



Vulnerability Listing by Host

This report shows a list of vulnerabilities detected for each host.

Date generated: 08/02/2006 09:15:59

Scan reference : file:SampleHostList.txt

Scan date & time : 30/01/2006 09:51:10

192.168.20.150 - ChrisDevB

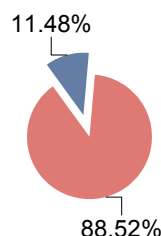
Operating System: Windows Server 2003

Service Pack: 1

Total Host Vulnerabilities: 7

Total Network Vulnerabilities: 61

Total Host / Total Network: 11.48%



| Category | Vulnerability Details |
|----------|---|
| Registry | AutoShareServer (1) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | AutoShareWKS (2) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | Cached Logon Credentials — Could lead to information exposure. Should be set to 0 |
| Registry | DCOM is enabled — DCOM is used to execute code on remote computers.Should be disabled if not used. |
| Registry | Last logged-on username visible — By default, NT/2k displays the last logged-on user |
| Registry | Windows AutoUpdate is enabled but require user intervention for both patch download and installation — Although windows AutoUpdate is enabled, the system relies on the end user to approve both patch download and installation. This could lead to a delay in patch installation or no installation at all. |
| Service | SNMP service is enabled on this host — Numerous vulnerabilities have been reported in multiple vendors' SNMP implementations. You should check if your system is vulnerable. |

192.168.20.33 - OfficeServer

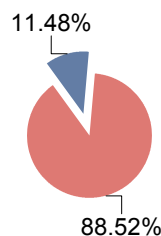
Operating System: Windows Server 2003

Service Pack: Gold

Total Host Vulnerabilities: 7

Total Network Vulnerabilities: 61

Total Host / Total Network: 11.48%



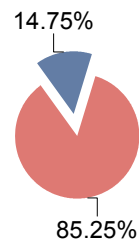
| Category | Vulnerability Details |
|----------|---|
| CGIAbuse | Netscape: Netscape PageServices — List page directory |
| Registry | AutoShareServer (1) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | AutoShareWKS (2) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |



| | |
|----------|---|
| Registry | Cached Logon Credentials — Could lead to information exposure. Should be set to 0 |
| Registry | DCOM is enabled — DCOM is used to execute code on remote computers.Should be disabled if not used. |
| Registry | Last logged-on username visible — By default, NT/2k displays the last logged-on user |
| Registry | Windows AutoUpdate is enabled but require user intervention for both patch download and installation — Although windows AutoUpdate is enabled, the system relies on the end user to approve both patch download and installation. This could lead to a delay in patch installation or no installation at all. |

192.168.20.35 - KeithTest

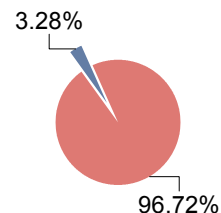
Operating System: Windows XP
Service Pack: 2
Total Host Vulnerabilities: 9
Total Network Vulnerabilities: 61
Total Host / Total Network: 14.75%



| Category | Vulnerability Details |
|----------|---|
| Backdoor | DummyTrojan.A.YY (1025) — |
| Backdoor | DummyTrojan.B.SSS (1026) — |
| Backdoor | DummyTrojan.B1Q (500) — |
| Registry | AutoShareServer (1) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | AutoShareWKS (2) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | Cached Logon Credentials — Could lead to information exposure. Should be set to 0 |
| Registry | DCOM is enabled — DCOM is used to execute code on remote computers.Should be disabled if not used. |
| Registry | Last logged-on username visible — By default, NT/2k displays the last logged-on user |
| Registry | LM Hash — It is recommended to use NTLM authentication instead of LM |

192.168.20.40 - KeithMain

Operating System: Windows XP
Service Pack: Unknown
Total Host Vulnerabilities: 2
Total Network Vulnerabilities: 61
Total Host / Total Network: 3.28%

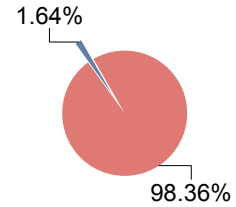


| Category | Vulnerability Details |
|----------|----------------------------|
| Backdoor | DummyTrojan.A.YY (1025) — |
| Backdoor | DummyTrojan.XB5.T (1134) — |



192.168.20.42 - InternServer

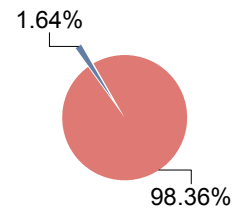
Operating System: Windows Server 2003
Service Pack: Unknown
Total Host Vulnerabilities: 1
Total Network Vulnerabilities: 61
Total Host / Total Network: 1.64%



| Category | Vulnerability Details |
|----------|---|
| CGIAbuse | Netscape: Netscape PageServices — List page directory |

192.168.22.125 - SQLServerXT

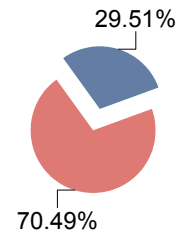
Operating System: Windows Server 2003
Service Pack: Unknown
Total Host Vulnerabilities: 1
Total Network Vulnerabilities: 61
Total Host / Total Network: 1.64%



| Category | Vulnerability Details |
|----------|---|
| CGIAbuse | Netscape: Netscape PageServices — List page directory |

192.168.22.90 - VMWin2K

Operating System: Windows 2000
Service Pack: Gold
Total Host Vulnerabilities: 18
Total Network Vulnerabilities: 61
Total Host / Total Network: 29.51%



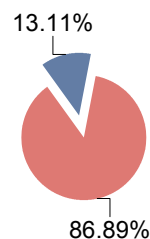
| Category | Vulnerability Details |
|----------|---|
| CGIAbuse | IIS: Escaped Characters Decoding Bug — Run arbitrary commands (IUSR_machinename level privileges) |
| CGIAbuse | IIS: Executable File Parsing Bug — Run arbitrary commands (IUSR_machinename level privileges) |
| CGIAbuse | IIS: Frontpage check (2) — Some versions of Frontpage are vulnerable to denial of service attacks |
| CGIAbuse | IIS: Frontpage check (3) — Some versions of Frontpage are vulnerable to denial of service attacks |
| CGIAbuse | IIS: IIS directory traversal — Run arbitrary commands |
| CGIAbuse | IIS: Unicode Directory Transversal Bug — Run arbitrary commands (IUSR_machinename level privileges) |
| CGIAbuse | IIS: Unicode Directory Transversal Bug (2) — Run arbitrary commands (IUSR_machinename level privileges) |
| CGIAbuse | Netscape: Netscape PageServices — List page directory |
| Registry | AutoShareServer (1) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |



| | |
|----------|--|
| Registry | AutoShareWKS (2) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | Cached Logon Credentials — Could lead to information exposure. Should be set to 0 |
| Registry | DCOM is enabled — DCOM is used to execute code on remote computers.Should be disabled if not used. |
| Registry | Guest users have access to the application log (1) — You should disable guest access by creating a DWORD key named "RestrictGuestAccess" with value of "1" (HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLog/Application) |
| Registry | Guest users have access to the security log (1) — You should disable guest access by creating a DWORD key named "RestrictGuestAccess" with value of "1" (HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLog/Security) |
| Registry | Guest users have access to the system log (1) — You should disable guest access by creating a DWORD key named "RestrictGuestAccess" with value of "1" (HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/EventLog/System) |
| Registry | LM Hash — It is recommended to use NTLM authentication instead of LM |
| Service | Alert service enabled — This service could be use in social engineering attacks.It is recommended to disable this service. |
| Service | Trivial FTP service running — Unrestricted tftp access allows remote sites to retrieve a copy of any world-readable file. You should remove this service, unless you really need it. |

192.168.25.10 - KeithServer2K3

Operating System: Windows Server 2003
Service Pack: 1
Total Host Vulnerabilities: 8
Total Network Vulnerabilities: 61
Total Host / Total Network: 13.11%

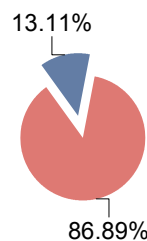


| Category | Vulnerability Details |
|----------|---|
| Backdoor | DummyTrojan.B.SSS (1026) — |
| Backdoor | DummyTrojan.B1Q (500) — |
| Registry | AutoShareServer (1) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | AutoShareWKS (2) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | Cached Logon Credentials — Could lead to information exposure. Should be set to 0 |
| Registry | DCOM is enabled — DCOM is used to execute code on remote computers.Should be disabled if not used. |
| Registry | Last logged-on username visible — By default, NT/2k displays the last logged-on user |
| Registry | Windows AutoUpdate is not enabled — Windows AutoUpdate is not enabled on the computer. This means security updates will no be installed automatically as they are issued by Microsoft. |



192.168.25.18 - ChrisTestServer

Operating System: Windows Server 2003
Service Pack: Gold
Total Host Vulnerabilities: 8
Total Network Vulnerabilities: 61
Total Host / Total Network: 13.11%



| Category | Vulnerability Details |
|----------|---|
| CGIAbuse | Netscape: Netscape PageServices — List page directory |
| Registry | AutoShareServer (1) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | AutoShareWKS (2) — The administrative shares (C\$,D\$,ADMIN\$,etc) are available on this machine. Internal networks: Generally required for administration tasks. Web Servers: Should be turned off. |
| Registry | Cached Logon Credentials — Could lead to information exposure. Should be set to 0 |
| Registry | DCOM is enabled — DCOM is used to execute code on remote computers. Should be disabled if not used. |
| Registry | Last logged-on username visible — By default, NT/2k displays the last logged-on user |
| Registry | Windows AutoUpdate is enabled but require user intervention for both patch download and installation — Although windows AutoUpdate is enabled, the system relies on the end user to approve both patch download and installation. This could lead to a delay in patch installation or no installation at all. |
| Service | POP3 server might be vulnerable to a remote buffer overflow exploit — Contains a buffer overflow that could result in the overwriting of process memory, including the return address within the stack, and code execution. |