://support.microsoft.com/support/kb/articles/q153/1/83.asp?FR=0>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0562>

Details:

Vulnerability Name: **open TCP port may allow unauthorized activity**

Risk: ■ 14

Vulnerability Description: NetRecon has discovered an open TCP port.

When this vulnerability is included in a NetRecon scan report, the
following pieces of information are in the Details section:
-port number

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't
know what this service is, or didn't expect to see it, verify that the
service is not a back door left by an attacker. If the service is

Vulnerability Name: **open TCP port may allow unauthorized activity** (cont.)

required only for internal use, protect it with a firewall. If the service is required for external use, consider running it from a demilitarized zone and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see:
<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = TCP, Port = 139, Service = nbsession

Vulnerability Name: **open UDP port may allow unauthorized activity**

Risk: ■ 17

Vulnerability Description: NetRecon has discovered an open UDP port.

Since the UDP protocol doesn't use a three-way handshake to establish connections the way TCP does, it is more susceptible to attacks involving spoofed IP addresses. There are a wide range of denial of service attacks that exploit this weakness in UDP to create infinite loops.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:
-port number

Note: There is a chance of UDP ports being incorrectly detected as open.

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, firewall it. If the service is required for external use, consider running it from a demilitarized zone, and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see:
<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = UDP, Port = 138

Protocol = UDP, Port = 137

Vulnerability Name: **out-of-band attack (malformed packet) possible**

Risk:  71

Vulnerability Description: Windows NT 4.0 systems without the appropriate hotfix are vulnerable to a denial of service attack called out of band that crashes the computer. The attack involves creating packets with the urgent flag set and then setting the urgent pointer to the end of the frame (where NT expects normal data to follow the urgent data).

Note: NetRecon detects this vulnerability based on version information, which means that NetRecon reports it even if you have applied the solution, as long as the version number remains the same.

Vulnerability Solution: Microsoft has created a post-SP3 hotfix called teardrop2-fix to address this and several other TCP/IP problems. Apply this hotfix or Windows NT 4.0 Service Pack 4 or greater. The hotfix can be downloaded from:
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/> (1)

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0153 (2)

Links: 1.
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/teardrop2-fix/>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0153>

Details:

Vulnerability Name: **password filter not enabled**

Risk:  48

Vulnerability Description: NetRecon has discovered a Windows system that does not have the password filter, which checks for the password strength, enabled. The password filter checks for things such as password length, the presence of numbers or symbols in the password, and forms of the user's name or username in the password. Without this filter, users can choose passwords that are easy to guess.

Vulnerability Solution: Add the password filter to the system.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, then click OK.

Vulnerability Name: **password filter not enabled**

(cont.)

3. In the Registry Editor, navigate to and then select the following key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

4. From the Edit menu, choose Add Value.

5. In the Add Value dialog box specify the following, then click OK:
Value Name: Notification Packages
Data Type: REG_MULTI_SZ

6. In the Multi-String Editor dialog box, specify the following, then click OK:
Data: PASSFILT

Note: If this key already exists and has any strings, add this data and leave any existing strings.

7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: This information, as well as a great deal of other security-related Windows NT information, can be found in Microsoft Windows NT 4.0 Security, Audit, and Control, published by Microsoft Press. See Common Vulnerabilities and Exposures CVE-1999-0570 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0570>

Details:Vulnerability Name: **registry accessed remotely**Risk:  44

Vulnerability Description: In Windows network resources, being able to access the registry remotely can provide a wealth of information gathering and attack possibilities.

For example, registry access lets an attacker find out which version of Windows is running. Windows 95 computers sometimes have plain text versions of passwords in the registry. Being able to write to the registry lets an attacker plant Trojan horse applications.

Vulnerability Solution: To prevent all remote access to the registry, disable the Windows NT Server service.

Note: Disabling this service prevents this system from being able to share its own resources (files, folders, printers, etc.) via Windows networking, though it doesn't prevent the system from accessing resources shared by other computers.

Vulnerability Name: **registry accessed remotely**

(cont.)

To disable the Server service:

1. Choose Start, Settings, Control Panel.
2. Double-click Services.
3. Select Server in the Service list.
4. Click Startup.
5. Click Disabled, then click OK.

6. Click Close. This change takes effect the next time you start Windows.

Additional Information: <http://support.microsoft.com/support/kb/articles/q153/1/83.asp?FR=0>
See Common Vulnerabilities and Exposures CVE-1999-0562 (2)

Links: 1. <http://support.microsoft.com/support/kb/articles/q153/1/83.asp?FR=0>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0562>

Details:Vulnerability Name: **SMB logon request size mismatch denial of service**Risk:  71

Vulnerability Description: Windows NT 4.0 can be crashed or rebooted by sending an SMB logon request which has a mismatched size.

Note: NetRecon detects this vulnerability based on version information, which means that NetRecon reports it even if you have applied the solution, as long as the version number remains the same.

Vulnerability Solution: Microsoft has released a hotfix to address this problem. Apply this hotfix or Windows NT 4.0 Service Pack 4 or greater.

Microsoft's hot-fix:
<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/srv-fix> (1)

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0225 (2)

Links: 1. <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3/srv-fix>

Vulnerability Name: **SMB logon request size mismatch denial of service** (cont.)

2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0225>

Details:

Vulnerability Name: **SMB message signing disabled (client)**

Risk:  50

Vulnerability Description: NetRecon has discovered that Server Message Block (SMB) message signing has not been configured or is disabled on this Windows network resource. SMB message signing counters spoofed and active message attacks. When message signing is enabled on a client, it will only communicate with servers that also have SMB message signing enabled.

Vulnerability Solution: A client system becomes SMB signing enabled by having Windows NT 4.0 Service Pack 3 or greater, and by adding two settings to the registry: RequireSecuritySignature and EnableSecuritySignature.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

The following instructions describe how and where to add these values.

To enable SMB message signing on this client:

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, and then click OK.
3. In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rdr\Parameters key.
4. From the Edit menu, choose Add Value.
5. Enter the following, and then click OK.
Value Name: EnableSecuritySignature
Data Type: REG_DWORD
6. In the DWORD Editor, type 1 in the Data field, and then click OK.
7. From the Edit menu, choose Add Value.

Vulnerability Name: **SMB message signing disabled (client)** (cont.)

8. Enter the following, and then click OK.
Value Name: RequireSecuritySignature
Data Type: REG_DWORD
9. In the DWORD Editor, type 1 in the Data field, and then click OK.
10. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: SMB message signing must also be enabled on the server or servers that will communicate with this workstation. For instructions on enabling SMB message signing on a server, see the SMB message signing disabled (server) vulnerability.

For additional information about this vulnerability, see Microsoft Knowledge Base article Q161372, available at:
<http://support.microsoft.com/support/kb/articles/q161/3/72.asp?FR=0>

You can download the latest Windows NT 4.0 service pack from:
<http://www.microsoft.com/ntworkstation/downloads/> (2)

- Links:**
1. <http://support.microsoft.com/support/kb/articles/q161/3/72.asp?FR=0>
 2. <http://www.microsoft.com/ntworkstation/downloads/>

Details:

Vulnerability Name: **SMB message signing disabled (server)**

Risk:  50

Vulnerability Description: NetRecon has discovered a vulnerability where Server Message Block (SMB) message signing has not been configured or is disabled. The SMB authentication protocol, also known as Common Internet File System (CIFS) provides a method for sending information between networked computers while supporting interoperability among varieties of networks. SMB counters spoofed and active message attacks by requiring message signing. When message signing is enabled on a server, the server will only communicate with clients that also have SMB enabled. And similarly, clients will only communicate with servers that are SMB enabled.

Vulnerability Solution: A server or client system becomes SMB signing enabled by having Windows NT 4.0 Service Pack 3 or greater, and by adding two settings to the registry: RequireSecuritySignature and EnableSecuritySignature. The following instructions describe how and where to add these values.

Vulnerability Name: **SMB message signing disabled (server)**

(cont.)

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, and then click OK.
3. In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters key.
4. From the Edit menu, choose Add Value.
5. Enter the following, and then click OK.
Value Name: EnableSecuritySignature
Data Type: REG_DWORD
6. In the DWORD Editor, type 1 in the Data field, and then click OK.
7. From the Edit menu, choose Add Value.
8. Enter the following, and then click OK.
Value Name: RequireSecuritySignature
Data Type: REG_DWORD
9. In the DWORD Editor, type 1 in the Data field, and then click OK.
10. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: SMB signing must also be enabled on the Workstation systems that will communicate with this server. For instructions, see the following Microsoft Knowledge base article:

<http://support.microsoft.com/support/kb/articles/q161/3/72.asp?FR=0>

You can download the latest Windows NT 4.0 service pack from:
<http://www.microsoft.com/ntworkstation/downloads/> (2)

- Links: 1. <http://support.microsoft.com/support/kb/articles/q161/3/72.asp?FR=0>
2. <http://www.microsoft.com/ntworkstation/downloads/>

Details:

Vulnerability Name: **unrestricted null session enumeration possible**

Risk:  37

Vulnerability Description: NetRecon has discovered the ability for anonymous logon users to list domain user names and shares. Once this information is obtained, the attacker could begin attacking other systems on the network. Windows NT 4.0 Service Pack 3 and a hotfix for Windows NT 3.51 provide a mechanism for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. The Windows NT ACL editor requires listing account names from Domain Controllers. For example, to obtain the list of users and groups to select whom a user wants to grant access rights. Listing account names is also used by Windows NT Explorer to select from list of users and groups to grant access to a share.

Vulnerability Solution: Update to the latest Windows NT service pack (if you have not already done so) and then add the RestrictAnonymous value to the registry.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, then click OK.
3. In the Registry Editor, navigate to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa key.
4. From the Edit menu, choose Add Value.
5. Enter the following values, then click OK.
Value Name: RestrictAnonymous
Data Type: REG_DWORD
6. In the DWORD Editor, type 1 in the Data field, then click OK.
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: Please refer to the following Microsoft Knowledgebase article for more information:
<http://support.microsoft.com/support/kb/articles/q143/4/74.asp?FR=0>

Links: 1.
<http://support.microsoft.com/support/kb/articles/q143/4/74.asp?FR=0>

Vulnerability Name: **unrestricted null session enumeration possible** (cont.)**Details:**Vulnerability Name: **username of last login displayed**Risk: ■ 16

Vulnerability Description: NetRecon has discovered a Windows system that displays the name of the last user to log in. By default, Windows NT 3.51 and 4.0 systems display this information in the Login Information dialog box. Displaying a valid username makes it easier for an attacker to access the computer. The Attacker can then attempt to guess the password and gain access to the system. Alternately, if the account lockout feature is enabled, the attacker could maliciously cause the account to be locked-out for the time period designated in the User Manager.

Vulnerability Solution: Enable the DontDisplayLastUserName value name in the Winlogon key of the Windows NT registry:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. On the Start menu, Click Run.
2. In the Open box, type Regedt32, then click OK.
3. In the Registry Editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
4. In the Edit menu, click Add Value.
5. In the Add Value dialog box specify the following, then click OK:
Value Name: DontDisplayLastUserName
Data Type: REG_SZ
6. In the String Editor dialog box, type 1, then click OK.
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: For more information on the hiding the last user login name, refer to Knowledge Base Article Q114463 in the Microsoft Support Online Library at:
<http://support.microsoft.com/support/kb/articles/Q114/4/63.ASP> (1).
See also Securing Microsoft Windows NT Installation at:

Vulnerability Name: **username of last login displayed** (cont.)

http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

See Common Vulnerabilities and Exposures CVE-1999-0592 (3)

- Links: 1. <http://support.microsoft.com/support/kb/articles/q114/4/63.asp?FR=0>
2. http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp
3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0592>

Details:

Vulnerability Name: **Windows NT page file not cleared at system shutdown**

Risk:  43

Vulnerability Description: NetRecon has discovered a Windows system that does not clear the page file at system shutdown. On Windows NT 3.51 or 4.0, some third-party programs can store unencrypted information in memory. If Windows NT does not clear the page file at shutdown, an attacker may be able to access the page file and learn sensitive information such as usernames and passwords.

Vulnerability Solution: Set the system to clear the page file upon shutdown:

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. On the Start menu, click Run.
2. In the Open box, type Regedt32, then click OK.
3. In the Registry Editor, navigate to the HKEY_Local_Machine\System\CurrentControlSet\Control\Session Manager\Memory Management key.
4. Select the ClearPageFileAtShutdown value.
5. In the Edit menu, click DWord to open the Dword editor.
6. In the Data box, set the value to 1.
7. Exit the Registry Editor. Changes take effect the next time Windows starts.

Vulnerability Name: **Windows NT page file not cleared at system shutdown** (cont.)

Additional Information: For more information on clearing the Page file, refer to Knowledge Base Article Q182086 in the Microsoft Support Online Library at: <http://support.microsoft.com/support/kb/articles/Q182/0/86.ASP> (1)
See also: Securing Microsoft Windows NT Installation at: http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp
See Common Vulnerabilities and Exposures CVE-1999-0595 (3)

Links: 1. <http://support.microsoft.com/support/kb/articles/q182/0/86.asp?FR=0>
2. http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp
3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0595>

Details:

Vulnerability Name: **Windows NT system caches logon credentials**

Risk:  48

Vulnerability Description: NetRecon has discovered a Windows NT system that caches the last interactive user's logon credentials for logging on to a domain. Windows NT 4.0 and 3.51 SP5 systems do this by default so that the user can login to a domain if the domain controller is offline or the computer is disconnected. An attacker could access the credential cache, learn the last user's logon credentials, and use those credentials to gain full access to the computer.

Vulnerability Solution: For the highest level of security, Microsoft recommends disabling logon credential caching. To do so, in the registry, add the CachedLogonsCount value and set it to 0, or, if it already exists, change the CachedLogonsCount value to be 0.

Note: After applying this solution, if the domain controller is offline or the computer is disconnected, the user will not be able to connect to the domain controller. However, the user can still login to a local account on the computer.

Warning: Carefully consider potential consequences before making modifications to the registry. While restricting user access to the registry may make it more secure, it may prevent users from running necessary programs. In addition, incorrectly modifying the registry may cause serious, system-wide problems.

1. From the Start menu, click Run.
2. In the Open box, type Regedt32, and then click OK.

Vulnerability Name: **Windows NT system caches logon credentials** (cont.)

3. In the Registry Editor, navigate to HKEY_Local_Machine\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount.

4. If the CachedLogonsCount value already exists, double-click it, follow step 5, and then skip to step 9. If it doesn't exist, follow steps 6-9.
The String Editor dialog box appears.

5. In the String text box, replace whatever is already there with a 0 (note that this character is the number zero, not the uppercase letter), then click OK.

6. If the CachedLogonsCount value does not exist, choose Edit, Add Value.
The Add Value dialog box appears.

7. In the Value Name text box, type CachedLogonsCount, leave the Data Type as REG_SZ, then click OK.
The String Editor dialog box appears.

8. Type 0 (note that this character is the number zero, not the uppercase letter), then click OK.

9. Exit the Registry Editor. Changes take effect the next time Windows starts.

Additional Information: For additional information on the CachedLogonsCount value name, see Securing Microsoft Windows NT Installation. You can download this document at:

http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp

See Common Vulnerabilities and Exposures CVE-1999-0595 (2)

Links: 1. http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0595>

Details:Network Resource: **blue.netrecon.com**

Resource Type: IP host, HP-UX, HP-UX B.10.00

Aliases: blue, 10.1.6.1, 08:00:04:3b:92:b1

of Unique Vulnerabilities: 34

Highest Risk Level Found: ● 93

Vulnerability Name: chargen service enabledRisk:  60

Vulnerability Description: NetRecon has discovered a network resource running the chargen service.

The chargen service causes a TCP server to send a constant stream of characters to the client until the client terminates the connection. chargen can be used legitimately for certain testing purposes.

Because chargen produces a continual stream of characters, it is susceptible to misuse for denial of service attacks. For example, spoofed packets can link the chargen port to the echo port, creating an infinite loop. This type of attack consumes increasing amounts of network bandwidth, degrading network performance or, in some cases, completely disabling portions of a network.

Vulnerability Solution: To avoid this type of attack, disable the chargen service. Additionally, monitoring attempts to access disabled services can alert you to the presence of attackers.

Microsoft has released a hotfix to address chargen attacks directed at Windows NT 4.0 Simple TCP/IP services. The hotfix can be downloaded from:

[ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix \(1\)](ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix (1))

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0103 (2)
See Common Vulnerabilities and Exposures CAN-1999-0639 (3)

Links: 1. <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0103>
3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0639>

Details:

Protocol = TCP, Port = 19, Service = chargen

Vulnerability Name: daytime service enabledRisk:  11

Vulnerability Description: NetRecon has discovered a network resource running the daytime service.

The daytime service returns the date and time.

The format of the daytime service can sometimes tell an attacker something about a network resource, such as the operating system

Vulnerability Name: **daytime service enabled** (cont.)

it is running. This service is potentially vulnerable to misaddressed packet attacks, which can link the daytime port to the echo port, or perform similar functions to consume network bandwidth.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0638 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0638>

Details:

Protocol = TCP, Port = 13, Service = daytime

Vulnerability Name: **discard service enabled**

Risk:  15

Vulnerability Description: NetRecon has discovered a network resource running the discard service.

The discard service reads packets sent to it and then discards them.

Attackers could use a connect response from this, or any service to verify the presence of a network resource.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0636 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0636>

Details:

Protocol = TCP, Port = 9, Service = discard

Vulnerability Name: **echo service enabled**

Risk:  60

Vulnerability Description: NetRecon has discovered a network resource running the echo service.

The echo service causes a server to return whatever a client sends. It can be used for a number of testing purposes, much like chargen.

Vulnerability Name: **echo service enabled** (cont.)

Since the echo port returns whatever is sent to it, it is susceptible to attacks that create false return addresses. For example, spoofed packets can link the echo port to the chargen port, creating an infinite loop. This type of attack consumes increasing amounts of network bandwidth, degrading network performance or, in some cases, completely disabling portions of a network.

Vulnerability Solution: To avoid this type of attack, disable the echo service. Additionally, monitoring attempted access to the echo service can alert you to the presence potential attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0635 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0635>

Details:

Protocol = TCP, Port = 7, Service = echo

Vulnerability Name: **exec service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the exec service.

The exec service (also called rexec) provides remote command execution facilities with authentication based on user names and passwords.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password guessing.

Vulnerability Solution: If possible, disable the exec service. Additionally, monitoring attempted access to the exec service can alert you to the presence potential attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0618 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0618>

Details:

Protocol = TCP, Port = 512, Service = exec

Vulnerability Name: **ftp service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the FTP

Vulnerability Name: **ftp service enabled** (cont.)

service.

FTP (File Transfer Protocol) is a protocol for transferring files between systems. Many applications use the FTP service for data communications. Some systems also allow users to connect to an FTP server to upload and download files.

Many FTP servers are vulnerable to a wide range of attacks designed to retrieve files without authorization (including password files) and execute commands on other parts of the server.

Vulnerability Solution: Obtain the latest patches from your vendor. Older versions of FTP on both UNIX and Windows NT contain many security holes. Disable anonymous FTP access unless it is absolutely necessary. Configure your system to log all FTP accesses and transfers, then periodically check these logs for patterns of misuse.

Make sure the home directory of your FTP server is not writable and disallow connections from system IDs (including root, uucp, nobody, and bin).

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0614 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0614>

Details:

Protocol = TCP, Port = 21, Service = ftp

Vulnerability Name: **ftpd signal handling allows remote file access as root**

Risk:  93

Vulnerability Description: NetRecon has discovered a network resource running a service that has a signal handling vulnerability. This vulnerability could allow unauthorized file access.

Depending on the configuration of the FTP server, FTP users (including anonymous) can read or write arbitrary files with root privileges.

Note: NetRecon detects this vulnerability based on version information, which means that NetRecon reports it even if you have applied the solution, as long as the version number remains the same.

Vulnerability Solution: Patch or upgrade your FTP daemon, or switch to a different FTP daemon.

Additional Information: For additional information about this vulnerability, see: <http://www.cert.org/advisories/CA-1997-16.html> (1)

Vulnerability Name: **ftpd signal handling allows remote file access as root** (cont.)

See Common Vulnerabilities and Exposures CVE-1999-0035 (2)

Links: 1. <http://www.cert.org/advisories/CA-1997-16.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0035>

Details:

Protocol = TCP, Port = 21, Service = ftp

Vulnerability Name: **IP address found from name**

Risk: ■ 5

Vulnerability Description: NetRecon has successfully discovered the IP address of a network resource using its name.

If NetRecon discovers the names of any network resources (via Windows networking, for example), it attempts to obtain their IP address as well.

Finding the IP address of a network resource verifies that the resource exists. It also helps attackers identify TCP/IP networks to scan for further resources. Having an IP address also opens up the possibility of a wide range of TCP/IP information gathering (port scans, for example) and attacks.

Vulnerability Solution: Do not allow hosts outside your firewall to resolve internal IP addresses unless absolutely necessary. Public DNS should contain only public systems.

Additional Information:

Links:

Details:

Alias = 10.1.6.1

Vulnerability Name: **IP name obtained**

Risk: ■ 10

Vulnerability Description: NetRecon has discovered the IP name of a network resource.

System names often reveal something about the system. For example, servers sometimes have the word server in the name, systems are named after their users, etc. Systems with an IP address but no name are usually either old, unused systems (which can be attacked with less risk of notice) or protected systems

Vulnerability Name: **IP name obtained** (cont.)

(containing highly significant information).

Knowing system names can, therefore, help attackers focus their attacks on key systems.

Vulnerability Solution: Do not allow hosts outside your firewall to resolve internal IP names or addresses unless absolutely necessary. Public DNS should contain only public systems.

Additional Information:

Links:

Details:

Alias = blue.netrecon.com

Alias = blue

Vulnerability Name: **login service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the login service.

The login service (sometimes referred to as rlogin) allows remote users to obtain user and sometimes administrator access to a system.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password guessing.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0593 (1)
See Common Vulnerabilities and Exposures CAN-1999-0651 (2)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0593>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0651>

Details:

Protocol = TCP, Port = 513, Service = login

Vulnerability Name: **network resource detected via ICMP protocol**

Risk: ■ 15

Vulnerability Description: NetRecon has discovered that this network resource responds using the ICMP protocol. ICMP, as part of the IP layer, handles error messaging and other control conditions. This message is a catch-all message because NetRecon has intercepted an ICMP datagram, regardless of its type. If you receive this message, you may also receive messages for the other ICMP vulnerabilities that NetRecon discovers, such as Responds to ICMP Echo (ping) Requests.

In discovering this vulnerability, NetRecon sent a UDP service request and a number of ICMP datagrams to this system and received one or more ICMP responses.

The following are known threats to the legitimate use of the ICMP protocol:

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:

Vulnerability Name: **network resource identified**

Risk: ■ 16

Vulnerability Name:	network resource identified (cont.)
Vulnerability Description:	NetRecon has obtained information that helps to identify a particular network resource. This information could include full or partial identification of the operating system, server types (SMB server, for example), whether a computer is an IP host, etc. Once an attacker has identified a specific target, he or she can find and exploit weakness in that resource.
Vulnerability Solution:	Using the data table in NetRecon, determine how the information was obtained. Either eliminate the service responsible or configure it to not give any clues that can help identify the network resource.
Additional Information:	
Links:	
Details:	
Type = IP host	
Type = HP-UX	
Type = HP-UX, Revision = B.10.00	
Type = IP host	

Vulnerability Name:	nfs service enabled
Risk:	▼ 65
Vulnerability Description:	NetRecon has discovered a network resource serving file systems using NFS. The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard. NFS is vulnerable to a wide range of problems, ranging from common misconfigurations (such as incorrect permissions) to serious bugs that can give an attacker full access to any file systems served by NFS. NFS also does host-based authentication, which can be spoofed fairly easily.
Vulnerability Solution:	Disable NFS if it is not necessary. If NFS is necessary, you should take steps to secure it (see the CERT advisory referenced under Additional Information).
Additional Information:	For more information about securing NFS, see: http://www.cert.org/advisories/CA-1994-15.html (1) See Common Vulnerabilities and Exposures CVE-1999-0631 (2)
Links:	1. http://www.cert.org/advisories/CA-1994-15.html

Vulnerability Name: **nfs service enabled**

(cont.)

2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0631>**Details:**

Service = nfs, Port = 2049, Protocol = UDP

Vulnerability Name: **open RPC service may allow unauthorized activity**Risk: ■ 18

Vulnerability Description: NetRecon has discovered an RPC service.

Remote Procedure Calls (RPC) is a client-server standard for network application communication, allowing applications to communicate and execute functions remotely without having to know anything about the underlying network operating systems.

Since the purpose of RPC services is to permit remote execution of programs and functions, a successful attack on an RPC service gives an attacker this ability or denies legitimate users this ability.

An example of a common RPC service is NFS, which is known to be vulnerable to a wide range of attacks, which could result in unauthorized access to files.

Vulnerability Solution: If the service found is not necessary, disable it. If it is necessary, consider using a TCP/UDP wrapper to limit which hosts can use the service. Firewall the portmap service (usually port 111) so that attackers cannot enumerate RPC services from outside the firewall.

Additional Information:

Links:

Details:

Port = 111, Protocol = TCP, Service = rpcbind, Revision = 2

Port = 929, Protocol = TCP, Service = llockmgr, Revision = 1

Port = 1028, Protocol = TCP, Service = ypbind, Revision = 1

Port = 1029, Protocol = UDP, Service = ypbind, Revision = 1

Port = 892, Protocol = UDP, Service = keyser, Revision = 1

Port = 920, Protocol = TCP, Service = nlockmgr, Revision = 1

Port = 1037, Protocol = UDP, Service = nlockmgr, Revision = 1

Port = 924, Protocol = TCP, Service = nlockmgr, Revision = 3

Port = 1039, Protocol = UDP, Service = llockmgr, Revision = 1

Port = 654, Protocol = TCP, Service = status, Revision = 1

Vulnerability Name: **open RPC service may allow unauthorized activity** (cont.)

Port = 932, Protocol = TCP, Service = nlockmgr, Revision = 2

Port = 635, Protocol = UDP, Service = mountd, Revision = 1

Port = 637, Protocol = TCP, Service = mountd, Revision = 1

Port = 2049, Protocol = UDP, Service = nfs, Revision = 2

Port = 652, Protocol = UDP, Service = status, Revision = 1

Port = 1038, Protocol = UDP, Service = nlockmgr, Revision = 3

Port = 1028, Protocol = TCP, Service = ypbind, Revision = 2

Port = 1029, Protocol = UDP, Service = ypbind, Revision = 2

Port = 111, Protocol = UDP, Service = rpcbind, Revision = 2

Vulnerability Name: **open TCP port may allow unauthorized activity**

Risk: ■ 14

Vulnerability Description: NetRecon has discovered an open TCP port.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:
-port number

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, protect it with a firewall. If the service is required for external use, consider running it from a demilitarized zone and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see:
<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = TCP, Port = 19, Service = chargen

Protocol = TCP, Port = 23, Service = telnet

Protocol = TCP, Port = 21, Service = ftp

Protocol = TCP, Port = 514, Service = shell

Protocol = TCP, Port = 513, Service = login

Protocol = TCP, Port = 512, Service = exec

Protocol = TCP, Port = 25, Service = smtp

Vulnerability Name: **open TCP port may allow unauthorized activity** (cont.)

Protocol = TCP, Port = 111, Service = portmap

Protocol = TCP, Port = 9, Service = discard

Protocol = TCP, Port = 513, Service = login

Protocol = TCP, Port = 7, Service = echo

Protocol = TCP, Port = 13, Service = daytime

Protocol = TCP, Port = 514, Service = shell

Protocol = TCP, Port = 19, Service = chargen

Protocol = TCP, Port = 21, Service = ftp

Protocol = TCP, Port = 23, Service = telnet

Protocol = TCP, Port = 25, Service = smtp

Protocol = TCP, Port = 111, Service = portmap

Protocol = TCP, Port = 512, Service = exec

Protocol = TCP, Port = 9, Service = discard

Protocol = TCP, Port = 13, Service = daytime

Vulnerability Name: **open UDP port may allow unauthorized activity**

Risk: ■ 17

Vulnerability Description: NetRecon has discovered an open UDP port.

Since the UDP protocol doesn't use a three-way handshake to establish connections the way TCP does, it is more susceptible to attacks involving spoofed IP addresses. There are a wide range of denial of service attacks that exploit this weakness in UDP to create infinite loops.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:
-port number

Note: There is a chance of UDP ports being incorrectly detected as open.

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, firewall it. If the service is required for external use, consider running it from a demilitarized zone, and use appropriate authentication.

Vulnerability Name: **open UDP port may allow unauthorized activity** (cont.)

Additional Information: If you think your system may have been compromised, see:
<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = UDP, Port = 9

Protocol = UDP, Port = 7

Protocol = UDP, Port = 13

Protocol = UDP, Port = 19

Protocol = UDP, Port = 111

Protocol = UDP, Port = 514

Vulnerability Name: **portmap service allows RPC services to be enumerated**

Risk: ■ 29

Vulnerability Description: NetRecon has discovered a network resource running the portmap service, and has used portmap to enumerate RPC services.

Remote Procedure Calls (RPC) is a client-server standard for network application communication, allowing applications to communicate and execute functions remotely without having to know anything about the underlying network operating systems.

The portmap service can be used to find out which RPC services are running and which ports they're running on, so that an RPC communications session can be started.

Many RPC services are vulnerable to attacks. Knowing which services are running and what ports they're running on helps attackers focus their efforts.

An example of a common RPC service is NFS, which is known to be vulnerable to a wide range of attacks, which could result in unauthorized access to files.

Vulnerability Solution: If it's not absolutely necessary, don't use RPC. If it is necessary, be sure to firewall the portmap port (usually 111). Consider using a TCP/UDP wrapper to limit which hosts can access portmap.

Additional Information:

Links:

Details:

Vulnerability Name: **portmap service allows RPC services to be enumerated**

(cont.)

Protocol = TCP, Port = 111, Service = portmap

Vulnerability Name: **responds to ICMP echo request (ping)**

Risk: ■ 15

Vulnerability Description: NetRecon has discovered that this system responds to an ICMP echo request (commonly referred to as ping). ICMP is part of the IP layer. It is used to handle IP status and control messages.

The following are known threats to the legitimate use of this service:

- An ICMP reply tells an attacker that a remote system exists and is running.

- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.

- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)

- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)

- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.) However, disabling ICMP on the firewall is only a partial solution. The complete solution should include patching or upgrading the OS kernel so that it can handle oversized ping requests (if possible with your OS). Many operating system vendors have created patches that prevent the Ping o' Death vulnerability. Consult your OS vendor to see if your system can handle oversized packets.

Additional Information: For additional information about ICMP's ping vulnerability, read CERT(R) Advisory CA-96.26 at the following URL:
<http://www.cert.org/advisories/CA-1996-26.html> (1)
See Common Vulnerabilities and Exposures CVE-1999-0128 (2)

Links: 1. <http://www.cert.org/advisories/CA-1996-26.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0128>

Details:

Vulnerability Name: **responds to ICMP echo request (ping)**

(cont.)

Vulnerability Name: **responds to ICMP information request**Risk: ■ 16

Vulnerability Description: NetRecon has discovered that this system responds to an ICMP information request. ICMP is part of the IP layer. It is used to handle IP status and control messages. The ICMP information request message type is an obsolete ICMP message request; however, some systems still respond to it.

The following are known threats to the legitimate use of this service:

- An ICMP reply tells an attacker that a remote system exists and is running.

- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.

- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)

- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)

- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:

Vulnerability Name: **responds to UDP requests with ICMP**Risk: ■ 20

Vulnerability Description: NetRecon has discovered that this system responds to UDP packets directed to unavailable service ports with an ICMP error message. This mechanism allows clients to determine if a service is

Vulnerability Name: **responds to UDP requests with ICMP** (cont.)

available on a remote system. If the service is available, then it will handle the service request; however, if no service is associated with the specified port, then an ICMP error message is returned indicating that no service was associated with that port.

The following are known threats to the legitimate use of the ICMP protocol:

- An attacker may send UDP requests to a server in an attempt to map ports on that server.
- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:Vulnerability Name: **service identified**

Risk:  39

Vulnerability Description: NetRecon has identified a service by software product, version, or both.

Knowing the product and/or version allows attackers to focus their attacks.

Berkeley sendmail, for example, is known to be vulnerable to certain exploits in some versions, but not in others. If attackers can

Vulnerability Name: **service identified** (cont.)

identify that you are running a vulnerable version of Berkeley sendmail they can direct known exploits towards those resources. Even for services with no known exploits, it is possible that vulnerabilities will be discovered in the future.

If attackers can obtain version information for a service, they can eliminate attacks known to fail with that version, or try attacks known to work with that version. Eliminating techniques to try is helpful in speeding up the attack, and can also help to avoid alerting administrators, since it is usually possible to monitor attempted exploits of fixed vulnerabilities.

Vulnerability Solution: Consider the benefits of product identification and weigh them against the security risk. Remove unique banners from services wherever practical. If the identifying information cannot be suppressed, consider using a different product.

For the extremely security conscious, it can be worthwhile to provide intentionally misleading identification of the service product and version. This misdirects attackers to attempt to exploit vulnerabilities that are not present. The administrator can monitor such attacks and take appropriate action to stop attackers before they are successful. However, incorrect banners will also deceive NetRecon.

Additional Information:

Links:

Details:

Service = status, Revision = 1, Protocol = TCP, Port = 654

Service = ftp, Revision = 1.7.110.9, Protocol = TCP, Port = 21

Service = ftp/HP, Revision = 1.7.110.9, Protocol = TCP, Port = 21

Service = ftp/HP, Protocol = TCP, Port = 21

Service = smtp/HP Sendmail, Revision = 1.38.110.45/16.2, Protocol = TCP, Port = 25

Service = smtp/HP Sendmail, Protocol = TCP, Port = 25

Service = status, Revision = 1, Protocol = UDP, Port = 652

Service = rpcbind, Revision = 2, Protocol = TCP, Port = 111

Service = rpcbind, Revision = 2, Protocol = UDP, Port = 111

Service = nfs, Revision = 2, Protocol = UDP, Port = 2049

Service = mountd, Revision = 1, Protocol = TCP, Port = 637

Service = mountd, Revision = 1, Protocol = UDP, Port = 635

Service = nlockmgr, Revision = 2, Protocol = TCP, Port = 932

Vulnerability Name: **service identified**

(cont.)

Service = llockmgr, Revision = 1, Protocol = TCP, Port = 929
Service = llockmgr, Revision = 1, Protocol = UDP, Port = 1039
Service = nlockmgr, Revision = 3, Protocol = UDP, Port = 1038
Service = nlockmgr, Revision = 3, Protocol = TCP, Port = 924
Service = nlockmgr, Revision = 1, Protocol = UDP, Port = 1037
Service = nlockmgr, Revision = 1, Protocol = TCP, Port = 920
Service = keyerv, Revision = 1, Protocol = UDP, Port = 892
Service = ypbind, Revision = 1, Protocol = UDP, Port = 1029
Service = ypbind, Revision = 1, Protocol = TCP, Port = 1028
Service = ypbind, Revision = 2, Protocol = UDP, Port = 1029
Service = ypbind, Revision = 2, Protocol = TCP, Port = 1028

Vulnerability Name: **shell service enabled**Risk:  42

Vulnerability Description: The shell service provides remote execution facilities with authentication based on privileged port numbers and trusted hosts.

It is possible to configure this service to allow anyone with a valid user name to execute commands without authentication.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information:

Links: 1.
http://www.cs.purdue.edu/coast/satan-html/tutorials/vulnerability/remote_shell_access.html

Details:

Protocol = TCP, Port = 514, Service = shell

Vulnerability Name: **SMTP allows remote command execution via bounce filter**

Vulnerability Name: **SMTP allows remote command execution via bounce filter** (cont.)

Risk:  86

Vulnerability Description: Attackers can execute arbitrary shell commands by specifying a filter as a return address e-mail in e-mail that will bounce.

Note: If your SMTP software does not support filters, this is not a vulnerability. If you are not sure if your SMTP software supports filters, contact your vendor.

Vulnerability Solution: Upgrade or replace your SMTP server, or verify that it does not support filters.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0203 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0203>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP allows user verification with rcpt**

Risk:  35

Vulnerability Description: NetRecon has discovered a network resource running an SMTP implementation that allows rcpt verification.

Some SMTP mail transport agents (MTAs) will return an error if the recipient of a mail message isn't valid. This fact can be used much like VRFY to determine whether particular mail accounts exist.

Vulnerability Solution: If possible, disable this feature in your MTA. If it is not possible, consider upgrading or switching to a MTA that permits disabling of rcpt verification.

Additional Information:

Links:

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP configuration allows relaying**

Risk:  61

Vulnerability Description: Your SMTP configuration allows relaying of e-mail between arbitrary hosts. This is the default in many older SMTP implementations. Some SMTP implementations do not allow you to block relaying.

Vulnerability Name: **SMTP configuration allows relaying** (cont.)

Berkeley Sendmail introduced relay blocking in version 8.8, but it must be enabled.

This vulnerability is actively exploited by bulk e-mail solicitors (spammers), allowing them to conceal their identity and decrease the demand on their own resources.

Exploitation can result in consumption of disk space and bandwidth. Recipients may mistakenly identifying your site as the source of unwanted e-mail, which can lead to further attacks or other sites blocking email from your site.

Note: If the host in question trusts the host running NetRecon, you may consider this alert a false positive.

Vulnerability Solution: Disable SMTP or upgrade and (if necessary) configure your SMTP server to deny relaying.

Additional Information: Sendmail home page:
<http://www.sendmail.org/> (1)
Hewlett-Packard Sendmail upgrade information:
<http://www.software.hp.com/software/HPsoftware/Sendmail/index.html>
Sun Microsystems states that Solaris 2.7 will ship with Sendmail 8.8, and that a backport of Sendmail 8.8 will be available soon for prior operating system versions.
See Common Vulnerabilities and Exposures CAN-1999-0512 (3)

Links: 1. <http://www.sendmail.org/>
2. <http://www.software.hp.com/software/HPsoftware/Sendmail/index.html>
3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0512>

Details:

Port = 25, Protocol = TCP, Service = smtp

Vulnerability Name: **SMTP connections can be established quickly**

Risk: ■ 20

Vulnerability Description: NetRecon has discovered an SMTP implementation that allows connections to be made very quickly.

Since SMTP mail transport agents (MTAs) are notorious for having many security problems, they are common targets for attackers. If an attacker can make quick connections to the MTA, they can test out a number of potential problems with relative ease. If, however, there is a substantial delay for each test performed, there is a greater chance that an attacker will lose patience and move on to

Vulnerability Name: **SMTP connections can be established quickly** (cont.)

another target.

Assuming the NetRecon system is not running an ident server, this vulnerability also typically indicates that the MTA does not attempt to ident the connection.

Vulnerability Solution: Some MTAs have a secure mode that prevents rapid connections. If possible, put your MTA into a secure mode. If it is not possible, consider upgrading or switching to another MTA.

Using ident authentication can make it easier to trace abuse and warn of possible e-mail forgeries. Enable ident authentication if your MTA supports it.

Additional Information:

Links:

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP decode alias enabled**

Risk:  45

Vulnerability Description: Including a decode mail alias in /etc/aliases makes it easier to send and receive binary files by e-mail.

A decode mail alias can be used to create or overwrite files on the system. For example, an attacker could use this vulnerability to plant a bogus message in the message queue. A few versions of uudecode allow the creation of SUID files, which would allow an attacker to use the decode alias to create an SUID daemon shell in an accessible directory.

Vulnerability Solution: Remove the decode alias from all aliases files.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0096 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0096>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP EXPN feature enabled**

Risk:  35

Vulnerability Description: The expn command allows a client to expand a mail address. If it is

Vulnerability Name: **SMTP EXPN feature enabled** (cont.)

a shell user address, it shows the results of aliasing through a user's ~/.forward file. If the address is an alias, it shows all the addresses that result from the alias expansion. The expn command is generally used for testing purposes, to test the validity of aliases.

Many systems have easily guessable mail distribution aliases (such as everyone, all, staff, etc.). Being able to expand such aliases to obtain particular user names is very useful to attackers. Some user names are the same as system names, and some accounts have identical user names and passwords.

The expn command also allows an attacker to verify particular user names.

Vulnerability Solution: Consider disabling the expn command in your MTA implementation (commonly sendmail). If you choose not to disable expn , enable logging. Some newer versions of sendmail allow detailed logging of requests and include a privacy option, which allows you to require that requesting sites identify themselves before certain operations can take place. Check with your vendor for the details of the latest MTA program version.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP recipient identified**

Risk:  37

Vulnerability Description: NetRecon has identified a valid mail account.

A valid mail account could be a user or an alias. Each valid account name is a potential login name for network resources on the same network. Knowing valid mail accounts opens up the possibility of social engineering attacks. Attackers can also use valid mail accounts for mail bombing attacks.

Vulnerability Solution: Disable features of your SMTP mail transport agent (MTA) that allow verification and discovery of mail accounts. The most common examples are: VRFY, EXPN, and rcpt notification.

Additional Information:

Links:

Details:

Vulnerability Name: **SMTP recipient identified**

(cont.)

Miscellaneous = SMTP recipient=decode, Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **smtp service enabled**Risk:  45

Vulnerability Description: The smtp service uses the Simple Mail Transfer Protocol (SMTP) to send electronic messages. The smtp service may be used to obtain information about valid user names and other systems in the network.

The smtp service is vulnerable to a variety of attacks and may also constitute a violation of acceptable use policies.


Vulnerability Solution: Disable this service if it isn't necessary.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0617 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0617>

Details:

Protocol = TCP, Port = 25, Service = smtp

Vulnerability Name: **SMTP supports EHLO greeting**Risk:  9

Vulnerability Description: NetRecon has discovered an SMTP implementation that responds to the EHLO greeting protocol.

The EHLO greeting protocol is an indication of the ESMTP (Extended Simple Mail Transfer Protocol) protocol. ESMTP has additional vulnerabilities, so knowing that a network resource supports it permits an attacker to focus their efforts.

Vulnerability Solution: Configure your mail transport agent (MTA) to permit the minimum amount of information transfer necessary for completing mail transport tasks.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP VRFY feature enabled**

Risk:  35

Vulnerability Description: NetRecon has discovered an SMTP implementation that allows mail accounts to be verified.

The smtp (the service used to handling e-mail) vrfy command allows a client to verify whether a particular address is valid. The vrfy command is sometimes used by e-mail applications to verify that users exist before sending them messages.

Being able to verify particular user names is very useful to attackers. Some user names are the same as system names, and some accounts have identical user names and passwords. An attacker can also use the vrfy command to search for common distribution aliases (such as everyone, all, or staff), which can then be expanded to reveal many valid user names.

Vulnerability Solution: Consider disabling the vrfy command in your MTA implementation (commonly sendmail). If vrfy is required by any of the applications you use, enable the logging option. Obtain the newest version of your MTA. Many newer versions of sendmail allow detailed logging of sendmail requests, including the hostname or IP address of the requester.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **telnet service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the telnet service.

The telnet service provides remote execution facilities with authentication based on user names and passwords.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password guessing.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted

Vulnerability Name: telnet service enabled

(cont.)

connections to this service.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0619 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0619>**Details:**

Protocol = TCP, Port = 23, Service = telnet

Vulnerability Name: user shell access obtained via login service**Risk:** ● 91

Vulnerability Description: NetRecon has connected to a network resource through the login service with user privileges.

NetRecon uses any login names and passwords obtained through other vulnerabilities to attempt to log in to any network resources running the login service. Being able to log in to a network resource with user privileges permits a wide range of activities, depending on the privileges of the user.

Vulnerability Solution: Fix the vulnerabilities that led to NetRecon being able to discover the password that provided access (right-click the vulnerability record in the Data Table pane and choose Path Analysis to see what information led NetRecon to find this vulnerability).

To increase the difficulty of cracking or guessing passwords, enforce the use of secure passwords. Passwords should be a combination of letters, numbers, and punctuation. They should not correspond to words in any language, names of people, places, fictional characters, initials, dates, etc. They should not be common or simple sequences of letters, numbers, or characters such as abcde or 12345. Additionally, passwords should be changed regularly and should never be reused.

Additional Information:

Links:**Details:**

Login Name = johnm, Password = a*s

Login Name = masonb, Password = s*r

Login Name = mikeb, Password = j*e

Login Name = willie, Password = k*1

Login Name = glennw, Password = f*e

Network Resource: **blue.netrecon.com**

(cont.)

Network Resource: **brown.netrecon.com**

Resource Type: IP host, Linux 2.2.12

Aliases: brown, 10.1.5.1, 00:00:f2:12:47:19

of Unique Vulnerabilities: 39

Highest Risk Level Found:  91

Vulnerability Name: **anonymous FTP access is enabled**

Risk:  53

Vulnerability Description: NetRecon has successfully logged on to an FTP server anonymously.

FTP (File Transfer Protocol) is a protocol for transferring files between computers. The FTP service is used by many applications for data communications. Some computers also allow users to connect to an FTP server to upload and download files.

FTP servers are vulnerable to a wide range of attacks designed to retrieve files without authorization (including password files) and execute commands on other parts of the server. Anonymous FTP means that anyone who can connect to the service can log in, greatly increasing the potential number of attackers and attacks. Attackers can also abuse anonymous FTP access a number of other ways, including using an anonymous FTP site as a drop zone for illegal files.

Vulnerability Solution: Never allow anonymous FTP access unless it is absolutely necessary. Configure your system to log all FTP accesses and transfers and periodically check these logs for patterns of misuse.

Make sure the home directory of your FTP server is not writable and disallow connections from system IDs (including root, uucp, nobody, and bin).

If practical, deny FTP access using a firewall.

Symantec Intruder Alert can be used to monitor any connections to the FTP port.

Additional Information: http://www.cert.org/tech_tips/anonymous_ftp_abuses.html (1)
See Common Vulnerabilities and Exposures CVE-1999-0497 (2)

Links: 1. http://www.cert.org/tech_tips/anonymous_ftp_abuses.html
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0497>

Details:

Port = 21, Protocol = TCP, Service = ftp

Vulnerability Name: **encrypted password cracked**

Risk: ● 89

Vulnerability Description: NetRecon has cracked an encrypted password it discovered through another vulnerability.

Many UNIX systems allow any user to read one or more files containing valid login names and encrypted passwords. NetRecon uses small (for speed) and large (for completeness) dictionaries of commonly used passwords, encrypts each of the words in the list, and then compares the results with the encrypted passwords in the map file obtained on the target system. Any matches obtained are stored in a valid password list, which can be used by NetRecon to gain access to network resources.

Knowledge of relatively few valid passwords allows immediate access to some resources. Additionally, because many people use the same passwords in multiple situations, knowing a few passwords often allows access to additional network resources.

Obtaining password maps and cracking them externally is a very powerful way to attack a system. Since attackers can work to crack passwords on any systems they can access, they can utilize many resources to crack the passwords, and they can do so without fear of detection.

Vulnerability Solution: To increase the difficulty of cracking or guessing passwords, enforce the use of secure passwords. Passwords should be a combination of letters, numbers, and punctuation. They should not correspond to words in any language, names of people, places, fictional characters, initials, dates, or the like. They should not be common or simple sequences of letters, numbers, or characters such as abcde or 12345. Additionally, passwords should be changed regularly and should never be reused.

Most versions of UNIX allow the use of shadow password files. These files prevent anyone other than system administrators from being able to view the encrypted passwords.

Symantec Enterprise Security Manager allows you to set and consistently apply a policy of using strong passwords.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0501 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0501>

Details:

Login Name = mikeb, Password = j*e, Encrypted Password = .ui18CmhiW5nY

Login Name = johnm, Password = a*s, Encrypted Password = ofRrZy.hBUMic

Vulnerability Name: **encrypted password cracked**

(cont.)

Login Name = masonb, Password = s*r, Encrypted Password = t56Udgb1BOcdY

Login Name = glenn, Password = f*e, Encrypted Password = OHTbplAx.E/Us

Login Name = willie, Password = k*1, Encrypted Password = EjBDy3BkqmfqM

Vulnerability Name: **finger service enabled**Risk:  37

Vulnerability Description: NetRecon has discovered a network resource running the finger service.

The finger service allows remote users and processes to obtain information about system processes and individual users.

Among other things, finger can provide the following information to an attacker:

- Valid login names
- Users' full names
- Names of other systems
- A user's login shell

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0612 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0612>

Details:

Protocol = TCP, Port = 79, Service = finger

Vulnerability Name: **FTP access obtained**Risk:  54

Vulnerability Description: NetRecon has successfully logged on to an FTP server either anonymously or by guessing the login name and password from a short list.

FTP (File Transfer Protocol) is a protocol for transferring files between systems. Many applications use the FTP service for data communications. Some systems also allow users to connect to an FTP server to upload and download files.

Many FTP servers are vulnerable to a wide range of attacks

Vulnerability Name: **FTP access obtained**

(cont.)

designed to retrieve files without authorization (including password files) and execute commands on other parts of the server. Anonymous FTP means that anyone who can connect to the service can log in, greatly increasing the potential number of attackers and attacks. Attackers can also abuse anonymous FTP access a number of other ways, including using an anonymous FTP site as a drop zone for illegal files.

Vulnerability Solution: Obtain the latest patches from your vendor. Older versions of FTP on both UNIX and Windows NT contain security vulnerabilities. Disable anonymous FTP access unless it is absolutely necessary. Configure your system to log all FTP accesses and transfers, then periodically check these logs for patterns of misuse.

Make sure that the home directory of your FTP server is not writable and disallow connections from system IDs (including root, uucp, nobody, and bin).

Use a firewall to protect FTP access where practical.

Additional Information: http://www.cert.org/tech_tips/anonymous_ftp_abuses.html (1)
See Common Vulnerabilities and Exposures CVE-1999-0497 (2)

Links: 1. http://www.cert.org/tech_tips/anonymous_ftp_abuses.html
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0497>

Details:

Port = 21, Protocol = TCP, Service = ftp, Login Name = ftp, Password = N*m

Port = 21, Protocol = TCP, Service = ftp, Login Name = anonymous, Password = N*m

Vulnerability Name: **ftp service enabled**Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the FTP service.

FTP (File Transfer Protocol) is a protocol for transferring files between systems. Many applications use the FTP service for data communications. Some systems also allow users to connect to an FTP server to upload and download files.

Many FTP servers are vulnerable to a wide range of attacks designed to retrieve files without authorization (including password files) and execute commands on other parts of the server.

Vulnerability Solution: Obtain the latest patches from your vendor. Older versions of FTP on both UNIX and Windows NT contain many security holes. Disable anonymous FTP access unless it is absolutely necessary.

Vulnerability Name: **ftp service enabled** (cont.)

Configure your system to log all FTP accesses and transfers, then periodically check these logs for patterns of misuse.

Make sure the home directory of your FTP server is not writable and disallow connections from system IDs (including root, uucp, nobody, and bin).

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0614 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0614>

Details:

Protocol = TCP, Port = 21, Service = ftp

Vulnerability Name: **HTTP allows execution of phf CGI**

Risk:  63

Vulnerability Description: NetRecon has discovered a network resource that permits execution of a CGI program named phf that may be susceptible to unauthorized command execution attacks.

phf is a CGI application used to query a QI/PH (also known as CSO) phonebook database. Many distributed versions of phf fail to filter a linefeed character that permits execution of shell commands with the privileges of the account running CGI processes (commonly nobody or daemon).

Note: NetRecon detects this vulnerability based on the ability to execute a particular CGI program, which means that NetRecon reports it even if you have already upgraded to a non-vulnerable version.

Vulnerability Solution: If it is not needed, remove the phf program from the CGI executable directory. If it is needed, upgrade to the newest version. The upgrade can be found at ftp://ftp.ncsa.uiuc.edu/Web/httpd/Unix/ncsa_httpd/current/ (1).

Additional Information: For more information about this vulnerability and possible solutions, see the following Cert Advisory: <http://www.cert.org/advisories/CA-1996-06.html> (2). See Common Vulnerabilities and Exposures CVE-1999-0067 (3)

Links: 1. ftp://ftp.ncsa.uiuc.edu/Web/httpd/Unix/ncsa_httpd/current/
2. <http://www.cert.org/advisories/CA-1996-06.html>
3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0067>

Details:

Service = http, Protocol = TCP, Port = 80

Vulnerability Name: **http service enabled**

Risk:  42

Vulnerability Description: The http service is enabled. HTTP is the protocol the World Wide Web uses. Many vulnerabilities are associated with this service, and new security problems are constantly being discovered with Web software.

The http service enabled means the system is running a Web server (as opposed to being able to connect to the WWW via a browser).

Vulnerability Solution: Disable HTTP on computers that should not be accessed via the Web.

If HTTP is necessary and is used to host a public Web site, consider placing the server in a demilitarized zone (DMZ) on a network segment isolated from systems containing sensitive data.

If HTTP is necessary only for internal use, restrict access from untrusted hosts with a firewall.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0633 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0633>

Details:

Service = http, Port = 80, Protocol = TCP

Vulnerability Name: **IP address found from name**

Risk:  5

Vulnerability Description: NetRecon has successfully discovered the IP address of a network resource using its name.

If NetRecon discovers the names of any network resources (via Windows networking, for example), it attempts to obtain their IP address as well.

Finding the IP address of a network resource verifies that the resource exists. It also helps attackers identify TCP/IP networks to scan for further resources. Having an IP address also opens up the possibility of a wide range of TCP/IP information gathering (port scans, for example) and attacks.

Vulnerability Solution: Do not allow hosts outside your firewall to resolve internal IP addresses unless absolutely necessary. Public DNS should contain only public systems.

Vulnerability Name: **IP address found from name**

(cont.)

Additional Information:

Links:

Details:

Alias = 10.1.5.1

Vulnerability Name: **IP name obtained**Risk:  10

Vulnerability Description: NetRecon has discovered the IP name of a network resource.

System names often reveal something about the system. For example, servers sometimes have the word server in the name, systems are named after their users, etc. Systems with an IP address but no name are usually either old, unused systems (which can be attacked with less risk of notice) or protected systems (containing highly significant information).

Knowing system names can, therefore, help attackers focus their attacks on key systems.

Vulnerability Solution: Do not allow hosts outside your firewall to resolve internal IP names or addresses unless absolutely necessary. Public DNS should contain only public systems.

Additional Information:

Links:

Details:

Alias = brown

Alias = brown.netrecon.com

Vulnerability Name: **IRC server identified**Risk:  61

Vulnerability Description: NetRecon tries to identify Internet Relay Chat (IRC) servers by checking commonly-used IRC ports. IRC servers are a common target of attacks, since controlling one allows an attacker to eavesdrop, harass users, and so forth.

Vulnerability Solution: Disable the IRC server if it is not necessary.

If an IRC server is necessary, consider placing the server in a demilitarized zone (DMZ) on a network segment isolated from

Vulnerability Name: **IRC server identified** (cont.)

systems containing sensitive data.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0645 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0645>

Details:

Protocol = TCP, Port = 6667, Service = irc

Vulnerability Name: **login service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the login service.

The login service (sometimes referred to as rlogin) allows remote users to obtain user and sometimes administrator access to a system.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password guessing.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0593 (1)
See Common Vulnerabilities and Exposures CAN-1999-0651 (2)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0593>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0651>

Details:

Protocol = TCP, Port = 513, Service = login

Vulnerability Name: **network resource detected via ICMP protocol**

Risk:  15

Vulnerability Description: NetRecon has discovered that this network resource responds using the ICMP protocol. ICMP, as part of the IP layer, handles error messaging and other control conditions. This message is a catch-all message because NetRecon has intercepted an ICMP datagram, regardless of its type. If you receive this message, you

Vulnerability Name: **network resource detected via ICMP protocol** (cont.)

may also receive messages for the other ICMP vulnerabilities that NetRecon discovers, such as Responds to ICMP Echo (ping) Requests.

In discovering this vulnerability, NetRecon sent a UDP service request and a number of ICMP datagrams to this system and received one or more ICMP responses.

The following are known threats to the legitimate use of the ICMP protocol:

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:


Vulnerability Name: **network resource identified**

Risk: ■ 16

Vulnerability Description: NetRecon has obtained information that helps to identify a particular network resource. This information could include full or partial identification of the operating system, server types (SMB server, for example), whether a computer is an IP host, etc.

Once an attacker has identified a specific target, he or she can find and exploit weakness in that resource.

Vulnerability Name: network resource identified (cont.)
Vulnerability Solution: Using the data table in NetRecon, determine how the information was obtained. Either eliminate the service responsible or configure it to not give any clues that can help identify the network resource.
Additional Information:
Links:
Details:
Type = IP host
Type = Linux
Type = Linux, Revision = 2.2.12
Type = IP host

Vulnerability Name: nfs service enabled
Risk:  65
Vulnerability Description: NetRecon has discovered a network resource serving file systems using NFS. The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard. NFS is vulnerable to a wide range of problems, ranging from common misconfigurations (such as incorrect permissions) to serious bugs that can give an attacker full access to any file systems served by NFS. NFS also does host-based authentication, which can be spoofed fairly easily.
Vulnerability Solution: Disable NFS if it is not necessary. If NFS is necessary, you should take steps to secure it (see the CERT advisory referenced under Additional Information).
Additional Information: For more information about securing NFS, see: http://www.cert.org/advisories/CA-1994-15.html (1) See Common Vulnerabilities and Exposures CVE-1999-0631 (2)
Links: 1. http://www.cert.org/advisories/CA-1994-15.html 2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0631
Details:
Service = nfs, Port = 2049, Protocol = UDP
Service = nfs, Port = 2049, Protocol = TCP

Vulnerability Name: **NIS client can be identified via passwd file**

Risk:  20

Vulnerability Description: NetRecon has identified an NIS client by examining the contents of a passwd file.

The NIS service allows transfer of information between hosts that share administrative control. On some systems, the NIS service is referred to as the YP (yellow pages) service. NIS servers typically contain databases (called maps) of passwords, host names and addresses, and mail aliases.

NetRecon has discovered a passwd file, examined its contents, and determined that it contains one or more items beginning with a "+", which indicates the presence of an NIS server somewhere on the network. Knowing that an NIS server exists helps an attacker narrow the focus of the attack, since NIS is such a valuable target.

When this vulnerability is included in a NetRecon scan report, the name of the network resource where the passwd file was found is in the Details section.

Vulnerability Solution: Use NetRecon path analysis to determine how NetRecon gained access to the passwd file. There are a number of possible ways, including finding a passwd file that has been exported via NFS, and gaining administrative access (through some other vulnerability), which permits access to the passwd file. Fix the vulnerabilities that allowed NetRecon to gain access to the passwd file.

Additional Information:

Links:

Details:

Vulnerability Name: **NIS domain name identified**

Risk:  46

Vulnerability Description: NetRecon has positively identified the NIS domain name by being able to execute a shell command.

The NIS service allows transfer of information between hosts that share administrative control. On some systems, the NIS service is referred to as the YP (yellow pages) service. NIS servers typically contain databases (called maps) of passwords, host names and addresses, and mail aliases.

If an attacker can obtain NIS map files, there is a high degree of probability that at least some passwords can be cracked. An

Vulnerability Name: **NIS domain name identified** (cont.)

attacker also gains a clearer picture of any local networks referred to in the maps.

Obtaining password maps and cracking them externally is a very powerful attack tool. Since attackers can work to crack passwords on their own systems, they can use large amounts of resources to crack the passwords, and they can do so without fear of detection.

Vulnerability Solution: Make it more difficult to obtain the NIS domain name by disabling the domainname command for normal users. Consider upgrading to NIS+.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0521 (2)

Links: 1. http://www.cs.purdue.edu/coast/satan-html/tutorials/vulnerability/NIS_password_file_access.html
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0521>

Details:

Domain = netrecon.com

Vulnerability Name: **NIS map passwd.byname obtained**

Risk:  49

Vulnerability Description: NetRecon has obtained an NIS map that contains passwords.

The NIS service allows transfer of information between hosts that share administrative control. On some systems, the NIS service is referred to as the YP (yellow pages) service. NIS databases are called maps.

If an attacker can obtain the passwd.byname map, there is a high degree of probability that at least some passwords can be cracked.

Obtaining password maps and cracking them externally is a very powerful attack tool. Since attackers can work to crack passwords on their own systems, they can use large amounts of resources to crack the passwords, and they can do so without fear of detection.

If NetRecon obtains this map, it will attempt to crack the passwords.

In many cases, an individual's full name can be found in the passwd map, providing a valuable social engineering tool.

Vulnerability Solution: To increase the difficulty of cracking or guessing passwords, enforce the use of secure passwords. Passwords should be a combination of letters, numbers, and punctuation. They should not correspond to words in any language, names of people, places,

Vulnerability Name: **NIS map passwd.byname obtained** (cont.)

fictional characters, initials, dates, etc. They should not be common or simple sequences of letters, numbers, or characters such as abcde or 12345. Additionally, passwords should be changed regularly and should never be reused.

Most versions of UNIX allow the use of shadow password files, which prevents anyone other than system administrators from being able to view the encrypted passwords.

Symantec's Enterprise Security Manager allows you to set and consistently apply a policy of using strong passwords.

The NIS domain name can be considered to be the NIS map password, and should therefore be something difficult to guess. It should never be the same as or similar to any other domain or system names used locally if at all avoidable. NetRecon tries to guess the NIS domain name based on the system name. Note that the NIS domain name can be obtained by any user with shell access to a host within the NIS domain.

Several vendors have added access control to their NIS server implementation. Check your system documentation or vendor patch list.

Consider blocking port 111 (portmap) on your network gateway. This makes attacks on NIS and nfs mount daemons much harder.

If NIS is not secure enough, consider upgrading to NIS+.

Additional Information:

Links: 1.
http://www.cs.purdue.edu/coast/satan-html/tutorials/vulnerability/NIS_password_file_access.html

Details:Vulnerability Name: **nis service allows account information to be obtained**

Risk: ■ 30

Vulnerability Description: NetRecon has discovered an NIS server and accessed an NIS map containing detailed account information.

The NIS service allows transfer of information between hosts that share administrative control. On some systems, the NIS service is referred to as the YP (yellow pages) service. NIS servers typically contain databases (called maps) of passwords, host names and addresses, and mail aliases.

Vulnerability Name: **nis service allows account information to be obtained** (cont.)

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- name of the map that contained account information
- login name obtained
- Miscellaneous user information, including the uid, gid, info, default directory, and shell
- service used to obtain the map
- protocol used to obtain the map

Vulnerability Solution: The NIS domain name can be considered to be the NIS map password, and should therefore be something difficult to guess. It should never be the same as or similar to any other domain or system names used locally if at all avoidable. NetRecon tries to guess the NIS domain name based on the system name. Note that the NIS domain name can be obtained by any user with shell access to a host within the NIS domain.

Several vendors have added access control to their NIS server implementation. Check your system documentation or vendor patch list.

Consider blocking port 111 (portmap) on your network gateway. This makes attacks on NIS and nfs mount daemons much harder.

If NIS is not secure enough, consider upgrading to NIS+.

Additional Information:

Links:

Details:

Map = passwd.byname

Vulnerability Name: **nis service allows encrypted passwords to be obtained**

Risk:  49

Vulnerability Description: NetRecon has discovered an NIS server and accessed an NIS map containing encrypted passwords.

The NIS service allows transfer of information between hosts that share administrative control. On some systems, the NIS service is referred to as the YP (yellow pages) service. NIS servers typically contain databases (called maps) of passwords, host names and addresses, and mail aliases.

Vulnerability Name: **nis service allows encrypted passwords to be obtained** (cont.)

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- name of the map that contained encrypted passwords
- login name obtained
- encrypted password obtained
- service used to obtain the map
- protocol used to obtain the map

Vulnerability Solution: The NIS domain name can be considered to be the NIS map password, and should therefore be something difficult to guess. It should never be the same as or similar to any other domain or system names used locally if at all avoidable. NetRecon tries to guess the NIS domain name based on the system name. Note that the NIS domain name can be obtained by any user with shell access to a host within the NIS domain.

Several vendors have added access control to their NIS server implementation. Check your system documentation or vendor patch list.

Consider blocking port 111 (portmap) on your network gateway. This makes attacks on NIS and nfs mount daemons much harder.

If NIS is not secure enough, consider upgrading to NIS+.

Additional Information:

Links:

Details:

Map = passwd.byname

Vulnerability Name: **nis service allows login names to be obtained**

Risk:  37

Vulnerability Description: NetRecon has discovered an NIS server and accessed an NIS map containing account names.

The NIS service allows transfer of information between hosts that share administrative control. On some systems, the NIS service is referred to as the YP (yellow pages) service. NIS servers typically contain databases (called maps) of passwords, host names and addresses, and mail aliases.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- name of the map that contained account information

Vulnerability Name: **nis service allows login names to be obtained** (cont.)

-login name obtained
-service used to obtain the map
-protocol used to obtain the map

Vulnerability Solution: The NIS domain name can be considered to be the NIS map password, and should therefore be something difficult to guess. It should never be the same as or similar to any other domain or system names used locally if at all avoidable. NetRecon tries to guess the NIS domain name based on the system name. Note that the NIS domain name can be obtained by any user with shell access to a host within the NIS domain.

Several vendors have added access control to their NIS server implementation. Check your system documentation or vendor patch list.

Consider blocking port 111 (portmap) on your network gateway. This makes attacks on NIS and nfs mount daemons much harder.

If NIS is not secure enough, consider upgrading to NIS+.

Additional Information:

Links:

Details:

Map = passwd.byname

Vulnerability Name: **open RPC service may allow unauthorized activity**

Risk: ■ 18

Vulnerability Description: NetRecon has discovered an RPC service.

Remote Procedure Calls (RPC) is a client-server standard for network application communication, allowing applications to communicate and execute functions remotely without having to know anything about the underlying network operating systems.

Since the purpose of RPC services is to permit remote execution of programs and functions, a successful attack on an RPC service gives an attacker this ability or denies legitimate users this ability.

An example of a common RPC service is NFS, which is known to be vulnerable to a wide range of attacks, which could result in unauthorized access to files.

Vulnerability Solution: If the service found is not necessary, disable it. If it is necessary, consider using a TCP/UDP wrapper to limit which hosts can use the service. Firewall the portmap service (usually port 111) so that

Vulnerability Name: **open RPC service may allow unauthorized activity** (cont.)

attackers cannot enumerate RPC services from outside the firewall.

Additional Information:

Links:

Details:

Port = 2049, Protocol = TCP, Service = nfs, Revision = 2
Port = 1024, Protocol = UDP, Service = nlockmgr, Revision = 1
Port = 1024, Protocol = UDP, Service = nlockmgr, Revision = 3
Port = 1024, Protocol = TCP, Service = nlockmgr, Revision = 1
Port = 1024, Protocol = TCP, Service = nlockmgr, Revision = 3
Port = 681, Protocol = UDP, Service = ypbind, Revision = 2
Port = 111, Protocol = TCP, Service = rpcbind, Revision = 2
Port = 111, Protocol = UDP, Service = rpcbind, Revision = 2
Port = 682, Protocol = UDP, Service = mountd, Revision = 1
Port = 683, Protocol = TCP, Service = ypbind, Revision = 2
Port = 682, Protocol = UDP, Service = mountd, Revision = 2
Port = 685, Protocol = TCP, Service = mountd, Revision = 1
Port = 685, Protocol = TCP, Service = mountd, Revision = 2
Port = 2049, Protocol = UDP, Service = nfs, Revision = 2

Vulnerability Name: **open TCP port may allow unauthorized activity**

Risk: ■ 14

Vulnerability Description: NetRecon has discovered an open TCP port.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:
-port number

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, protect it with a firewall. If the service is required for external use, consider running it from a demilitarized zone and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see:
<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Vulnerability Name: **open TCP port may allow unauthorized activity** (cont.)

Details:

Protocol = TCP, Port = 514, Service = shell
Protocol = TCP, Port = 513, Service = login
Protocol = TCP, Port = 79, Service = finger
Protocol = TCP, Port = 80
Protocol = TCP, Port = 111, Service = portmap
Protocol = TCP, Port = 513, Service = login
Protocol = TCP, Port = 514, Service = shell
Protocol = TCP, Port = 2049
Protocol = TCP, Port = 25, Service = smtp
Protocol = TCP, Port = 6667
Protocol = TCP, Port = 21, Service = ftp
Protocol = TCP, Port = 22
Protocol = TCP, Port = 23, Service = telnet
Protocol = TCP, Port = 111, Service = portmap
Protocol = TCP, Port = 80
Protocol = TCP, Port = 79, Service = finger
Protocol = TCP, Port = 22
Protocol = TCP, Port = 21, Service = ftp
Protocol = TCP, Port = 25, Service = smtp
Protocol = TCP, Port = 23, Service = telnet

Vulnerability Name: **open UDP port may allow unauthorized activity**

Risk: ■ 17

Vulnerability Description: NetRecon has discovered an open UDP port.

Since the UDP protocol doesn't use a three-way handshake to establish connections the way TCP does, it is more susceptible to attacks involving spoofed IP addresses. There are a wide range of denial of service attacks that exploit this weakness in UDP to create infinite loops.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

Vulnerability Name: **open UDP port may allow unauthorized activity** (cont.)

-port number

Note: There is a chance of UDP ports being incorrectly detected as open.

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, firewall it. If the service is required for external use, consider running it from a demilitarized zone, and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see: <http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = UDP, Port = 512

Protocol = UDP, Port = 111

Vulnerability Name: **passwd file obtained**

Risk:  49

Vulnerability Description: NetRecon has obtained a password file called passwd.

This is the file used to store passwords on some UNIX network resources. If an attacker can gain access to this file using other vulnerabilities, and if shadow passwords are not implemented, there is a high probability that some passwords can be cracked using widely distributed password cracking tools for UNIX.

Vulnerability Solution: Implement shadow passwords, which prevent an attacker from gaining access to passwords.

Additional Information:

Links:

Details:

Vulnerability Name: **phf CGI allows remote command execution**

Risk:  86

Vulnerability Description: NetRecon has discovered a network resource that permits execution of a CGI program named phf that is susceptible to unauthorized command execution attacks.

Vulnerability Name: **phf CGI allows remote command execution** (cont.)

Some versions of this white pages directory service program pass unchecked newline characters to the UNIX shell.

Vulnerable versions included those shipped with NCSA 1.5a and earlier and Apache 1.0.5 and earlier.

Vulnerability Solution: Remove or otherwise disable the phf CGI program, or upgrade to a non-vulnerable version.

Additional Information: The vulnerable phf program shipped with older versions of NCSA and Apache Web servers, which contain some other vulnerabilities. Consider upgrading the entire Web server package. (1)
See Common Vulnerabilities and Exposures CVE-1999-0067 (2)

Links: 2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0067>

Details:

Protocol = TCP, Port = 80, Service = cgi/phf

Vulnerability Name: **portmap service allows RPC services to be enumerated**

Risk: ■ 29

Vulnerability Description: NetRecon has discovered a network resource running the portmap service, and has used portmap to enumerate RPC services.

Remote Procedure Calls (RPC) is a client-server standard for network application communication, allowing applications to communicate and execute functions remotely without having to know anything about the underlying network operating systems.

The portmap service can be used to find out which RPC services are running and which ports they're running on, so that an RPC communications session can be started.

Many RPC services are vulnerable to attacks. Knowing which services are running and what ports they're running on helps attackers focus their efforts.

An example of a common RPC service is NFS, which is known to be vulnerable to a wide range of attacks, which could result in unauthorized access to files.

Vulnerability Solution: If it's not absolutely necessary, don't use RPC. If it is necessary, be sure to firewall the portmap port (usually 111). Consider using a TCP/UDP wrapper to limit which hosts can access portmap.

Additional Information:

Vulnerability Name: **portmap service allows RPC services to be enumerated**

(cont.)

Links:

Details:

Protocol = TCP, Port = 111, Service = portmap

Vulnerability Name: **responds to ICMP echo request (ping)**

Risk: ■ 15

Vulnerability Description: NetRecon has discovered that this system responds to an ICMP echo request (commonly referred to as ping). ICMP is part of the IP layer. It is used to handle IP status and control messages.

The following are known threats to the legitimate use of this service:

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.) However, disabling ICMP on the firewall is only a partial solution. The complete solution should include patching or upgrading the OS kernel so that it can handle oversized ping requests (if possible with your OS). Many operating system vendors have created patches that prevent the Ping o' Death vulnerability. Consult your OS vendor to see if your system can handle oversized packets.

Additional Information: For additional information about ICMP's ping vulnerability, read CERT(R) Advisory CA-96.26 at the following URL:
<http://www.cert.org/advisories/CA-1996-26.html> (1)
See Common Vulnerabilities and Exposures CVE-1999-0128 (2)

Vulnerability Name: **responds to ICMP echo request (ping)**

(cont.)

Links: 1. <http://www.cert.org/advisories/CA-1996-26.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0128>

Details:Vulnerability Name: **responds to UDP requests with ICMP**Risk: ■ 20

Vulnerability Description: NetRecon has discovered that this system responds to UDP packets directed to unavailable service ports with an ICMP error message. This mechanism allows clients to determine if a service is available on a remote system. If the service is available, then it will handle the service request; however, if no service is associated with the specified port, then an ICMP error message is returned indicating that no service was associated with that port.

The following are known threats to the legitimate use of the ICMP protocol:

- An attacker may send UDP requests to a server in an attempt to map ports on that server.
- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:

Vulnerability Name: **service identified**

Risk:  39

Vulnerability Description: NetRecon has identified a service by software product, version, or both.

Knowing the product and/or version allows attackers to focus their attacks.

Berkeley sendmail, for example, is known to be vulnerable to certain exploits in some versions, but not in others. If attackers can identify that you are running a vulnerable version of Berkeley sendmail they can direct known exploits towards those resources. Even for services with no known exploits, it is possible that vulnerabilities will be discovered in the future.

If attackers can obtain version information for a service, they can eliminate attacks known to fail with that version, or try attacks known to work with that version. Eliminating techniques to try is helpful in speeding up the attack, and can also help to avoid alerting administrators, since it is usually possible to monitor attempted exploits of fixed vulnerabilities.

Vulnerability Solution: Consider the benefits of product identification and weigh them against the security risk. Remove unique banners from services wherever practical. If the identifying information cannot be suppressed, consider using a different product.

For the extremely security conscious, it can be worthwhile to provide intentionally misleading identification of the service product and version. This misdirects attackers to attempt to exploit vulnerabilities that are not present. The administrator can monitor such attacks and take appropriate action to stop attackers before they are successful. However, incorrect banners will also deceive NetRecon.

Additional Information:

Links:

Details:

Service = smtp/Berkeley Sendmail, Revision = 8.9.3, Protocol = TCP, Port = 25

Service = ssh/UNIX, Revision = 2.0-2.0.13, Protocol = TCP, Port = 22

Service = ftp/wu, Revision = 2.4.2-VR16(1), Protocol = TCP, Port = 21

Service = nfs, Revision = 2, Protocol = TCP, Port = 2049

Service = ypbind, Revision = 2, Protocol = UDP, Port = 681

Service = ssh/UNIX, Protocol = TCP, Port = 22

Service = mountd, Revision = 1, Protocol = TCP, Port = 685

Vulnerability Name: **service identified**

(cont.)

Service = mountd, Revision = 2, Protocol = UDP, Port = 682

Service = mountd, Revision = 1, Protocol = UDP, Port = 682

Service = nlockmgr, Revision = 3, Protocol = TCP, Port = 1024

Service = mountd, Revision = 2, Protocol = TCP, Port = 685

Service = ypbind, Revision = 2, Protocol = TCP, Port = 683

Service = nfs, Revision = 2, Protocol = UDP, Port = 2049

Service = ftp/wu, Protocol = TCP, Port = 21

Service = http/NCSA, Revision = 1.4.2, Protocol = TCP, Port = 80

Service = smtp/Berkeley Sendmail, Protocol = TCP, Port = 25

Service = cgi/phf, Protocol = TCP, Port = 80

Service = nlockmgr, Revision = 1, Protocol = TCP, Port = 1024

Service = http/NCSA, Protocol = TCP, Port = 80

Service = nlockmgr, Revision = 3, Protocol = UDP, Port = 1024

Service = rpcbind, Revision = 2, Protocol = UDP, Port = 111

Service = nlockmgr, Revision = 1, Protocol = UDP, Port = 1024

Service = rpcbind, Revision = 2, Protocol = TCP, Port = 111

Vulnerability Name: **shell service enabled**Risk:  42

Vulnerability Description: The shell service provides remote execution facilities with authentication based on privileged port numbers and trusted hosts.

It is possible to configure this service to allow anyone with a valid user name to execute commands without authentication.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information:

Links: 1.
http://www.cs.purdue.edu/coast/satan-html/tutorials/vulnerability/remote_shell_access.html

Details:

Vulnerability Name: **shell service enabled**

(cont.)

Protocol = TCP, Port = 514, Service = shell

Vulnerability Name: **SMTP connections can be established quickly**Risk:  20

Vulnerability Description: NetRecon has discovered an SMTP implementation that allows connections to be made very quickly.

Since SMTP mail transport agents (MTAs) are notorious for having many security problems, they are common targets for attackers. If an attacker can make quick connections to the MTA, they can test out a number of potential problems with relative ease. If, however, there is a substantial delay for each test performed, there is a greater chance that an attacker will lose patience and move on to another target.

Assuming the NetRecon system is not running an ident server, this vulnerability also typically indicates that the MTA does not attempt to ident the connection.

Vulnerability Solution: Some MTAs have a secure mode that prevents rapid connections. If possible, put your MTA into a secure mode. If it is not possible, consider upgrading or switching to another MTA.

Using ident authentication can make it easier to trace abuse and warn of possible e-mail forgeries. Enable ident authentication if your MTA supports it.

Additional Information:

Links:

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP decode alias enabled**Risk:  45

Vulnerability Description: Including a decode mail alias in /etc/aliases makes it easier to send and receive binary files by e-mail.

A decode mail alias can be used to create or overwrite files on the system. For example, an attacker could use this vulnerability to plant a bogus message in the message queue. A few versions of uudecode allow the creation of SUID files, which would allow an

Vulnerability Name: **SMTP decode alias enabled** (cont.)

attacker to use the decode alias to create an SUID daemon shell in an accessible directory.

Vulnerability Solution: Remove the decode alias from all aliases files.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0096 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0096>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP EXPN feature enabled**

Risk:  35

Vulnerability Description: The expn command allows a client to expand a mail address. If it is a shell user address, it shows the results of aliasing through a user's ~/.forward file. If the address is an alias, it shows all the addresses that result from the alias expansion. The expn command is generally used for testing purposes, to test the validity of aliases.

Many systems have easily guessable mail distribution aliases (such as everyone, all, staff, etc.). Being able to expand such aliases to obtain particular user names is very useful to attackers. Some user names are the same as system names, and some accounts have identical user names and passwords.

The expn command also allows an attacker to verify particular user names.

Vulnerability Solution: Consider disabling the expn command in your MTA implementation (commonly sendmail). If you choose not to disable expn , enable logging. Some newer versions of sendmail allow detailed logging of requests and include a privacy option, which allows you to require that requesting sites identify themselves before certain operations can take place. Check with your vendor for the details of the latest MTA program version.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP recipient identified**

Vulnerability Name: **SMTP recipient identified**

(cont.)

Risk:  37

Vulnerability Description: NetRecon has identified a valid mail account.

A valid mail account could be a user or an alias. Each valid account name is a potential login name for network resources on the same network. Knowing valid mail accounts opens up the possibility of social engineering attacks. Attackers can also use valid mail accounts for mail bombing attacks.

Vulnerability Solution: Disable features of your SMTP mail transport agent (MTA) that allow verification and discovery of mail accounts. The most common examples are: VRFY, EXPN, and rcpt notification.

Additional Information:

Links:

Details:

Miscellaneous = SMTP recipient=majordomo, Service = smtp, Protocol = TCP, Port = 25

Miscellaneous = SMTP recipient=decode, Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **smtp service enabled**Risk:  45

Vulnerability Description: The smtp service uses the Simple Mail Transfer Protocol (SMTP) to send electronic messages. The smtp service may be used to obtain information about valid user names and other systems in the network.

The smtp service is vulnerable to a variety of attacks and may also constitute a violation of acceptable use policies.

Vulnerability Solution: Disable this service if it isn't necessary.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0617 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0617>**Details:**

Protocol = TCP, Port = 25, Service = smtp

Vulnerability Name: **SMTP supports EHLO greeting**Risk:  9

Vulnerability Name: **SMTP supports EHLO greeting** (cont.)

Vulnerability Description: NetRecon has discovered an SMTP implementation that responds to the EHLO greeting protocol.

The EHLO greeting protocol is an indication of the ESMTP (Extended Simple Mail Transfer Protocol) protocol. ESMTP has additional vulnerabilities, so knowing that a network resource supports it permits an attacker to focus their efforts.

Vulnerability Solution: Configure your mail transport agent (MTA) to permit the minimum amount of information transfer necessary for completing mail transport tasks.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP VRFY feature enabled**

Risk:  35

Vulnerability Description: NetRecon has discovered an SMTP implementation that allows mail accounts to be verified.

The smtp (the service used to handling e-mail) vrfy command allows a client to verify whether a particular address is valid. The vrfy command is sometimes used by e-mail applications to verify that users exist before sending them messages.

Being able to verify particular user names is very useful to attackers. Some user names are the same as system names, and some accounts have identical user names and passwords. An attacker can also use the vrfy command to search for common distribution aliases (such as everyone, all, or staff), which can then be expanded to reveal many valid user names.

Vulnerability Solution: Consider disabling the vrfy command in your MTA implementation (commonly sendmail). If vrfy is required by any of the applications you use, enable the logging option. Obtain the newest version of your MTA. Many newer versions of sendmail allow detailed logging of sendmail requests, including the hostname or IP address of the requester.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **telnet service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the telnet service.

The telnet service provides remote execution facilities with authentication based on user names and passwords.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password guessing.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0619 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0619>

Details:

Protocol = TCP, Port = 23, Service = telnet

Vulnerability Name: **user shell access obtained via login service**

Risk:  91

Vulnerability Description: NetRecon has connected to a network resource through the login service with user privileges.

NetRecon uses any login names and passwords obtained through other vulnerabilities to attempt to log in to any network resources running the login service. Being able to log in to a network resource with user privileges permits a wide range of activities, depending on the privileges of the user.

Vulnerability Solution: Fix the vulnerabilities that led to NetRecon being able to discover the password that provided access (right-click the vulnerability record in the Data Table pane and choose Path Analysis to see what information led NetRecon to find this vulnerability).

To increase the difficulty of cracking or guessing passwords, enforce the use of secure passwords. Passwords should be a combination of letters, numbers, and punctuation. They should not

Network Resource: **brown.netrecon.com**

(cont.)

Vulnerability Name: **user shell access obtained via login service** (cont.)

correspond to words in any language, names of people, places, fictional characters, initials, dates, etc. They should not be common or simple sequences of letters, numbers, or characters such as abcde or 12345. Additionally, passwords should be changed regularly and should never be reused.

Additional Information:

Links:

Details:

Login Name = johnm, Password = a*s

Login Name = masonb, Password = s*r

Login Name = glennw, Password = f*e

Login Name = willie, Password = k*1

Login Name = mikeb, Password = j*e

Network Resource: **grey.netrecon.com**

Resource Type: IP host, IRIX, System V 4

Aliases: grey, 10.1.6.2, 08:00:63:92:77:f1

of Unique Vulnerabilities: 44

Highest Risk Level Found:  91

Vulnerability Name: **chargen service enabled**

Risk:  60

Vulnerability Description: NetRecon has discovered a network resource running the chargen service.

The chargen service causes a TCP server to send a constant stream of characters to the client until the client terminates the connection. chargen can be used legitimately for certain testing purposes.

Because chargen produces a continual stream of characters, it is susceptible to misuse for denial of service attacks. For example, spoofed packets can link the chargen port to the echo port, creating an infinite loop. This type of attack consumes increasing amounts of network bandwidth, degrading network performance or, in some cases, completely disabling portions of a network.

Vulnerability Solution: To avoid this type of attack, disable the chargen service.

Vulnerability Name: chargen service enabled (cont.)

Additionally, monitoring attempts to access disabled services can alert you to the presence of attackers.

Microsoft has released a hotfix to address chargen attacks directed at Windows NT 4.0 Simple TCP/IP services. The hotfix can be downloaded from:

<ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix> (1)

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0103 (2)
See Common Vulnerabilities and Exposures CAN-1999-0639 (3)

Links: 1. <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0103>
3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0639>

Details:

Protocol = TCP, Port = 19, Service = chargen

Vulnerability Name: daytime service enabled**Risk:** ■ 11

Vulnerability Description: NetRecon has discovered a network resource running the daytime service.

The daytime service returns the date and time.

The format of the daytime service can sometimes tell an attacker something about a network resource, such as the operating system it is running. This service is potentially vulnerable to misaddressed packet attacks, which can link the daytime port to the echo port, or perform similar functions to consume network bandwidth.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0638 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0638>

Details:

Protocol = TCP, Port = 13, Service = daytime

Vulnerability Name: discard service enabled

Vulnerability Name: **discard service enabled**

(cont.)

Risk:  15

Vulnerability Description: NetRecon has discovered a network resource running the discard service.

The discard service reads packets sent to it and then discards them.

Attackers could use a connect response from this, or any service to verify the presence of a network resource.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0636 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0636>

Details:

Protocol = TCP, Port = 9, Service = discard

Vulnerability Name: **echo service enabled**Risk:  60

Vulnerability Description: NetRecon has discovered a network resource running the echo service.

The echo service causes a server to return whatever a client sends. It can be used for a number of testing purposes, much like chargen.

Since the echo port returns whatever is sent to it, it is susceptible to attacks that create false return addresses. For example, spoofed packets can link the echo port to the chargen port, creating an infinite loop. This type of attack consumes increasing amounts of network bandwidth, degrading network performance or, in some cases, completely disabling portions of a network.

Vulnerability Solution: To avoid this type of attack, disable the echo service. Additionally, monitoring attempted access to the echo service can alert you to the presence potential attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0635 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0635>

Details:

Protocol = TCP, Port = 7, Service = echo

Vulnerability Name: **exec service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the exec service.

The exec service (also called rexec) provides remote command execution facilities with authentication based on user names and passwords.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password guessing.

Vulnerability Solution: If possible, disable the exec service. Additionally, monitoring attempted access to the exec service can alert you to the presence potential attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0618 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0618>

Details:

Protocol = TCP, Port = 512, Service = exec

Vulnerability Name: **finger service allows null redirects**

Risk:  59

Vulnerability Description: NetRecon has discovered a network resource running a finger service that allows null redirects. The finger service acts as a proxy to itself when no target host is specified. This can be used to make a query look as if it came from the target host, potentially revealing restricted information.

Vulnerability Solution: Finger should be configured to disable redirection, and unless it is absolutely necessary, finger should be disabled completely. If it must be enabled, finger should reveal minimal information about users, and should require very specific queries.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0106 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0106>

Details:

Protocol = TCP, Port = 79, Service = finger

Vulnerability Name: **finger service allows recursive null redirects**

Vulnerability Name: **finger service allows recursive null redirects** (cont.)**Risk:** ▼ 59

Vulnerability Description: NetRecon has discovered a network resource running a finger service that allows recursive null redirects. The finger service acts as a proxy to itself when no target host is specified, redirecting queries to itself multiple times. By using null redirects, system resources can be consumed, slowing the system to the point of being unusable. With an excessive number of null redirects, system resources can be exhausted, causing a failure of important services.

Vulnerability Solution: Finger should be configured to disable redirection, and unless it is absolutely necessary, finger should be disabled completely. If it must be enabled, finger should reveal minimal information about users, and should require very specific queries.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0797 (1)
See Common Vulnerabilities and Exposures CAN-1999-0106 (2)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0797>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0106>**Details:**

Protocol = TCP, Port = 79, Service = finger

Vulnerability Name: **finger service enabled****Risk:** ▼ 37

Vulnerability Description: NetRecon has discovered a network resource running the finger service.

The finger service allows remote users and processes to obtain information about system processes and individual users.

Among other things, finger can provide the following information to an attacker:

- Valid login names
- Users' full names
- Names of other systems
- A user's login shell

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0612 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0612>**Details:**

Protocol = TCP, Port = 79, Service = finger

Vulnerability Name: **finger service lists users currently logged in**

Risk:  37

Vulnerability Description: NetRecon has found a network resource running a finger service that is configured to answer queries for information about users that are currently logged in. This allows remote attackers to monitor usage of the system, obtain useful social engineering information, and identify some active accounts.

Vulnerability Solution: Configure finger to disallow this query, and unless it is absolutely necessary, disable finger completely. If it must be enabled, finger should reveal minimal information about users, and should require very specific queries.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0612 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0612>

Details:

Protocol = TCP, Port = 79, Service = finger

Vulnerability Name: **finger service recursively redirects queries**

Risk:  77

Vulnerability Description: NetRecon has found a network resource running a finger service that is configured to allow recursive redirects. Under this configuration, the finger service will act as a proxy, redirecting queries multiple times (possibly through multiple hosts). This can potentially be used to reach computers that are otherwise unreachable. Also, by using a complex series of redirections, an attacker can make it difficult to identify the source of the original query. Furthermore, if an attacker recursively redirects queries to localhost, the query can consume system resources, slowing the system to the point of being unusable.

Vulnerability Solution: Configure the finger service to disable redirection, and unless it is absolutely necessary, disable finger completely. If it must be enabled, finger should reveal minimal information about users, and should require very specific queries.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0106 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0106>

Details:

Protocol = TCP, Port = 79, Service = finger

Vulnerability Name: **finger service redirects queries**

Risk:  59

Vulnerability Description: NetRecon has found a network resource running a finger service that is configured to allow redirection of queries. Under this configuration, the finger service will act as a proxy, redirecting queries. This can potentially be used to reach computers that are otherwise unreachable, as well as make it difficult to identify the person actually performing the query.

Vulnerability Solution: Configure the finger service to disable redirection, and unless it is absolutely necessary, disable finger completely. If it must be enabled, finger should reveal minimal information about users, and should require very specific queries.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0106 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0106>

Details:

Protocol = TCP, Port = 79, Service = finger

Vulnerability Name: **ftp service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the FTP service.

FTP (File Transfer Protocol) is a protocol for transferring files between systems. Many applications use the FTP service for data communications. Some systems also allow users to connect to an FTP server to upload and download files.

Many FTP servers are vulnerable to a wide range of attacks designed to retrieve files without authorization (including password files) and execute commands on other parts of the server.

Vulnerability Solution: Obtain the latest patches from your vendor. Older versions of FTP on both UNIX and Windows NT contain many security holes. Disable anonymous FTP access unless it is absolutely necessary. Configure your system to log all FTP accesses and transfers, then periodically check these logs for patterns of misuse.

Make sure the home directory of your FTP server is not writable and disallow connections from system IDs (including root, uucp, nobody, and bin).

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0614 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0614>

Vulnerability Name: **ftp service enabled**

(cont.)

Details:

Protocol = TCP, Port = 21, Service = ftp

Vulnerability Name: **IP address found from name**Risk: ■ 5

Vulnerability Description: NetRecon has successfully discovered the IP address of a network resource using its name.

If NetRecon discovers the names of any network resources (via Windows networking, for example), it attempts to obtain their IP address as well.

Finding the IP address of a network resource verifies that the resource exists. It also helps attackers identify TCP/IP networks to scan for further resources. Having an IP address also opens up the possibility of a wide range of TCP/IP information gathering (port scans, for example) and attacks.

Vulnerability Solution: Do not allow hosts outside your firewall to resolve internal IP addresses unless absolutely necessary. Public DNS should contain only public systems.

Additional Information:

Links:

Details:

Alias = 10.1.6.2

Vulnerability Name: **IP name obtained**Risk: ■ 10

Vulnerability Description: NetRecon has discovered the IP name of a network resource.

System names often reveal something about the system. For example, servers sometimes have the word server in the name, systems are named after their users, etc. Systems with an IP address but no name are usually either old, unused systems (which can be attacked with less risk of notice) or protected systems (containing highly significant information).

Knowing system names can, therefore, help attackers focus their attacks on key systems.

Vulnerability Name: IP name obtained (cont.)
Vulnerability Solution: Do not allow hosts outside your firewall to resolve internal IP names or addresses unless absolutely necessary. Public DNS should contain only public systems.
Additional Information:
Links:
Details:
Alias = grey.netrecon.com
Alias = grey

Vulnerability Name: IRIX LOCKOUT allows remote file writing as root
Risk: ● 72
Vulnerability Description: NetRecon has discovered a network resource running an operating system that may be susceptible to unauthorized file access attacks. IRIX features a LOCKOUT feature that will lock a user account after a given number of failed login attempts. The implementation of the LOCKOUT feature allows attackers to create or corrupt arbitrary files. Note: This vulnerability is detected based on identification of an operating system, which means that NetRecon reports it even if you have already applied the appropriate patch.
Vulnerability Solution: Disable the LOCKOUT feature or obtain a vendor patch (if available).
Additional Information: See CERT Advisory: http://www.cert.org/advisories/CA-1997-15.html (1) See Common Vulnerabilities and Exposures CVE-1999-0036 (2)
Links: 1. http://www.cert.org/advisories/CA-1997-15.html 2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0036
Details:

Vulnerability Name: IRIX overflows allow shell users root access
Risk: ● 91
Vulnerability Description: NetRecon has discovered a network resource running an operating system that may be susceptible to unauthorized access attacks. Some versions of IRIX ship with versions of df , eject , login/scheme , ordist , and xlock which are vulnerable to buffer

Vulnerability Name: **IRIX overflows allow shell users root access** (cont.)

overflows that can be used to gain root privileges. In addition, pset allows a buffer overflow that can be used to obtain sys group privileges, which could in turn be used to gain root privileges.

Any user with shell access could potentially exploit these vulnerabilities.

Note: This vulnerability is detected based on identification of an operating system, which means NetRecon reports it even if you have already applied the appropriate patch.

Vulnerability Solution: Patch or upgrade the utilities (if a patch is available), work around the problem using the method described in the CERT advisory, or install the wrapper program developed by AUSCERT.

Additional Information: For additional information, see the following CERT advisory:
<http://www.cert.org/advisories/CA-1997-21.html> (1)
See Common Vulnerabilities and Exposures CVE-1999-0025-0030 (2)

Links: 1. <http://www.cert.org/advisories/CA-1997-21.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0025>

Details:Vulnerability Name: **login service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the login service.

The login service (sometimes referred to as rlogin) allows remote users to obtain user and sometimes administrator access to a system.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password guessing.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0593 (1)
See Common Vulnerabilities and Exposures CAN-1999-0651 (2)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0593>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0651>

Vulnerability Name: **login service enabled**

(cont.)

Details:

Protocol = TCP, Port = 513, Service = login

Vulnerability Name: **network resource detected via ICMP protocol**Risk: ■ 15

Vulnerability Description: NetRecon has discovered that this network resource responds using the ICMP protocol. ICMP, as part of the IP layer, handles error messaging and other control conditions. This message is a catch-all message because NetRecon has intercepted an ICMP datagram, regardless of its type. If you receive this message, you may also receive messages for the other ICMP vulnerabilities that NetRecon discovers, such as Responds to ICMP Echo (ping) Requests.

In discovering this vulnerability, NetRecon sent a UDP service request and a number of ICMP datagrams to this system and received one or more ICMP responses.

The following are known threats to the legitimate use of the ICMP protocol:

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:

Vulnerability Name: **network resource detected via ICMP protocol**

(cont.)

Vulnerability Name: **network resource identified**Risk:  16

Vulnerability Description: NetRecon has obtained information that helps to identify a particular network resource. This information could include full or partial identification of the operating system, server types (SMB server, for example), whether a computer is an IP host, etc.

Once an attacker has identified a specific target, he or she can find and exploit weakness in that resource.

Vulnerability Solution: Using the data table in NetRecon, determine how the information was obtained. Either eliminate the service responsible or configure it to not give any clues that can help identify the network resource.

Additional Information:

Links:

Details:

Type = IP host

Type = IRIX

Type = System V, Revision = 4

Type = System V

Type = IP host

Vulnerability Name: **nfs service enabled**Risk:  65

Vulnerability Description: NetRecon has discovered a network resource serving file systems using NFS.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

NFS is vulnerable to a wide range of problems, ranging from common misconfigurations (such as incorrect permissions) to serious bugs that can give an attacker full access to any file systems served by NFS. NFS also does host-based authentication, which can be spoofed fairly easily.

Vulnerability Solution: Disable NFS if it is not necessary.

Vulnerability Name: **nfs service enabled**

(cont.)

If NFS is necessary, you should take steps to secure it (see the CERT advisory referenced under Additional Information).

Additional Information: For more information about securing NFS, see:
<http://www.cert.org/advisories/CA-1994-15.html> (1)
See Common Vulnerabilities and Exposures CVE-1999-0631 (2)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0631>

Details:

Service = nfs, Port = 2049, Protocol = UDP

Vulnerability Name: **open RPC service may allow unauthorized activity**Risk: ■ 18

Vulnerability Description: NetRecon has discovered an RPC service.

Remote Procedure Calls (RPC) is a client-server standard for network application communication, allowing applications to communicate and execute functions remotely without having to know anything about the underlying network operating systems.

Since the purpose of RPC services is to permit remote execution of programs and functions, a successful attack on an RPC service gives an attacker this ability or denies legitimate users this ability.

An example of a common RPC service is NFS, which is known to be vulnerable to a wide range of attacks, which could result in unauthorized access to files.

Vulnerability Solution: If the service found is not necessary, disable it. If it is necessary, consider using a TCP/UDP wrapper to limit which hosts can use the service. Firewall the portmap service (usually port 111) so that attackers cannot enumerate RPC services from outside the firewall.

Additional Information:

Links:

Details:

Port = 1035, Protocol = UDP, Service = rquotad, Revision = 1

Port = 1033, Protocol = UDP, Service = walld, Revision = 1

Port = 1072, Protocol = TCP, Service = 100083, Revision = 1

Port = 111, Protocol = TCP, Service = rpcbind, Revision = 2

Port = 111, Protocol = UDP, Service = rpcbind, Revision = 2

Vulnerability Name: open RPC service may allow unauthorized activity (cont.)

Port = 2049, Protocol = UDP, Service = nfs, Revision = 2
Port = 764, Protocol = UDP, Service = status, Revision = 1
Port = 766, Protocol = TCP, Service = status, Revision = 1
Port = 773, Protocol = TCP, Service = nlockmgr, Revision = 1
Port = 775, Protocol = UDP, Service = nlockmgr, Revision = 1
Port = 778, Protocol = UDP, Service = nlockmgr, Revision = 3
Port = 784, Protocol = TCP, Service = nlockmgr, Revision = 2
Port = 786, Protocol = UDP, Service = nlockmgr, Revision = 2
Port = 1053, Protocol = TCP, Service = mountd, Revision = 1
Port = 1030, Protocol = UDP, Service = mountd, Revision = 1
Port = 1056, Protocol = TCP, Service = 391004, Revision = 1
Port = 1031, Protocol = UDP, Service = 391004, Revision = 1
Port = 1032, Protocol = UDP, Service = rstatd, Revision = 1
Port = 1032, Protocol = UDP, Service = rstatd, Revision = 2
Port = 1032, Protocol = UDP, Service = rstatd, Revision = 3
Port = 1034, Protocol = UDP, Service = rusersd, Revision = 1
Port = 1036, Protocol = UDP, Service = sprayd, Revision = 1
Port = 1037, Protocol = UDP, Service = bootparam, Revision = 1
Port = 1065, Protocol = TCP, Service = 391011, Revision = 1
Port = 1067, Protocol = TCP, Service = 391002, Revision = 1
Port = 781, Protocol = UDP, Service = llockmgr, Revision = 1

Vulnerability Name: open TCP port may allow unauthorized activityRisk: ■ 14**Vulnerability Description:** NetRecon has discovered an open TCP port.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:
-port number

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, protect it with a firewall. If the service

Vulnerability Name: **open TCP port may allow unauthorized activity** (cont.)

is required for external use, consider running it from a demilitarized zone and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see:
<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = TCP, Port = 512, Service = exec
Protocol = TCP, Port = 19, Service = chargen
Protocol = TCP, Port = 111, Service = portmap
Protocol = TCP, Port = 513, Service = login
Protocol = TCP, Port = 514, Service = shell
Protocol = TCP, Port = 21, Service = ftp
Protocol = TCP, Port = 23, Service = telnet
Protocol = TCP, Port = 25, Service = smtp
Protocol = TCP, Port = 79, Service = finger
Protocol = TCP, Port = 25, Service = smtp
Protocol = TCP, Port = 13, Service = daytime
Protocol = TCP, Port = 9, Service = discard
Protocol = TCP, Port = 7, Service = echo
Protocol = TCP, Port = 9, Service = discard
Protocol = TCP, Port = 13, Service = daytime
Protocol = TCP, Port = 19, Service = chargen
Protocol = TCP, Port = 23, Service = telnet
Protocol = TCP, Port = 79, Service = finger
Protocol = TCP, Port = 111, Service = portmap
Protocol = TCP, Port = 512, Service = exec
Protocol = TCP, Port = 513, Service = login
Protocol = TCP, Port = 514, Service = shell
Protocol = TCP, Port = 7, Service = echo
Protocol = TCP, Port = 21, Service = ftp

Vulnerability Name: **open UDP port may allow unauthorized activity**

Risk: ■ 17

Vulnerability Description: NetRecon has discovered an open UDP port.

Since the UDP protocol doesn't use a three-way handshake to establish connections the way TCP does, it is more susceptible to attacks involving spoofed IP addresses. There are a wide range of denial of service attacks that exploit this weakness in UDP to create infinite loops.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:
-port number

Note: There is a chance of UDP ports being incorrectly detected as open.

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, firewall it. If the service is required for external use, consider running it from a demilitarized zone, and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see:
<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = UDP, Port = 7

Protocol = UDP, Port = 9

Protocol = UDP, Port = 13

Protocol = UDP, Port = 19

Protocol = UDP, Port = 111

Protocol = UDP, Port = 514

Vulnerability Name: **portmap service allows RPC services to be enumerated**

Risk: ■ 29

Vulnerability Description: NetRecon has discovered a network resource running the portmap service, and has used portmap to enumerate RPC services.

Remote Procedure Calls (RPC) is a client-server standard for

Vulnerability Name: **portmap service allows RPC services to be enumerated** (cont.)

network application communication, allowing applications to communicate and execute functions remotely without having to know anything about the underlying network operating systems.

The portmap service can be used to find out which RPC services are running and which ports they're running on, so that an RPC communications session can be started.

Many RPC services are vulnerable to attacks. Knowing which services are running and what ports they're running on helps attackers focus their efforts.

An example of a common RPC service is NFS, which is known to be vulnerable to a wide range of attacks, which could result in unauthorized access to files.

Vulnerability Solution: If it's not absolutely necessary, don't use RPC. If it is necessary, be sure to firewall the portmap port (usually 111). Consider using a TCP/UDP wrapper to limit which hosts can access portmap.

Additional Information:

Links:

Details:

Protocol = TCP, Port = 111, Service = portmap

Vulnerability Name: **responds to ICMP echo request (ping)**

Risk: ■ 15

Vulnerability Description: NetRecon has discovered that this system responds to an ICMP echo request (commonly referred to as ping). ICMP is part of the IP layer. It is used to handle IP status and control messages.

The following are known threats to the legitimate use of this service:

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack

Vulnerability Name: **responds to ICMP echo request (ping)** (cont.)

sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)

- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.) However, disabling ICMP on the firewall is only a partial solution. The complete solution should include patching or upgrading the OS kernel so that it can handle oversized ping requests (if possible with your OS). Many operating system vendors have created patches that prevent the Ping o' Death vulnerability. Consult your OS vendor to see if your system can handle oversized packets.

Additional Information: For additional information about ICMP's ping vulnerability, read CERT(R) Advisory CA-96.26 at the following URL:
<http://www.cert.org/advisories/CA-1996-26.html> (1)
See Common Vulnerabilities and Exposures CVE-1999-0128 (2)

Links: 1. <http://www.cert.org/advisories/CA-1996-26.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0128>

Details:Vulnerability Name: **responds to ICMP information request**

Risk: ■ 16

Vulnerability Description: NetRecon has discovered that this system responds to an ICMP information request. ICMP is part of the IP layer. It is used to handle IP status and control messages. The ICMP information request message type is an obsolete ICMP message request; however, some systems still respond to it.

The following are known threats to the legitimate use of this service:

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack

Vulnerability Name: **responds to ICMP information request** (cont.)

sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)

- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:

Vulnerability Name: **responds to UDP requests with ICMP**

Risk: ■ 20

Vulnerability Description: NetRecon has discovered that this system responds to UDP packets directed to unavailable service ports with an ICMP error message. This mechanism allows clients to determine if a service is available on a remote system. If the service is available, then it will handle the service request; however, if no service is associated with the specified port, then an ICMP error message is returned indicating that no service was associated with that port.

The following are known threats to the legitimate use of the ICMP protocol:

- An attacker may send UDP requests to a server in an attempt to map ports on that server.

- An ICMP reply tells an attacker that a remote system exists and is running.


- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.


- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)

- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)

- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet

Vulnerability Name: responds to UDP requests with ICMP (cont.) floods may result in a partial or complete denial of service.)
Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)
Additional Information:
Links:
Details:

Vulnerability Name: Sendmail allows information obscuring via long HELO/EHLO
Risk:  45
Vulnerability Description: If an excessively long HELO/EHLO greeting is used, Sendmail will truncate important information relating to the origin of the e-mail. This allows e-mail to be sent with no traceability. Sendmail versions prior to 8.9.0 are vulnerable.
Vulnerability Solution: Upgrade sendmail to the latest version, or select another SMTP package. This vulnerability is addressed in version 8.9.0.
Additional Information: http://www.sendmail.org (1) See Common Vulnerabilities and Exposures CVE-1999-0098 (2)
Links: 1. http://www.sendmail.org 2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0098
Details: Protocol = TCP, Port = 25, Service = smtp

Vulnerability Name: Sendmail gecos overflow allows shell users root access
Risk:  82
Vulnerability Description: NetRecon has detected a version of Berkeley sendmail allows shell users to obtain privileges of root and the default user account (usually daemon). Versions up to and including 8.7.5 are vulnerable.
Vulnerability Solution: Upgrade sendmail.
Additional Information: See the following CERT Advisory: http://www.cert.org/advisories/CA-1996-20.html (1) See Common Vulnerabilities and Exposures CVE-1999-0131 (2)
Links: 1. http://www.cert.org/advisories/CA-1996-20.html

Vulnerability Name: **Sendmail gecoss overflow allows shell users root access** (cont.)

2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0131>

Details:

Protocol = TCP, Port = 25, Service = smtp

Vulnerability Name: **Sendmail header denial of service possible**

Risk:  60

Vulnerability Description: NetRecon has discovered a network resource running a version of Sendmail susceptible to a denial of service attack.

Sendmail is a Mail Transport Agent (MTA), used to send and receive electronic messages.

Sendmail versions prior to 8.9.3 can be slowed or even stopped by connecting multiple times and sending a message header with a very large number of recipients.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

-protocol used to connect to sendmail
-port used to connect to sendmail

Vulnerability Solution: Upgrade to Sendmail 8.9.3 or later.

Additional Information: Additional information about this problem, including exploit source code, can be found at:
<http://www.rootshell.com/archive-j457nxiqi3gg59dv/199902/sendmail892against.txt.html>
See Common Vulnerabilities and Exposures CVE-1999-0478 (2)

Links: 1.
<http://www.rootshell.com/archive-j457nxiqi3gg59dv/199902/sendmail892against.txt.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0478>

Details:

Protocol = TCP, Port = 25, Service = smtp

Vulnerability Name: **Sendmail redirect possible**

Risk:  34

Vulnerability Description: Versions up to and including 8.8.0 of Berkeley sendmail contain a bug which allows users to redirect any e-mail in the queue addressed to an unqualified domain name to a host of their

Vulnerability Name: **Sendmail redirect possible** (cont.)

choosing. In some versions, users may be able to redirect mail even with fully qualified addresses.

Vulnerability Solution: Upgrade sendmail.

Additional Information:

Links:

Details:

Protocol = TCP, Port = 25, Service = smtp

Vulnerability Name: **Sendmail resource starvation allows shell users root access**

Risk:  83

Vulnerability Description: NetRecon has detected that versions up to and including 8.7.5 of Berkeley sendmail allow shell users to execute commands as the default user.

Vulnerability Solution: Upgrade sendmail.

Additional Information: See the following CERT Advisory:
<http://www.cert.org/advisories/CA-1996-20.html> (1)
See Common Vulnerabilities and Exposures CVE-1999-0131 (2)

Links: 1. <http://www.cert.org/advisories/CA-1996-20.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0131>

Details:

Protocol = TCP, Port = 25

Vulnerability Name: **service identified**

Risk:  39

Vulnerability Description: NetRecon has identified a service by software product, version, or both.

Knowing the product and/or version allows attackers to focus their attacks.

Berkeley sendmail, for example, is known to be vulnerable to certain exploits in some versions, but not in others. If attackers can identify that you are running a vulnerable version of Berkeley sendmail they can direct known exploits towards those resources. Even for services with no known exploits, it is possible that vulnerabilities will be discovered in the future.

Vulnerability Name: **service identified**

(cont.)

If attackers can obtain version information for a service, they can eliminate attacks known to fail with that version, or try attacks known to work with that version. Eliminating techniques to try is helpful in speeding up the attack, and can also help to avoid alerting administrators, since it is usually possible to monitor attempted exploits of fixed vulnerabilities.

Vulnerability Solution: Consider the benefits of product identification and weigh them against the security risk. Remove unique banners from services wherever practical. If the identifying information cannot be suppressed, consider using a different product.

For the extremely security conscious, it can be worthwhile to provide intentionally misleading identification of the service product and version. This misdirects attackers to attempt to exploit vulnerabilities that are not present. The administrator can monitor such attacks and take appropriate action to stop attackers before they are successful. However, incorrect banners will also deceive NetRecon.

Additional Information:

Links:

Details:

Service = mountd, Revision = 1, Protocol = TCP, Port = 1053
Service = mountd, Revision = 1, Protocol = UDP, Port = 1030
Service = 391004, Revision = 1, Protocol = TCP, Port = 1056
Service = 391004, Revision = 1, Protocol = UDP, Port = 1031
Service = rstatd, Revision = 1, Protocol = UDP, Port = 1032
Service = rstatd, Revision = 2, Protocol = UDP, Port = 1032
Service = rstatd, Revision = 3, Protocol = UDP, Port = 1032
Service = walld, Revision = 1, Protocol = UDP, Port = 1033
Service = rquotad, Revision = 1, Protocol = UDP, Port = 1035
Service = bootparam, Revision = 1, Protocol = UDP, Port = 1037
Service = 391011, Revision = 1, Protocol = TCP, Port = 1065
Service = 391002, Revision = 1, Protocol = TCP, Port = 1067
Service = nlockmgr, Revision = 2, Protocol = TCP, Port = 784
Service = 100083, Revision = 1, Protocol = TCP, Port = 1072
Service = rpcbind, Revision = 2, Protocol = TCP, Port = 111
Service = nlockmgr, Revision = 2, Protocol = UDP, Port = 786

Vulnerability Name: **service identified**

(cont.)

Service = status, Revision = 1, Protocol = UDP, Port = 764
Service = llockmgr, Revision = 1, Protocol = UDP, Port = 781
Service = nlockmgr, Revision = 3, Protocol = UDP, Port = 778
Service = nlockmgr, Revision = 1, Protocol = UDP, Port = 775
Service = nlockmgr, Revision = 1, Protocol = TCP, Port = 773
Service = nfs, Revision = 2, Protocol = UDP, Port = 2049
Service = rpcbind, Revision = 2, Protocol = UDP, Port = 111
Service = status, Revision = 1, Protocol = TCP, Port = 766
Service = smtp/Berkeley Sendmail, Revision = 8.6.9, Protocol = TCP, Port = 25
Service = smtp/IRIX Sendmail, Revision = 8.6.9, Protocol = TCP, Port = 25
Service = rusersd, Revision = 1, Protocol = UDP, Port = 1034
Service = smtp/Berkeley Sendmail, Revision = 25, Protocol = TCP, Port = 25
Service = smtp/IRIX Sendmail, Protocol = TCP, Port = 25
Service = smtp/Berkeley Sendmail, Protocol = TCP, Port = 25
Service = sprayd, Revision = 1, Protocol = UDP, Port = 1036

Vulnerability Name: **shell service enabled**Risk:  42

Vulnerability Description: The shell service provides remote execution facilities with authentication based on privileged port numbers and trusted hosts.

It is possible to configure this service to allow anyone with a valid user name to execute commands without authentication.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information:

Links: 1.
http://www.cs.purdue.edu/coast/satan-html/tutorials/vulnerability/remote_shell_access.html

Details:

Protocol = TCP, Port = 514, Service = shell

Vulnerability Name: **SMTP allows remote command execution via bounce filter**

Risk:  86

Vulnerability Description: Attackers can execute arbitrary shell commands by specifying a filter as a return address e-mail in e-mail that will bounce.

Note: If your SMTP software does not support filters, this is not a vulnerability. If you are not sure if your SMTP software supports filters, contact your vendor.

Vulnerability Solution: Upgrade or replace your SMTP server, or verify that it does not support filters.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0203 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0203>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP allows user verification with rcpt**

Risk:  35

Vulnerability Description: NetRecon has discovered a network resource running an SMTP implementation that allows rcpt verification.

Some SMTP mail transport agents (MTAs) will return an error if the recipient of a mail message isn't valid. This fact can be used much like VRFY to determine whether particular mail accounts exist.

Vulnerability Solution: If possible, disable this feature in your MTA. If it is not possible, consider upgrading or switching to a MTA that permits disabling of rcpt verification.


Additional Information:

Links:

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP configuration allows relaying**

Risk:  61

Vulnerability Name: **SMTP configuration allows relaying** (cont.)

Vulnerability Description: Your SMTP configuration allows relaying of e-mail between arbitrary hosts. This is the default in many older SMTP implementations. Some SMTP implementations do not allow you to block relaying. Berkeley Sendmail introduced relay blocking in version 8.8, but it must be enabled.

This vulnerability is actively exploited by bulk e-mail solicitors (spammers), allowing them to conceal their identity and decrease the demand on their own resources.

Exploitation can result in consumption of disk space and bandwidth. Recipients may mistakenly identifying your site as the source of unwanted e-mail, which can lead to further attacks or other sites blocking email from your site.

Note: If the host in question trusts the host running NetRecon, you may consider this alert a false positive.

Vulnerability Solution: Disable SMTP or upgrade and (if necessary) configure your SMTP server to deny relaying.

Additional Information: Sendmail home page:
<http://www.sendmail.org/> (1)
Hewlett-Packard Sendmail upgrade information:
<http://www.software.hp.com/software/HPsoftware/Sendmail/index.html>
Sun Microsystems states that Solaris 2.7 will ship with Sendmail 8.8, and that a backport of Sendmail 8.8 will be available soon for prior operating system versions.
See Common Vulnerabilities and Exposures CAN-1999-0512 (3)

Links: 1. <http://www.sendmail.org/>
2. <http://www.software.hp.com/software/HPsoftware/Sendmail/index.html>
3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0512>

Details:

Port = 25, Protocol = TCP, Service = smtp

Vulnerability Name: **SMTP connections can be established quickly**

Risk: ■ 20

Vulnerability Description: NetRecon has discovered an SMTP implementation that allows connections to be made very quickly.

Since SMTP mail transport agents (MTAs) are notorious for having many security problems, they are common targets for attackers. If an attacker can make quick connections to the MTA, they can test

Vulnerability Name: **SMTP connections can be established quickly** (cont.)

out a number of potential problems with relative ease. If, however, there is a substantial delay for each test performed, there is a greater chance that an attacker will lose patience and move on to another target.

Assuming the NetRecon system is not running an ident server, this vulnerability also typically indicates that the MTA does not attempt to ident the connection.

Vulnerability Solution: Some MTAs have a secure mode that prevents rapid connections. If possible, put your MTA into a secure mode. If it is not possible, consider upgrading or switching to another MTA.

Using ident authentication can make it easier to trace abuse and warn of possible e-mail forgeries. Enable ident authentication if your MTA supports it.

Additional Information:

Links:

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP EXPN feature enabled**

Risk:  35

Vulnerability Description: The expn command allows a client to expand a mail address. If it is a shell user address, it shows the results of aliasing through a user's ~/.forward file. If the address is an alias, it shows all the addresses that result from the alias expansion. The expn command is generally used for testing purposes, to test the validity of aliases.

Many systems have easily guessable mail distribution aliases (such as everyone, all, staff, etc.). Being able to expand such aliases to obtain particular user names is very useful to attackers. Some user names are the same as system names, and some accounts have identical user names and passwords.

The expn command also allows an attacker to verify particular user names.

Vulnerability Solution: Consider disabling the expn command in your MTA implementation (commonly sendmail). If you choose not to disable expn, enable logging. Some newer versions of sendmail allow detailed logging of requests and include a privacy option, which allows you to require that requesting sites identify themselves before certain operations can take place. Check with your vendor for the details of the latest MTA program version.

Vulnerability Name: **SMTP EXPN feature enabled**

(cont.)

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **smtp service enabled**

Risk:  45

Vulnerability Description: The smtp service uses the Simple Mail Transfer Protocol (SMTP) to send electronic messages. The smtp service may be used to obtain information about valid user names and other systems in the network.

The smtp service is vulnerable to a variety of attacks and may also constitute a violation of acceptable use policies.

Vulnerability Solution: Disable this service if it isn't necessary.


Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0617 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0617>

Details:

Protocol = TCP, Port = 25, Service = smtp

Vulnerability Name: **SMTP supports EHLO greeting**

Risk:  9

Vulnerability Description: NetRecon has discovered an SMTP implementation that responds to the EHLO greeting protocol.

The EHLO greeting protocol is an indication of the ESMTP (Extended Simple Mail Transfer Protocol) protocol. ESMTP has additional vulnerabilities, so knowing that a network resource supports it permits an attacker to focus their efforts.

Vulnerability Solution: Configure your mail transport agent (MTA) to permit the minimum amount of information transfer necessary for completing mail transport tasks.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Vulnerability Name: **SMTP supports EHLO greeting**

(cont.)

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **SMTP VRFY feature enabled**Risk:  35

Vulnerability Description: NetRecon has discovered an SMTP implementation that allows mail accounts to be verified.

The smtp (the service used to handling e-mail) vrfy command allows a client to verify whether a particular address is valid. The vrfy command is sometimes used by e-mail applications to verify that users exist before sending them messages.

Being able to verify particular user names is very useful to attackers. Some user names are the same as system names, and some accounts have identical user names and passwords. An attacker can also use the vrfy command to search for common distribution aliases (such as everyone, all, or staff), which can then be expanded to reveal many valid user names.

Vulnerability Solution: Consider disabling the vrfy command in your MTA implementation (commonly sendmail). If vrfy is required by any of the applications you use, enable the logging option. Obtain the newest version of your MTA. Many newer versions of sendmail allow detailed logging of sendmail requests, including the hostname or IP address of the requester.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **telnet service enabled**Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the telnet service.

The telnet service provides remote execution facilities with authentication based on user names and passwords.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password

Vulnerability Name: **telnet service enabled** (cont.)

guessing.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0619 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0619>

Details:

Protocol = TCP, Port = 23, Service = telnet

Vulnerability Name: **user shell access obtained via login service**

Risk:  91

Vulnerability Description: NetRecon has connected to a network resource through the login service with user privileges.

NetRecon uses any login names and passwords obtained through other vulnerabilities to attempt to log in to any network resources running the login service. Being able to log in to a network resource with user privileges permits a wide range of activities, depending on the privileges of the user.

Vulnerability Solution: Fix the vulnerabilities that led to NetRecon being able to discover the password that provided access (right-click the vulnerability record in the Data Table pane and choose Path Analysis to see what information led NetRecon to find this vulnerability).

To increase the difficulty of cracking or guessing passwords, enforce the use of secure passwords. Passwords should be a combination of letters, numbers, and punctuation. They should not correspond to words in any language, names of people, places, fictional characters, initials, dates, etc. They should not be common or simple sequences of letters, numbers, or characters such as abcde or 12345. Additionally, passwords should be changed regularly and should never be reused.

Additional Information:

Links:

Details:

Login Name = lp, Password =

Login Name = guest, Password =

Network Resource: **grey.netrecon.com**

(cont.)

Vulnerability Name: **user shell access obtained via login service**

(cont.)

Login Name = guest, Password = g*t

Login Name = EZsetup, Password = *

Login Name = demos, Password = *

Network Resource: **purple.netrecon.com**

Resource Type: IP host, Linux 2.2.10

Aliases: purple, 10.1.6.3, 00:10:6d:c4:27:81

of Unique Vulnerabilities: 41

Highest Risk Level Found:  95

Vulnerability Name: **anonymous FTP access is enabled**

Risk:  53

Vulnerability Description: NetRecon has successfully logged on to an FTP server anonymously.

FTP (File Transfer Protocol) is a protocol for transferring files between computers. The FTP service is used by many applications for data communications. Some computers also allow users to connect to an FTP server to upload and download files.

FTP servers are vulnerable to a wide range of attacks designed to retrieve files without authorization (including password files) and execute commands on other parts of the server. Anonymous FTP means that anyone who can connect to the service can log in, greatly increasing the potential number of attackers and attacks. Attackers can also abuse anonymous FTP access a number of other ways, including using an anonymous FTP site as a drop zone for illegal files.

Vulnerability Solution: Never allow anonymous FTP access unless it is absolutely necessary. Configure your system to log all FTP accesses and transfers and periodically check these logs for patterns of misuse.

Make sure the home directory of your FTP server is not writable and disallow connections from system IDs (including root, uucp, nobody, and bin).

If practical, deny FTP access using a firewall.

Symantec Intruder Alert can be used to monitor any connections to the FTP port.

Vulnerability Name: **anonymous FTP access is enabled** (cont.)

Additional Information: http://www.cert.org/tech_tips/anonymous_ftp_abuses.html (1)
See Common Vulnerabilities and Exposures CVE-1999-0497 (2)

Links: 1. http://www.cert.org/tech_tips/anonymous_ftp_abuses.html
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0497>

Details:

Port = 21, Protocol = TCP, Service = ftp

Vulnerability Name: **encrypted password cracked**

Risk:  89

Vulnerability Description: NetRecon has cracked an encrypted password it discovered through another vulnerability.

Many UNIX systems allow any user to read one or more files containing valid login names and encrypted passwords. NetRecon uses small (for speed) and large (for completeness) dictionaries of commonly used passwords, encrypts each of the words in the list, and then compares the results with the encrypted passwords in the map file obtained on the target system. Any matches obtained are stored in a valid password list, which can be used by NetRecon to gain access to network resources.

Knowledge of relatively few valid passwords allows immediate access to some resources. Additionally, because many people use the same passwords in multiple situations, knowing a few passwords often allows access to additional network resources.

Obtaining password maps and cracking them externally is a very powerful way to attack a system. Since attackers can work to crack passwords on any systems they can access, they can utilize many resources to crack the passwords, and they can do so without fear of detection.

Vulnerability Solution: To increase the difficulty of cracking or guessing passwords, enforce the use of secure passwords. Passwords should be a combination of letters, numbers, and punctuation. They should not correspond to words in any language, names of people, places, fictional characters, initials, dates, or the like. They should not be common or simple sequences of letters, numbers, or characters such as abcde or 12345. Additionally, passwords should be changed regularly and should never be reused.

Most versions of UNIX allow the use of shadow password files. These files prevent anyone other than system administrators from being able to view the encrypted passwords.

Vulnerability Name: **encrypted password cracked** (cont.)

Symantec Enterprise Security Manager allows you to set and consistently apply a policy of using strong passwords.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0501 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0501>

Details:

Login Name = glennw, Password = f*e, Encrypted Password = I0Y3T7JPqWPws

Login Name = norman, Password = b*r, Encrypted Password = wmFHfKAWmT01s

Login Name = walter, Password = w*r, Encrypted Password = SlcFFpyHgs5Dk

Vulnerability Name: **finger service enabled**

Risk:  37

Vulnerability Description: NetRecon has discovered a network resource running the finger service.

The finger service allows remote users and processes to obtain information about system processes and individual users.

Among other things, finger can provide the following information to an attacker:

- Valid login names
- Users' full names
- Names of other systems
- A user's login shell

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0612 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0612>

Details:

Protocol = TCP, Port = 79, Service = finger

Vulnerability Name: **FTP access obtained**

Risk:  54

Vulnerability Description: NetRecon has successfully logged on to an FTP server either anonymously or by guessing the login name and password from a short list.

Vulnerability Name: **FTP access obtained**

(cont.)

FTP (File Transfer Protocol) is a protocol for transferring files between systems. Many applications use the FTP service for data communications. Some systems also allow users to connect to an FTP server to upload and download files.

Many FTP servers are vulnerable to a wide range of attacks designed to retrieve files without authorization (including password files) and execute commands on other parts of the server. Anonymous FTP means that anyone who can connect to the service can log in, greatly increasing the potential number of attackers and attacks. Attackers can also abuse anonymous FTP access a number of other ways, including using an anonymous FTP site as a drop zone for illegal files.

Vulnerability Solution: Obtain the latest patches from your vendor. Older versions of FTP on both UNIX and Windows NT contain security vulnerabilities. Disable anonymous FTP access unless it is absolutely necessary. Configure your system to log all FTP accesses and transfers, then periodically check these logs for patterns of misuse.

Make sure that the home directory of your FTP server is not writable and disallow connections from system IDs (including root, uucp, nobody, and bin).

Use a firewall to protect FTP access where practical.

Additional Information: http://www.cert.org/tech_tips/anonymous_ftp_abuses.html (1)
See Common Vulnerabilities and Exposures CVE-1999-0497 (2)

Links: 1. http://www.cert.org/tech_tips/anonymous_ftp_abuses.html
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0497>

Details:

Port = 21, Protocol = TCP, Service = ftp, Login Name = ftp, Password = N*m

Port = 21, Protocol = TCP, Service = ftp, Login Name = anonymous, Password = N*m

Vulnerability Name: **FTP root directory is writable**Risk:  63

Vulnerability Description: NetRecon has discovered an FTP server with a home directory that can be written to by an anonymous user. An attacker can use a number of known exploits to compromise many FTP servers that have writable root directories, including vulnerabilities that let them retrieve password files and execute commands as a user on the server.

Vulnerability Name: **FTP root directory is writable** (cont.)

FTP (File Transfer Protocol) is a protocol for transferring files between systems. Many applications use the FTP service for data communications. Some systems also allow users to connect to an FTP server to upload and download files.

Vulnerability Solution: Disable anonymous FTP access unless it is absolutely necessary. Configure your system to log all FTP accesses and transfers, then periodically check these logs for patterns of misuse.

Make sure that the home directory of your FTP server is not writable and disallow connections from system IDs (including root, uucp, nobody, and bin).

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0527 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0527>

Details:

Port = 21, Protocol = TCP, Service = ftp

Vulnerability Name: **ftp service enabled**

Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the FTP service.

FTP (File Transfer Protocol) is a protocol for transferring files between systems. Many applications use the FTP service for data communications. Some systems also allow users to connect to an FTP server to upload and download files.

Many FTP servers are vulnerable to a wide range of attacks designed to retrieve files without authorization (including password files) and execute commands on other parts of the server.

Vulnerability Solution: Obtain the latest patches from your vendor. Older versions of FTP on both UNIX and Windows NT contain many security holes. Disable anonymous FTP access unless it is absolutely necessary. Configure your system to log all FTP accesses and transfers, then periodically check these logs for patterns of misuse.

Make sure the home directory of your FTP server is not writable and disallow connections from system IDs (including root, uucp, nobody, and bin).

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0614 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0614>

Details:

Vulnerability Name: **ftp service enabled**

(cont.)

Protocol = TCP, Port = 21, Service = ftp

Vulnerability Name: **http service enabled**Risk:  42

Vulnerability Description: The http service is enabled. HTTP is the protocol the World Wide Web uses. Many vulnerabilities are associated with this service, and new security problems are constantly being discovered with Web software.

The http service enabled means the system is running a Web server (as opposed to being able to connect to the WWW via a browser).

Vulnerability Solution: Disable HTTP on computers that should not be accessed via the Web.

If HTTP is necessary and is used to host a public Web site, consider placing the server in a demilitarized zone (DMZ) on a network segment isolated from systems containing sensitive data.


If HTTP is necessary only for internal use, restrict access from untrusted hosts with a firewall.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0633 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0633>

Details:

Service = http, Port = 80, Protocol = TCP


Vulnerability Name: **IP address found from name**Risk:  5


Vulnerability Description: NetRecon has successfully discovered the IP address of a network resource using its name.

If NetRecon discovers the names of any network resources (via Windows networking, for example), it attempts to obtain their IP address as well.

Finding the IP address of a network resource verifies that the resource exists. It also helps attackers identify TCP/IP networks to scan for further resources. Having an IP address also opens up the possibility of a wide range of TCP/IP information gathering (port

Vulnerability Name: IP address found from name	(cont.)
scans, for example) and attacks.	
Vulnerability Solution:	Do not allow hosts outside your firewall to resolve internal IP addresses unless absolutely necessary. Public DNS should contain only public systems.
Additional Information:	
Links:	
Details:	
Alias = 10.1.6.3	

Vulnerability Name: IP name obtained	
Risk:  10	
Vulnerability Description:	NetRecon has discovered the IP name of a network resource. System names often reveal something about the system. For example, servers sometimes have the word server in the name, systems are named after their users, etc. Systems with an IP address but no name are usually either old, unused systems (which can be attacked with less risk of notice) or protected systems (containing highly significant information). Knowing system names can, therefore, help attackers focus their attacks on key systems.
Vulnerability Solution:	Do not allow hosts outside your firewall to resolve internal IP names or addresses unless absolutely necessary. Public DNS should contain only public systems.
Additional Information:	
Links:	
Details:	
Alias = purple	
Alias = purple.netrecon.com	

Vulnerability Name: login service enabled	
Risk:  42	
Vulnerability Description:	NetRecon has discovered a network resource running the login service.

Vulnerability Name: **login service enabled** (cont.)

The login service (sometimes referred to as rlogin) allows remote users to obtain user and sometimes administrator access to a system.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password guessing.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0593 (1)
See Common Vulnerabilities and Exposures CAN-1999-0651 (2)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0593>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0651>

Details:

Protocol = TCP, Port = 513, Service = login

Vulnerability Name: **mountd service allows directory to be mounted**

Risk:  90

Vulnerability Description: NetRecon has mounted a directory using the mountd service. The mountd service can be used to access local and remote file systems. The mountd can allow attackers access to your file system, usually with root privileges.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- directory NetRecon mounted
- service used to obtain access
- protocol used to obtain access

Vulnerability Solution: Check file permissions on the mounted directory and make them as restrictive as possible. Make sure you are using the latest mountd program. Contact your vendor for more information.

Additional Information:

Links:

Details:

Directory = /home, Service = mountd, Protocol = RPC/UDP, Mounted = yes

Directory = /etc, Service = mountd, Protocol = RPC/UDP, Mounted = yes

Vulnerability Name: **mountd service allows discovery of network resources**

Risk: ■ 14

Vulnerability Description: NetRecon has discovered a network resource running mountd that permits network resources to be enumerated.

mountd can be used to access local and remote file systems via the Network File System (NFS).

An attacker can use mountd to list any network resources currently using file systems via NFS. Knowing the names of network resources on a network is one of the first steps in attacking those resources.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- service used to enumerate resources
- protocol used to enumerate resources

Vulnerability Solution: If NFS isn't necessary, disable mountd.

Additional Information:

Links:

Details:

Discovered Network Resource = turquoise.netrecon.com, Service = mountd, Protocol = RPC/UDP

Discovered Network Resource = black.netrecon.com, Service = mountd, Protocol = RPC/UDP

Discovered Network Resource = white.netrecon.com, Service = mountd, Protocol = RPC/UDP

Discovered Network Resource = ORANGE.netrecon.com, Service = mountd, Protocol = RPC/UDP

Discovered Network Resource = YELLOW.netrecon.com, Service = mountd, Protocol = RPC/UDP

Discovered Network Resource = violet.netrecon.com, Service = mountd, Protocol = RPC/UDP

Discovered Network Resource = pink.netrecon.com, Service = mountd, Protocol = RPC/UDP

Vulnerability Name: **mountd service discloses authorized client list**

Vulnerability Name: **mountd service discloses authorized client list** (cont.)Risk:  37

Vulnerability Description: NetRecon has discovered a network resource running mountd that permits authorized NFS clients to be enumerated.

mountd can be used to access local and remote file systems via the Network File System (NFS).

If the list of authorized clients for a particular file system is empty, anyone can access that file system without having to authenticate.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- directory for which client list was obtained
- client(s) allowed
- service used to enumerate clients
- protocol used to enumerate clients

Vulnerability Solution: If NFS isn't necessary, disable mountd.

Additional Information:

Links:

Details:

Directory = /home, Allowed = *.netrecon.com, Service = mountd, Protocol = RPC/UDP

Directory = /etc, Allowed = *.netrecon.com, Service = mountd, Protocol = RPC/UDP

Vulnerability Name: **network resource detected via ICMP protocol**Risk:  15

Vulnerability Description: NetRecon has discovered that this network resource responds using the ICMP protocol. ICMP, as part of the IP layer, handles error messaging and other control conditions. This message is a catch-all message because NetRecon has intercepted an ICMP datagram, regardless of its type. If you receive this message, you may also receive messages for the other ICMP vulnerabilities that NetRecon discovers, such as Responds to ICMP Echo (ping) Requests.

In discovering this vulnerability, NetRecon sent a UDP service request and a number of ICMP datagrams to this system and received one or more ICMP responses.

The following are known threats to the legitimate use of the ICMP protocol:

Vulnerability Name: **network resource detected via ICMP protocol** (cont.)

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:

Vulnerability Name: **network resource identified**

Risk: ■ 16

Vulnerability Description: NetRecon has obtained information that helps to identify a particular network resource. This information could include full or partial identification of the operating system, server types (SMB server, for example), whether a computer is an IP host, etc.

Once an attacker has identified a specific target, he or she can find and exploit weakness in that resource.

Vulnerability Solution: Using the data table in NetRecon, determine how the information was obtained. Either eliminate the service responsible or configure it to not give any clues that can help identify the network resource.

Additional Information:

Links:

Details:

Type = IP host

Vulnerability Name: **network resource identified**

(cont.)

Type = IP host

Type = Linux, Revision = 2.2.10

Type = Linux

Type = IP host

Vulnerability Name: **nfs service allows account information to be obtained from passwd file**Risk: ■ 30

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a passwd file containing account information.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

The passwd file often contains valuable information that can be used to gain access to network resources. Even if passwords or encrypted passwords cannot be obtained, possessing account information is valuable for attackers attempting to gain unauthorized access, since the password can sometimes be guessed.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file obtained, including its path
- login name obtained
- Miscellaneous user information, including the uid, gid, info, default directory, and shell
- service used to obtain the passwd file
- protocol used to obtain the passwd file

Vulnerability Solution: Remove the passwd file from the export list.

Additional Information: Additional information about securing NFS can be found in the following CERT advisory:
<http://www.cert.org/advisories/CA-1994-15.html> (1)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

File = /home/shadow-bill, Service = nfs, Protocol = RPC/UDP

File = /home/passwd.OLD, Service = nfs, Protocol = RPC/UDP

File = /home/passwd-, Service = nfs, Protocol = RPC/UDP

File = /home/passwd, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service allows account information to be obtained from passwd file** (cont.)

File = /home/ftp/etc/passwd, Service = nfs, Protocol = RPC/UDP

File = /home/shadow-, Service = nfs, Protocol = RPC/UDP

File = /home/shadow, Service = nfs, Protocol = RPC/UDP

File = /etc/passwd.OLD, Service = nfs, Protocol = RPC/UDP

File = /etc/passwd, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service allows device creation**

Risk:  95

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that permits device file creation.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

Some versions of NFS permit a user to create a file with the device attribute. An attacker could create a memory device that can read and write kernel memory, which can be used to gain root access.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- directory where NetRecon was able to create a device file
- service used to create the device
- protocol used to create the device

Vulnerability Solution: Patch or upgrade your version of NFS. Contact your vendor for more information about patches and upgrades.

Some mountd programs can be configured to prevent device creation. Check the documentation that came with your operating system or contact your vendor to see if this is possible and get configuration instructions.

Additional Information: Additional information about securing NFS can be found in the following CERT advisory:
<http://www.cert.org/advisories/CA-1994-15.html> (1)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

Directory = /home, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service allows encrypted passwords to be obtained from passwd file**

Risk:  49

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a passwd file containing encrypted passwords.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

The passwd file may contain encrypted passwords, which are susceptible to password cracking. NetRecon will attempt to crack any encrypted passwords it discovers using a password dictionary.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file obtained, including its path
- encrypted password obtained
- login name obtained
- service used to obtain the file
- protocol used to obtain the file

Vulnerability Solution: Remove the passwd file from the export list.

Additional Information: Additional information about securing NFS can be found in the following CERT advisory:
<http://www.cert.org/advisories/CA-1994-15.html> (1)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

File = /home/passwd.OLD, Service = nfs, Protocol = RPC/UDP

File = /home/passwd-, Service = nfs, Protocol = RPC/UDP

File = /home/shadow-bill, Service = nfs, Protocol = RPC/UDP

File = /home/ftp/etc/passwd, Service = nfs, Protocol = RPC/UDP

File = /home/passwd, Service = nfs, Protocol = RPC/UDP

File = /home/shadow-, Service = nfs, Protocol = RPC/UDP

File = /home/shadow, Service = nfs, Protocol = RPC/UDP

File = /etc/passwd, Service = nfs, Protocol = RPC/UDP

File = /etc/passwd.OLD, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service allows login names to be obtained from .netrc files**

Vulnerability Name: **nfs service allows login names to be obtained from .netrc files** (cont.)

Risk:  37

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a .netrc file containing one or more login names.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

.netrc files are used to automate network processes, typically logging into FTP servers, performing operations, logging off, etc.

Since .netrc files are used to access remote servers, they usually contain server addresses, account names, and passwords, all of which an attacker can use to attack the particular server referenced in the .netrc file as well as other network resources (since users typically use the same account and password in many situations).

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file obtained, including its path
- login name obtained
- service used to obtain the file
- protocol used to obtain the file

Vulnerability Solution: Remove the .netrc file from the export list. As a general rule, .netrc files should not be used in a secure environment.

Additional Information: Additional information about securing NFS can be found in the following CERT advisory:
<http://www.cert.org/advisories/CA-1994-15.html> (1)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

File = /home/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/peterk/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/walter/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/peterk/.vnc/.netrc, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service allows login names to be obtained from passwd file**

Risk:  37

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a passwd file containing login names.

Vulnerability Name: **nfs service allows login names to be obtained from passwd file** (cont.)

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

The passwd file often contains valuable information that can be used to gain access to network resources. Even if passwords or encrypted passwords cannot be obtained, login names are valuable for attackers attempting to gain unauthorized access, since the password can sometimes be guessed.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file obtained, including its path
- login name obtained
- service used to obtain the file
- protocol used to obtain the file

Vulnerability Solution: Remove the passwd file from the export list.

Additional Information: Additional information about securing NFS can be found in the following CERT advisory:
<http://www.cert.org/advisories/CA-1994-15.html> (1)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

File = /home/shadow-bill, Service = nfs, Protocol = RPC/UDP

File = /home/passwd.OLD, Service = nfs, Protocol = RPC/UDP

File = /home/passwd-, Service = nfs, Protocol = RPC/UDP

File = /home/ftp/etc/passwd, Service = nfs, Protocol = RPC/UDP

File = /home/passwd, Service = nfs, Protocol = RPC/UDP

File = /home/shadow-, Service = nfs, Protocol = RPC/UDP

File = /home/shadow, Service = nfs, Protocol = RPC/UDP

File = /etc/passwd.OLD, Service = nfs, Protocol = RPC/UDP

File = /etc/passwd, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service allows network resource names to be obtained from .netrc files**

Risk: ■ 31

Vulnerability Description: NetRecon has discovered a network resource with an NFS server

Vulnerability Name: **nfs service allows network resource names to be obtained from .netrc files** (cont.)

that exports a .netrc file containing one or more network resource names.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

.netrc files are used to automate network processes, typically logging into FTP servers, performing operations, logging off, etc.

Since .netrc files are used to access remote servers, they usually contain server addresses, account names, and passwords, all of which an attacker can use to attack the particular server referenced in the .netrc file as well as other network resources (since users typically use the same account and password in many situations).

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file obtained, including its path
- service used to obtain the file
- protocol used to obtain the file

Vulnerability Solution: Remove the .netrc file from the export list. As a general rule, .netrc files should not be used in a secure environment.

Additional Information: Additional information about securing NFS can be found in the following CERT advisory:
<http://www.cert.org/advisories/CA-1994-15.html> (1)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

File = /home/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/peterk/.vnc/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/peterk/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/walter/.netrc, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service allows passwords to be obtained from .netrc files**

Risk:  89

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a .netrc file containing one or more passwords.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call

Vulnerability Name: **nfs service allows passwords to be obtained from .netrc files** (cont.)

(RPC) standard.

.netrc files are used to automate network processes, typically logging into FTP servers, performing operations, logging off, etc.

Since .netrc files are used to access remote servers, they usually contain server addresses, account names, and passwords, all of which an attacker can use to attack the particular server referenced in the .netrc file as well as other network resources (since users typically use the same account and password in many situations).

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file obtained, including its path
- login name obtained
- password obtained
- account obtained
- service used to obtain the file
- protocol used to obtain the file

Vulnerability Solution: Remove the .netrc file from the export list. As a general rule, .netrc files should not be used in a secure environment.

Additional Information: Additional information about securing NFS can be found in the following CERT advisory:
<http://www.cert.org/advisories/CA-1994-15.html> (1)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

File = /home/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/peterk/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/peterk/.vnc/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/walter/.netrc, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service allows trust relationship information to be obtained**

Risk:  36

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a hosts.equiv or .rhosts file.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

Vulnerability Name: **nfs service allows trust relationship information to be obtained** (cont.)

.rhosts and hosts.equiv files are user defined lists of remote computers that can use local services (such as rlogin, rsh, rcmd, etc.) without having to supply a password.

An attacker could use this information to masquerade as a trusted host or to attack a trusted host with weaker security.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- hosts file obtained, including its path
- service used to obtain the file
- protocol used to obtain the file

Vulnerability Solution: Remove the .rhosts and hosts.equiv file from the export list.

Additional Information: Additional information about securing NFS can be found in the following CERT advisory:
<http://www.cert.org/advisories/CA-1994-15.html> (1)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

File = /home/root/.rhosts, Service = nfs, Protocol = RPC/UDP

File = /etc/hosts.equiv, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service enabled**

Risk:  65

Vulnerability Description: NetRecon has discovered a network resource serving file systems using NFS.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

NFS is vulnerable to a wide range of problems, ranging from common misconfigurations (such as incorrect permissions) to serious bugs that can give an attacker full access to any file systems served by NFS. NFS also does host-based authentication, which can be spoofed fairly easily.

Vulnerability Solution: Disable NFS if it is not necessary.

If NFS is necessary, you should take steps to secure it (see the CERT advisory referenced under Additional Information).

Additional Information: For more information about securing NFS, see:
<http://www.cert.org/advisories/CA-1994-15.html> (1)

Vulnerability Name: **nfs service enabled**

(cont.)

See Common Vulnerabilities and Exposures CVE-1999-0631 (2)

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0631>**Details:**

Service = nfs, Port = 2049, Protocol = TCP

Service = nfs, Port = 2049, Protocol = UDP

Vulnerability Name: **nfs service exports writable .netrc file**Risk:  89

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a writable .netrc file.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

.netrc files are used to automate network processes, typically logging into FTP servers, performing operations, logging off, etc.

Being able to write to a .netrc file permits an attacker to insert commands into the file that a user might unwittingly execute, essentially giving the attacker the same privileges as that user.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file obtained, including its path
- service used to obtain the file
- protocol used to obtain the file

Vulnerability Solution: Remove the .netrc file from the export list. As a general rule, .netrc files should not be used in a secure environment.

Additional Information: For more information about securing NFS, see: <http://www.cert.org/advisories/CA-1994-15.html> (1).Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>**Details:**

File = /home/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/peterk/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/walter/.netrc, Service = nfs, Protocol = RPC/UDP

File = /home/peterk/.vnc/.netrc, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service exports writable directory**

Risk:  90

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a writable directory.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

Depending on the directory being exported, this problem could allow an attacker to launch other attacks. At a minimum, it allows an attacker to modify or destroy data.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- directory found to be writable
- service used to obtain access
- protocol used to obtain access

Vulnerability Solution: Make sure this directory needs to be exported as a writable directory. Wherever possible, mount file systems to be exported read only and export file systems read only.

Additional Information: For more information about securing NFS, see: <http://www.cert.org/advisories/CA-1994-15.html> (1).

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

- Service = nfs, Protocol = RPC/UDP, Directory = /home/ftp
- Service = nfs, Protocol = RPC/UDP, Directory = /home
- Service = nfs, Protocol = RPC/UDP, Directory = /home/davidp
- Service = nfs, Protocol = RPC/UDP, Directory = /home/walter
- Service = nfs, Protocol = RPC/UDP, Directory = /home/frankn
- Service = nfs, Protocol = RPC/UDP, Directory = /home/freddy
- Service = nfs, Protocol = RPC/UDP, Directory = /etc/dhpcp
- Service = nfs, Protocol = RPC/UDP, Directory = /etc/ssh2
- Service = nfs, Protocol = RPC/UDP, Directory = /home/peterk
- Service = nfs, Protocol = RPC/UDP, Directory = /home/root
- Service = nfs, Protocol = RPC/UDP, Directory = /home/wendyr
- Service = nfs, Protocol = RPC/UDP, Directory = /home/glennw
- Service = nfs, Protocol = RPC/UDP, Directory = /home/root2
- Service = nfs, Protocol = RPC/UDP, Directory = /home/billsm

Vulnerability Name: **nfs service exports writable directory**

(cont.)

Service = nfs, Protocol = RPC/UDP, Directory = /etc/rc.d

Service = nfs, Protocol = RPC/UDP, Directory = /etc/slip

Service = nfs, Protocol = RPC/UDP, Directory = /etc/msgs

Service = nfs, Protocol = RPC/UDP, Directory = /etc/vga

Service = nfs, Protocol = RPC/UDP, Directory = /etc/skel

Vulnerability Name: **nfs service exports writable login script**Risk:  91

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a writable .cshrc, .profile, or .login file.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

.cshrc, profile, and .login files are scripts that are executed when a user logs in to a system.

Exporting a writable login file makes it possible for an attacker to insert commands to be executed the next time the user logs in, essentially giving the attacker the same privileges as that user.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file found to be writable, including its path
- service used to obtain the file
- protocol used to obtain the file

Vulnerability Solution: Remove the .cshrc, .profile, or .login file from the export list.

Additional Information: For more information about securing NFS, see:
<http://www.cert.org/advisories/CA-1994-15.html> (1).

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

File = /home/peterk/.cshrc, Service = nfs, Protocol = RPC/UDP

File = /home/peterk/.login, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **nfs service exports writable trusted host configuration file**

Vulnerability Name: **nfs service exports writable trusted host configuration file** (cont.)

Risk:  89

Vulnerability Description: NetRecon has discovered a network resource with an NFS server that exports a writable hosts.equiv or .rhosts file.

The Network File System (NFS) is a client/server application used to serve file systems remotely, using the Remote Procedure Call (RPC) standard.

The hosts.equiv file is a system-wide list and .rhosts files are user-defined lists of remote computers that can use local services (such as rlogin, rsh, rcmd, etc.) without having to supply a password.

When trusted hosts files are exported as writable, attackers can add themselves to the list of trusted hosts, giving them access to any of the remote services.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file found to be writable, including its path
- service used to obtain the file
- protocol used to obtain the file

Vulnerability Solution: Remove the hosts.equiv or .rhosts file from the export list.

Additional Information: For more information about securing NFS, see: <http://www.cert.org/advisories/CA-1994-15.html> (1).

Links: 1. <http://www.cert.org/advisories/CA-1994-15.html>

Details:

File = /home/root/.rhosts, Service = nfs, Protocol = RPC/UDP

File = /etc/hosts.equiv, Service = nfs, Protocol = RPC/UDP

Vulnerability Name: **NIS client can be identified via passwd file**

Risk:  20

Vulnerability Description: NetRecon has identified an NIS client by examining the contents of a passwd file.

The NIS service allows transfer of information between hosts that share administrative control. On some systems, the NIS service is referred to as the YP (yellow pages) service. NIS servers typically contain databases (called maps) of passwords, host names and addresses, and mail aliases.

Vulnerability Name: NIS client can be identified via passwd file (cont.)

NetRecon has discovered a passwd file, examined its contents, and determined that it contains one or more items beginning with a "+", which indicates the presence of an NIS server somewhere on the network. Knowing that an NIS server exists helps an attacker narrow the focus of the attack, since NIS is such a valuable target.

When this vulnerability is included in a NetRecon scan report, the name of the network resource where the passwd file was found is in the Details section.

Vulnerability Solution: Use NetRecon path analysis to determine how NetRecon gained access to the passwd file. There are a number of possible ways, including finding a passwd file that has been exported via NFS, and gaining administrative access (through some other vulnerability), which permits access to the passwd file. Fix the vulnerabilities that allowed NetRecon to gain access to the passwd file.

Additional Information:

Links:

Details:

Service = nfs, Protocol = RPC/UDP, File = /home/passwd

Service = nfs, Protocol = RPC/UDP, File = /home/passwd-

Service = nfs, Protocol = RPC/UDP, File = /etc/passwd

Vulnerability Name: open RPC service may allow unauthorized activityRisk: ■ 18

Vulnerability Description: NetRecon has discovered an RPC service.

Remote Procedure Calls (RPC) is a client-server standard for network application communication, allowing applications to communicate and execute functions remotely without having to know anything about the underlying network operating systems.

Since the purpose of RPC services is to permit remote execution of programs and functions, a successful attack on an RPC service gives an attacker this ability or denies legitimate users this ability.

An example of a common RPC service is NFS, which is known to be vulnerable to a wide range of attacks, which could result in unauthorized access to files.

Vulnerability Solution: If the service found is not necessary, disable it. If it is necessary, consider using a TCP/UDP wrapper to limit which hosts can use the service. Firewall the portmap service (usually port 111) so that attackers cannot enumerate RPC services from outside the firewall.

Vulnerability Name: **open RPC service may allow unauthorized activity** (cont.)

Additional Information:

Links:

Details:

Port = 979, Protocol = UDP, Service = mountd, Revision = 2

Port = 979, Protocol = UDP, Service = mountd, Revision = 1

Port = 2049, Protocol = TCP, Service = nfs, Revision = 2

Port = 2049, Protocol = UDP, Service = nfs, Revision = 2

Port = 111, Protocol = UDP, Service = rpcbind, Revision = 2

Port = 111, Protocol = TCP, Service = rpcbind, Revision = 2

Port = 982, Protocol = TCP, Service = mountd, Revision = 1

Port = 982, Protocol = TCP, Service = mountd, Revision = 2

Vulnerability Name: **open TCP port may allow unauthorized activity**

Risk: ■ 14

Vulnerability Description: NetRecon has discovered an open TCP port.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:
-port number

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, protect it with a firewall. If the service is required for external use, consider running it from a demilitarized zone and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see:
<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = TCP, Port = 513, Service = login

Protocol = TCP, Port = 111, Service = portmap

Protocol = TCP, Port = 80

Protocol = TCP, Port = 514, Service = shell

Protocol = TCP, Port = 21, Service = ftp

Protocol = TCP, Port = 22

Vulnerability Name: **open TCP port may allow unauthorized activity** (cont.)

Protocol = TCP, Port = 23, Service = telnet

Protocol = TCP, Port = 79, Service = finger

Protocol = TCP, Port = 25, Service = smtp

Protocol = TCP, Port = 80

Protocol = TCP, Port = 111, Service = portmap

Protocol = TCP, Port = 513, Service = login

Protocol = TCP, Port = 514, Service = shell

Protocol = TCP, Port = 2049

Protocol = TCP, Port = 22

Protocol = TCP, Port = 21, Service = ftp

Protocol = TCP, Port = 79, Service = finger

Protocol = TCP, Port = 25, Service = smtp

Protocol = TCP, Port = 23, Service = telnet

Vulnerability Name: **open UDP port may allow unauthorized activity**

Risk: ■ 17

Vulnerability Description: NetRecon has discovered an open UDP port.

Since the UDP protocol doesn't use a three-way handshake to establish connections the way TCP does, it is more susceptible to attacks involving spoofed IP addresses. There are a wide range of denial of service attacks that exploit this weakness in UDP to create infinite loops.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:
-port number

Note: There is a chance of UDP ports being incorrectly detected as open.

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, firewall it. If the service is required for external use, consider running it from a demilitarized zone, and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see:

Vulnerability Name: **open UDP port may allow unauthorized activity** (cont.)

<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = UDP, Port = 111

Protocol = UDP, Port = 512

Vulnerability Name: **portmap service allows RPC services to be enumerated**

Risk: ■ 29

Vulnerability Description: NetRecon has discovered a network resource running the portmap service, and has used portmap to enumerate RPC services.

Remote Procedure Calls (RPC) is a client-server standard for network application communication, allowing applications to communicate and execute functions remotely without having to know anything about the underlying network operating systems.

The portmap service can be used to find out which RPC services are running and which ports they're running on, so that an RPC communications session can be started.

Many RPC services are vulnerable to attacks. Knowing which services are running and what ports they're running on helps attackers focus their efforts.

An example of a common RPC service is NFS, which is known to be vulnerable to a wide range of attacks, which could result in unauthorized access to files.

Vulnerability Solution: If it's not absolutely necessary, don't use RPC. If it is necessary, be sure to firewall the portmap port (usually 111). Consider using a TCP/UDP wrapper to limit which hosts can access portmap.

Additional Information:

Links:

Details:

Protocol = TCP, Port = 111, Service = portmap

Vulnerability Name: **responds to ICMP echo request (ping)**

Risk: ■ 15

Vulnerability Name: **responds to ICMP echo request (ping)** (cont.)

Vulnerability Description: NetRecon has discovered that this system responds to an ICMP echo request (commonly referred to as ping). ICMP is part of the IP layer. It is used to handle IP status and control messages.

The following are known threats to the legitimate use of this service:

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.) However, disabling ICMP on the firewall is only a partial solution. The complete solution should include patching or upgrading the OS kernel so that it can handle oversized ping requests (if possible with your OS). Many operating system vendors have created patches that prevent the Ping o' Death vulnerability. Consult your OS vendor to see if your system can handle oversized packets.

Additional Information: For additional information about ICMP's ping vulnerability, read CERT(R) Advisory CA-96.26 at the following URL:
<http://www.cert.org/advisories/CA-1996-26.html> (1)
See Common Vulnerabilities and Exposures CVE-1999-0128 (2)

Links: 1. <http://www.cert.org/advisories/CA-1996-26.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0128>

Details:Vulnerability Name: **responds to UDP requests with ICMP**

Risk: ■ 20

Vulnerability Description: NetRecon has discovered that this system responds to UDP packets directed to unavailable service ports with an ICMP error

Vulnerability Name: **responds to UDP requests with ICMP** (cont.)

message. This mechanism allows clients to determine if a service is available on a remote system. If the service is available, then it will handle the service request; however, if no service is associated with the specified port, then an ICMP error message is returned indicating that no service was associated with that port.

The following are known threats to the legitimate use of the ICMP protocol:

- An attacker may send UDP requests to a server in an attempt to map ports on that server.
- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:

Vulnerability Name: **service identified**

Risk:  39

Vulnerability Description: NetRecon has identified a service by software product, version, or both.

Knowing the product and/or version allows attackers to focus their attacks.

Berkeley sendmail, for example, is known to be vulnerable to

Vulnerability Name: **service identified**

(cont.)

certain exploits in some versions, but not in others. If attackers can identify that you are running a vulnerable version of Berkeley sendmail they can direct known exploits towards those resources. Even for services with no known exploits, it is possible that vulnerabilities will be discovered in the future.

If attackers can obtain version information for a service, they can eliminate attacks known to fail with that version, or try attacks known to work with that version. Eliminating techniques to try is helpful in speeding up the attack, and can also help to avoid alerting administrators, since it is usually possible to monitor attempted exploits of fixed vulnerabilities.

Vulnerability Solution: Consider the benefits of product identification and weigh them against the security risk. Remove unique banners from services wherever practical. If the identifying information cannot be suppressed, consider using a different product.

For the extremely security conscious, it can be worthwhile to provide intentionally misleading identification of the service product and version. This misdirects attackers to attempt to exploit vulnerabilities that are not present. The administrator can monitor such attacks and take appropriate action to stop attackers before they are successful. However, incorrect banners will also deceive NetRecon.

Additional Information:**Links:****Details:**

Service = smtp/Berkeley Sendmail, Revision = 8.9.3, Protocol = TCP, Port = 25

Service = smtp/Berkeley Sendmail, Protocol = TCP, Port = 25

Service = ftp/wu, Protocol = TCP, Port = 21

Service = http/Apache, Protocol = TCP, Port = 80

Service = http/Apache, Revision = 1.3.6 (Unix), Protocol = TCP, Port = 80

Service = ssh/UNIX, Revision = 2.0-2.0.13, Protocol = TCP, Port = 22

Service = ssh/UNIX, Protocol = TCP, Port = 22

Service = ftp/wu, Revision = 2.4.2-VR16(1), Protocol = TCP, Port = 21

Service = mountd, Revision = 2, Protocol = UDP, Port = 979

Service = mountd, Revision = 1, Protocol = UDP, Port = 979

Service = mountd, Revision = 2, Protocol = TCP, Port = 982

Service = nfs, Revision = 2, Protocol = TCP, Port = 2049

Service = nfs, Revision = 2, Protocol = UDP, Port = 2049

Vulnerability Name: **service identified**

(cont.)

Service = mountd, Revision = 1, Protocol = TCP, Port = 982

Service = rpcbind, Revision = 2, Protocol = TCP, Port = 111

Service = rpcbind, Revision = 2, Protocol = UDP, Port = 111

Vulnerability Name: **shell service enabled**Risk:  42

Vulnerability Description: The shell service provides remote execution facilities with authentication based on privileged port numbers and trusted hosts.

It is possible to configure this service to allow anyone with a valid user name to execute commands without authentication.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information:

Links: 1.

http://www.cs.purdue.edu/coast/satan-html/tutorials/vulnerability/remote_shell_access.html

Details:

Protocol = TCP, Port = 514, Service = shell

Vulnerability Name: **smtp service enabled**Risk:  45

Vulnerability Description: The smtp service uses the Simple Mail Transfer Protocol (SMTP) to send electronic messages. The smtp service may be used to obtain information about valid user names and other systems in the network.

The smtp service is vulnerable to a variety of attacks and may also constitute a violation of acceptable use policies.

Vulnerability Solution: Disable this service if it isn't necessary.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0617 (1)


Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0617>

Vulnerability Name: **smtp service enabled**

(cont.)

Details:

Protocol = TCP, Port = 25, Service = smtp

Vulnerability Name: **SMTP supports EHLO greeting**Risk:  9

Vulnerability Description: NetRecon has discovered an SMTP implementation that responds to the EHLO greeting protocol.

The EHLO greeting protocol is an indication of the ESMTP (Extended Simple Mail Transfer Protocol) protocol. ESMTP has additional vulnerabilities, so knowing that a network resource supports it permits an attacker to focus their efforts.

Vulnerability Solution: Configure your mail transport agent (MTA) to permit the minimum amount of information transfer necessary for completing mail transport tasks.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0531 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0531>

Details:

Service = smtp, Protocol = TCP, Port = 25

Vulnerability Name: **telnet service enabled**Risk:  42

Vulnerability Description: NetRecon has discovered a network resource running the telnet service.

The telnet service provides remote execution facilities with authentication based on user names and passwords.

Since the service relies on user names and passwords for authentication, it is vulnerable to user name and password guessing.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Symantec's Intruder Alert can be used to monitor attempted connections to this service.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0619 (1)

Network Resource: purple.netrecon.com

(cont.)

Vulnerability Name: **telnet service enabled**

(cont.)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0619>

Details:

Protocol = TCP, Port = 23, Service = telnet

Vulnerability Name: **user shell access obtained via login service**

Risk:  91

Vulnerability Description: NetRecon has connected to a network resource through the login service with user privileges.

NetRecon uses any login names and passwords obtained through other vulnerabilities to attempt to log in to any network resources running the login service. Being able to log in to a network resource with user privileges permits a wide range of activities, depending on the privileges of the user.

Vulnerability Solution: Fix the vulnerabilities that led to NetRecon being able to discover the password that provided access (right-click the vulnerability record in the Data Table pane and choose Path Analysis to see what information led NetRecon to find this vulnerability).

To increase the difficulty of cracking or guessing passwords, enforce the use of secure passwords. Passwords should be a combination of letters, numbers, and punctuation. They should not correspond to words in any language, names of people, places, fictional characters, initials, dates, etc. They should not be common or simple sequences of letters, numbers, or characters such as abcde or 12345. Additionally, passwords should be changed regularly and should never be reused.

Additional Information:

Links:

Details:

Login Name = glennw, Password = f*e

Login Name = norman, Password = b*r

Login Name = walter, Password = w*r

Network Resource: red.netrecon.com

Network Resource: **red.netrecon.com** (cont.)

Resource Type: NetWare, NetWare 3.12, IP host, Windows Networking resource

Aliases: red, 10.1.8.1, 00:a0:29:42:b1:2d

of Unique Vulnerabilities: 18

Highest Risk Level Found:  95

Vulnerability Name: **chargen service enabled**

Risk:  60

Vulnerability Description: NetRecon has discovered a network resource running the chargen service.

The chargen service causes a TCP server to send a constant stream of characters to the client until the client terminates the connection. chargen can be used legitimately for certain testing purposes.

Because chargen produces a continual stream of characters, it is susceptible to misuse for denial of service attacks. For example, spoofed packets can link the chargen port to the echo port, creating an infinite loop. This type of attack consumes increasing amounts of network bandwidth, degrading network performance or, in some cases, completely disabling portions of a network.

Vulnerability Solution: To avoid this type of attack, disable the chargen service. Additionally, monitoring attempts to access disabled services can alert you to the presence of attackers.

Microsoft has released a hotfix to address chargen attacks directed at Windows NT 4.0 Simple TCP/IP services. The hotfix can be downloaded from:

[ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix \(1\)](ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix (1))

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0103 (2)
See Common Vulnerabilities and Exposures CAN-1999-0639 (3)

Links: 1. <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/simptcp-fix>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0103>
3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0639>

Details:

Protocol = TCP, Port = 19, Service = chargen

Vulnerability Name: **connected to resource via Windows Networking**

Risk:  90

Vulnerability Name: **connected to resource via Windows Networking** (cont.)

Vulnerability Description: NetRecon has successfully logged on to a network resource with user privileges.

NetRecon uses all known login name and password combinations to connect with each network resource it has discovered.

Many people mistakenly believe that only certain critical network resources need to have a high level of security. Attackers often try to gain access to weak links in a network, and then exploit trust relationships between network resources to access more secure resources.

Vulnerability Solution: To increase the difficulty of cracking or guessing passwords, enforce the use of secure passwords. Passwords should be a combination of letters, numbers, and punctuation. They should not correspond to words in any language, names of people, places, fictional characters, initials, dates, or similar things. They should not be common or simple sequences of letters, numbers, or characters such as abcde or 12345. Additionally, passwords should be changed regularly and should never be reused.

Additional Information:

Links:

Details:

Share = \\RED\VOL1, Login Name = administrator, Password =

Share = \\RED\VOL1, Login Name = administrator, Password = a*n

Share = \\red\SYS, Login Name = administrator, Password = a*n

Share = \\red\SYS, Login Name = administrator, Password =

Share = \\RED\SYS, Login Name = administrator, Password = a*n

Share = \\RED\SYS, Login Name = administrator, Password =

Vulnerability Name: **discard service enabled**

Risk: ■ 15

Vulnerability Description: NetRecon has discovered a network resource running the discard service.

The discard service reads packets sent to it and then discards them.

Attackers could use a connect response from this, or any service to verify the presence of a network resource.

Vulnerability Solution: Disable the service if you do not need it. If you need it, but not

Vulnerability Name: **discard service enabled** (cont.)

externally, protect this service with a firewall. Monitoring attempts to access disabled services can alert you to the presence of attackers.

Additional Information: See Common Vulnerabilities and Exposures CAN-1999-0636 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0636>

Details:

Protocol = TCP, Port = 9, Service = discard

Vulnerability Name: **echo service enabled**

Risk:  60

Vulnerability Description: NetRecon has discovered a network resource running the echo service.

The echo service causes a server to return whatever a client sends. It can be used for a number of testing purposes, much like chargen.

Since the echo port returns whatever is sent to it, it is susceptible to attacks that create false return addresses. For example, spoofed packets can link the echo port to the chargen port, creating an infinite loop. This type of attack consumes increasing amounts of network bandwidth, degrading network performance or, in some cases, completely disabling portions of a network.

Vulnerability Solution: To avoid this type of attack, disable the echo service. Additionally, monitoring attempted access to the echo service can alert you to the presence potential attackers.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0635 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0635>

Details:

Protocol = TCP, Port = 7, Service = echo

Vulnerability Name: **file shares may be enumerated remotely**

Risk:  42

Vulnerability Description: NetRecon has discovered a Windows network resource that permits file shares to be enumerated from a remote system.

Windows networking (netbios) permits file sharing and information about file sharing to be sent to remote computers. An attacker could use this information to gain access to shared files.

Vulnerability Name: **file shares may be enumerated remotely**

(cont.)

This exposure also applies to UNIX servers running Samba, a freeware program that allows UNIX systems to share files on a Windows network.

When this exposure is included in a NetRecon scan report, the following pieces of information are in the Details section:

- file or folder shared
- type of share

Vulnerability Solution: Don't share files unless absolutely necessary.

Windows NT

If the network resource that allows shares to be enumerated is running Windows NT, consider disabling the server service.

Note: Disabling this service prevents this system from being able to share its own resources via Windows networking (though it doesn't prevent the system from accessing resources shared by other computers).

To disable the Server service:

1. Choose Start, Settings, Control Panel.
2. Double-click Services.
3. Select Server in the Service list.
4. Click Startup.
5. Click Disabled, then click OK.
6. Click Close. This change takes effect the next time you start Windows.

Windows 9x

If the network resource that allows shares to be enumerated is running Windows 9x, consider disabling file sharing.

1. Right-click Network Neighborhood, and then click Properties.
2. Click File and Print Sharing.
3. Deselect I want to be able to give others access to my files, and then click OK.
4. Click OK to close the Network dialog box.

Samba

To disable the Samba Server on most UNIX systems:

Vulnerability Name: **file shares may be enumerated remotely** (cont.)

1. Execute a shell command to stop the Samba service by typing:
sh smbdc stop
2. Find the name of the RPM that installed Samba by typing: rpm
-qf smbdc
3. Enter the name returned by the above command into the following command: rpm -e [SambaRPMName.rpm]
This will extract or uninstall the Samba service.

Additional Information: See Common Vulnerabilities and Exposures CVE-1999-0621 (1)

Links: 1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0621>

Details:

Share = \\RED\VOL1, Type = Windows Networking resource

Share = \\RED\SYS, Type = Windows Networking resource

Vulnerability Name: **IP address found from name**

Risk: ■ 5

Vulnerability Description: NetRecon has successfully discovered the IP address of a network resource using its name.

If NetRecon discovers the names of any network resources (via Windows networking, for example), it attempts to obtain their IP address as well.

Finding the IP address of a network resource verifies that the resource exists. It also helps attackers identify TCP/IP networks to scan for further resources. Having an IP address also opens up the possibility of a wide range of TCP/IP information gathering (port scans, for example) and attacks.

Vulnerability Solution: Do not allow hosts outside your firewall to resolve internal IP addresses unless absolutely necessary. Public DNS should contain only public systems.

Additional Information:

Links:

Details:

Alias = 10.1.8.1

Vulnerability Name: IP name obtained

Risk:  10

Vulnerability Description: NetRecon has discovered the IP name of a network resource.

System names often reveal something about the system. For example, servers sometimes have the word server in the name, systems are named after their users, etc. Systems with an IP address but no name are usually either old, unused systems (which can be attacked with less risk of notice) or protected systems (containing highly significant information).

Knowing system names can, therefore, help attackers focus their attacks on key systems.

Vulnerability Solution: Do not allow hosts outside your firewall to resolve internal IP names or addresses unless absolutely necessary. Public DNS should contain only public systems.

Additional Information:

Links:

Details:

Alias = red.netrecon.com

Alias = red

Vulnerability Name: NetWare console not secured

Risk:  42

Vulnerability Description: A NetWare Console should always be secured. This means you need physical access to the Console to use it.

Note: NetRecon detects this vulnerability based on version information, which means that NetRecon reports it even if you have applied the solution, as long as the version number remains the same.

Vulnerability Solution: Secure the console by adding SECURE CONSOLE to autoexec.ncf.

Additional Information:

Links:

Details:

Vulnerability Name: **NetWare server with DOS not removed from memory**

Risk:  43

Vulnerability Description: DOS should be removed from memory so that a user cannot exit out of the NetWare server and have DOS access to the file server, which has no security implemented to protect the files.

Note: NetRecon detects this vulnerability based on version information, which means that NetRecon reports it even if you have applied the solution, as long as the version number remains the same.

Vulnerability Solution: Remove DOS by adding REMOVE DOS to autoexec.ncf.

Additional Information:

Links:

Details:

Vulnerability Name: **NetWare startup file read access obtained**

Risk:  44

Vulnerability Description: NetWare startup files (.NCF files) contain information about what utilities/services are loaded and information about security settings, such as packet signature levels. Read access to this information permits an attacker to focus on the parts of the system that may be weaker.

Vulnerability Solution: Change access to indicated .NCF files to allow only authorized personnel (according to the company's security policy) to have access.

Additional Information:

Links:

Details:

Miscellaneous = read access obtained to file \\red\SYS\SYSTEM\STARTUP.NCF

Miscellaneous = read access obtained to file \\red\SYS\SYSTEM\AUTOEXEC.NCF

Miscellaneous = read access obtained to file \\red\SYS\SYSTEM\BSTOP.NCF

Miscellaneous = read access obtained to file \\red\SYS\SYSTEM\BSTART.NCF

Vulnerability Name: **NetWare startup file write access obtained**

Risk:  95

Vulnerability Name: **NetWare startup file write access obtained** (cont.)

Vulnerability Description: NetWare startup files (.NCF files) contain information about what utilities/services are loaded and information about security settings, such as packet signature levels. Write access to this information permits an attacker to change security settings, disable system auditing, load executables (such as backdoors) that can be used later to compromise the system again, and so forth.

Vulnerability Solution: Change access to indicated .NCF files to allow only authorized personnel (according to the company's security policy) to have access.

Additional Information:

Links:

Details:

Miscellaneous = write access obtained to file \\red\SYS\SYSTEM\STARTUP.NCF

Miscellaneous = write access obtained to file
\\red\SYS\SYSTEM\AUTOEXEC.NCF

Vulnerability Name: **NetWare SYS:SYSTEM directory write access obtained**

Risk:  94

Vulnerability Description: The NetWare SYS:SYSTEM directory contains many critical systems files. Having write access to this directory permits an attacker to launch a wide range of attacks by adding and replacing system files.

Vulnerability Solution: Change access to the SYS:SYSTEM directory to allow only authorized personnel (according to the company's security policy) to have access.

Additional Information:

Links:

Details:

Miscellaneous = NWWvuln

Vulnerability Name: **network resource detected via ICMP protocol**

Risk:  15

Vulnerability Description: NetRecon has discovered that this network resource responds using the ICMP protocol. ICMP, as part of the IP layer, handles error messaging and other control conditions. This message is a

Vulnerability Name: **network resource detected via ICMP protocol** (cont.)

catch-all message because NetRecon has intercepted an ICMP datagram, regardless of its type. If you receive this message, you may also receive messages for the other ICMP vulnerabilities that NetRecon discovers, such as Responds to ICMP Echo (ping) Requests.

In discovering this vulnerability, NetRecon sent a UDP service request and a number of ICMP datagrams to this system and received one or more ICMP responses.

The following are known threats to the legitimate use of the ICMP protocol:

- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details:Vulnerability Name: **network resource identified**

Risk: ■ 16

Vulnerability Description: NetRecon has obtained information that helps to identify a particular network resource. This information could include full or partial identification of the operating system, server types (SMB server, for example), whether a computer is an IP host, etc.

Vulnerability Name:	network resource identified (cont.)
	Once an attacker has identified a specific target, he or she can find and exploit weakness in that resource.
Vulnerability Solution:	Using the data table in NetRecon, determine how the information was obtained. Either eliminate the service responsible or configure it to not give any clues that can help identify the network resource.
Additional Information:	
	Links:
Details:	
	Type = IP host
	Type = NetWare
	Type = Windows Networking resource
	Type = IP host

Vulnerability Name:	open TCP port may allow unauthorized activity
Risk:	■ 14
Vulnerability Description:	NetRecon has discovered an open TCP port. When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section: -port number
Vulnerability Solution:	If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, protect it with a firewall. If the service is required for external use, consider running it from a demilitarized zone and use appropriate authentication.
Additional Information:	If you think your system may have been compromised, see: http://www.cert.org/nav/recovering.html (1)
	Links: 1. http://www.cert.org/nav/recovering.html
Details:	
	Protocol = TCP, Port = 19, Service = chargen
	Protocol = TCP, Port = 7, Service = echo
	Protocol = TCP, Port = 9, Service = discard
	Protocol = TCP, Port = 19, Service = chargen
	Protocol = TCP, Port = 9, Service = discard
	Protocol = TCP, Port = 7, Service = echo

Vulnerability Name: **open UDP port may allow unauthorized activity**

Risk: ■ 17

Vulnerability Description: NetRecon has discovered an open UDP port.

Since the UDP protocol doesn't use a three-way handshake to establish connections the way TCP does, it is more susceptible to attacks involving spoofed IP addresses. There are a wide range of denial of service attacks that exploit this weakness in UDP to create infinite loops.

When this vulnerability is included in a NetRecon scan report, the following pieces of information are in the Details section:
-port number

Note: There is a chance of UDP ports being incorrectly detected as open.

Vulnerability Solution: If the service using this port is not necessary, disable it. If you don't know what this service is, or didn't expect to see it, verify that the service is not a back door left by an attacker. If the service is required only for internal use, firewall it. If the service is required for external use, consider running it from a demilitarized zone, and use appropriate authentication.

Additional Information: If you think your system may have been compromised, see:
<http://www.cert.org/nav/recovering.html> (1)

Links: 1. <http://www.cert.org/nav/recovering.html>

Details:

Protocol = UDP, Port = 19

Protocol = UDP, Port = 9

Protocol = UDP, Port = 7

Vulnerability Name: **responds to ICMP echo request (ping)**

Risk: ■ 15

Vulnerability Description: NetRecon has discovered that this system responds to an ICMP echo request (commonly referred to as ping). ICMP is part of the IP layer. It is used to handle IP status and control messages.

The following are known threats to the legitimate use of this service:
- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to

Vulnerability Name: **responds to ICMP echo request (ping)** (cont.)

map a network and infer trust relationships.

- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)

- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)

- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.) However, disabling ICMP on the firewall is only a partial solution. The complete solution should include patching or upgrading the OS kernel so that it can handle oversized ping requests (if possible with your OS). Many operating system vendors have created patches that prevent the Ping o' Death vulnerability. Consult your OS vendor to see if your system can handle oversized packets.

Additional Information: For additional information about ICMP's ping vulnerability, read CERT(R) Advisory CA-96.26 at the following URL:
<http://www.cert.org/advisories/CA-1996-26.html> (1)
See Common Vulnerabilities and Exposures CVE-1999-0128 (2)

Links: 1. <http://www.cert.org/advisories/CA-1996-26.html>
2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0128>

Details:

Vulnerability Name: **responds to UDP requests with ICMP**

Risk: ■ 20

Vulnerability Description: NetRecon has discovered that this system responds to UDP packets directed to unavailable service ports with an ICMP error message. This mechanism allows clients to determine if a service is available on a remote system. If the service is available, then it will handle the service request; however, if no service is associated with the specified port, then an ICMP error message is returned indicating that no service was associated with that port.

The following are known threats to the legitimate use of the ICMP protocol:

Vulnerability Name: **responds to UDP requests with ICMP** (cont.)

- An attacker may send UDP requests to a server in an attempt to map ports on that server.
- An ICMP reply tells an attacker that a remote system exists and is running.
- An attacker could use the data contained in an ICMP reply to map a network and infer trust relationships.
- An attacker could use ICMP as a covert channel. (A covert channel is a means of hiding information in a communication medium, or in other words, a means of transmitting information under the noses of security folks.)
- An attacker may create malformed packets, which may cause problems for systems with bugs in the TCP stack, such as denial of service or code execution. (An example of a malformed ICMP packet attack is the Ping o' Death attack. The Ping o' Death attack sends an oversized ping packet in an attempt to overflow the system's buffer. Receiving oversized ICMP datagrams may crash, freeze, or reboot the system.)
- An attacker may also flood the system with ICMP requests or use this system and other systems to flood a target system (Packet floods may result in a partial or complete denial of service.)

Vulnerability Solution: Filter all incoming and outgoing ICMP requests on the firewall, except Source Quench. (For instructions on how to disable ICMP on your firewall, consult your firewall product's documentation.)

Additional Information:

Links:

Details: