Auditing a print and scan server protected by the VisNetic for Workstation firewall

An Independent Auditor's perspective

GSNA Practical Version 2.1, Option 1

Author: Carmen AUBRY
Date: 12 February 2004

1 Abstract

Print servers, generally designed to be hosted on a private network, weren't usually viewed as a threat by network administrators. The general perception was that nothing can be done on a print server, except stealing confidential data. These systems were viewed as peripheral devices.

But the world is changing and the number of viruses that infected corporate networks changed the network administrator's perceptions. The administrators start requiring devices with a good level of security. Furthermore, solving security problems are now perceived as costly by maintenance services.

This paper documents the audit of a print server protected by a host-based firewall. The audit was performed from an independent auditor's perspective. This audit was requested by a company trying to improve the security level of its products. The company requested a penetration analysis in order to assess the security of the system.

Table of Contents

2 Terms

ACL

Short for access control list, information owned by the operating system describing the rights owned by each user or group to access to a specific system object, such as a directory or a file.

Binaries

Binaries can be any file containing machine language instructions or binary data used at software execution time.

Malware

Short for malicious software. Software designed specifically to damage a controller or steal
information, such as a virus or a Trojan horse.

Network service

A network service is a software module that offers some kind of remote connectivity. It covers either basic protocol support (LPD, FTP,…), or remote communication mechanisms used by remote applications (RPC, socket,…).

OS

Short for Operating System.

Patch

Piece of software to correct bugs.
This term must be understood as hotfix, patch, service pack or upgrade that is provided by the
original software supplier.

Security patch

A security patch is a patch classified by the OS/component vendor as relative to a correction of a security issue. OS/component vendor usually calls this kind of patch a security patch.

Sensitive file

A file that has high impact on the system in case of corruption. In this document, sensitive files include all OS binaries.

Consolidation tests

Consolidation tests are tests to validate product compliance with its specification before release to manufacturing.

3 Assignment 1 - Research in Audit, Measurement Practice, and Control

3.1 Identify the system to be audited

The system being audited is a print and scan server produced by the company XYZ Inc.
This product offers the following services:

- receives print jobs from the LAN and directs them to a proprietary printer physically attached
- receives scan jobs from a proprietary scanner and directs them to SMB or FTP file servers on the LAN
- allow remote job monitoring and management

The system consists in a PC with an Intel CPU running Windows XP Sp1 and additional software.
The software running on the PC is composed of:

- In-house developed software
- Microsoft products
- third-party products

The print and scan server is connected to the customer LAN. It has the following connections:

- a LAN network interface
- a local interface (monitor, keyboard, mouse)
- proprietary interfaces for the scanner and printer

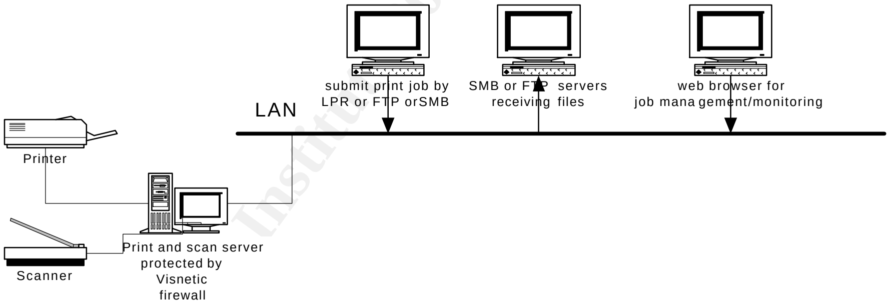


Figure 1: Print and scan server network connections

This print and scan server must be hosted on a network isolated from the Internet by a firewall or other security devices. This requirement is included in the product installation guide.

In order to improve the system security, the company has decided to use a host-based firewall. This firewall must protect the print and scan server. The firewall is VisNetic for workstation version 2.1.3. This software firewall will run on the same PC as the print and scan server and is considered to be part of the system.

The company tries to improve the security level of its products and it requested a penetration analysis in order to assess the security of the system. The company doesn't have a security policy targeted for this kind of product. This audit report will be used to create one. However, the company has a general security policy and the compliancy to corporate policy must be checked.

This is an internal audit and it will be conducted from an independent auditor's perspective. The company XYZ Inc. decided to provide the auditor with administrative level control over the system because they want him to perform all the tests required for an in-depth risk analysis. Furthermore, the auditor received detailed system information.

The audit scope is to determine at which level the Print/scan server (internal version 0.9) produced by the company XYZ Inc. and protected by the VisNetic for workstation firewall (version 2.1.3) is vulnerable to malicious traffic designed to break the system integrity and is compliant to the company security policy. The audit scope is limited to the network services. The locally accessible interfaces (interfaces that need someone physically present in front of the system) are outside the scope of the audit.

3.2 Evaluate the risk to the system

3.2.1 The assets

The assets identified by the company XYZ Inc. are the integrity of their customers LANs and the system itself. The company XYZ Inc. is willing to protect these assets against worms, viruses and hackers taking advantage of common and relatively public vulnerabilities.

These are the only assets included within this security audit.
The denial of service attacks, the integrity and the confidentiality of the print and scan jobs are outside the scope of the audit.

3.2.2 The threats

The following threats may harm the integrity of the system and customer LAN:
T1: the integrity of the system is compromised
T2: the system compromises the integrity of the LAN to which it is attached

3.2.3 Security relevant functions

In order to identify the security risks, the existing system and environment should be understood. This audit is limited to network services. Based on what enters and leaves the system via the LAN interface, the system may be abstracted as follows:

- LPD server that allows receiving print jobs (in-house developed application)
- FTP server allows putting/getting files from predefined folders (in-house developed application). The FTP server has one account: the anonymous account. The FTP put is used to submit print jobs. The FTP get is used to download scanned documents or log files. This server supports active and passive mode.

- Web interface (Jigsaw web server) allowing print job monitoring and management. This interface doesn't allow file upload/download.
- SMB server allows receiving print jobs and publishing print drivers (Windows XP native one).
- FTP client (in-house developed application) allows automatic uploading of scanned documents to an FTP server on the local network. This client supports the active and the passive mode.
- SMB client (in-house developed application) allows automatic uploading of scanned documents to a SMB server on the local network
- Windows DHCP client
- Windows DNS client
- Graphical language interpreters that convert print jobs into printable bitmaps (the only security relevant language supported is PostScript)
- Rest of the print and scan server software, the operating system and the hardware platform

The system administration requires console access and this system is not part of an administrative Windows domain.

The correct DHCP and DNS client behaviors depend on the LAN sanity. The customer network administrator is supposed to take care of this issue. However, if the DHCP server or DNS server on the LAN are substituted by fake servers, this will most likely generate a denial of service for the print server, which is outside the scope of this audit.

The firewall used to protect the system is a stateful one. It controls inbound and outbound traffic. This kind of firewall will either block or allow the traffic to/from a given port. It can't, for instance, dynamically allow traffic originating from a trusted application (application level firewalls can do it). The stateful inspection packet filters are aware only of the data layer 4 (TCP and UDP) of the OSI model.

The company security policy requires:
<u>Rule no. 1</u>: The OS of a product must be up-to-date.
The latest major update of the operating system (Microsoft OS service pack or equivalent for other platforms) must be used. This rule must be applied when the interval between the operating system update availability and the moment the product must enter the consolidation tests is greater than 3 months. If a security patch is issued more than two weeks before the consolidation tests start-up, it must be applied.
<u>Rule no. 2</u>: The third party servers included in a product must be up-to-date.
The latest version of the servers must be used. This rule must be applied when the interval between the new version availability and the moment the product must enter the consolidation tests is greater than 3 months. If the new version contains security fixes, the interval is reduced to two weeks.
<u>Rule no. 3</u>: The web server remote administration should be performed only using a secure connection otherwise it must be prohibited.
<u>Rule no. 4</u>: The product remote administration using SMB must be prohibited.
<u>Rule no. 5</u>: If a product is protected by a firewall, remote firewall administration via a corporate LAN must be prohibited.

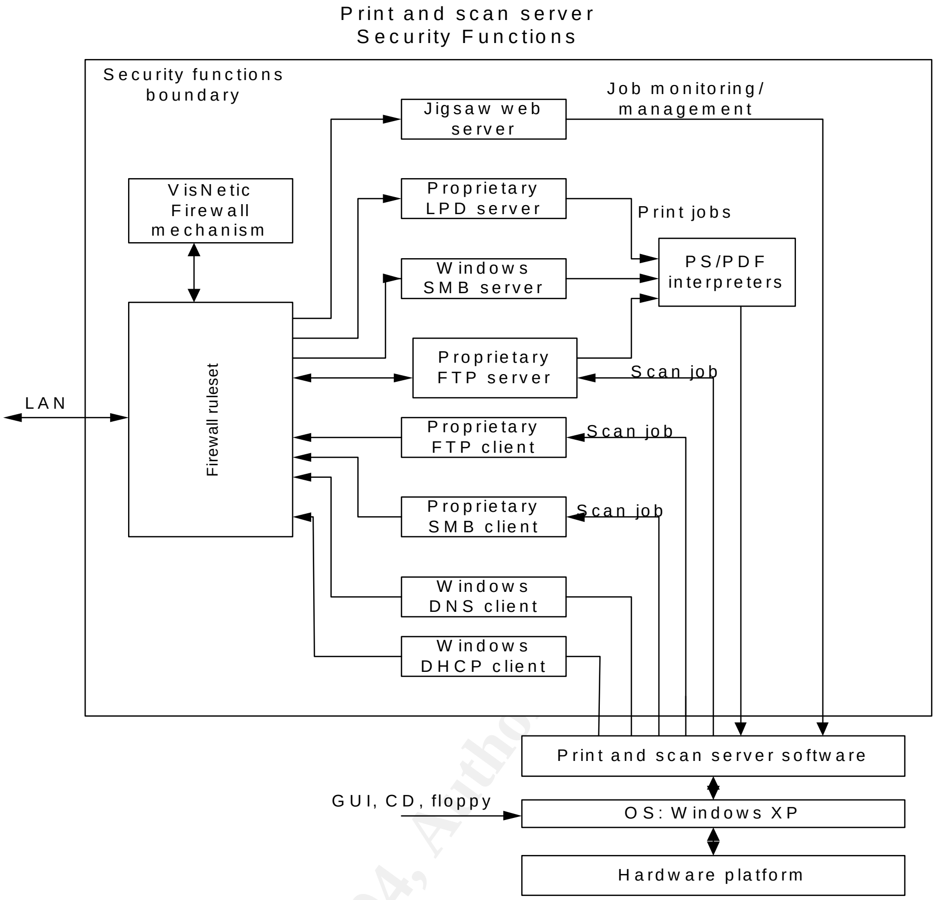


Figure 2: System security functions

3.2.4 The security risks

The risks analysis is started by analyzing the traffic between the LAN and the print and scan server, and the associated risks.

3.2.4.1 System integrity threat

The system integrity (threat T1) can be compromised by inbound traffic. This paragraph identifies the security errors that may allow or facilitate the realization of the system integrity threat.

<u>System ports scanning</u>

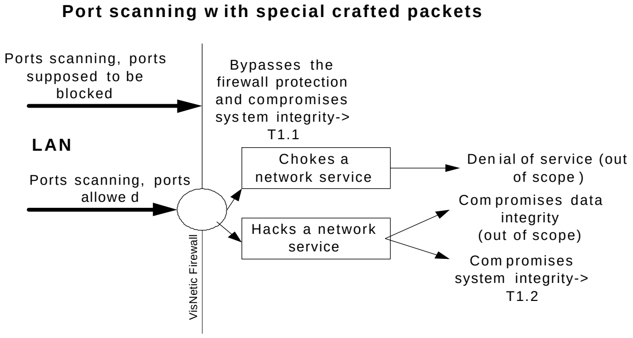

Port scanning with special crafted packets
Ports scanning, ports supposed to be blocked
LAN
Ports scanning, ports allowed
Bypasses the firewall protection and compromises system integrity-> T1.1
Chokes a network service
Denial of service (out of scope)
Hacks a network service
Compromises data integrity (out of scope)
Compromises system integrity-> T1.2
VisNetic Firewall

Figure 3: Security risks associated with ports scanning

The traffic directed towards the server network interface may be:

- Traffic that probes the firewall in order to bypass the firewall protection and to access network services that aren't supposed to be accessible from the outside. Security errors may impact the system integrity (T1.1).
- Traffic that uses one of the open ports to exploit protocol implementation vulnerabilities. This may allow choking one of the available network services (induces denial of service, not relevant for this audit) or worse hacking one of them. If the network service is hacked the data integrity may be compromised (out of scope) or the system integrity is compromised (T1.2).

T1.1 can be discovered using:

a) Scan tools like nmap.
b) Looking on the web for vulnerabilities concerning the firewall
c) Downloading the firewall's code and looking for vulnerabilities

T1.1 can be exploited using

a) Traffic targeting vulnerable services that were not appropriately protected because the firewall is not correctly configured
b) Traffic targeting vulnerable services that were not appropriately protected because the firewall during the normal function doesn't performs some checks (for instance the firewall doesn't filter packets with unexpected TCP flags)
c) exploits found on the web allowing to subvert the firewall
d) hacker crafted commands based on published vulnerabilities or based on the his own findings because he has access to the same firewall

A typical example of vulnerability associated with T1.2 is buffer overrun.
T1.2 can be discovered using:

a) vulnerability scanners if it concerns a well-known server that contains published vulnerabilities (Windows SMB server or Jigsaw Web server)
b) by downloading and looking for vulnerabilities if it concerns a server that doesn't contain published vulnerabilities (Jigsaw Web server)
c) blind guess, simple hazard if it concerns an in-house developed server (LPD or FTP server)

T1.2 can be exploited using:

a) exploits found on the web (Windows SMB server or Jigsaw Web server)
b) hacker crafted commands based on published vulnerabilities or based on the hacker's findings because he has access to a similar server (Windows SMB server or Jigsaw Web server)
c) hacker crafted commands based on the hacker findings due to blind guess, simple hazard or access to the print server software (because the hacker can't download a similar server from the web)

Buffer overrun can be done not only on the network services exposed by the print server, but also in the print server code (for instance in the language interpreters). However, crafting commands to exploit this kind of errors supposes having access to the print server (for instance running a debugger on it). This supposes a very motivated and skilled hacker, with enough time to perform the analysis on this particular print server software.

Files that can be put on the system

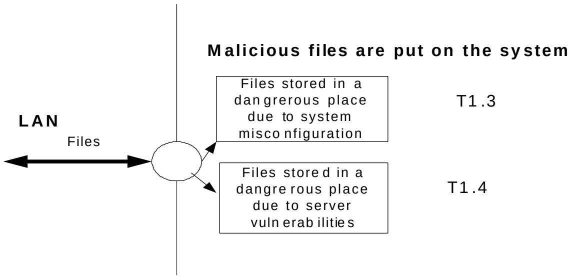

Malicious files are put on the system
LAN
Files
Files stored in a dangrerous place due to system misconfiguration
T1.3
Files stored in a dangrerous place due to server vulnerabilities
T1.4

Figure 4: Security risks associated with file uploaded to the system

T1.3 can be discovered using:
a) the functionalities offered by the system

T1.3 can be exploited:
a) putting the file in a dangerous place based on blind guess or simple hazard (for instance if the system automatically launches code from a shared directory exposed by the print server)
b) putting the file in a place well-known as dangerous if the hacker knows that a given server will download code from a given directory (for instance the directories included in the CLASSPATH of the Jigsaw web server) if the hacker knows which server runs and how it is configured

A typical example of vulnerability associated with T1.4 is directory traversal.
T1.4 can be discovered using:
a) vulnerability scanners if it concerns a well-known server that contains published vulnerabilities (Windows SMB server)
b) vulnerability scanners if it concerns a well-known protocol feature known to be incorrectly implemented by several servers (Jigsaw Web server, FTP server, PostScript interpreter; the auditor included the PostScript interpreter because PostScript is a powerful interpretative language that allows browsing a file system, creating and deleting files)
c) by downloading and looking for vulnerabilities if it concerns a server that doesn't contain published vulnerabilities (Jigsaw Web server)
d) blind guess or simple hazard if it concerns an in-house developed server (FTP server)

T1.4 can be exploited:
a) putting the file in a place well-known as dangerous if the hacker knows which OS runs (adding executable or scripts in the start-up folder, replacing binaries from system32)
b) putting the file in a place well-known as dangerous if the hacker knows that a given server will download code from a given directory (for instance the directories included in the CLASSPATH of the Jigsaw web server) if the hacker knows which server runs and how it is configured

Files that can be retrieved from the system

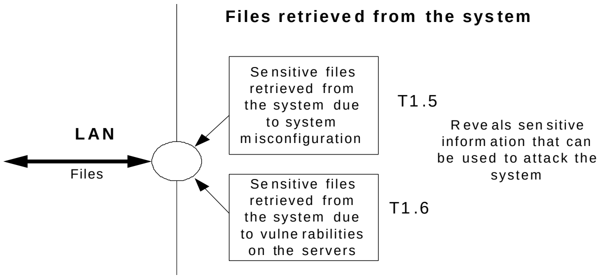

Files retrieved from the system
Sensitive files retrieved from the system due to system misconfiguration
T1.5
Reveals sensitive information that can be used to attack the system
LAN
Files
Sensitive files retrieved from the system due to vulnerabilities on the servers
T1.6

Figure 5: Security risks associated with files retrieved from the system

T1.5 can be discovered using:

a) the functionalities offered by the system

T1.5 can be exploited using:

a) the functionalities offered by the system

A typical example of vulnerability associated with T1.6 is directory traversal.
T1.6 can be discovered using:

a) vulnerability scanners if it concerns a well-known server that contain published vulnerabilities (Windows SMB server)
b) vulnerability scanners if it concerns a well-known protocol feature known to be incorrectly implemented by several servers (Jigsaw Web server, FTP server, PostScript interpreter because PostScript is a powerful interpretative language that allows browsing a file system, creating and deleting files)
c) by downloading and looking for vulnerabilities if it concerns a well-known server that doesn't contain published vulnerabilities (Jigsaw Web server)
d) blind guess or simple hazard if it concerns a in-house developed server (FTP server)

T1.6 can be exploited:

a) starting point for other attacks

Remote system management applications

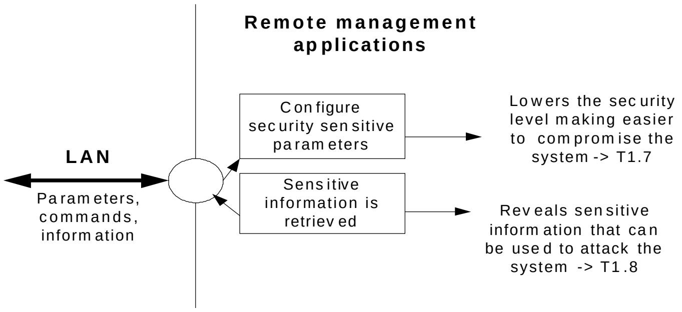

Remote management applications
Configure security sensitive parameters
Lowers the security level making easier to compromise the system -> T1.7
LAN
Parameters, commands, information
Sensitive information is retrieved
Reveals sensitive information that can be used to attack the system -> T1.8

Figure 6: Security risks associated with the remote management

Abuse of the remote management features may allow putting the system in a less secure state where the system integrity is easily compromised (T1.7). For instance the remote firewall management may allow reducing system protection. The remote system management applications may also reveal sensitive information that can be used to attack the system (T1.8). For instance the remote web server management may allow retrieving server configuration files.

T1.7 and T1.8 can be discovered using:

a) vulnerabilities published on the web if it concerns a known application (Windows SMB server, Jigsaw Web server, firewall mailing lists)
b) sniffing the traffic on the wire (if the traffic is unencrypted)
c) brute forcing if the passwords don't respect a complexity level

T1.7 can be exploited:

a) Using the remote management application

T1.8 can be exploited:

a) starting point for other attacks

3.2.4.2 Customer's network integrity threat

The customer's network integrity (threat T2) can be compromised by outbound connections:

1. following the system integrity corruption when the hacker gains administrative privileges (he may disable the firewall, reconfigure the web server; the product specification doesn't include any protection to mitigate the risk once the hacker gains administrative privileges).
2. when the hacker can run a malware on the system but he has not gained administrative privilege
3. when the hacker uses the features offered by the product to distribute malwares without gaining administrative privilege

Outbound traffic on ports supposed to be blocked

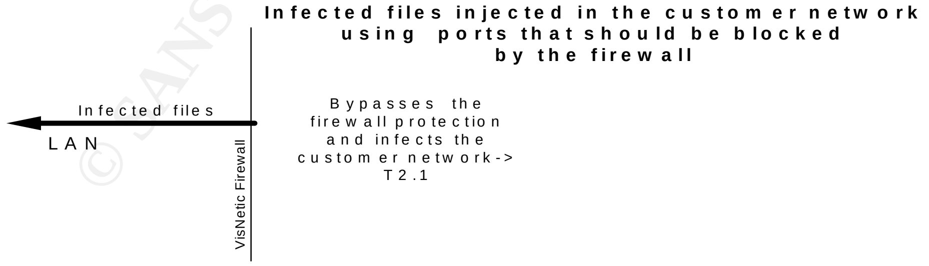

Infected files injected in the customer network using ports that should be blocked by the firewall
Infected files
LAN
VisNetic Firewall
Bypasses the firewall protection and infects the customer network-> T2.1

Figure 7: Security risks associated with ports supposed to be blocked

The hacker didn't gain administrative rights. However, he introduced a malware on the system. The malware is used to infect the customer's network bypassing the firewall (T2.1).

T2.1 can be discovered using:

a) vulnerabilities published on the web concerning the firewall, if the firewall used by the product has known/published vulnerabilities
b) simple hazard because the firewall is not correctly configured

T2.1 can be exploited using:

a) the hacker find a way to execute the malware on the system

<u>Outbound traffic on allowed ports</u>

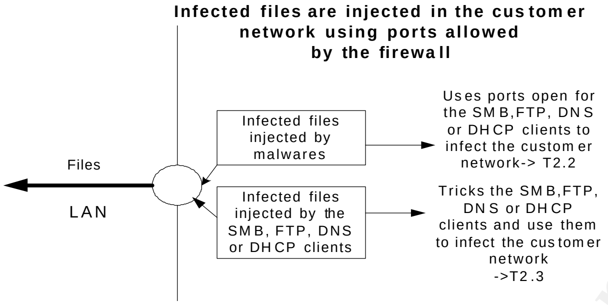

Infected files are injected in the customer network using ports allowed by the firewall
Files
LAN
Infected files injected by malwares
Infected files injected by the SMB, FTP, DNS or DHCP clients
Uses ports open for the SMB,FTP, DNS or DHCP clients to infect the customer network-> T2.2
Tricks the SMB,FTP, DNS or DHCP clients and use them to infect the customer network ->T2.3

Figure 8: Security risks associated with ports allowed by the firewall

The hacker didn't gain administrative rights. However, he introduced a malware on the system. This malware uses the ports allowed for the SMB, FTP, DNS or DHCP clients to send infected files to systems on the customer network (T2.2).

T2.2 can be discovered:

a) the hacker knows that SMB, FTP, DNS or DHCP clients are included in the product specification
b) the hacker sniff the traffic and sees FTP, DNS or DHCP commands leaving the system

T2.2 can be exploited using:

a) the hacker find a way to execute the malware

T2.3: The hacker didn't gain administrative rights. However, he introduced a malwares on the system and he knows how to trick the legal clients into sending infected files to systems on the customer network.

T2.3 can be discovered using:

a) the hacker knows that SMB, FTP, DNS or DHCP clients are included in the product specification

T2.3 can be exploited using:

a) the hacker finds a way to trick the legal clients into sending infected files on the customer's network

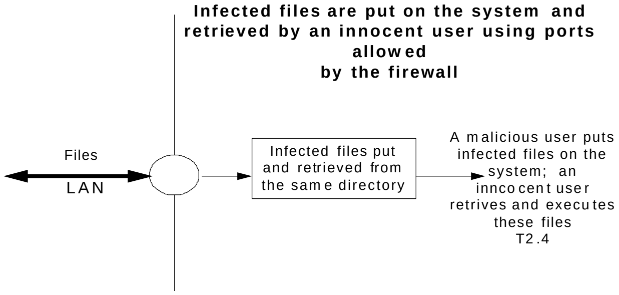

Infected files are put on the system and retrieved by an innocent user using ports allowed by the firewall
Files
LAN
Infected files put and retrieved from the same directory
A malicious user puts infected files on the system; an innocent user retrives and executes these files
T2.4

Figure 9: Security risks associated with files uploaded or downloaded

T2.4: The systems on the customer network can be compromised without even compromising the print server. Infected files can be put on the system using one of the servers (for instance the FTP server) and retrieved by an innocent user.

T2.4 can be discovered using:

a) the functionalities offered by the system
b) using vulnerability scanners (for instance by finding a directory traversal on one of the servers)

T2.4 can be exploited using:

a) the functionalities offered by the system

3.2.4.3 Security risk tables

Because everyone may have its own estimation of consequences of damage, the following table describes the different levels for the "Impact" indicator of the vulnerabilities established by the company XYZ Inc. for its products.

Impact	Description	Details
High	Code execution, Getting data write access, Privilege elevation, Password retrieval.	Everything that may cause system damage and leads to the customer network compromise.
Medium	Retrieval of information not intended to be public. Change system settings.	Information that is not supposed to be retrieved and could be used to attack the system.
Low	Other information not directly related to the company XYZ Inc. products, Vulnerabilities on inactive components.	Other kind of information: e.g. detecting the system is Windows-based.

Table 1: Levels for the vulnerability "Impact" indicator

The “likelihood” for a particular vulnerability to be exploited can also have several levels. The next table describes the different levels for the "Likelihood" indicator. As no previous audit report was supplied by the company for this kind of product, no assumption about controls in place can be made.

Likelihood	Description
Low	Fairly skilled and motivated people are required to be able to compromise the system because there are no tools allowing to detect (requires “blind trial & error”) or exploit the vulnerability
Medium	The tools to exploit the vulnerability are not widely available on the Internet, or are not easy to use. Possibly easy access (debug/disassemble/trace) to the code to hack
High	The tools to detect and exploit the vulnerability are easy to found and to use.

Table 2: Levels for the vulnerability "Likelihood" indicator

The following table summarizes the possible system integrity vulnerabilities. If the same vulnerability may cause several damages, the worst case is mentioned in this first high level risk table. For instance, if the fact that the ACLs are not correctly set allows replacing sensitive files (high impact) and retrieving sensitive information (medium impact), only the High impact is mentioned.

Risk identification	What may go wrong?	Traffic identification in “System integrity” paragraph	How likely?	Consequences
R1.1	The firewall doesn’t fulfill the expected security function	T1.1	**Medium**: Tools to detect the vulnerability are available; the firewall is evaluated for the first time by the company and may not be correctly configured; as this is one of the main security feature of the system, it may be the prime target for attacks	**High**: If vulnerable services are not protected they may allow code execution
R1.2	A buffer overrun on the LPD server is exploited by the attacker	T1.2	**Low**: The LPD server is an in-house developed application; the known LPD exploits are generally related to a buffer overflow for a specific LPD server and can’t be used against this server. A hacker needs to analyze this implementation and look	**High**: If a buffer overrun can be exploited it may allow code execution or privilege elevation (depends on the LPD server privilege)

			for vulnerabilities in order to hack this server.	
R1.3	A buffer overrun on the FTP server is exploited by the attacker	T1.2	**Low**: It needs a skilled hacker willing to attack this in-house developed application because tools to exploit eventual vulnerabilities will probably be difficult to find	**High**: If a buffer overrun can be exploited it may allow code execution or privilege elevation (depends on the FTP server privilege)
R1.4	The web server has high risk vulnerabilities	T1.2 T1.4 T1.6	**Medium**: Based on the number of tools allowing to detect and exploit vulnerabilities (the likelihood wasn't considered as high because this is not a well-known web server)	**High**: If dangerous features (like HTTP PUT) are not correctly implemented and protected they may allow writing data on the system
R1.5	The SMB server has high risk vulnerabilities	T1.2 T1.4 T1.6	**High**: Based on the number of tools allowing to detect and exploit vulnerabilities	**High**: If a buffer overrun can be exploited it may allow code execution or privilege elevation
R1.6	Transient services may appears on ports that can't be filtered due some special protocols (like passive FTP data server)	T1.2	**Low**: Because the attack window is reduced (attacks that must be performed during the laps of time where these dynamic ports are open) the tools in order to detect and exploit eventual vulnerable services will probably be difficult to find	**High**: If the transient vulnerable services are not protected they may allow code execution
R1.7	The PostScript interpreter is misconfigured	T1.3 T1.5	**Medium**: The standard PostScript language is supported and the reference manual specifies how to use the security relevant commands	**High**: If the PostScript disks give access to OS sensitive files that can be replaced or modified
R1.8	The FTP server is	T1.3 T1.5	**Medium**: FTP clients allowing to put files on	**High**: If sensitive OS files can be

	misconfigured		the server are included in most of the client OS on the end-user's PCs; as this is the first security audit for this product the likelihood that the server isn't correctly configured can't be considered as low	replaced or if the virtual directories are mapped to directories from which the binaries are automatically launched
R1.9	The SMB server is misconfigured	T1.3 T1.5	**Medium**: SMB clients allowing to put files on the server are included in all Windows systems; as this is the first security audit for this product the likelihood that the server isn't correctly configured can't be considered as low	**High**: If sensitive OS files can be replaced or if the shares are mapped to directories from which the binaries are automatically launched
R1.10	The web server is misconfigured	T1.3 T1.5	**Medium**: Tools allowing HTTP traffic interception and modification are available on the web; furthermore, this product contains several servers that allow putting/retrieving files on/from the system; as this is the first security audit for this product the likelihood that the server isn't correctly configured can't be considered as low	**High**: If malicious servlets can be added to the web server they may allow exposing sensitive information; if new classes may be added to the web server, the system integrity may be impacted.
R1.11	The FTP server incorrectly implements sensitive commands	T1.4 T1.6	**Medium**: FTP clients allowing to put files on the server are included in most of the client OS on the end-user's PCs; as this is the first security audit for this product the likelihood that the server incorrectly implemented sensitive commands can't be considered as low	**High**: If sensitive OS files can be replaced or if the directories from which the binaries are automatically launched can be accessed due to directory traversal access
R1.12	The PostScript interpreter incorrectly	T1.4 T1.6	**Medium**: The standard PostScript language is supported and the reference manual	**High**: If sensitive OS files can be replaced or if the directories from

	implements sensitive commands		specifies how to use the security relevant commands	which binaries are automatically launched can be accessed due to directory traversal access
R1.13	Dangerous remote SMB commands can be executed	T1.7, T1.8	**Medium**: Tools exploiting dangerous commands (like PS Tools suite) can be easily found on the web. If the traffic isn't encrypted, tools to sniff the network traffic are available. Even if the traffic is encrypted, if the password doesn't respect a given level of complexity, there are several tools allowing the password brute forcing.	**High**: If the SMB server is not correctly configured, dangerous commands may allow code execution
R1.14	The firewall's remote administration is hacked	T1.7, T1.8	**Medium**: This may be a prime target for attacks because it is a very important security feature. If the traffic isn't encrypted, tools to sniff the network traffic are available. Even if the traffic is encrypted, if the password doesn't respect a given level of complexity, there are several tools allowing the password brute forcing.	**High**: If the remote administration is used to stop the firewall, vulnerable services that are not protected may allow code execution
R1.15	The Web server's remote administration is hacked	T1.7, T1.8	**Medium**: If the traffic isn't encrypted, many tools to sniff, intercept or modify HTTP traffic are available. Even if the traffic is encrypted, if the password doesn't respect a given level of complexity, there are several tools allowing the password brute forcing.	**High**: If the remote administration is used to activate dangerous features (this may allow to an attacker to write data on the system)

Table 3: System integrity security risks

The following table summarizes the possible network integrity vulnerabilities**.**

Risk identification.	What may go wrong	Traffic identification in "Network integrity" paragraph	How likely?	Consequences
R2.1	Firewall doesn't fulfill the expected function and leaves open ports supposed to be blocked	T2.1	**Medium**: The firewall is evaluated for the first time by the company and may not be correctly configured. However, the hacker needs to find a way to enter the system and then to execute the malwares. As this is the first security audit for this product the likelihood that the print server isn't correctly configured can't be considered as low.	**High**: The malware may compromise the customer network
R2.2	Ports open for FTP, SMB, DNS or DHCP clients are used by malwares to access the LAN	T2.2	**Medium**: Malwares might use these well-known ports to leave the system	**High**: The malware may compromise the customer network
R2.3	The SMB and FTP clients are tricked into sending infected files on the LAN	T2.3	**Low**: The two clients are in-house developed applications and the files sent on the LAN must result from the scan server internal processing. Consequently it is difficult to subvert them.	**High**: The malware may compromise the customer network
R2.4	The DHCP client is tricked in sending infected files on the LAN	T2.3	**Not applicable**: DHCP protocol isn't designed for file transfer from DHCP client to the server	**High**: The malware may compromise the customer network
R2.5	The DNS client is	T2.3	**Not applicable**: The protocol isn't designed to allow a client	**High**: The malware may

	tricked in sending infected files on the LAN		to send files over the network.	compromise the customer network
R2.6	A malicious file is put on the system and retrieved from the same directory by an innocent user	T2.4	**Medium**: This system includes several servers that may allow putting/retrieving files to/from the system without any access control; an attacker may craft special PostScript file that can be downloaded by innocent users or an attacker may put an executable and hope that innocent users, not aware that they are accessing a print server, retrieve and execute it. However, the user must execute these files in order to infect its system.	**High**: The malware may compromise the customer LAN network

Table 4: Network integrity security risks

The audited system uses an important number of network services and this increases the attack surface.
The auditor should take into account the balance between the security insurance and the resources (time and personnel) needed to audit and secure the system. Consequently, the auditor excluded from this security audit the attacks that require finding flaws or weakness in in-house developed applications in order to craft the appropriate command to hack the system. The probability that a skilled hacker will spend time to craft packets that can be used only against this print server (protected from Internet by other security devices like routers and firewalls maintained by the customer administrator) is low enough to justify the exclusion from this first security audit.

Only the risks mentioned in the following table will be used to develop the audit checklist.

Risk identification	Short risk description	The controls that will prevent or mitigate the risk
R1.1	Firewall doesn't fulfill the expected security function	Included in firewall and company security policy checklists
R1.4	The web server has high risk vulnerabilities	Included in web server and company security policy checklists
R1.5	The SMB server has high risk vulnerabilities	Included in SMB server and company security policy checklists
R1.7	The PostScript interpreter is misconfigured	Included in PostScript interpreter checklists
R1.8	The FTP server is	Included in FTP server checklists

	misconfigured	
R1.9	The SMB server is misconfigured	Included in SMB checklists
R1.10	The Web server is misconfigured	Included in Web servers checklists
R1.11	The FTP server incorrectly implements sensitive commands	Included in FTP checklists
R1.12	The PostScript interpreter incorrectly implements sensitive commands	Included in PostScript interpreter checklists
R1.13	Dangerous remote SMB commands can be executed	Included in company security policy
R1.14	The firewall's remote administration is hacked	Included in company security policy
R1.15	The Web server's remote administration is hacked	Included in company security policy
R2.1	Firewall doesn't fulfill the expected function and leaves open ports supposed to be blocked	Included in firewall checklists
R2.2	Ports open for FTP, SMB, DNS or DHCP clients are used by malwares to access the LAN	- The firewall used in this product can't protect against this risk because it is a packet filter that controls only ports (it doesn't associate applications with ports) - The product specification doesn't include any integrity checker or antivirus that may allow this risk detection or prevention <u>Conclusion</u>: once the system is infected this risk can't be covered with the current product specification. The only way to mitigate this risk is: a) don't allow malwares to enter (already covered by the others risks in this table) b) don't allow malwares to execute on the system (Included in malwares execution checklist).
R2.6	A malicious file is put on the system and retrieved from the same directory by an innocent user	Included malware execution checklist.

Remark:
The audited system is a print and scan server. For the rest of this report the auditor will identify it as a print server because this audit focuses on the print server controls.

3.3 What is the current state of practice, if any?

In order to create the checklists for this system, the auditor needs information on:

- print servers,
- firewall checklists,
- the SMB and FTP servers vulnerabilities,
- the Jigsaw web server checklists
- the PostScript interpreter checklists.

Personal experience of the auditor helped in understanding the security context of a print and scan server, SMB and FTP issues.
Numerous articles and books are available for anyone willing to understand the SMB, FTP and HTTP security related issues. However, there are two books very interesting when performing a security audit:

1) “Hacking exposed”-Third Edition- by Stuart McClure, Joel Scambray and George Kurtz (McGraw-Hill/Osborne
2) “Writing secure code” by Michael Howard and David LeBlanc (Microsoft Press)

In order to create the checklist for this print and scan server, the auditor performed supplementary research on firewalls checklists, Jigsaw web server and the PostScript language.

3.3.1 Firewall checklists

There are a lot of firewall checklists on the web. Furthermore, there are a lot of very interesting reports on this subject on the SANS reading room. Even if, due to this system particularity, none of the checklists can be used as it, a combination of them can give a good starting point.
A search on the web was also performed to look for:

- known security vulnerabilities for VisNetic for workstation firewall version (ICAT metabase)
- known problems (on the forum dedicated to this firewall)

No securit vulnerability was found in the ICAT metabase (http://icat.nist.gov) and in the firewall dedicated forum.

3.3.2 Web server checklists

In order to create the Jigsaw web server checklists one may start by collecting general information on its architecture and configuration from http://www.w3.org/Jigsaw/. This web server, fully implemented in Java, is different from the regular web servers and not well known. No Jigsaw security checklists or tools to secure this web server were found on the web. The Jigsaw web server checklist was created based on the general web server audit checklist suggested by David Rhoades in his “Auditing web-based application” SANS track. The next step was to see how it applies to Jigsaw and which controls should be tested.

Further research was performed on general web server security issues. A very interesting World Wide Web security FAQ is hosted on http://www.w3.org/Security/Faq/wwwsf3.html containing Server Side Security issues. There are some pointers on setting file permissions on the web server and document roots, the danger of running the server with administrative privilege and known security problems with widespread servers (Jigsaw was not mentioned).

A better understanding of the Jigsaw security may be achieved by installing the web server and playing with for some time. When installing the server one can understand the danger that someone may add code to the server via a variable called CLASSPATH.
The CLASSPATH environment variable is a standard property that Java depends on. It shall list all paths from where the Java Virtual Machine will load needed Java classes. The CLASSPATH variable can either point to a directory with class files, a ZIP file or a JAR (Java archive) file. This environment variable shouldn't point to a world/group writable directory. If this variable contains only archives, no archive should be world writable.

Most of the checklists for the web servers require checking the file system rights on the cgi-bin directory. For Jigsaw this is not sufficient because in most of the cases the Jigsaw Web developers prefer to use servlets. This is the usual way to execute server side code on a Jigsaw web server. In order to access a web-based servlet the following steps should be performed:

- place the servlet's class file somewhere in the server's root directory (for instance in the servlet directory)
- the servlet can be called from a remote browser as follows: http://<hostname>/ servlet/ServletName

When checking the web server filesystem ACL's, the directory where the servlets are placed should also be considered.

Jigsaw has also a very powerful but dangerous feature: it allows users to upload Web pages. The method used to allow web publishing is HTTP PUT. This method allows updating information on the server or even creating a new resource on the server. Only authorized users should be able to use this method and it should be used to update only web content files. In order to update files on the server, the servlet that will offer this method must have enough permission to write or create the content file. A bug or a security hole in one of the servlets would allow an Intranet user to change any of the files (the audited system is not accessible from Internet). The Web pages upload, modification or delete features aren't included in the specifications of the print and scan server. Consequently, a control should be introduced for the Web server to be sure that no "putable" or "allow-delete" resources are exposed.

Another security relevant issue is the remote web server administration. The tool allowing remotely configuring Jigsaw is called JigAdmin. It's a graphical interface that communicates with an Administration server, called JigAdmin Server. The Jigsaw web server default configuration files provided by the default installation are designed to start two servers, an instance of **Jigsaw** and one **JigAdmin** Server. From a remote station one can access the administration server by installing the JigAdmin client locally (included in the default Jigsaw web server distribution) and calling the remote administration server as follows:

```
java org.w3c.jigadmin.Main [-root root] [url_of_the_remote_Admin_Server]
```

A search on the web was also performed to look for:

- known security vulnerabilities for Jigsaw web server 2.2.2 (ICAT metabase)
- known problems (on the forum dedicated to Jigsaw)

There are no ICAT vulnerabilities for the Jigsaw web server 2.2.2 used by the print server. The Jigsaw dedicated mailing list (http://www.w3.org/Search/Mail/Public) doesn't mention any security problems for this version on Windows platforms (there are some issues about SSL but the audited system doesn't use it). However, two up-to-date vulnerabilities scanners were used to double-check these findings and to see if this server has general web server vulnerabilities (canonicalization, Unicode input validation, etc).

3.3.3 PostScript interpreter checklists

In order to understand the possible risks related to PostScript files one can find information on this language in the book: "PostScript Language Reference – Adobe Systems Incorporated".

The PostScript language provides access to files on a storage device. The file access capabilities are part of the integration of the language with an underlying file system. The operators allowing access to files are: file, deletefile, renamefiles, status, filenameforall, setfileposition and fileposition. In an interpreter that runs on top of an operating system, there may be a device that represents the complete file system provided by the operating system. If so, by convention that device's name is "os". Depending on the PostScript interpreter it may be possible to access by reference all drives (C:/..) as "%os%c:/*". In an interpreter that controls a dedicated product, such as printer product, there can be one or more devices that represent filesystems on disks (for instance %disk0%, %disk1%). Depending on the PostScript interpreter it may be possible to access files on a PostScript disk device by using relative path constructs, like "../" or "..\".

After identifying the security sensitive operators (file, deletefile, renamefiles, filenameforall) the controls for them can be created. In order to exploit these commands some PostScript skills are needed. A PostScript file that contains all these operators was created for this audit. This print file will be sent to the print server. The bitmap that retrieved from the printer physically linked to the print server will contain the results.

4 Assignment 2 –Create an Audit Checklist

In order to establish the checklist for the system, the following particularities included in the product specifications should be taken into account:

- every remote user can send a print job (The anonymous/guest accounts are activated by default. Consequently, controls must be introduced to verify what the guest/anonymous accounts can do)
- every local user can scan a job
- the web application allows only job monitoring and management (it doesn't allow web server configuration and operating system management)
- the system must be seen from the LAN (it must answer to ping)

A local user is someone that must be physically present in front of the system in order to use it.
A remote user is someone that needs only an access to the corporate LAN in order to use the system.

Before starting the audit, the auditor required the following documents:

- the company's general security policy (necessary because the product compliancy to this policy must be checked; this document will be referenced as DOC_GEN_POLICY)
- the official statement about the date when the product must enter the consolidation tests (needed in order to check if the OS and the servers are up-to-date; this document will be referenced as DOC_PROD_CONSOLIDATION)
- the documentation concerning the ports used by the servers and the clients included in the product specification (needed in order to create the test cases allowing to check that all traffic not included in the product specification is filtered; this document will be referenced as DOC_SERVERS_PORTS)
- the documentation concerning
  - all the virtual directories used by the servers and their physical mapping to the local file system and the user accounts;
  - the spool directories where the print jobs arrive
  - for the web server, this document should include:
    - all the directories used by the web server,
    - the java virtual machine used
    - the web server version
    - the directory where the java virtual machine runs (needed in order to check the ACLs and the java virtual machine version)

  (This document will be referenced as DOC_SERVERS_DIRS_USERS
- the documentation concerning the protocols installed on the product (needed for the firewall checklist; this document will be referenced as DOC_PROTOCOLS)
- the documentation concerning the PostScript interpreter disks and the mapping to the local file system (needed for the PostScript checklist; this document will be referenced as DOC_PS)

When auditing the server's vulnerability, it is recommended to use at least two vulnerability scanners. This will reduce the risk to miss vulnerabilities.

4.1 Security policy compliancy checklist

The system must be compliant to the global company security policy.
P1: Check if the OS of the system is up-to-date -> Rule 1 (please see the paragraph "Security relevant functions" for further details)
P2: Check the Web server version -> Rule 2
P3: Check the remote Web server administration -> Rule 3
P4: Check the system remote SMB administration -> Rule 4
P5: Check the remote firewall administration-> Rule 5

4.2 Firewall checklist

When assembling the checklist for the firewall used in the system, the following facts should be considered:

1. it is a host based firewall
2. it is a stateful inbound/outbound firewall that control ports and not applications
3. the protected system must be seen from the LAN (answering to ping is part of the product specifications)
4. the requirements for the environment where the system must be hosted stipulate that the system must be protected from Internet by other security devices managed by the customer LAN administrator (the system access from Internet shouldn't be checked)
5. only the remote access to the system is audited; the local interfaces protections are outside the scope. The audit of the local access protection for the firewall management interface is also outside the scope.

The following information was retrieved from the document concerning the ports used by the servers and the clients included in the product specification (DOC_SERVERS_PORTS). This is mentioned here because it is considered a particularity for this system:

- The product specification requires a passive FTP server. When being in the passive mode, the FTP server gives a dynamic port number for the data connection. The FTP client uses this port to connect to the server. The FTP server provided by company XYZ Inc. doesn't implement any mechanism in order to reduce the port range used for the data connection. If this kind of server is protected by a stateful packet filter like the VisNetic firewall, all the ports greater then 1023 must not be blocked for the inbound traffic. Consequently the system should either not have any application listening on ports greater then 1023 or provide a rule explicitly blocking the access to any port greater then 1023 not included in the product specification. This point must be verified when checking the firewall ruleset against the product specification.
- The product specification requires also a FTP server data active. When being in the active (normal) mode, the FTP server connects to a FTP client on a port greater then 1023. Generally, the data transfer is initiated on the server's TCP port 20. The FTP server provided by company XYZ Inc. doesn't respect this convention, the data port may be any dynamic port greater than 1023.

The documentation concerning the protocols (DOC_PROTOCOLS) specifies that the product supports only the IP protocol.

The firewall checklist is:

F1: Check the firewall software patch level
F2: Check the firewall ruleset against the product specification
F3: Check what happens when the firewall is not running
F4: Check how the firewall protects the system from attacks with unexpected TCP flags
F5: Check how the firewall protects the system from attacks on other IP protocols and on other protocols
F6: Check if the firewall detects unauthorized network activities on the system

4.3 Web server checklist

The following list covers the checks usually associated to the Web servers:

1. check the web server patch level (already covered by 4.1 Security policy compliancy checklist)
2. check how the web server controls access to information
3. check if the web server provide adequate forensic evidence in the event of an attempted or successful security breach
4. check if the web server minimizes services (keep turned off the unused features)
5. check web server security vulnerabilities

Before describing the controls for "check how the web server controls access to information", answering the question "Who may access sensitive information?" is recommended.

- local users with console access because the Web server's directories aren't appropriately protected; no control to be provided because the local console access is outside the scope of this audit
- remote users entering the system via the Web server port using dangerous features (HTTP PUT, DELETE); a control checking the "putable" or "allow-delete" resources access must be introduced; this control is included in "check if the web server minimizes services"
- remote users entering the system by the Web server port and exploiting known bugs in the executables running on the Web server and designed to offer dynamic content: CGI scripts, servlets (use CGI and vulnerability scanners to detect known bugs; check the filesystem ACLs on cgi-bin directory and on the directories containing servlets)
- remote users exploiting remote Web server administration pages (already covered by 4.1 Security policy compliancy checklist)
- remote users entering the system via other services (like FTP) and accessing Web directories because they aren't appropriately protected (check the filesystem ACLs on web server directories)

The resulted Web server checklist is:
W1: Check that the web server is minimizing services
W2: Check the filesystem ACLs on web server directories
W3: Check if Web server logging is appropriate
W4: Evaluate the Web server with two CGI scanners
W5: Evaluate the Web server with two vulnerability scanners
W6: Check the Web server permissions
W7: Check that the Java Virtual Machine where the server runs is up-to-date

4.4 SMB server checklist

The following list cover the risks categories associated to the SMB server:

1. The Guest account should be used only to print. The SMB shares should be only : IPC$, PRINT$, PRINTQUEUE (no file sharing included in the product specification) and the ACLs should be set appropriately(IPC$ admin only, PRINT$ allows read only for everyone, Print queues: everyone can read/write)
2. SMB server security vulnerabilities (The files arriving on the print queues are received by the Windows server service and sent to the Windows spooler service. Any security errors in the server and spooler services impacts on the system integrity (for instance a security error that allows executing code on the system).
3. system remote administration*:* check what kind of information can be retrieved with remote administration tools and what kind of remote operations are possible. Already covered by 4.1 Security policy compliancy checklist

The SMB server checklist is:

SMB1: Only PRINT$, IPC$ and PRINTQUEUE shares should be exposed and the appropriate ACLs should be set
SMB2: Check the SMB server security with two vulnerability scanners

4.5 FTP server checklist

The following check list covers the risks associated to the FTP server:
FTP1: Check FTP server virtual directories ACLs.
FTP2: Check if the FTP server has well-known security vulnerabilities
FTP3: Check the FTP server permissions

4.6 PostScript interpreter checklist

The following check list covers the risks associated to the PostScript interpreter:
PS1: Check how the PostScript interpreter controls access to information
PS2: Check PostScript devices/directories ACLs (a PostScript device is mapped as a filesystem directory)
PS3: Check PostScript interpreter directory traversal access
PS4: Check PostScript interpreter permissions

4.7 Malware execution protection checklist

The following checklist covers the risk associated with malwares execution:
MAL1: Check that no directories simultaneously writable and readable are exposed by the print server
MAL2: Check that in every writable directory exposed by the print server is not possible to execute code (the spool directories are included)

4.8 System control objectives

The following paragraphs describe the controls to be performed in order to assess system security level. Each control is justified by a risk identified in the paragraph “security risks tables” (Page 15). Only the risk identification will be given. Please check the “Table 1: System integrity security risks” and “Table 2: Network integrity security risks” for a detailed risk description.

4.8.1 Security policy compliancy controls

Control no. 1	**P1: Check if the OS of the system is up-to-date**
Control objective: Check if the OS version follows the company security policy concerning major updates and security patches.	**Objective**
Why the test is performed Known exploits may be present if the operating system is not patched. The operating system security level can impact the security of all applications running on it: the firewall, the different network services (it may allow remote code execution, for instance). *Reference: R1.1, R1.5, R2.1, R2.2*	
What test control design is to be performed The latest major update of the operating system must be used. This rule must be applied when the interval between the operating system update availability and the moment the product must enter the consolidation tests is greater than 3 months. If a security patch is issued more then two weeks before the consolidation tests start-up, it must be applied.	
How to perform the test Use the document containing the official statement about the date when the product must enter the consolidation tests (DOC_PROD_CONSOLIDATION) to retrieve the date used as a reference for this control. Download the latest `mssecure.xml` from Miscrosoft. Install and run locally `hfnetcheck`: `Hfnetcheck –x mssecure.xml –vv > c:\temp\audit\hfnetck.txt` Install and run locally mbsa. Choose “`Scan the local system`”	
Consequence High: Because a vulnerability allowing remote code execution may exist	**Likelihood** High: Based on the frequency of Windows security patches and the number of exploits that can be found on the web
Compliance Test passes if either the OS major update is applied or the time between the major update and the start of the consolidation tests is smaller then 3 month. If the first part of the test fails the control fails. If the first part of the test passes, look also to the OS security patches. This control passes if either all the security patches are applied or the time between last security patch and the start of the consolidation tests is smaller then 2 weeks.	
References Company XYZ Inc. security policy rule number 1 (DOC_GEN_POLICY).	

Control no. 2	**P2: Check the Web server version**
Control objective: Check if the web server version follows the company security policy concerning major updates and security patches.	**Subjective**

Why the test is performed Known exploits may be present if the software is not patched. This may allow viewing sensitive files and directories through the web server. *Reference R1.4*	
What test control design is to be performed The latest version of the Jigsaw web server must be used. This rule must be applied when the interval between the new version availability and the moment the product must enter the consolidation tests is greater than 3 months. If the new web server version contains security bugs correction, the interval is reduced to two weeks.	
How to perform the test Use the document containing the official statement about the date when the product must enter the consolidation tests (DOC_PROD_CONSOLIDATION) to retrieve the date used as a reference for this control. Look for `http-server.props` in the directory where Jigsaw is installed. Retrieve the web server version (corresponds to `org.w3c.jigsaw.server`). The system owner may decide to modify this value in order to hide the web server version (this is a good security practice) If this is the case, use the DOC_SERVERS_DIRS_USERS document to retrieve the web server version.	
Consequence Medium: The buffer overrun vulnerabilities were not considered for this server because it runs in a java virtual machine; the directory traversal exploits may exist and this can allow reading sensitive data	**Likelihood** Medium : This server is not well-known; however, many tools to detect vulnerabilities can be easily found; furthermore, the web server may have general vulnerabilities related to the implementation of sensitive commands
Compliance Test passes if either the last Jigsaw version is applied or the time between the new version and the start of the consolidation tests is smaller then 3 month. If the new web server version contains security bugs correction, the interval is reduced to two weeks.	
References Company XYZ Inc. security policy rule number 2 (DOC_GEN_POLICY).	

Control no. 3	**P3: Check the remote Web server administration**
Control objective: Check if the remote Web server administration follows the company security policy concerning access to the Web server administration.	**Objective-stimulus response**
Why the test is performed If anybody can access the Web server administration, it may put the server in a less secure mode where the system integrity can be easily corrupted. If the traffic is not encrypted someone may sniff on the LAN during a remote administration connection and find out the administrative password. *Reference R1.15*	
What test control design is to be performed	

<table>
<tr><td colspan="2">The web server remote administration should be performed only using a secure connection otherwise it must be prohibited</td></tr>
<tr><td colspan="2"><b>How</b> to perform the test
Use the documentation concerning the ports used by the servers and the clients included in the product specification(DOC_SERVERS_PORTS) in order to retrieve Jigsaw administration port and the web server port (it will be referenced as WEB_SERVER_PORT).
If there is no web server remote administration port, stop here. The control passes.
<b>Test 1</b>
If a port is mentioned, it will be referenced as ADMIN_PORT.
Install the JigAdmin client on a remote system (included in the default Jigsaw web server distribution) and call the remote administration server as follows:
<code>java org.w3c.jigadmin.Main [-root root]</code>
<code>http://WEB_SERVER_ADDRESS:ADMIN_PORT</code>
<b>Test 1 passes</b> if it is not possible to launch the remote administration console on HTTP (only a secure connection as HTTPS should be possible).

<b>Test 2</b>
From a remote browser try:
<code>http://WEB_SERVER_ADDRESS:ADMIN_PORT</code>
<b>Test 2 passes</b> if the page can’t be found (only a secure connection as HTTPS should be possible).

<b>Test 3</b>
From a remote browser try:
<code>http://WEB_SERVER_ADDRESS:WEB_SERVER_PORT/admin</code>
<b>Test 3 passes</b> if the page can’t be found (only a secure connection as HTTPS should be possible).</td></tr>
<tr><td><b>Consequence</b>
High: If the remote administration is used to activate dangerous features this may allow to an attacker to write data on the system</td><td><b>Likelihood</b>
Medium: If the traffic isn’t encrypted, many tools to sniff, intercept or modify HTTP traffic can be easily found. Even if the traffic is encrypted, if the password doesn’t respect a given level of complexity, there are several tools allowing the password brute forcing.</td></tr>
<tr><td colspan="2"><b>Compliance</b>
The control passes if all the intermediary tests pass.</td></tr>
<tr><td colspan="2"><b>References</b>
Company XYZ Inc. security policy rule number 3 (DOC_GEN_POLICY).</td></tr>
</table>

<table>
<tr><td><b>Control no. 4</b></td><td colspan="2"><b>P4: Check the system remote SMB administration</b></td></tr>
<tr><td colspan="2"><b>Control objective:</b>
Check that no dangerous remote administration SMB commands are accessible from the customer LAN as requested by the company’s security policy.</td><td><b>Objective-stimulus response</b></td></tr>
</table>

Why the test is performed

If the remote system administration is possible, some dangerous tools may be used remotely to gain sensitive information (using PsLoggedOn, PsFile, PsLogList, PsInfo, PsList, PsGetSid) or control sensitive processes (using PsService, PsExec, PsKill, PsShutdown, PsSuspend) or even change accounts on the system (using PsPasswd).

REFERENCE R1.13

What test control design is to be performed

Check that the [**PStools**] suite fails on well known accounts.

Check also that no dangerous tools can be used remotely, even when the OS-administrator password is known (because the administrator password may be found by brute force, sniffed on the wire or by social engineering).

How to perform the test

Use [**Pstools**] suite to attempt remote operations on a Windows based platform system, and to retrieve administration information.

Test 1

Use `PsLoggedOn`, `PsFile`, `PsLogList`, `PsPasswd`, `PsService`, `PsExec`, `PsGetSid`, `PsInfo`, `PsKill`, `PsList`, `PsShutdown`, `PsSuspend` with well known accounts (user documented, guest and standard administrator account name).

Test 1 passes when all these tools do nothing.

Test 2

Use `PsPasswd`, `PsService`, `PsExec`, `PsKill`, `PsSuspend`, `PsGetSid` used with the OS-administrator account.

Test 2 passes when all these tools do nothing.

Consequence	**Likelihood**
High: Dangerous SMB commands may allow executing code on the system	Medium: Tools exploiting dangerous commands (like PS Tools suite) can be easily found on the web. If the traffic isn't encrypted, tools to sniff the network traffic can also be easily found. Even if the traffic is encrypted, if the password doesn't respect a given level of complexity, there are several tools allowing the password brute forcing.

Compliance

Control passes if all the intermediary tests pass.

References

Company XYZ Inc. security policy rule number 4 (DOC_GEN_POLICY).

Control no. 5	**P5: Check the remote firewall administration**
Control objective: Check if firewall administration follows the company security policy concerning remote access to the firewall administration.	**Objective-stimulus response**

Why the test is performed

Unauthorized remote users may disable the firewall or change the settings. The system is left without protection and may get infected or may infect the network. *Reference R1.14*

What test control design is to be performed

Verify the firewall remote administration status.

How to perform the test

Test 1

Logon as system administrator.

Double click on the VisNetic Firewall shortcut to launch the firewall management application.

Verify that

```
View-> Settings-> Administration
                              "Enable Remote Administration"
```

is not checked.

Record the value of the default administration port.

Test 1 passes if the remote administration checkbox isn't enabled.

Test 2

Reboot the system.

Scan the print server LAN interface from a remote PC using nmap.

```
Nmap –sT –p1-65535 xxx.xxx.xxx.xxx
```

Test 2 passes if the administration port isn't mentioned as open.

Consequence	**Likelihood**
High: If the remote administration is used to stop the firewall, several network services may be accessible. If these services aren't correctly configured or are not up-to-date they may contain vulnerabilities (a buffer overrun vulnerability may allow remote code execution)	Medium: This may be a prime target for attacks because it is very important security feature. If the traffic isn't encrypted, tools to sniff the network traffic can also be easily found. Even if the traffic is encrypted, if the password doesn't respect a given level of complexity, there are several tools allowing the password brute forcing.

Compliance

Control passes if all the intermediary tests pass.

References

Company XYZ Inc. security policy rule number 5 (DOC_GEN_POLICY).

VisNetic user guide

4.8.2 Firewall controls

Control no. 6	**F1: Check the firewall software patch level**	
Control objective: The firewall software must be kept up to date.		**Objective**
Why the test is performed Known exploits may be present if the software is not patched. *Reference R1.1, R2.1*		
What test control design is to be performed Retrieve the firewall patch version. Verify that the firewall is up to date.		
How to perform the test Use the document containing the official statement about the date when the product must enter the consolidation tests (DOC_PROD_CONSOLIDATION) to retrieve the date used as a reference for this control. Logon as system administrator. Double click on the `VisNetic` icon in the system tray. Choose from the `Help` menu the item "`About VisNetic Firewall`". Retrieve the firewall version and check it against the last version on the firewall web page http://www.deerfield.com/products/visnetic-firewall/ and the security fixes included.		
Consequence High: If the missing security patch concerns a buffer overflow it may allow remote code execution	**Likelihood** Low: It is not possible to detect remotely the firewall version. However, a blind attack may be successful because a fix concerning an important security feature is missing.	
Compliance Control passes if either the last firewall version is applied or the time between the new version and the start of the consolidation tests is less then 3 months. If the new firewall version contains security fixes, the interval is reduced to two weeks.		
References Egil Andresen, "Auditing Perimeter defenses in Home Office Environment with D-LINK Broadband Router and Kerio Personal Firewall"		

Control no. 7	**F2: Check the firewall ruleset against the product specification**
Control objective: The firewall ruleset must allow only the ports mandatory for the product to comply to the specification.	**Objective-stimulus response**

Why the test is performed

If the firewall is more permissive that the product specification, it may let traffic directed to network services that weren't hardened to be attacked or it may supply information allowing a remote user to enter into the system.

Reference R1.1, R2.1

What test control design is to be performed

Check that all traffic not included in the product specification is filtered.

A. The default rule must be "deny all" access if no other rule applies.

B. Check that every unfiltered inbound/outbound port is associated to one of the functionalities described in the product specification.

SMB server
LPD server
Web server
FTP server: passive and active mode
FTP client passive and active mode
SMB client
DHCP client
DNS client

No application should listen permanently on ports >1023 or a rule filtering this application shall be provided. Only the FTP server may listen on a port > 1023 during data transfer.

C. The product specification requires the system to answer to ICMP "echo" messages. All other ICMP messages should be filtered.

How to perform the test

Use the documentation concerning the ports used by the servers and the clients included in the product specification in order to create the test cases allowing to check that all traffic not included in the product specification is filtered (DOC_SERVERS_PORTS)

This document specifies an application running on a TCP ports greater then 1023 and this port should be filtered.

In this section "MyAddress" is the printserver address (this name is proposed by default by VisNetic firewall for the address of the host that the firewall must protect).

The traffic that the firewall is supposed to allow is:

For the SMB server
Allow MyAddress [139] <- All addresses [1024-65535] TCP
Allow MyAddress [137-138] <-> All addresses [137-138] UDP

For the LPD server
Allow MyAddress [515] <- All addresses [All] TCP

For the Web server
Allow MyAddress [80] <- All addresses [1024-65535] TCP

For the FTP server
Allow MyAddress [21] <- All addresses [1024-65535] TCP
Allow MyAddress [1024-65535] -> All addresses [1024-65535] TCP (FTP server data active-> this is rather unusual, please see paragraph 4.2 for further details)
Allow MyAddress [1024-65535] <- All addresses [1024-65535] TCP (FTP server data passive)
The firewall rule becomes:
Allow MyAddress [1024-65535] <- >All addresses [1024-65535] TCP (FTP server data passive and active)

For the FTP client
Allow MyAddress [1024-65535] -> All addresses [21] TCP
Allow MyAddress [1024-65535] <- All addresses [20] TCP
Allow MyAddress [1024-65535] -> All addresses [1024-65535] TCP (FTP client data: passive); this rule is included in the rule for FTP server data active and passive)

For the SMB client
Allow MyAddress [1024-65535] -> All addresses [139] TCP

For the DHCP client
Allow MyAddress [68] <-> All addresses [67] UDP

For the DNS client
Allow My Address[1024-65535] <-> All addresses [53]

Allow ping requests
Allow MyAddress [0] <-> All addresses [8] ICMP

This firewall can also filter the ARP traffic. The product specification doesn't explicitly mention that the incoming ARP traffic should be allowed because it was considered an implicit requirement.
Allow ARP requests
Allow MyAddress <-> All addresses

The traffic summary is:
For inbound TCP connections (IN_TCP):

a) *Traffic from ports between 1024-65535 is allowed to enter the system on the ports 21 (FTP server control link), 80(web server), 139(SMB server - over Netbios), 515 (LPD server) and on any ports between 1024-65535 (FTP server data passive).*
b) *Traffic from port 20 is allowed to enter the system on ports between 1024-65535 (FTP client data active)*

For outbound TCP connections (OUT_TCP): all traffic from ports between 1024-65535 is allowed to leave the system if the target is one of the following ports: 21(FTP client control link), 139(SMB client – over Netbios), 1024-65535(FTP client data passive and in-house developed FTP server data active that doesn't respect the convention to use the port 20 to initiate data connection).
A rule is provided to block the inbound and outbound traffic associated with an

application listening on a port > 1023 (this application is mentioned in DOC_SERVERS_PORTS).

For inbound UDP connections (IN_UDP and OUT_UDP): all traffic from ports 53/67/137/138 is allowed to enter the system if the destination ports are >1024/68/137/138 (DNS client, DHCP client, Netbios service).
For outbound UDP connections (IN_UDP and OUT_UDP): all traffic from ports >1024/68/137/138 is allowed to leave the system if the destination ports are 53/67/137/138 (DNS client, DHCP client, Netbios service).

For inbound ICMP connections (IN_ICMP): The system must answer to ping requests.
Everything else should be blocked.

Reboot the system.

(IN_TCP) Check that the firewall blocks the inbound traffic on TCP ports not necessary for the product specification.

Test 1
Inbound connections on allowed/blocked TCP ports coming from authorized remote ports

Run nmap on a remote machine on the same subnet.
`Nmap –sT–P0 –p1-65535 xxx.xxx.xxx.xxx`
Test 1 passes if only the following ports will be reported as unfiltered:
`TCP 21, 80, 139, 515` (By default nmap will use a source port > 1024)

Test 2
Inbound connections on allowed/blocked TCP ports coming from unauthorized remote ports

Run nmap on a remote machine on the same subnet.
`Nmap –sS–P0 –p1-65535 xxx.xxx.xxx.xxx –g Y` (where Y is a port available on the remote PC where nmap runs, Y<1024)
Test 2 passes if all the ports are reported as filtered.

(OUT_TCP) Check that the firewall blocks the outbound traffic from TCP ports not necessary for the product specification.

Test 3
Outbound connections to unauthorized remote TCP ports

Run Netcat on a remote system on the same subnet. Make it listen on a TCP port <1024 (for instance 80).
`Nc –n -v -p 80 -l`

Run another Netcat on the print server. Try to create a connection to the remote system.
`Nc –n -v -p port_greater_then_1023 “remote_PC_address” 80` (on a port

between 1024-65535)
Test 3 passes if the connection is blocked.

Test 4
Outbound connections from unauthorized local TCP ports to authorized remote ports

Run Netcat on a remote system on the same subnet. Make it listen on a TCP port <1024 (for instance 21).

```
Nc –n –v –l –p 21
```

Stop the LPD server and replace it with a Netcat session (run Netcat on TCP port 515).

```
Nc –n –v –p 515 “remote_PC_address” 21
```

Try to create a connection to the remote system.

```
Nc –n –v –l –p 21
```

Test 4 passes if the connection is blocked.

(IN_UDP) Check that the firewall blocks the inbound traffic on UDP ports not necessary for the product specification.

Test 5
Inbound connections on allowed/blocked UDP ports coming from authorized remote ports

Run nmap on a remote machine on the same subnet.

```
Nmap –sU –P0 –p1-65535 xxx.xxx.xxx.xxx –g 53
```

Test passes if all ports are reported as filtered, excepting UDP ports > 1024 (Allowed for the DNS client).

```
Nmap –sU –P0 –p1-65535 xxx.xxx.xxx.xxx –g 67
```

Test passes if all ports are reported as filtered, excepting UDP port 68 (allowed for the DHCP client).

```
Nmap –sU –P0 –p1-65535 xxx.xxx.xxx.xxx –g 137
```

Test passes if all ports are reported as filtered, excepting UDP port 137 (allowed for NETBIOS Name Service).

```
Nmap –sU –P0 –p1-65535 xxx.xxx.xxx.xxx –g 138
```

Test passes if all ports are reported as filtered, excepting UDP port 138(allowed for NETBIOS Datagram Service).

Test 5 passes if all intermediary tests pass.

Test 6
Inbound connections on allowed/blocked UDP ports coming from unauthorized remote ports

Run nmap on a remote machine on the same subnet.

```
Nmap –sU –P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 6 passes if all ports will be reported as filtered. (By default nmap will use a source port > 1024)

(OUT_UDP) Check that the firewall blocks the outbound traffic from UDP ports not necessary for the product specification.

Test 7
Outbound UDP connection: unauthorized association between local and remote ports

Run Netcat on a remote system on the same subnet. Make it listen on a UDP port <1024 (for instance 53).

```
Nc –u –n –v –p 53 –l
```

On the print server run Netcat on port 67 UDP. Try to create a connection to the remote system.

```
Nc –u –n –v –p 67 "remote_PC_address" 53
```

Test 7 passes if the connection is blocked.

(IN_ICMP) tests
Test 8
ICMP timestamp requests should be filtered
The ICMP Time Stamp Request (Type 13) allows a node to query another for the current time.

Run nmap on a remote machine on the same subnet.
First solution: use nmap

```
  Nmap –P0 –PP xxx.xxx.xxx.xxx
```

Test 8 passes if the host doesn't respond.

Second solution use hping2

```
  Hping2 –V –c 3 –icmp –icmptype 13 xxx.xxx.xxx.xxx
```

Test 8 passes if you receive:
----- hping statistic----
3 packets transmitted, 0 packets received, 100% packet loss

Test 9
ICMP address subnet mask requests should be filtered
ICMP Address Mask Request (Type 17) will also allow to an attacker to gain knowledge about the network configuration.

Run nmap on a remote machine on the same subnet.
First solution: use nmap

```
  Nmap –P0 –PM xxx.xxx.xxx.xxx
```

Test 9 passes if the host doesn't respond.

Second solution use hping2

```
    Hping2 –V –c 3 –icmp –icmptype 17 xxx.xxx.xxx.xxx
```

Test 9 passes if you receive:

```
    ----- hping statistic----
                 2  packets transmitted, 0 packets received, 100% packet
                    loss
```

3

Consequence	**Likelihood**
High: If the firewall doesn't fulfill the expected security function, several network services may be accessible. If these services aren't correctly configured or are not up-to-date they may contain vulnerabilities (a buffer overrun vulnerability may allow remote code execution)	Medium: Tools to detect an eventual firewall misconfiguration can be easily found; the firewall is evaluated for the first time by the company and may not be correctly configured; as this is one of the main security feature of the system, it may be the prime target for attacks
Compliance The control passes if all the intermediary tests pass.	
References to source of step Auditor's personal experience. The documentation concerning the ports used by the servers and the clients included in the product specification (DOC_SERVERS_PORTS) Ofir Arkin - ICMP Usage in Scanning. The Complete Know-How	

Control no. 8	**F3: Check what happens when the firewall is not running**
Control objective: The firewall must block all traffic when not running.	**Objective-stimulus response**
Why the test is performed The system shouldn't be unprotected when the firewall is not running. If the firewall is not blocking the traffic when it doesn't run, the system is vulnerable between the system launch and the firewall start-up or if an attacker succeeds in stopping the firewall. *Reference R1.1 and R2.1*	
What test control design is to be performed Check the that the firewall blocks the traffic when it doesn't run.	

How to perform the test and condition for non-compliance
Logon as system administrator.
Double click on the VisNetic Firewall shortcut to launch the firewall management application.
Step 1: Check that
`View-> Settings-> When not running`
"`Block all traffic`" is checked.
 	
Step 2: Check that the firewall is correctly configured
From a local PC situated on the same LAN, use nmap to scan the audited system interface.
`Nmap –sT –P0 –p1-65535 xxx.xxx.xxx.xxx`
`Nmap –sU –P0 –p1-65535 xxx.xxx.xxx.xxx`
 	
The unfiltered ports should be:
`TCP 21, 80, 139, 515`
 	
Step 3: Log locally on the system with the administrator account. Disable the service corresponding to the firewall.	

Step 4: Reboot the system

Test 1

Step 5: Inbound TCP and UDP connections should be blocked

From a PC situated on the same LAN, use nmap to scan the system interface to the LAN.

```
Nmap –sT –P0 –p1-65535 xxx.xxx.xxx.xxx
Nmap –sU –P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 1 passes if all the ports are unfiltered ports.

Test 2

Step 6: Outbound TCP and UDP connections should be blocked

On a remote system run two Netcat sessions: one on TCP port 21 and another on UDP 68.

```
Nc –n –v -l -p 21
Nc –u –n –v -l -p 68
```

On the print server run Netcat on TCP port 515 and UDP port 67. Try to create connections to the remote system.

```
Nc –n -v -p 515 “remote_PC_address” 21
Nc –u -n -v -p 67 “remote_PC_address” 68
```

Test 2 passes if all the connections are blocked.

Consequence	**Likelihood**
High: If the firewall doesn’t fulfill the expected security function, several network services may be accessible. If these services aren’t correctly configured or are not up-to-date they may contain vulnerabilities (a buffer overrun vulnerability may allow remote code execution)	Medium: Tools to detect an eventual firewall misconfiguration can be easily found; the firewall is evaluated for the first time by the company and may not be correctly configured; as this is one of the main security feature of the system, it may be the prime target for attacks

Compliance

The control passes if all the intermediary tests pass.

References to source of step

NIST: Guidelines on Firealls and Firewall Policy (John Wack, Ken Cutler, Jamie Pole)

Control no. 9	**F4: Check how the firewall protects the system from attacks with unexpected TCP flags**
Control objective: The firewall should restrict the access to the ports required in the ruleset, no matter which flags are used to scan the system.	**Objective-stimulus response**

Why the test is performed

Some firewalls may watch only for the SYNs to restricted ports and may let other traffic to pass through unmolested. Some firewalls incorrectly deal with SYN, FIN, XMAS or NULL scans with tiny fragmented packets. If the firewall doesn’t fulfill its function, depending on the vulnerability that is exposed, the system integrity may be impacted (for instance the vulnerability may allow executing code on the system). *Reference R1.1*

What test control design is to be performed

Check that the traffic is allowed only on the required ports, even if the IP fragmentation and unexpected TCP flags are used.

How to perform the test

Test 1

Run nmap from a remote client against the LAN interface, using the following command:

```
Nmap –sS –P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 1 passes if the unfiltered ports are:

```
TCP 21, 80, 139, 515
```

Test 2

Run nmap from a remote client against the LAN interface, using the following commands:

`Nmap –sS –f -P0 –p1-65535 xxx.xxx.xxx.xxx –g Y` (where Y is a port available on the remote PC where nmap runs, Y<1024)

Test 2 passes if the system being audited does not respond to the previous nmap scan.

Test 3

```
Nmap –sF –P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 4

```
Nmap –sX –P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 5

```
Nmap –sN –P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 6

```
Nmap –sA –P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 7

```
Nmap –sF –f -P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 8

```
Nmap –sX –f -P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 9

```
Nmap –sN –f -P0 –p1-65535 xxx.xxx.xxx.xxx
```

Test 10

```
Nmap –sA –f –P0 –p1-65535 xxx.xxx.xxx.xxx
```

Tests 3, 4, 5, 6, 7, 8, 9, 10 pass if the system being audited does not respond to the previous nmap scans.

Consequence	**Likelihood**
Medium: If the firewall let the traffic to pass-through unmolested because the TCP flags are unexpected, the attacker may retrieve information on the services running on the system	Medium: Tools to detect that the firewall lets the traffic to pass-through unmolested can be easily found.

Compliance

The control passes if all the intermediary tests pass.

References to source of step

Horace B. Jones- Horace B. Jones - Administratively Auditing the Security Provided by Norton Personal Firewall 2002

<table>
<tr><td><b>Control no. 10</b></td><td colspan="2"><b>F5: Check how the firewall protects the system from attacks on other IP protocols and on other protocols</b></td></tr>
<tr><td colspan="2"><b>Control objective:</b>
The firewall should restrict the access to system, no matter which protocols are used to scan the system.</td><td><b>Objective-stimulus response</b></td></tr>
<tr><td colspan="3"><b>Why</b> the test is performed
Some firewalls may watch only for TCP, UDP and ICMP packets and ignore other protocols. Attacks can be launched on protocols that are not enough hardened because the firewall is supposed to protect the system. If the firewall doesn’t fulfill its function, depending on the vulnerability that is exposed, the system integrity may be impacted (for instance the vulnerability may allow executing code on the system).
<i>Reference R1.1</i></td></tr>
<tr><td colspan="3"><b>What</b> test control design is to be performed
Check that IP protocols other then TCP, UDP, ICMP and ARP are blocked.
Check that all protocols other then IP are blocked.</td></tr>
<tr><td colspan="3"><b>How</b> to perform the test
<b>Test 1</b>
Check that the protocols other then UDP, TCP, ICMP are filtered
Use hping2 to simulate a connection on another ip protocol.
<code>Hping2 –rawip –ipproto <b>IpProtocolNumber</b> –n PrintSeverIpAddress</code>
where <code>IpProtocolNumber!= 1(ICMP), 6(TCP, 17(UDP)</code>
<b>Test 1 passes</b> if the firewall logged and blocked the connection attempt.

<b>Test 2</b>
Use the documentation concerning the protocols supported by the print server (DOC_PROTOCOLS). This document says that the only supported protocol is IP. In order to double-check that no protocols other then IP are installed, logon as administrator on the print server. Right-click on the “<code>My Network Places</code>” and select “<code>Properties</code>.” Right-click on the network connection and select “<code>Properties</code>”.
<b>Test 2 passes</b> if the only protocol installed is IP.</td></tr>
<tr><td><b>Consequence</b>
Medium: It may allow exploiting vulnerable protocols and executing code on the system</td><td colspan="2"><b>Likelihood</b>
Medium: Tools to detect that the firewall lets the traffic to pass-through unmolested can be easily found</td></tr>
<tr><td colspan="3"><b>Compliance</b>
The control passes if all the intermediary tests pass.</td></tr>
<tr><td colspan="3"><b>References</b> to source of step
Auditor’s personal experience.</td></tr>
</table>

<table>
<tr><td><b>Control no. 11</b></td><td colspan="2"><b>F5: Check if the firewall detects unauthorized network activities on the system</b></td></tr>
<tr><td colspan="2"><b>Control objective:</b>
Check that the firewall logs information and the logging level is adequate.</td><td><b>Objective</b></td></tr>
<tr><td colspan="3"><b>Why</b> the test is performed</td></tr>
</table>

Insufficient logging will reduce the capacity to identify attacks and how do they happened.
This is not related to a risk identified, it derives from the “security best practices”

What test control design is to be performed
Look for the following information in the firewall log, if the log exists:

- time and date
- IP address and the destination port if the protocols are UDP or TCP

How to perform the test
Check
`View-> Settings-> Log File` to see the log file directory.

Test 1
Perform Control 9: “Check how the firewall protects the system from attacks with unexpected TCP flags”
Test 1 passes if the attacks are logged and for each attack, the following information is found:

a) time and date
b) IP address involved
c) Destination port (if the protocols are UDP or TCP)

Test 2
Perform a test verifying that the outbound connections are controlled.
Run locally Netcat to a port between 1024-65535. Try to create a connection to another Netcat running on a remote PC that listens on port 80.
Test passes if the attacks are logged and for each attack, the following information is found:

- time and date
- IP address involved
- Source and destination port (if the protocols are UDP or TCP)

Consequence	**Likelihood**
Low	Medium

Compliance
The control passes if all the intermediary tests pass.

References
Horace B. Jones, “Administratively auditing the security provided by Norton Personal Firewall 2002

4.8.3 Web server controls

Control no. 12	**W1: Check if the Web server is minimizing services (keep turned off unused features)**
Control objective: It shouldn’t be allowed to remotely put or delete resources in the web server document root.	**Objective**
Why the test is performed The HTTP PUT method allows updating information on the server or even creating a new resource on the server. In order to update files on the server, the servlet that will offer this method must have enough permission to write or create the content file. A bug or a security hole in one of the other servlets would allow an Intranet user to change any of the files. Depending on the files that can be changed, this may allow defacing the web server pages, denial of services or even corrupting the system integrity if other vulnerabilities coexist (for instance directory traversal problems). The same risks apply to the HTTP DELETE method. *Reference R1.10(T1.3-T1.5)*	
What test control design is to be performed Verify the web server configuration to be sure that here are no “putable” or “allow-delete” resources in the web server document root. Confirm using Nessus that no PUT or DELETE methods are implemented. “Test HTTP dangerous methods” (from the Remote File Access family)	

How to perform the test
Look for http-server.props in the directory where Jigsaw is installed.
Retrieve the configuration directory for the server (corresponds to `org.w3c.jigsaw.config`). We will name it CONFIG_DIR.
In `$CONFIG_DIR\stores\root.xml` check for every resource that the attributes “`putable`” and “`allow-delete`” are set to false.
 	
For instance:
`<attribute name='allow-delete' flag='2'`
`class='org.w3c.tools.resources.BooleanAttribute'>false</attribute>`
`<attribute name='putable' flag='2'`
`class='org.w3c.tools.resources.BooleanAttribute'>false</attribute>`
Test passes if no “`putable`” or “`allow-delete`” resource is found.
Run Nessus (see the test corresponding to: “W6 Evaluate Web server security with a vulnerability scanner” for details on how to do it). Select “`Test HTTP dangerous methods`” (from the `Remote File Access` family)	

Consequence High: If sensitive OS files can be replaced or if the virtual directories –aliases are mapped to directories from which the binaries are automatically launched, especially if the web server runs with	**Likelihood** Medium: web browsers allowing to put files on the web server can be found on the web; as this is the first security audit for this product the likelihood that the server isn’t correctly configured can’t be considered as low

administrative privileges and the web server didn’t correctly impersonate the remote web server users	
Compliance Control passes if no PUT or DELETE methods are found.	
References to source of step David Rhoades in his “Auditing web-based application” SANS track Auditor’s personal experience	
Remark Example of tools allowing HTTP PUT: Winie (HTTP/1.1 PUT Tool)	

Control no. 13	**W2: Check the filesystem ACLs on web server directories**
Control objective: Appropriate ACLs should be set on the web server’s directories	**Objective**
Why the test is performed 1a) If any user can view web server configuration and administration files, he may gain information needed to break into the system (*Reference R1.10: T1.5*). 1b) If everybody can write the web server configuration and administration files he may put the server in a less secure mode where the system integrity can be easily corrupted (*Reference R1.10: T1.3, T1.5*). 2a) If everybody can read the log files, a knowledgeable remote user can find out every access that anyone's made to the server (*Reference R1.10: T1.5*). 2b) If everybody can write the web server log files he may hide information needed to diagnose an attack. 3) Every servlet (or similar) that gets launched with administrative permissions will have access everywhere in the system and may corrupt system integrity. If everybody can add new servlets the system integrity may be impacted. (*Reference R1.10: T1.3, T1.5*) The same risk is encountered with cgi-bin directory but in order to add a CGI script adding the file in this directory is not enough to have the script executed. One also needs to access to the web server administration in order to add a new GCI script. 4) If everybody can write the document root, new web pages may be added or the existing one may be modified. This may cause bad reputation if the web server pages are defaced or denial of service (*Reference R1.10: T1.3*). 5) Aliases may expose sensitive files. Depending on the access that it is allowed (read/write) sensitive information may be revealed or worse, sensitive files may be corrupted. The system integrity may be impacted (*Reference R1.10: T1.3, T1.5*). 6) Someone may add code to the web server via CLASSPATH environment variable, if this variable contains a world/group writable directory. The system integrity may be impacted (*Reference R1.10: T1.3*).	
What test control design is to be performed 1a) and 2a) The server root configuration and log directories should not be world readable.	

1b) and 2b) The server root configuration and log directories should be set up so that only the Web administration/webmaster can write to the configuration and log directories and to their contents.
3) The directory where the servlets are placed and its contents should be world executable and readable, but not writable. Same for cgi-bin directory.
4) The document root must be readable by the server while it is running under the permissions of a standard user. Therefore the document root directory and its subdirectories should be owned by the group of web pages authors (administration/webmaster included), world readable, and group writable.
5) Check if aliases are used. For every alias check the physical directory sensitivity. If this directory contains sensitive files that may impact on the system integrity they shouldn't be word readable and writable.
6) Check that CLASSPATH environment variable points to directories that are not world/group writable.

How to perform the test
Use the documentation containing all the directories used by the web server (DOC_SERVERS_DIRS_USERS) in order to retrieve:

- configuration directory for the server; it will be referenced as CONFIG_DIR.
- web server directory; it will be referenced as SERVER_ROOT_DIR.
- log directory for the server; it will be referenced as LOG_DIR
- web server document root directory; it will be referenced as DOC_ROOT_DIR.
- server administration configuration directory it will be referenced as CONFIG_ADMIN_DIR.
- any directory containing servlets and CGI scripts ; it will be referenced as SERVLETS_DIRi and CGI-BIN_DIR
- any directory included in CLASSPATH environment variable; it will be referenced as CLASSPATHi (CLASSPATH1, CLASSPATH2, …, it depends on the number of directories included in the CLASSPATH environment variable)

In the `$CONFIG_DIR\stores\root.xml` look for the resource `PassDirectory` (corresponds to `org.w3c.jigsaw.resources.PassDirectory`). Retrieve the directory name corresponding to the attribute "`pass-target`" ("`org.w3c.tools.resources.FileAttribute`">PHYSICAL_DIRECTORY)

There are "special accounts": administrator accounts, system accounts and web master account.

Test 1
Check config dir permissions

```
dumpsec /rpt=dir=$CONFIG_DIR /showexceptions /saveas=fixed /noheader
/showall /outfile=dumpsec_dir_config.txt
dumpsec /rpt=dir=$CONFIG_ADMIN_DIR /showexceptions /saveas=fixed
/noheader /showall /outfile=dumpsec_dir_admin_config.txt
```

Test 1 passes if in `dumpsec_dir_config.txt` and `dumpsec_dir_admin_config.txt` for every account other than special accounts no permission is displayed in the Dir and File colons.

Test 2

Check log dir permissions

```
dumpsec /rpt=dir=$LOG_DIR /  showexceptions /saveas=fixed /noheader
/showall /outfile=dumpsec_dir_logs.txt
```

Test 2 passes if in `dumpsec_dir_logs.txt` for every account other than special accounts no permission is displayed in the Dir and File colons.

Test 3

Check servlets and cgi-bin dir permissions

Check where on the document root the servlets are placed. For each directory containing servlets, do:

```
 dumpsec /rpt=dir=$SERVLETS_DIR /showexceptions /saveas=fixed /noheader
/showall /outfile= dumpsec_servlets_dir.txt
dumpsec /rpt=dir=$CGI -BIN /showexceptions /saveas=fixed /noheader
/showall /outfile= dumpsec_cgi -bin_dir.txt
```

Test 3 passes if in `dumpsec_servlets_dir.txt dumpsec_cgi-bin_dir.txt` and for every account other than special accounts the following permissions aren't displayed in the Dir and File colons:

- `W, D,      P, O, All`
- if `axhhhhhhh` is displayed (corresponds to non-standard allow permissions or audit settings), use the "`Advanced Security Settings -> EffectivePermissions`" (accessible from the folder `Properties-> Security icon`) to verify that the following permissions aren't granted: `Create Files/Write Data, Create Folders/Append Data, Write Attributes, Write Extended Attributes, Delete Subfolders and Files, Delete, Change Permissions, Take ownership`

Test 4

Check doc root permissions

```
dumpsec /rpt=dir=$DOC_ROOT_DIR /showexceptions /saveas=fixed /noheader
/showall /outfile=dumpsec_dir_doc_root.txt
```

Test 4 passes if in dumpsec_dir_doc_root.txt for every account other than special accounts the following permissions aren't displayed in the Dir and File colons:

- `W, D,     P, O, All`
- if `axhhhhhhh` is displayed verify that the following permissions aren't granted: `Create Files/Write Data, Create Folders/Append Data, Write Attributes, Write Extended Attributes, Delete Subfolders and Files,  Delete, Change Permissions, Take ownership`

Test 5

Check aliases permissions

```
dumpsec /rpt=dir=$PHYSICAL_DIRECTORY /showexceptions /saveas=fixed
/noheader /showall /outfile=dumpsec_phys_dir.txt
```

The "extended accounts" contain: "special accounts" + an authenticated user account that may have read or write rights on the directory where the alias points.

Test 5 passes if in `dumpsec_phys_dir.txt` for every account other than "extended accounts**"** the following permissions aren't displayed in the Dir and File colons:

`- W, D,      P, O, All`

- if `axhhhhhhh` is displayed verify that the following permissions aren't granted: `Create Files/Write Data, Create Folders/Append Data, Write Attributes, Write Extended Attributes, Delete Subfolders and Files, Delete, Change Permissions, Take ownership`

Test 6

Check CLASSPATH pointed dirs permissions

For each directory CLASSPATHi pointed to by the CLASSPATH environment variable, do:

```
dumpsec /rpt=dir=$CLASSPATHi /showexceptions /saveas=csv /noheader
/showall /outfile=dumpsec_DIRi.t xt
```

Test 6 passes if in `dumpsec_DIRi.txt` for every account other than special accounts the following permissions aren't displayed in the Dir and File colons:

`- W, D,      P, O, All`

- if `axhhhhhhh` is displayed (corresponds to non-standard allow permissions or audit settings), use the "`Advanced Security Settings -> EffectivePermissions`" (accessible from the folder `Properties-> Security icon`) to verify that the following permissions aren't granted: `Create Files/Write Data, Create Folders/Append Data, Write Attrib utes, Write Extended Attributes, Delete Subfolders and Files, Delete, Change Permissions, Take ownership`

Consequence	**Likelihood**
High: If malicious servlets can be add to the web server they may allow exposing sensitive information-> impact Medium; if new classes may be added to the web server the system integrity may be impacted-> High	Medium: tools allowing HTTP traffic interception and modification are available on the web; furthermore, this product contains several servers that allow putting/retrieving files on/from the system; as this is the first security audit for this product the likelihood that the server isn't correctly configured can't be considered as low

Compliance

The control passes if all the intermediary tests pass.

References to source of step

World Wide Web security FAQ hosted at http://www.w3.org/Security/Faq/wwwsf3.html

David Rhoades in his "Auditing web-based application" SANS track

Control no. 14	**W3: Check the Web server logging level**
Control objective: The Web server logging should be enabled and the appropriate level of information should be retrieved from the Web server logs	**Objective**

Why the test is performed

If the Web server log isn't enabled it will not be possible to diagnose or prove successful attacks against the server.

This is not related to a risk identified, it is a rule from the "security best practices"

What test control design is to be performed Check that the web server's logs allow retrieving the proofs of a web server vulnerability scan.	
How to perform the test Use the documentation containing all the directories used by the web server (DOC_SERVERS_DIRS_USERS) in order to retrieve the log directory for the server. It will be referenced as LOG_DIR Perform a web server vulnerability scan using Nessus (please see the control number 16: W5 Evaluate web server security with two vulnerability scanners" to see how to configure Nessus in order to perform this scan).. Go to: $ LOG_DIR and check that the scan was logged and that the attacker IP address and the requested URL are recorded.	
Consequence Low	**Likelihood** Medium
Compliance The control passes if a web server vulnerability scan is logged.	
References to source of step David Rhoades in his "Auditing web-based application" SANS track	

Control no. 15	**W4: Evaluate Web server security with two CGI scanners**	
Control objective: Use two up-to-date CGI scanners to check that no default and unjustified material is found.		**Objective**
Why the test is performed The default material provided to assist the web administrator in testing the web server can be dangerous if it is left on the server after it is deployed into production. This material may contain for instance insufficiently hardened CGI scripts. *Reference R1.4: T1.2, T1.4, T1.6*		
What test control design is to be performed Use a GCI scanner to test various CGIs and material included with the base install of the web server.		
How to perform the test Use N-Stealth and Nikto to perform CGI scanning. For N-Stealth in the `ScanRule` menu check "`Complete scan`". For Nikto use the following command line: `Nikto –allcgi –generic –host printServerIpAddress –nolookup –output resFile.log –port PortValue –version`		
Consequence High: Every script that gets launched with administrative permissions will have access everywhere in the system	**Likelihood** Medium: Tools to detect eventual vulnerabilities can be found easily; the web servers CGI exploits in general and the default material problems are well-known and they are prime targets for attacks; the likelihood is not considered as High because this	

and may corrupt system integrity	web server isn’t not well known and by default no CGI scripts are installed
Compliance The control passes if any default material found by the CGI scanner is justified by the product specification.	
References to source of step David Rhoades- Auditing Web servers and applications- SANS track	

Control no. 16	**W5: Evaluate Web server security with two vulnerability scanners**
Control objective: Use two up-to-date vulnerability scanners to check that no medium and high risk known vulnerabilities are detected for web server	**Objective**
Why the test is performed Security problems found in the web server may allow taking control over the server and compromising system security. *Reference R1.4: T1.2, T1.4, T1.6*	
What test control design is to be performed No high or medium security vulnerability not related to the product specification must be found by the vulnerabilities scanners. No security problems (bugs) should be detected.	
How to perform the test Run the Nessus client. Create a new session. Right click on the new session and: step1: choose “`Connect`” in order to connect to Nessus server step 2: choose “`Properties`” to configure the session. From the “`Plugins`” window check “`Use session-specifig plugin set`” and click on “`Select plugins`”. In the pluggins list, start by “`Disable all`” and then enable the following plugins families: • `CGI abuses, Misc, Denial of services, Gain Root remotely, General, Settings, Remote File Access` step4: choose “`Execute`” to perform the scan. Step5: when the sac is finished, from the “Manage Session Results” choose “`Export`” to generate the scan report. Run Retina. From `Tools-> Policies` For `Policies` choose “`Complete Scan`” , check `CHAM HTTP` and uncheck everything else For `Ports`- uncheck “`Perform Full Scan`” For `Audits` choose the following families: • `CGI scripts, CHAM, DoS, Miscellaneous` • `Web servers` When the scan is completed choose `Tools->Reports` to generate the scan report.	
Consequence High: Every script that gets launched with administrative	**Likelihood** High: Tools to detect eventual vulnerabilities can be easily found; even if

permissions will have access everywhere in the system and may corrupt system integrity-> High; the directory traversal access may reveal sensitive information-> Medium	this web server is not well-known it may have errors related to general HTTP commands implementation
Compliance The control passes if no medium and high level alerts are generated.	
References to source of step David Rhoades- Auditing Web servers and applications	

Control no. 17:	**W6: Check the Web server permissions**
Control objective: The Web server shouldn't run with administrative privileges.	**Objective**
Why the test is performed If a remote attacker gains access on the Web server or manages to trick the server in performing malicious actions, the harm that he can generate in the system depends on the Web server rights. *Reference R1.4: T1.2, T1.4, T1.6, R1.10: T1.3, T1.5*	
What test control design is to be performed Check that the Web server isn't run with administrative privilege.	
How to perform the test Use the documentation concerning all the virtual directories used by the servers and the user accounts (DOC_SERVERS_DIRS_USERS) to retrieve the name of all OS users and their privileges. Logon as one of the OS users. On the print server use "`tasklist`" command to obtain information about all the running processes. `tasklist /v   > tasklist_verbose.txt` Check the user name for the Web server process.	
Consequence High: Even if the server runs by default with administrative privileges, the threads deserving remote user's requests must take the remote user credentials (user impersonalisation). Errors in the user impersonalisation process may reveal sensitive information-> Medium; if the server runs with administrative privileges, any code added to server because the CLASSPATH isn't correctly protected allows executing attacker code with administrative access and the impact is High	**Likelihood** Low: It is not easy to detect remotely if the web server runs with administrative privileges
Compliance The control passes if the user name doesn't correspond to an administrative account (the user shouldn't be NT AUTHORITY\SYSTEM or	

PrintServerName\Administrator or PrintServerName \UserWithAdminRights).
References to source of step Auditor’s personal experience.

Control no. 18:	**W7: Check that the JavaVirtual Machine is up-to-date**
Control objective: The java virtual machine used to run the web server should be up-to-date	**Objective**
Why the test is performed As the web server runs in a java virtual machine, the server security depends on java virtual machine security. Furthermore, the virtual machine is the guarantee that no buffer overflow exploits may happen for this server. Consequently, a security bug in the virtual machine is critical for the system integrity. *Reference R1.4: T1.2, T1.4, T1.6*	
What test control design is to be performed Check that the Java Virtual Machine version running on the server has the latest security patches.	
How to perform the test In order to check the java machine version used by the web server: Use the documentation concerning the directory where the java virtual machine runs (DOC_SERVERS_DIRS_USERS). This directory will be referenced as DIR_SERVER_JAVA_MACHINE. This documentation should also specify which java virtual machine uses. This print server uses the SUN JRE. Type: `% DIR_SERVER_JAVA_MACHINE%\java.exe -version` Record the value returned. Check on the web the version of the last java virtual machine and the security patches included.	
Consequence High: The virtual machine guaranties that buffer overruns can’t appear in a java web server; if this is not the case, the buffer overrun allows adding code on the system the impact is High	**Likelihood** Low: It is not easy to detect the version of the virtual machine used by the web server (unless if the web application is not using applets and is not issuing a message requiring a given java machine version for the client system
Compliance Test passes if either the last virtual machine version is applied or the time between the new version and the start of the consolidation tests is smaller then 3 month. If the new virtual machine version contains security bugs correction, the interval is reduced to two weeks.	
References to source of step Auditor’s personal experience.	

4.8.4 SMB server controls

Control no. 19	**SMB1: Check the shares exposed by the SMB server**
Control objective: Only PRINT$, IPC$ and PRINTQUEUES shares should be exposed and appropriate ACLs should be set	**Objective**
Why the test is performed SMB shares are prime targets for attacks due to SMB protocol vulnerabilities and number of security patches issued monthly by Microsoft. If the server allows putting or removing files in/from sensitive folders, the system integrity may be compromised by removing a sensitive file or by introducing a malware in the system. If sensitive files can be retrieved remotely they may reveal information that facilitates further attacks against the system. *Reference R1.9: T1.3, T1.5*	
What test control design is to be performed Only the SMB shares mandatory for SMB printing should be exposed and ACLs should be set appropriately(IPC$ admin only, PRINT$ allows everyone to read only, Print queues: everyone can read/write)	

How to perform the test
From a PC on the same LAN use `DumpSec` to list the shares and the permissions assigned to those shares:
`dumpsec printServerIpAddress /rpt=shares /saveas=csv /noheader /outfile=dumpsec_shares.txt`
Test passes when in the `dumpsec_shares.txt` contains:
`IPC$= (special admin share),      , admin -only (no dacl)`
`Print$ Everyone read`
`ForEachPrintQueue Everyone all`
Where `ForEachPrintQueue` represents every print queue that the print server exports	

Consequence High: If sensitive OS files can be replaced or if the shares are mapped to directories from which the binaries are automatically launched	**Likelihood** Medium: SMB clients allowing to put files on the server are included in all Windows systems; as this is the first security audit the likelihood that this server is misconfigured can't be considered as low
Compliance This control passes if `DumpSec` result shows only the minimal shares with the minimal permissions allowing everyone to print (as specified in the previous lines).	
References to source of step Auditor's personal experience.	

Control no. 20	**SMB2: Evaluate SMB server security with two vulnerability scanners**

Control objective: Use two up-to-date vulnerability scanners to check that no medium and high risk known vulnerabilities are detected for the SMB server	**Objective**

Why the test is performed

Known security vulnerabilities will increase the chances that the SMB server is hacked. Security problems found in the SMB server may allow taking control over the server and compromising system security.

Reference R1.5: T1.2, T1.4, T1.6

What test control design is to be performed

No high and medium level security vulnerability not related to the product specification must be found by the vulnerabilities scanners. No security problems (bugs) should be detected.

How to perform the test

Run Retina and Nessus against the system.

Run the Nessus client. Create a new session. Right click on the new session and:

step1: choose “`Connect`” in order to connect to Nessus server

step 2: choose “`Properties`” to configure the session. From the “`Plugins`” window check “`Use session-specifig plugin set`” and click on “`Select plugins`”. In the pluggins list, start by “`Disable all`” and then enable the following plugins families:

- `Windows, Windows: user management, RPC, Gain Root remotely`

step4: choose “`Execute`” to perform the scan.

step5: when the scan is finished, from the “`Manage Session Results`” choose “`Export`” to generate the scan report.

Run Retina. From `Tools-> Policies`

For Policies choose “`Complete Scan`” and uncheck everything else

For `Ports`- uncheck “`Perform Full Scan`”

For `Audits` choose the following families:

- `Accounts, Netbios, Registry, Remote access, RPC services`

Consequence High: If a buffer overrun can be exploited it may allow code execution or privilege elevation	**Likelihood** High: Based on the number of tools allowing to detect and exploit vulnerabilities

Compliance

This test passes if no medium and high risk vulnerabilities are found for the SMB server. The false positives and the settings mandatory for the server to be compliant with the product specifications are excluded from the high and medium risk vulnerabilities.

References to source of step

Auditor’s personal experience.

4.8.5 FTP server controls

Control no. 21	**FTP1: Check FTP server virtual directories ACLs**

Control objective: Verify that virtual directories have correct ACLs.	**Objective**

Why the test is performed

If the server allows putting or removing files in/from sensitive folders, the system integrity may be compromised by removing a sensitive file or by introducing a malware in the system.

If sensitive files can be retrieved remotely they may reveal information that facilitates further attacks against the system integrity.

A writable directory mapped to the Start-up folder may allow an attacker to execute code on the system.

Reference R 1.8: T1.3, T1.5

What test control design is to be performed

For each remotely accessible FTP directory, check that no OS sensitive files are exposed (dlls and executables) and that it is not possible to retrieve files from write only directories and that we can't write files in read only directories.

Check that, no writable directories aren't mapped to a Start-up folder.

How to perform the test

Use the documentation concerning all the virtual directories used by the servers and the user accounts (DOC_SERVERS_DIRS_USERS) to retrieve the name of the FTP server users.

This document mentioned that:

- This server has one user: the anonymous user.
- The virtual directories are not mapped to physical filesystem directories. Consequently, the tests if the writable directories are mapped to a Start-up folder, are not applicable.

On a remote station, use a FTP client to log on the system.

```
ftp printServerIpAddress
user anonymous
password anonymous
dir
```

(to see the virtual directories)

Test 1

`cd readableDir` (for each read only folder)

`put file1` (if it is a directory specified to be readable only)

`dir` (to see if sensitive OS files are included)

Test 1 passes if no file can be added in this directory and no OS sensitive files are included.

Test 2

`cd ..`

`cd writeableDir` (for each read only folder)

`get file1` (if it is a directory specified to be write only)

Test 2passes if no file can be retrieved from this directory.	
Consequence High: If sensitive OS files can be replaced or if the virtual directories are mapped to directories from which the binaries are automatically launched	**Likelihood** Medium: The FTP clients are common tools included in most of the clients (Windows or Unix platforms); as this is the first security audit for this product the likelihood that the server isn’t correctly configured can’t be considered as low
Compliance The control passes if all intermediary tests pass.	
References Auditor’s personal experience	

Control no. 22	**FTP2: Check that FTP server has no well-known security vulnerabilities**
Control objective: Use two up-to-date vulnerability scanners to check that no medium and high risk known vulnerabilities are detected for the FTP server	**Objective**
Why the test is performed Known security vulnerabilities will increase the chances that the FTP server is hacked. Security problems found in the FTP server may allow taking control over the server and compromising system security. For instance if the server allows accessing sensitive directories by exploiting directory traversal vulnerabilities, sensitive files can be remotely be retrieved and information to perform further attacks can be obtained. Even worse, sensitive files may be deleted,replaced or malwares can be installed in these directories. The FTP bounce attack can allow laundering connections through an FTP server by abusing the support for “proxy” FTP connections (use the anonymous FTP server on the print server in order to hide the attacker true address). *Reference R 1.11: T1.4, T1.6*	
What test control design is to be performed No high and medium level security vulnerability not related to the product specification must be found by the vulnerabilities scanners. No security problems (bugs) should be detected. The bounce scanning attack against the print server should fail.	
How to perform the test **Test 1** Run the Nessus client. Create a new session. Right click on the new session and: step1: choose “`Connect`” in order to connect to Nessus server step 2: choose “Properties” to configure the session. From the “`Plugins`” window check “`Use session-specifig plugin set`” and click on “`Select plugins`”. In the plug-in list, choose “`Enable all`” from the FTP family: **Test 1passes** if no medium and high risk vulnerabilities are found for the FTP server.	

Test 2 Run Retina. From `Tools-> Policies` For `Policies` choose "`Complete Scan`" and uncheck everything else For `Ports`- uncheck "`Perform Full Scan`" For `Audits` choose the plugins from the FTP family. **Test 2 passes** if no medium and high risk vulnerabilities are found for the FTP server. **Test 3** Launch a bounce attack using nmap: `Nmap –b PrintServerName –sT O victim` **Test 3 passes** if bounce attack fails.	
Consequence High: If sensitive OS files may be replaced or the directories from which the binaries are automatically launched can be accessed due to directory traversal	**Likelihood** High: Tools allowing to find vulnerabilities are widely available; once the vulnerability found FTP clients allowing to put files on the server are included in most of the clients (Unix or Windows platforms)
Compliance This test passes if no medium and high risk vulnerabilities are found for the FTP server. The false positives and the settings mandatory for the server to follow the product specifications are excluded from the high and medium risk vulnerabilities.	
References Auditor's personal experience. "Hacking exposed"-Third Edition- by Stuart McClure, Joel Scambray and George Kurtz (McGraw-Hill/Osborne LittleWolf(a.k.a. Dennis W. Mattison -"Network Printer and Other Peripherals-Vulnerability and fixes"	
Remark This server has a proprietary implementation. For this reason, most of the security bugs related to other FTP servers (like buffer overflows) aren't applicable. However, general FTP server implementation errors may still be found.	

Control no. 23:	**FTP3: Check FTP server permissions**
Control objective: The FTP server shouldn't run with administrative privilege	**Objective**
Why the test is performed If a remote attacker gains access on the FTP server or manages to trick the server in performing malicious actions, the harm that can be generated in the system depends on the FTP server rights. *ReferenceR1.8, R1.11*	
What test control design is to be performed Check that the FTP server isn't run with administrative privilege.	
How to perform the test	

Use the documentation concerning all the virtual directories used by the servers and the user accounts (DOC_SERVERS_DIRS_USERS) to retrieve the name of all OS users and their privileges. Logon as one of the OS users. On the print server use “tasklist” command to obtain information about all the running processes. `tasklist /v   > tasklist_verbose.txt` Check the user name for the FTP server process.	
Consequence High: If the server runs with administrative privileges, the errors in the FTP server configuration or implementation may allow an attacker to gain administrative privileges over the system	**Likelihood** Low: It is not easy to detect remotely if the FTP server has administrative privileges
Compliance The control passes if the user name doesn’t correspond to an administrative account (the user shouldn’t be NT AUTHORITY\SYSTEM or PrintServerName\Administrator or PrintServerName \UserWithAdminRights).	
References to source of step Auditor’s personal experience.	

4.8.6 PostScript interpreter controls

Control no. 24	**PS1: Check how the PostScript interpreter controls access to information**
Control objective: It should not be possible to retrieve information on file system partitions using a PostScript file	**Objective**

Why the test is performed
In PostScript it is possible to access by reference all drives (C:/...). A standard PostScript device exists for that: "%os%" that you can use as "%os%c:/*". This allows people to
access resources installed on the print server. A remote user may use system partition information to break the system (for instance exploiting a directory traversal vulnerability).
Reference R1.7: T1.3, T1.5

What test control design is to be performed
Check that the interpreter implementation doesn't allow enumerating system partitions.

How to perform the test
Prepare a PostScript file that will output on printed pages all the file system disks seen by the PostScript interpreter, try to browse the disk and try to browse a root drive (for instance C:\) and output the result in the same printed pages.

This PostScript file allows retrieving information on every disk of a PostScript interpreter that respects Adobe's PostScript reference. The auditor deliberately chosen not to give the entire PostScript file because it may allow finding vulnerabilities in other PostScript interpreters. The auditor wants to avoid entering any debate concerning publishing exploits. However, the auditor supplied parts of this file in order to prove that the test was realized and to give an indication about the commands that should be tested in order to detect PostScript security vulnerabilities.

This test will test the **filenameforall** operator capabilities.
The PostScript file should contain the following steps
a) enumerate all the disk seen by the PostScript interpreter

```
/devarray
[    (*) {dup length string copy}
    50 string /IODevice  resourceforall
] def
```

b) for each file system disk display the access type that should be allowed and perform several actions

```
 (devarray {==} forall)
 devarray
{
    /device_name exch def
    ..............................................
    {
       /DevParams device_name currentdevparams def
       DevParams /Type  get /FileSystem eq { DevParams /Writeable get
```

```
         {( writeable) concat_str} {( readonly) concat_str} ifelse } {}
         ifelse
       dup print (\n) print shownl
       list_device
       test_drive
 } forall
```

b1) list the files in the disk

```
/list_device
{
……………..
    device_name (*) concat_str { Count 10 le {dup == 1024 string cvs
shownl /Count Count 1 add def} if } 1024 string filenameforall
} def
```

b2) list the files in the drive C:\

```
/test_drive
{
……………………
    device_name (C:/*) concat_str { Count 10 le {dup = = 1024 string cvs
shownl /Count Count 1 add def} if } 1024 string filenameforall
} def
```

Consequence	**Likelihood**
Medium: If the attacker can gain information about the system because the PostScript disks contain OS sensitive files	Medium: The standard PostScript language is supported and the reference manual specifies how to use the security relevant commands

Compliance

The control passes if the files that are listed are not OS dlls or binaries and the root drives can't be browsed

References to source of step

Auditor's personal experience.

Control no. 25	**PS2: Check PostScript directories ACLs**
Control objective: The access rights on PostScript file system should be set appropriately	**Objective-stimulus response**

Why the test is performed

In PostScript it is possible to Create, Copy, Overwrite or Delete files, as well as Read content of a file and print it.

If the PostScript interpreter allows accessing sensitive directories and the file system rights aren't set correctly, sensitive files may be remotely retrieved and information to perform further attacks can be obtained. Even worse, sensitive files may be deleted or replaced or malwares can be installed in these directories.

Reference R1.7: T1.3, T1.5

What test control design is to be performed

For each disk seen by the PostScript interpreter, check that it is not possible to write, delete and rename files from a readonly disk. Check also that the files that it is not possible to read, overwrite, rename or create OS sensitive files (dlls and executables). Check that the writable PostScript disks are not executable.

How to perform the test

Prepare a PostScript file that will output on several printed pages all the file system disks seen by the PostScript interpreter. Try to open/delete/rename files from every disk and output the result in the same printed pages.

This test will test the **file**, **deletefile**, **renamefile** operator capabilities.
This test uses the same PS file as for the Control 24: “PS1: Check how the PostScript interpreter controls access to information”. For every disk, try to create a file, delete a file and rename a file.

```
/test_open
{
    {device_name (toto) concat_str (w)  file pop} stopped
} def

/test_delete
{
    {file_delete deletefile} stopped
} def

/test_rename
{
    {file_rename device_name (titi) concat_str renamefile} stopped
} def
```

Test passes if it is not possible to create, delete, rename file in the disks flagged as readonly and in every disk the OS sensitive files can’t be created, deleted, and renamed.

Consequence	**Likelihood**
High: If the PostScript disks contains OS sensitive files that can be replaced	Medium: The standard PostScript language is supported and the reference manual specifies how to use the security relevant commands

Compliance

Control passes if all intermediary tests pass.

References to source of step

Auditor’s personal experience.

Control no. 26	**PS3: Check PostScript interpreter directory traversal access**

Control objective: Parent relative access from the PostScript interpreter should be forbidden	**Objective**

Why the test is performed

If the PostScript interpreter allows accessing sensitive directories by using parent relative access and the file system permissions aren’t correctly set, sensitive files may be remotely retrieved and information to perform further attacks can be

obtained. Even worse, sensitive files may be deleted or replaced or malwares can be installed in these directories.
Reference R1.12: T1.4, T1.6

What test control design is to be performed
Check that the interpreter implementation doesn't allow to traverse the directories up to the root drive.

How to perform the test
Prepare a PostScript file that will output on a bitmap all the file system disks seen by the PostScript interpreter. From every disk try to traverse one level up and output the result in the bitmap.

This test will test "../ ." path relative access.
This test uses the same PS file as for the Control 23: "PS1:Check how the PostScript interpreter controls access to information". For every disk, we will try to traverse one level up to the root drive. If this is possible the first 10 files from the upper level directory will be displayed.

```
/test_parent
{
    /Count 0 def
    device_name (../*) concat_str { Count 10 le {dup == 1024 string cvs
shownl /Count Count 1 add def} if } 1024 string filenameforall
} def
```

Consequence	**Likelihood**
High: If sensitive OS files can be replaced or if the directories from which the binaries are automatically launched can be accessed due to directory traversal access	Medium: The standard PostScript language is supported and the reference manual specifies how to use the security relevant commands

Compliance
The control passes if it is not possible to go one level up to the root drive.

References to source of step
Auditor's personal experience.

Control no. 27	**PS4: Check PostScript interpreter permissions**

Control objective: PostScript interpreter shouldn't run with administrative privilege.	**Objective**

Why the test is performed
If a remote attacker manages to trick the PostScript interpreter in performing malicious actions, the harm that he can generate in the system depends on the interpreter rights.
Reference R1.7, R1.12

What test control design is to be performed
Check that the interpreter isn't run with administrative privilege.

How to perform the test
Use the documentation concerning all the virtual directories used by the servers and the user accounts (DOC_SERVERS_DIRS_USERS) to retrieve the name of all OS users and their privileges.
Logon as one of the OS users.

On the print server use “`tasklist`” command to obtain information about all the running processes.

```
tasklist /v   > tasklist_verbose.txt
```

Check the user name for the PostScript interpreter process.

Consequence	**Likelihood**
High: If the PostScript interpreter runs with administrative privileges, the errors in the interpreter configuration or implementation may allow an attacker to gain administrative privileges over the system	Low: It is not easy to detect remotely if a PostScript interpreter has administrative privileges

Compliance
The control passes if the user name doesn’t correspond to an administrative account
(the user shouldn’t be NT AUTHORITY\SYSTEM or PrintServerName\Administrator or PrintServerName \UserWithAdminRights).

References to source of step
Auditor’s personal experience.

4.8.7 Malware execution controls

Control no. 28	**MAL1: Check that no directories simultaneously writable and readable are exposed by the print server**
Control objective: The print server should not expose for the regular users simultaneously readable and writable directories .	**Objective**

Why the test is performed

A malicious file can be put on the system and retrieved from the same directory by an innocent user.

Reference R2.6: T2.4

What test control design is to be performed

No directories simultaneously readable and writable should be exposed for the normal users.

How to perform the test

Use the documentation concerning all the virtual directories used by the servers and the user accounts (DOC_SERVERS_DIRS_USERS) to retrieve the name of all servers exposing directories.

This document specifies that there are two servers exposing folders to the regular users:

- FTP server
- Windows SMB server (exposes print drivers and print queues)

Test 1

For the FTP server:

On a remote station, use a FTP client to log on the system.

```
ftp printServerIpAddress
user anonymous
password anonymous
dir                          (to see the virtual directories)
```

Test 1 passes if no directories with read and write access are listed.

Test 2

For the SMB server:

From a PC on the same LAN use DumpSec to list the shares and the permissions assigned to those shares:

```
dumpsec printServerIpAddress /rpt=shares /saveas=csv /noheader
/outfile=dumpsec_shares.txt
```

Test 2 passes when in the dumpsec_shares.txt contains:

```
IPC$= (special admin share),        , admin -only (no dacl)
Print$ Everyone read
ForEachPrintQueue Everyone all
```

Where `ForEachPrintQueue` represents every print queue that the print server exports

The print queues are simultaneously writable and readable but this is not a problem. The users can only see the description of the jobs submitted by another user. They can not retrieve the job.

Consequence	**Likelihood**
High: The malware may compromise the	Medium: This system includes several servers that may allow putting/retrieving files to/from the system without

customer network	any access control; providing a read and write share for anonymous users constitutes a risk because: - an attacker may craft special PostScript file that can be downloaded by innocent users - an attacker may even put an executable and hope that innocent users, not aware that they are accessing a print server, retrieve and execute it However, the user must execute these files in order to infect its system.
Compliance The control passes if all the intermediary tests pass.	
References to source of step Auditor's personal experience.	

Control no. 29	**MAL2: Check that no code can be executed in every writable directory exposed by the print server**
Control objective: The print server should not allow executing code in the exposed writable directories	**Objective-stimulus response**

Why the test is performed

In any place on the system where files can be anonymously added, it must be not possible to execute them. This will reduce the risk to have malicious code executed on the system.

Reference R2.2: T2.2

What test control design is to be performed

No writable and executable directories should be accessible.

How to perform the test

Use DOC_SERVERS_DIRS_USERS to obtain:

- the physical mapping for every FTP server virtual directory; this document specifies that there is no physical mapping for the FTP folders;
- the physical mapping for the SMB server shares; this document specifies that the only writable SMB shares are the print queues;
- the physical mapping for the spool directories (the directories were the print jobs arrive); they will be referenced as DOC_SPOOL_DIRS

Use DOC_PS to obtain:

- the physical mapping for every writable PostScript disk; they will be referenced as DOC_PS_DIRS

Test 1

<u>Check FTP</u>

Use an ftp client to put nc.exe (Netcat) on the system, on every writable folder.

```
put  FOLDER_CONTAINING_NC\nc.exe
```

For every writable folder, log on the print server with administrative privileges. Search everywhere in the system for nc.exe (these program is not supposed to be on the system; if it is found somewhere it means that the FTP client just add it).

Test 1 passes if:

1) the executable can’t be found (because it was not recognized by the graphical language interpreters and was erased from the disk).
2) the executable can be found but it can’t be executed (by double-clicking on it).

Test 2

Check SMB

From a remote Windows system, in a command window, type:

```
copy  FOLDER_CONTAINING_NC\nc.exe \\PrintServerName\PrintQueueName
```

Log on the print server with administrative privileges. Search everywhere in the system for nc.exe (these program is not supposed to be on the system; if it is found somewhere it means that the SMB client just add it).

Test 2 passes if:
1) the executable can’t be found (because it was not recognized by the graphical language interpreters and was erased from the disk).
2) the executable can be found but it can’t be executed (by double-clicking on it).

Test 3

Check the spool and PostScript disks:

Log on the print server with administrative privileges.
For every directory included in DOC_SPOOL_DIRS and DOC_PS_DIRS:

- try to write and execute a program in every directory

Test 3 passes if nc.exe can’t be executed.

Consequence	**Likelihood**
Medium: If another vulnerability exists and it allows to an attacker to execute code on the system, allowing execute permissions on the writable directories facilitates its work	Low: It is not easy to detect remotely if code can be executed in a directory

Compliance

The control passes if all the intermediary tests pass.

References to source of step

Auditor’s personal experience.

5 Assignment 3 – Audit Evidence

5.1 Conduct the audit.

5.1.1 Introduction

The print server audit was conducted using the checklists described in the previous chapter. In order to limit the time needed to read this document and the space required, only specific items will be detailed in this chapter. These items were selected based on the following criteria:

- they represent the minimal subset allowing to assess the system security level
- they include failed controls
- it represent the original contribution of the audit (there are some items mandatory for every audit not detailed here because a lot of information is already available on the web)

The checklist items selected to be detailed in this chapter are:
F2: Check the firewall ruleset against the product specification
F4: Check how the firewall protects the system from attacks with unexpected TCP flags
W2: Check the filesystem ACLs on web server directories
W3: Check if Web server logging is appropriate
W5: Evaluate the Web server with two vulnerability scanners
SMB1: Only PRINT$, IPC$ and PRINTQUEUES shares should be exposed and the appropriate ACLs should be set
SMB2: Check the SMB server security with two vulnerability scanners
FTP1: Check virtual directories ACLs.
PS1: Check how the PostScript interpreter controls access to information
PS2: Check PostScript directories ACLs
PS3: Check PostScript interpreter directory traversal access
MAL2: Check that no code can be executed in every writable directory exposed by the print server

5.1.2 General notes concerning the audit evidence

In order to protect the confidentiality of the company's name some data was erased from the screen shots used as audit evidence.

Sometimes a control included same kind of tests with different inputs. In order to reduce the size of the document and not to bore the reader with these repetitive tests, the audit evidence was included in appendix.

5.1.3 Audit environment

A small test network has been set up for the needs of this audit.

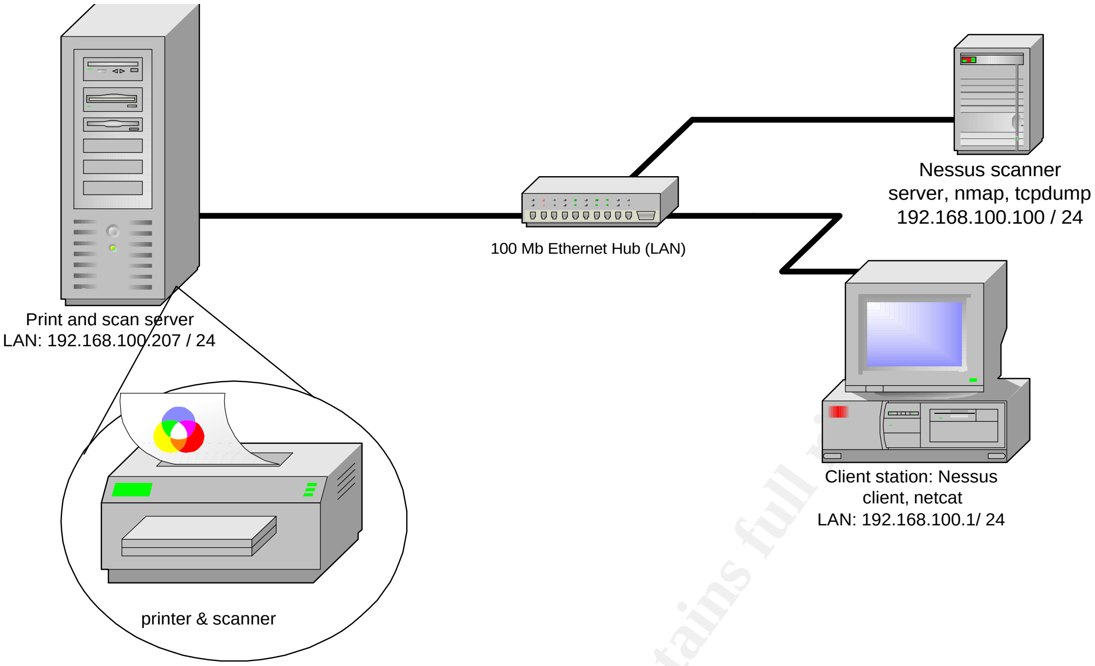


Figure 10: Audit network

Note that all IP addresses in the above figure are specified using the <CIDR> notation.

The following audit tool was executed locally on the print server:
Netcat v1.10 (for Windows)

Client station software

The installed operating system was Windows 2000 SP2. Additionally, the following audit tools were installed on the client station, note that they were run while logged in as a local administrator of the client station. Here are the tools:

- eEye Retina Network Security Scanner 4.9.140 [Retina], a vulnerability assessment tool

(CVE Database Version 20030102).

- NessusWX 1.4.2 [NessusWX], a GUI front-end to the Nessus scanner server.
- Microsoft Network Monitor 2.0 [NetMon] was used mainly during wiretapping tests, to collect the information sent and received by the controller.
- Sysinternals PsTools 1.6 [PsTools], used to retrieve administration information on PLC, from the client station.
- Netcat v1.10 (for Windows)

Nessus station software

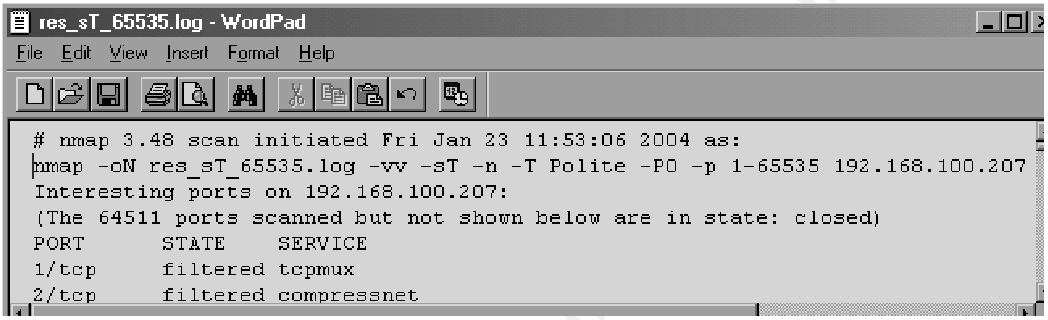
The installed operating system was Linux Red Hat 8.0. Additionally, the Nessus Security Scanner 2.0.9 server [Nessus] was installed on this station as it requires a Unix-like operating system to run.

5.1.4 Firewall tests

Control no. 7	**F2: Check the firewall ruleset against the product specification**
Control objective: The firewall ruleset must allow only the ports mandatory for the product to follow the specification.	**Objective- stimulus response**

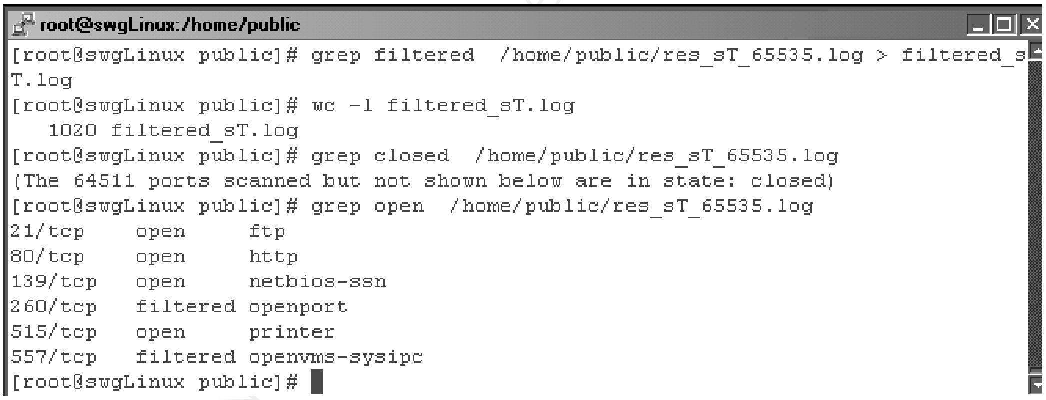
In order to reduce the size of the main document, the screen- shots with the firewall configuration are included in Appendix 1 (Page 114).

IN_TCP: Test 1



```
# nmap 3.48 scan initiated Fri Jan 23 11:53:06 2004 as:
nmap -oN res_sT_65535.log -vv -sT -n -T Polite -P0 -p 1-65535 192.168.100.207
Interesting ports on 192.168.100.207:
(The 64511 ports scanned but not shown below are in state: closed)
PORT      STATE    SERVICE
1/tcp     filtered tcpmux
2/tcp     filtered compressnet
```

Figure 11: nmap session on a remote system on the same LAN



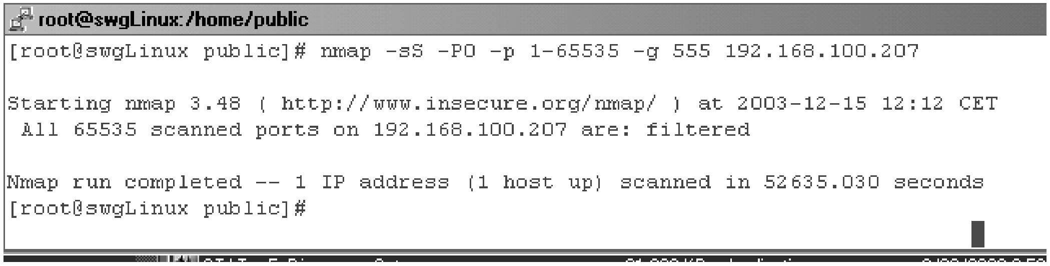
```
[root@swgLinux public]# grep filtered  /home/public/res_sT_65535.log > filtered_s
T.log
[root@swgLinux public]# wc -l filtered_sT.log
   1020 filtered_sT.log
[root@swgLinux public]# grep closed  /home/public/res_sT_65535.log
(The 64511 ports scanned but not shown below are in state: closed)
[root@swgLinux public]# grep open  /home/public/res_sT_65535.log
21/tcp    open     ftp
80/tcp    open     http
139/tcp   open     netbios-ssn
260/tcp   filtered openport
515/tcp   open     printer
557/tcp   filtered openvms-sysipc
[root@swgLinux public]#
```

Figure 12: Check filtered and closed ports

The previous screen shots shows a nmap TCP full connect scan of the print server. There are 1020 ports seen as filtered and 64511 ports closed. Consequently only 4 ports are seen as open. The open TCP ports are 21, 80, 139, 515. The ports needed for FTP server data connections (> 1024) are not seen by nmap because they are dynamic ports closed after the data transfer finishes.

Test 1 passes.

IN_TCP: Test 2

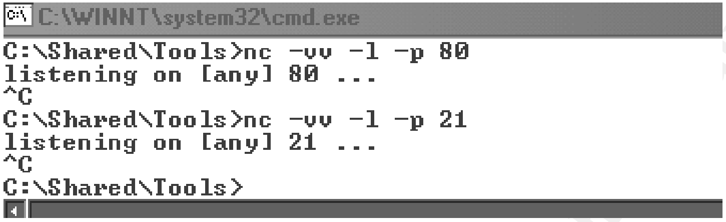


```
[root@swgLinux public]# nmap -sS -P0 -p 1-65535 -g 555 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-15 12:12 CET
 All 65535 scanned ports on 192.168.100.207 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 52635.030 seconds
[root@swgLinux public]#
```

Figure 13: nmap session on a remote system on the same LAN

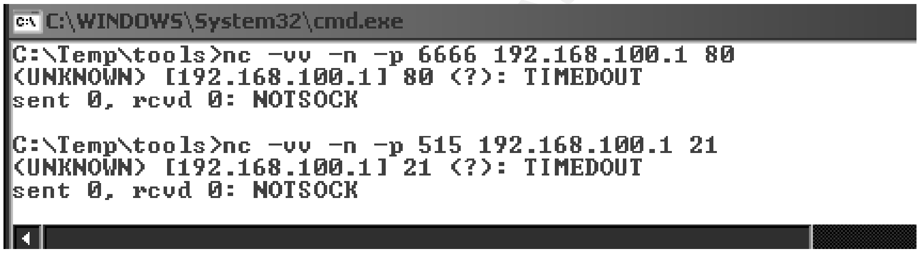
The previous screen shot shows a nmap TCP half connect scan of the print server. There are no open ports on the print server because the remote port isn't authorized.
Test 2 passes.

OUT_TCP: Test 3, Test 4



```
C:\Shared\Tools>nc -vv -l -p 80
listening on [any] 80 ...
^C
C:\Shared\Tools>nc -vv -l -p 21
listening on [any] 21 ...
^C
C:\Shared\Tools>
```

Figure 14: Netcat sessions on a remote system on the same LAN

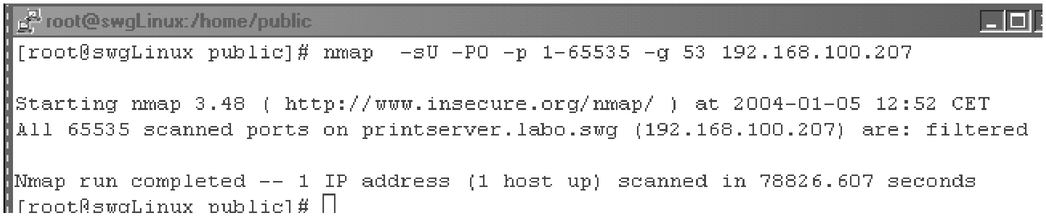


```
C:\Temp\tools>nc -vv -n -p 6666 192.168.100.1 80
<UNKNOWN> [192.168.100.1] 80 (?): TIMEDOUT
sent 0, rcvd 0: NOTSOCK

C:\Temp\tools>nc -vv -n -p 515 192.168.100.1 21
<UNKNOWN> [192.168.100.1] 21 (?): TIMEDOUT
sent 0, rcvd 0: NOTSOCK
```

Figure 15: Netcat sessions on the print server

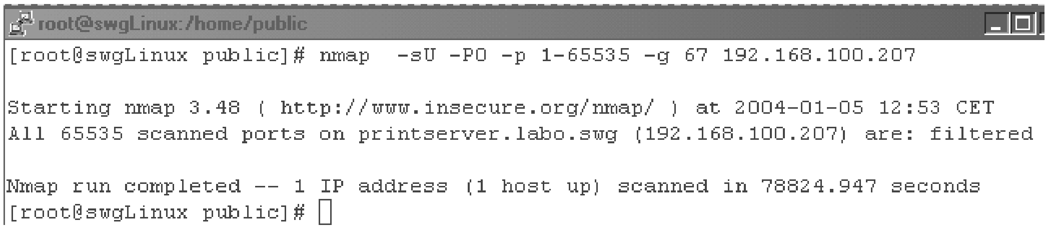
The previous screen shots show two successive connections from `netcat` sessions on TCP ports greater than1024/515 running on the print server to remote TCP ports listening on 80/21. The two connections are blocked (the first one because output to the remote port 80 isn't authorized: test 3, the second one because the output from the local port 515 isn't authorized: test 4).
Test 3 passes.
Test 4 passes.

IN_UDP: Test 5



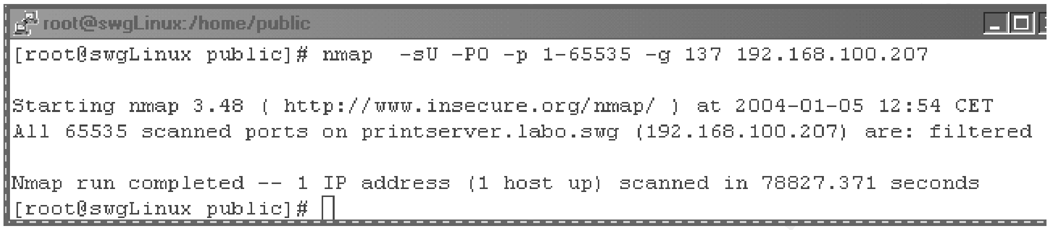
```
[root@swgLinux public]# nmap  -sU -P0 -p 1-65535 -g 53 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-01-05 12:52 CET
All 65535 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 78826.607 seconds
[root@swgLinux public]#
```

Figure 16: nmap session on a remote system on the same LAN



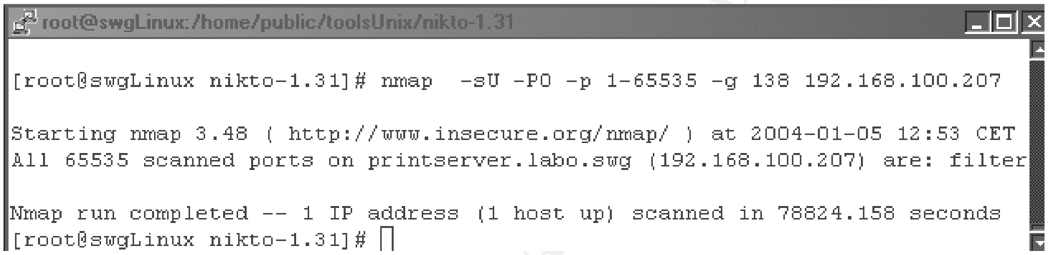
```
[root@swgLinux public]# nmap  -sU -P0 -p 1-65535 -g 67 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-01-05 12:53 CET
All 65535 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 78824.947 seconds
[root@swgLinux public]# 
```

Figure 17: nmap session on a remote system on the same LAN



```
[root@swgLinux public]# nmap  -sU -P0 -p 1-65535 -g 137 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-01-05 12:54 CET
All 65535 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 78827.371 seconds
[root@swgLinux public]# 
```

Figure 18: nmap session on a remote system on the same LAN

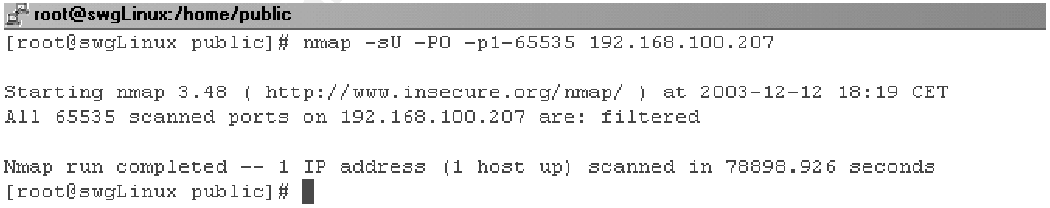


```
[root@swgLinux nikto-1.31]# nmap  -sU -P0 -p 1-65535 -g 138 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-01-05 12:53 CET
All 65535 scanned ports on printserver.labo.swg (192.168.100.207) are: filter

Nmap run completed -- 1 IP address (1 host up) scanned in 78824.158 seconds
[root@swgLinux nikto-1.31]# 
```

Figure 19: nmap session on a remote system on the same LAN

The previous screen shot shows four complete (destination ports 1-65535) UDP nmap scans with a UDP source scan 53/67/137/138. In fact nmap decided that even 68/137/138 ports are filtered because when scanning all 65535 UDP ports no ICMP port unreachable message was received.
Test 5 passes.

IN_UDP: Test 6

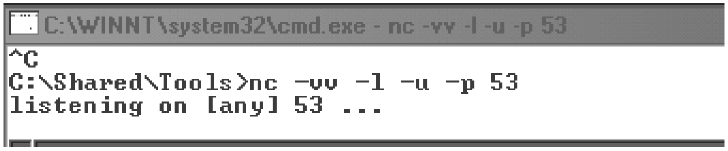


```
[root@swgLinux public]# nmap -sU -P0 -p1-65535 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-12 18:19 CET
All 65535 scanned ports on 192.168.100.207 are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 78898.926 seconds
[root@swgLinux public]# 
```

Figure 20: nmap session on a remote system on the same LAN

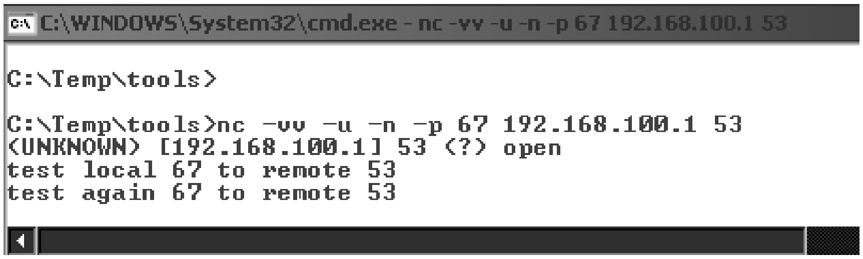
The previous screen shot shows a nmap UDP scan of the print server. There are no open ports on the print server because the remote port isn't authorized.
Test 6 passes.

OUT_UDP: 7



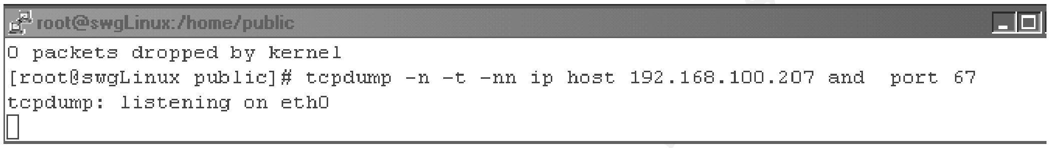
```
C:\WINNT\system32\cmd.exe - nc -vv -l -u -p 53
^C
C:\Shared\Tools>nc -vv -l -u -p 53
listening on [any] 53 ...
```

Figure 21: Netcat sessions on a remote on the same LAN



```
C:\WINDOWS\System32\cmd.exe - nc -vv -u -n -p 67 192.168.100.1 53

C:\Temp\tools>

C:\Temp\tools>nc -vv -u -n -p 67 192.168.100.1 53
(UNKNOWN) [192.168.100.1] 53 (?) open
test local 67 to remote 53
test again 67 to remote 53
```

Figure 22: Netcat sessions on the print server



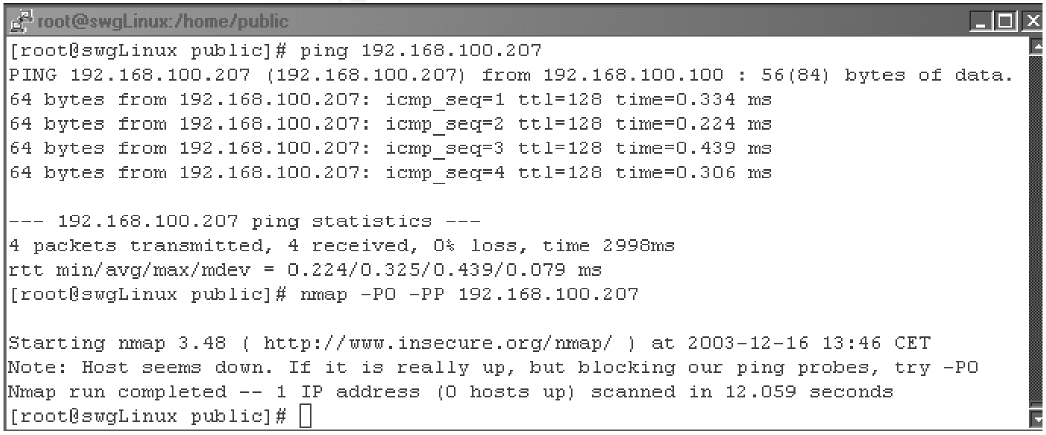
```
root@swgLinux:/home/public
0 packets dropped by kernel
[root@swgLinux public]# tcpdump -n -t -nn ip host 192.168.100.207 and  port 67
tcpdump: listening on eth0
```

Figure 23: tcpdump running on a remote station on the same subnet

The previous screen shot shows a netcat session running on the UDP port 67 of the print server trying to establish a connection to a remote UDP port 53. The fact that the remote port 53 is indicated as open doesn't mean that the connection is established (netcat gives this message without sending any data). We understand that the traffic is blocked because on the netcat session running on the remote PC no data arrives and because a tcpdump that surveys traffic related to the port 67 on the print server doesn't see any.

Test 7 passes.

IN_ICMP: Test 8



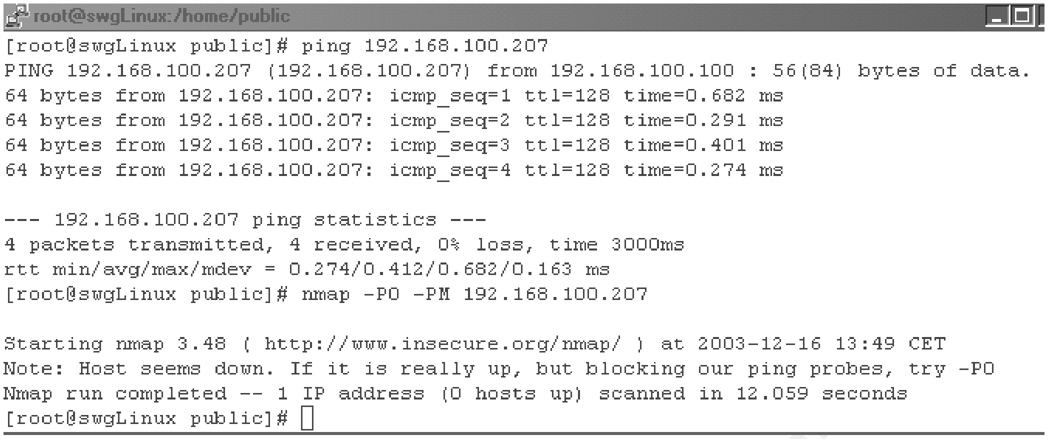
```
root@swgLinux:/home/public
[root@swgLinux public]# ping 192.168.100.207
PING 192.168.100.207 (192.168.100.207) from 192.168.100.100 : 56(84) bytes of data.
64 bytes from 192.168.100.207: icmp_seq=1 ttl=128 time=0.334 ms
64 bytes from 192.168.100.207: icmp_seq=2 ttl=128 time=0.224 ms
64 bytes from 192.168.100.207: icmp_seq=3 ttl=128 time=0.439 ms
64 bytes from 192.168.100.207: icmp_seq=4 ttl=128 time=0.306 ms

--- 192.168.100.207 ping statistics ---
4 packets transmitted, 4 received, 0% loss, time 2998ms
rtt min/avg/max/mdev = 0.224/0.325/0.439/0.079 ms
[root@swgLinux public]# nmap -P0 -PP 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-16 13:46 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 12.059 seconds
[root@swgLinux public]#
```

Figure 24: nmap session on a remote system on the same LAN

The previous screen shot shows a nmap sending a timestamp request without receiving any answer.

Test 8 passes.

IN_ICMP: Test 9



```
[root@swgLinux public]# ping 192.168.100.207
PING 192.168.100.207 (192.168.100.207) from 192.168.100.100 : 56(84) bytes of data.
64 bytes from 192.168.100.207: icmp_seq=1 ttl=128 time=0.682 ms
64 bytes from 192.168.100.207: icmp_seq=2 ttl=128 time=0.291 ms
64 bytes from 192.168.100.207: icmp_seq=3 ttl=128 time=0.401 ms
64 bytes from 192.168.100.207: icmp_seq=4 ttl=128 time=0.274 ms

--- 192.168.100.207 ping statistics ---
4 packets transmitted, 4 received, 0% loss, time 3000ms
rtt min/avg/max/mdev = 0.274/0.412/0.682/0.163 ms
[root@swgLinux public]# nmap -P0 -PM 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-16 13:49 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 12.059 seconds
[root@swgLinux public]# 
```

Figure 25: nmap session on a remote system on the same LAN

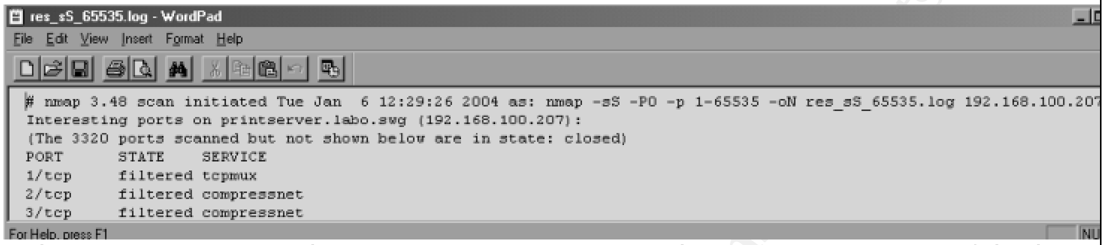
The previous screen shot shows a nmap sending a subnet mask request without receiving any answer.
Test 9 passes.

Compliance
Control No. 7 passes because all the intermediary tests pass.

Control no. 9	**F4: Check how the firewall protects the system from attacks with unexpected TCP flags**
Control objective: The firewall should restrict the access to the ports required in the ruleset, no matter which flags are used to scan the system.	**Objective- stimulus response**

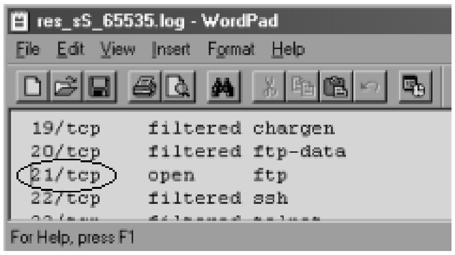
Test results

Test 1

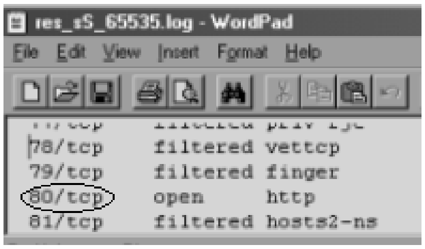


```
# nmap 3.48 scan initiated Tue Jan  6 12:29:26 2004 as: nmap -sS -P0 -p 1-65535 -oN res_sS_65535.log 192.168.100.207
Interesting ports on printserver.labo.swg (192.168.100.207):
(The 3320 ports scanned but not shown below are in state: closed)
PORT      STATE    SERVICE
1/tcp     filtered tcpmux
2/tcp     filtered compressnet
3/tcp     filtered compressnet
```

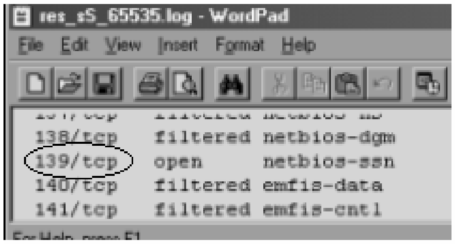
Figure 26: nmap session on a remote system on the same LAN: Start of the log file



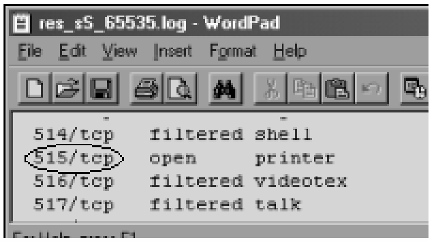
```
19/tcp     filtered chargen
20/tcp     filtered ftp-data
21/tcp     open     ftp
22/tcp     filtered ssh
```



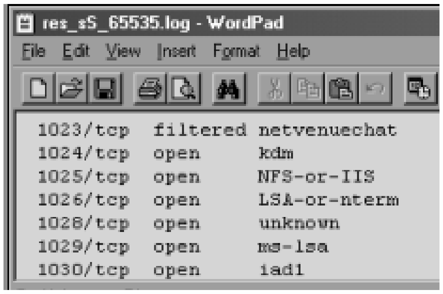
```
78/tcp     filtered vettcp
79/tcp     filtered finger
80/tcp     open     http
81/tcp     filtered hosts2-ns
```



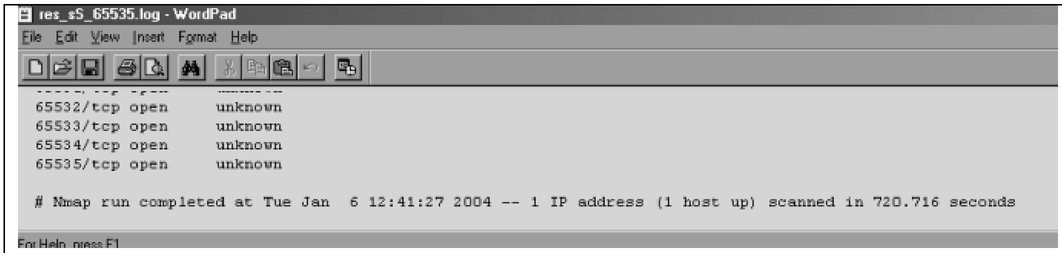
```
138/tcp    filtered netbios-dgm
139/tcp    open     netbios-ssn
140/tcp    filtered emfis-data
141/tcp    filtered emfis-cntl
```



```
514/tcp    filtered shell
515/tcp    open     printer
516/tcp    filtered videotex
517/tcp    filtered talk
```



```
1023/tcp  filtered netvenuechat
1024/tcp  open     kdm
1025/tcp  open     NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
```

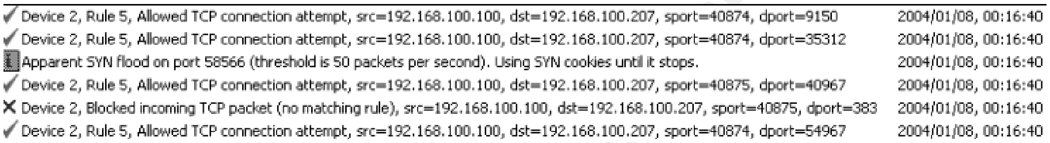


```
 65532/tcp open     unknown
 65533/tcp open     unknown
 65534/tcp open     unknown
 65535/tcp open     unknown

 # Nmap run completed at Tue Jan  6 12:41:27 2004 -- 1 IP address (1 host up) scanned in 720.716 seconds
```

Figure 27: nmap session on a remote system: End of the log file

In the previous screen shots shows that for ports less then 1024 only the ports TCP 21, 80, 139, 515 are open.
Test 1 passes.

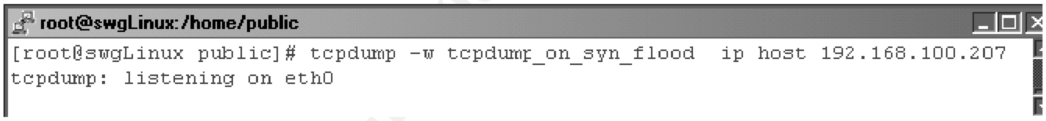
In the last two screen shots all the ports >= 1024 are seen as open. This may seem strange because the system doesn't have all this ports open, of course. The explanation is the firewall protection against syn flooding. The following screen shots will prove it.



```
✓ Device 2, Rule 5, Allowed TCP connection attempt, src=192.168.100.100, dst=192.168.100.207, sport=40874, dport=9150         2004/01/08, 00:16:40
✓ Device 2, Rule 5, Allowed TCP connection attempt, src=192.168.100.100, dst=192.168.100.207, sport=40874, dport=35312        2004/01/08, 00:16:40
  Apparent SYN flood on port 58566 (threshold is 50 packets per second). Using SYN cookies until it stops.                   2004/01/08, 00:16:40
✓ Device 2, Rule 5, Allowed TCP connection attempt, src=192.168.100.100, dst=192.168.100.207, sport=40875, dport=40967        2004/01/08, 00:16:40
✗ Device 2, Blocked incoming TCP packet (no matching rule), src=192.168.100.100, dst=192.168.100.207, sport=40875, dport=383  2004/01/08, 00:16:40
✓ Device 2, Rule 5, Allowed TCP connection attempt, src=192.168.100.100, dst=192.168.100.207, sport=40874, dport=54967        2004/01/08, 00:16:40
```

Figure 28: Firewall logs during a Syn scan

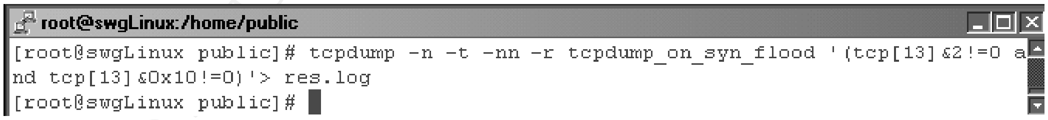
The previous screen shot is a capture of the firewall log. The firewall detected a syn flooding and activates the cookies mechanism. This means that the firewall will answer with a Syn-Ack packet even for closed ports.



```
[root@swgLinux public]# tcpdump -w tcpdump_on_syn_flood  ip host 192.168.100.207
tcpdump: listening on eth0
```

Figure 29: tcpdump on a remote station on the same LAN

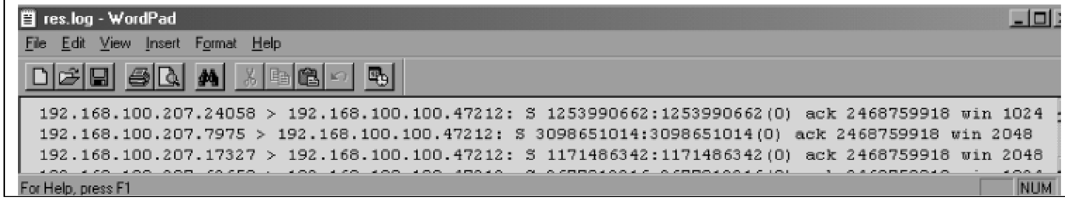
The previous screen shot shows tcpdump listening during the previous nmap scan and writing raw packets to a file (tcp_dump_on_syn_flood).



```
[root@swgLinux public]# tcpdump -n -t -nn -r tcpdump_on_syn_flood '(tcp[13]&2!=0 a
nd tcp[13]&0x10!=0)'> res.log
[root@swgLinux public]# 
```

Figure 30: tcpdump filter

The previous screen shot shows a tcpdump filtering for successful inbound connections (outbound syn-ack packets) and putting the result in a file (res.log).



```
 192.168.100.207.24058 > 192.168.100.100.47212: S 1253990662:1253990662(0) ack 2468759918 win 1024
 192.168.100.207.7975 > 192.168.100.100.47212: S 3098651014:3098651014(0) ack 2468759918 win 2048
 192.168.100.207.17327 > 192.168.100.100.47212: S 1171486342:1171486342(0) ack 2468759918 win 2048
```

Figure 31: First SYN-Ack sent by the print server

The previous screen shot shows the first line of the successful inbound connections corresponds to the port for which the syn cookies mechanism was activated (port 24058).

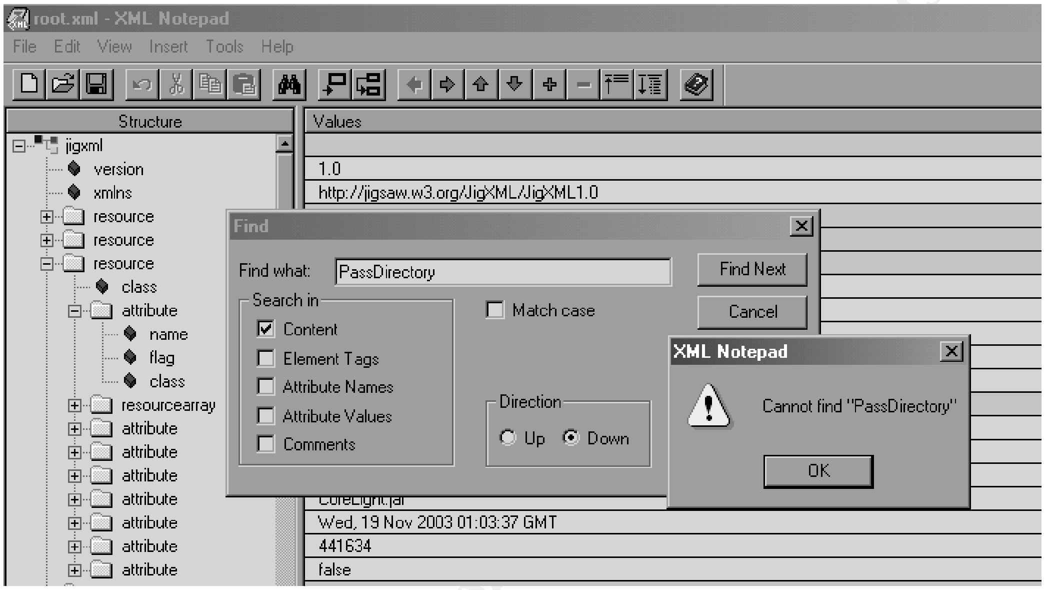
T**ests 2, 3, 4, 5, 6, 7, 8, 9, 10**
The screen shots can be found in Appendix 2 (Page 116).
The screen shots show that the system being audited does not respond to the nmap scan.
Test s 2, 3, 4, 5, 6, 7, 8, 9, 10 pass.

Compliance
Control No. 9 passes because all intermediary tests pass.

5.1.5 Web server tests

Control no. 13	**W2: Check the filesystem ACLs on web server directories**
Control objective: Appropriate ACLs should be set on the web server's directories	**Objective**

Test results



1.0
http://jigsaw.w3.org/JigXML/JigXML1.0
CoreLight.jar
Wed, 19 Nov 2003 01:03:37 GMT
441634
false

Find what: PassDirectory
☑ Content
☐ Element Tags
☐ Attribute Names
☐ Attribute Values
☐ Comments
☐ Match case
○ Up ● Down

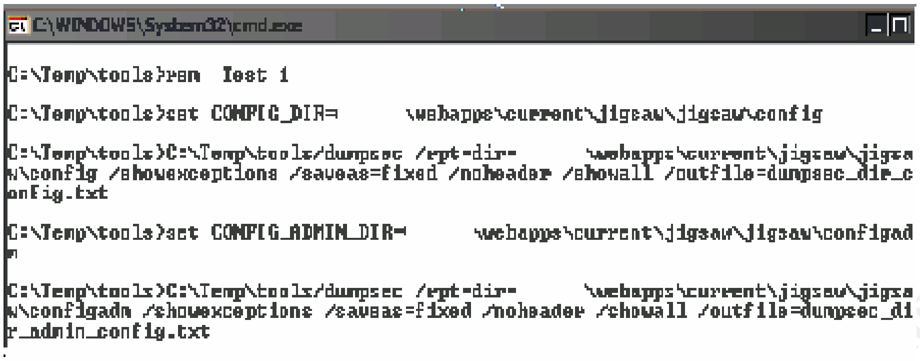
Cannot find "PassDirectory"

Figure 32: Jigsaw root.xml file

The previous screen shot shows that there is no `PassDirectory` resource in the `root.xml` file. It can be concluded that this server doesn't use symbolic links.

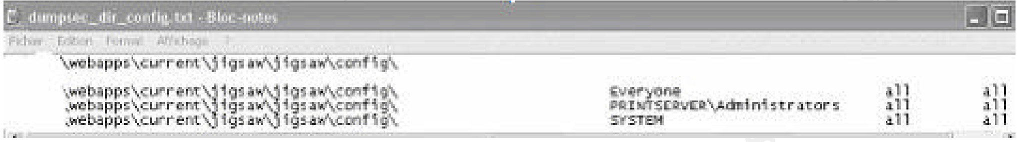
`Dumpsec` will be used in order to check the permissions for the directories and files.
In order to understand the `dumpsec` results file, we must keep in mind that:
- the header is always:
- “`Path (dir and file exceptions) Account        Own Dir   File` “
- reporting by exception was required (only files and directories whose ownership, permissions and/or audit settings differ from those of the parent directory are displayed)
- if an account has “all” permission it means that it can list the contents of the directory, add new files and subdirectories to the directory, traverse the directory as part of a path, delete the entire directory, change permissions for the directory and all files and subdirectories, change ownership of the directory.

Test 1



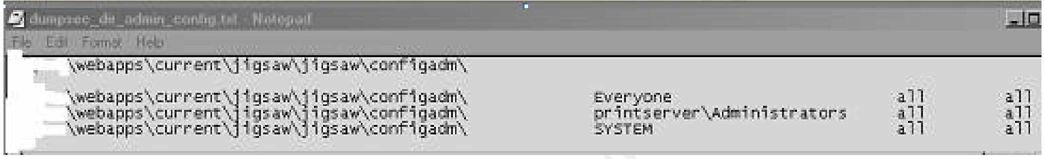
```
C:\Temp\tools>rem  Test 1

C:\Temp\tools>set CONFIG_DIR=      \webapps\current\jigsaw\jigsaw\config

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jigsaw\jigsa
w\config /showexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_dir_c
onfig.txt

C:\Temp\tools>set CONFIG_ADMIN_DIR=      \webapps\current\jigsaw\jigsaw\configad
m

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jigsaw\jigsa
w\configadm /showexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_di
r_admin_config.txt
```

Figure 33: Run dumpsec for CONFIG_DIR and CONFIG_ADMIN_DIR



```
     \webapps\current\jigsaw\jigsaw\config\

     \webapps\current\jigsaw\jigsaw\config\                    Everyone                         all       all
     \webapps\current\jigsaw\jigsaw\config\                    PRINTSERVER\Administrators       all       all
     \webapps\current\jigsaw\jigsaw\config\                    SYSTEM                           all       all
```

Figure 34: dumpsec log file for CONFIG_DIR directory



```
     \webapps\current\jigsaw\jigsaw\configadm\

     \webapps\current\jigsaw\jigsaw\configadm\                 Everyone                         all       all
     \webapps\current\jigsaw\jigsaw\configadm\                 printserver\Administrators       all       all
     \webapps\current\jigsaw\jigsaw\configadm\                 SYSTEM                           all       all
```

Figure 35: dumpsec log file for CONFIG_ADMIN_DIR directory

The previous screen shot shows part of the file containing the permissions of the server configuration and server administration configuration directories. “Everyone “ has “all” permissions. This is not correct.
Test 1 fails.

Test 2
The tools and test method used for this test are similar with the previous ones. The screen shots can be found in Appendix 3 (Page 120).
The screen shots show part of the dumpsec log file containing the permissions of the server log directories. “Everyone “ has “all” permissions for the directory and this is not correct.
There is also part of the dumpsec log file containing the permissions for one web server’s logging file. “Everyone “ has “all” permissions for logging file. This is not correct.
Test 2 fails.

Test 3
The tools and test method used for this test are similar with the previous ones. The screen shots can be found in Appendix 3 (Page 120).
The screen shots show parts of the files containing the permissions of directories containing servlets and the directory containing GCI scripts. “Everyone “ has “all” permissions. This is not correct.
Test 3 fails.

Test 4
The tools and test method used for this test are similar with the previous ones.

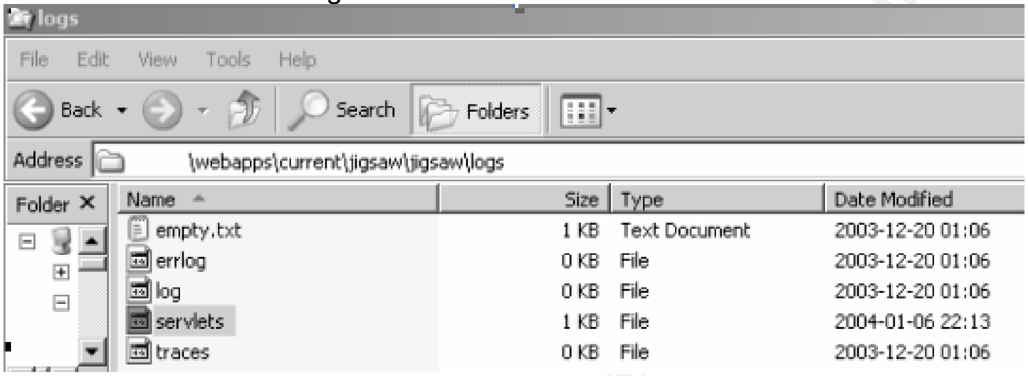
The screen shots can be found in Appendix 3 (Page 120). The screen shots show part of the dumpsec log file containing the permissions of the server document root directory. “Everyone “ has “all” permissions. This is not correct. **Test 4 fails.** **Test 5: not applicable because there are no symbolic links.** **Test 6** The tools and test method used for this test are similar with the previous ones. The screen shots can be found in Appendix 3 (Page 120). The screen shots show parts of the dumpsec log file containing the permissions of the directories included in the CLASSPATH environment variable. “Everyone “ has “all” permissions. This is not correct. **Test 6 fails.**
Compliance **Control No. 13 fails because all intermediary tests failed.**

Control no. 14	**W3: Check the Web server logging level**
Control objective: The Web server logging should be enabled and the information retrieved from the Web server logs should allow detecting a vulnerability scan	**Objective- stimulus response**

Test results

Perform a Retina vulnerability scan of the Web server as described in the Control no. 16.

Check the web server log files to see if the scan can be detected.

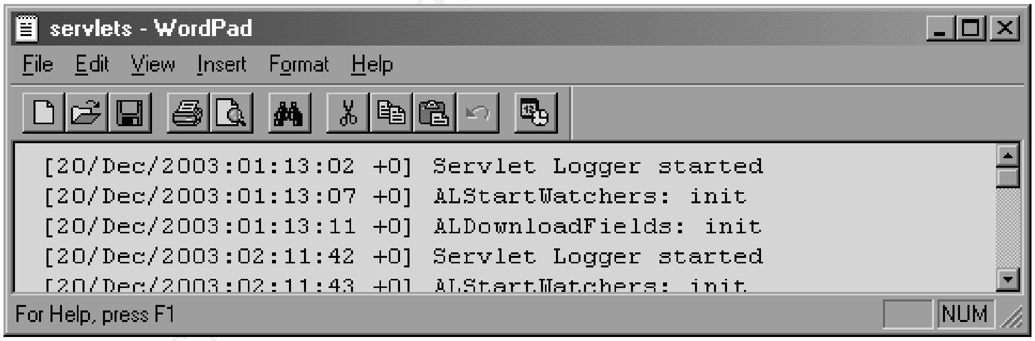


logs
File Edit View Tools Help
Back Search Folders
Address \webapps\current\jigsaw\jigsaw\logs
Folder ×

Name	Size	Type	Date Modified
empty.txt	1 KB	Text Document	2003-12-20 01:06
errlog	0 KB	File	2003-12-20 01:06
log	0 KB	File	2003-12-20 01:06
servlets	1 KB	File	2004-01-06 22:13
traces	0 KB	File	2003-12-20 01:06

Figure 36: Display log directory

In the following screen shot shows the web server log directory. The only log file containing data is “servlets”. Consequently, the only log file that may contain data allowing the vulnerability scan detection is the “servlets” file.



```
[20/Dec/2003:01:13:02 +0] Servlet Logger started
[20/Dec/2003:01:13:07 +0] ALStartWatchers: init
[20/Dec/2003:01:13:11 +0] ALDownloadFields: init
[20/Dec/2003:02:11:42 +0] Servlet Logger started
[20/Dec/2003:02:11:43 +0] ALStartWatchers: init
```

Figure 37: Servlet log file

The previous shows part of “servlets” file. This log file doesn’t contain information useful to diagnose an attack.

Compliance

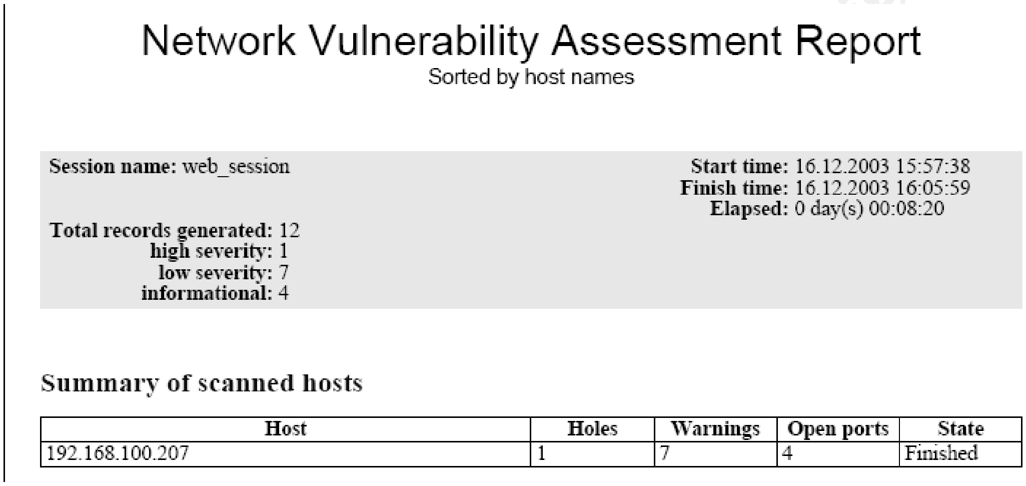
Control No. 14 fails.

Control no. 16	**W5: Evaluate Web server security with two vulnerability scanners**
Control objective: Use two up-to-date vulnerability scanners to check that no medium and high risk known vulnerabilities are detected for web server	**Objective**

Test results

The Retina scanner version used for this test is 4.9.140, CVE Database Version 20030102

Test 1 (Nessus):



Network Vulnerability Assessment Report

Sorted by host names

Session name: web_session

Start time: 16.12.2003 15:57:38
Finish time: 16.12.2003 16:05:59
Elapsed: 0 day(s) 00:08:20

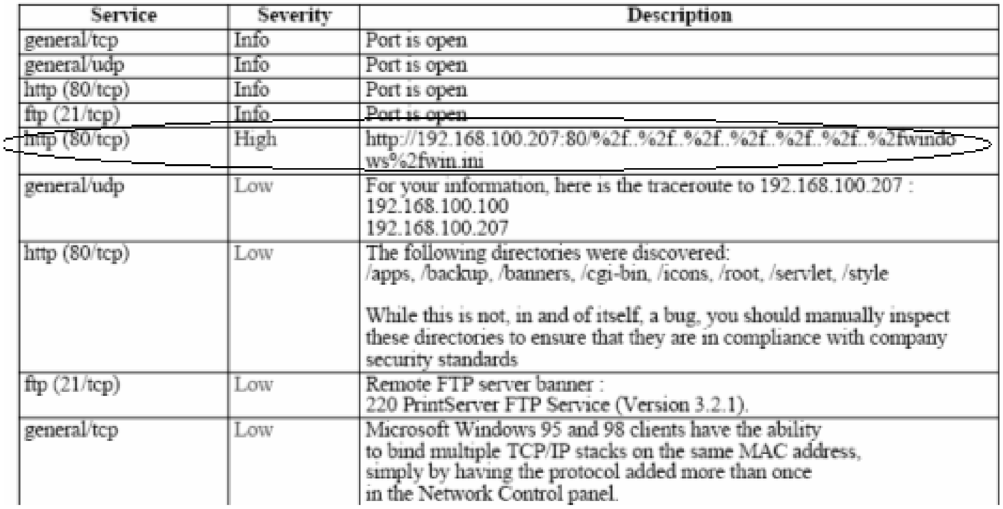
Total records generated: 12
high severity: 1
low severity: 7
informational: 4

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
192.168.100.207	1	7	4	Finished

Figure 38: Nessus web server vulnerability assessment report executive summary

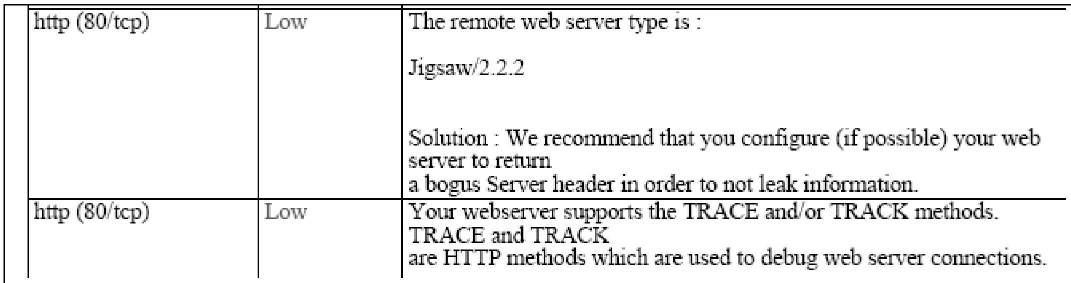
The previous screen shot shows the summary of the vulnerabilities found by Nessus.



Service	Severity	Description
general/tcp	Info	Port is open
general/udp	Info	Port is open
http (80/tcp)	Info	Port is open
ftp (21/tcp)	Info	Port is open
http (80/tcp)	High	http://192.168.100.207:80/%2f..%2f..%2f..%2f..%2f..%2f..%2fwindows%2fwin.ini
general/udp	Low	For your information, here is the traceroute to 192.168.100.207 : 192.168.100.100 192.168.100.207
http (80/tcp)	Low	The following directories were discovered: /apps, /backup, /banners, /cgi-bin, /icons, /root, /servlet, /style While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards
ftp (21/tcp)	Low	Remote FTP server banner : 220 PrintServer FTP Service (Version 3.2.1).
general/tcp	Low	Microsoft Windows 95 and 98 clients have the ability to bind multiple TCP/IP stacks on the same MAC address, simply by having the protocol added more than once in the Network Control panel.

Figure 39: Nessus web server vulnerability assessment report

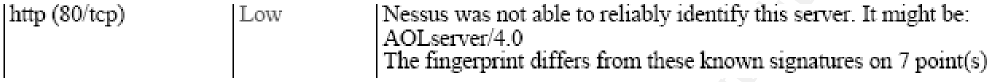
In the previous screen shot we can see that this server has a directory traversal vulnerability and this represents a high risk vulnerability. The server exposes some directories. For this reason this test fails.



http (80/tcp)	Low	The remote web server type is : Jigsaw/2.2.2 Solution : We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.
http (80/tcp)	Low	Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Figure 40: Nesssus web server vulnerability assessment report

In the previous screen shot we can see that this server expose HTTP TRACE method and it shouldn't be the case for a server in production mode. However, this is not a high or medium level vulnerability and has no impact on the control status (fail or pass).

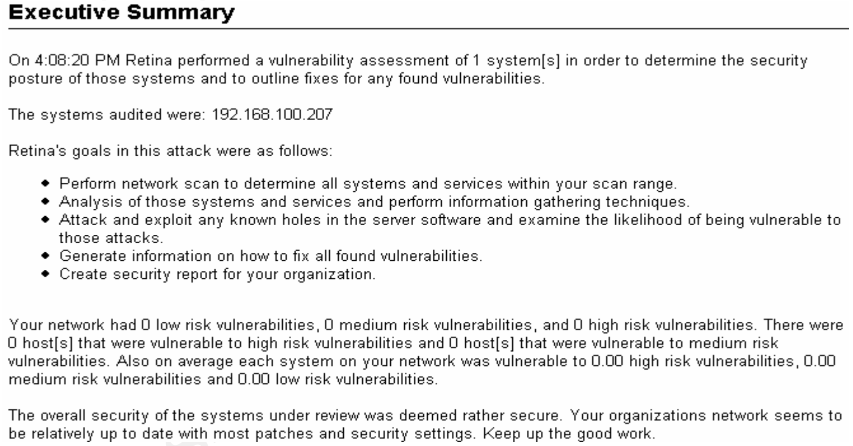


http (80/tcp)	Low	Nessus was not able to reliably identify this server. It might be: AOLserver/4.0 The fingerprint differs from these known signatures on 7 point(s)

Figure 41: Nesssus web server vulnerability assessment report

The previous screen shot shows a Nessus inconsistency because it pretends not to reliably identify the server and Nessus gives a wrong server name, while in a previous screen shot we can see that it already identified it.
Nessus web server vulnerabilities scan test fails because Nessus identified a high risk vulnerability (directory traversal).

Test 2 (Retina):



Executive Summary

On 4:08:20 PM Retina performed a vulnerability assessment of 1 system[s] in order to determine the security posture of those systems and to outline fixes for any found vulnerabilities.

The systems audited were: 192.168.100.207

Retina's goals in this attack were as follows:

- Perform network scan to determine all systems and services within your scan range.
- Analysis of those systems and services and perform information gathering techniques.
- Attack and exploit any known holes in the server software and examine the likelihood of being vulnerable to those attacks.
- Generate information on how to fix all found vulnerabilities.
- Create security report for your organization.

Your network had 0 low risk vulnerabilities, 0 medium risk vulnerabilities, and 0 high risk vulnerabilities. There were 0 host[s] that were vulnerable to high risk vulnerabilities and 0 host[s] that were vulnerable to medium risk vulnerabilities. Also on average each system on your network was vulnerable to 0.00 high risk vulnerabilities, 0.00 medium risk vulnerabilities and 0.00 low risk vulnerabilities.

The overall security of the systems under review was deemed rather secure. Your organizations network seems to be relatively up to date with most patches and security settings. Keep up the good work.

The previous screen shot shows the executive summary of the web vulnerabilities found by Retina. Retina doesn't find any medium or high risk vulnerability.
Retina web server vulnerabilities scan test passes.

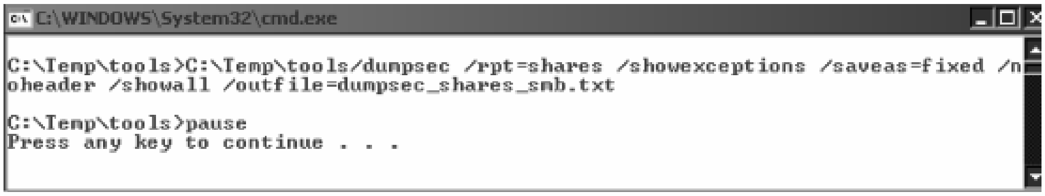
Test fails because one high risk vulnerability has been identified by Nessus. The fact that two tools didn't find the same vulnerabilities enforces the good practice recommendation to use at least two vulnerabilities scanners.

Compliance
Control No. 16 fails because one of the intermediary tests fails.

5.1.6 SMB server tests

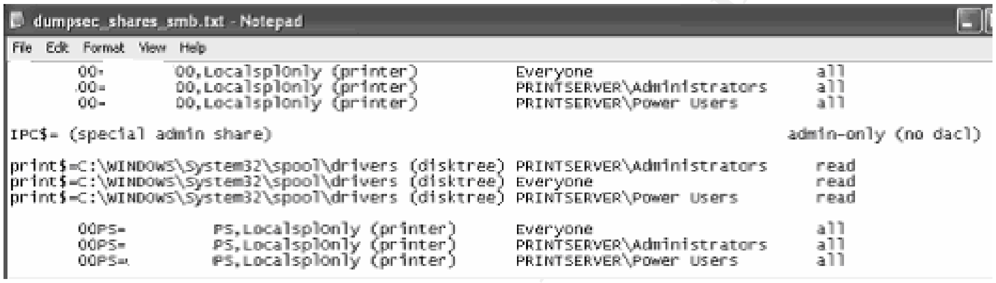
Control no. 19	**SMB1: Check the shares exposed by the SMB server**
Control objective: Only PRINT$, IPC$ and PRINTQUEUES shares should be exposed and that appropriate ACLs should be set	**Objective**

Test results



```
C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=shares /showexceptions /saveas=fixed /n
oheader /showall /outfile=dumpsec_shares_smb.txt

C:\Temp\tools>pause
Press any key to continue . . .
```

Figure 42: Run dumpsec for the SMB shares



```
       00=        00,LocalsplOnly (printer)        Everyone                       all
       00=        00,LocalsplOnly (printer)        PRINTSERVER\Administrators     all
       00=        00,LocalsplOnly (printer)        PRINTSERVER\Power Users        all

IPC$= (special admin share)                                              admin-only (no dacl)

print$=C:\WINDOWS\System32\spool\drivers (disktree) PRINTSERVER\Administrators     read
print$=C:\WINDOWS\System32\spool\drivers (disktree) Everyone                       read
print$=C:\WINDOWS\System32\spool\drivers (disktree) PRINTSERVER\Power Users        read

       00PS=        PS,LocalsplOnly (printer)      Everyone                       all
       00PS=        PS,LocalsplOnly (printer)      PRINTSERVER\Administrators     all
       00PS=        PS,LocalsplOnly (printer)      PRINTSERVER\Power Users        all
```

Figure 43: dumpsec log file for the SMB shares

The previous screen shot shows the file containing the permissions of the SMB shares. The two print queues have “all” permissions set and this is correct because everyone should be allowed to print on the print server. The print driver’s directory has “read’ access for everyone and this is also correct. The IPC$ share is only available for the administrator.

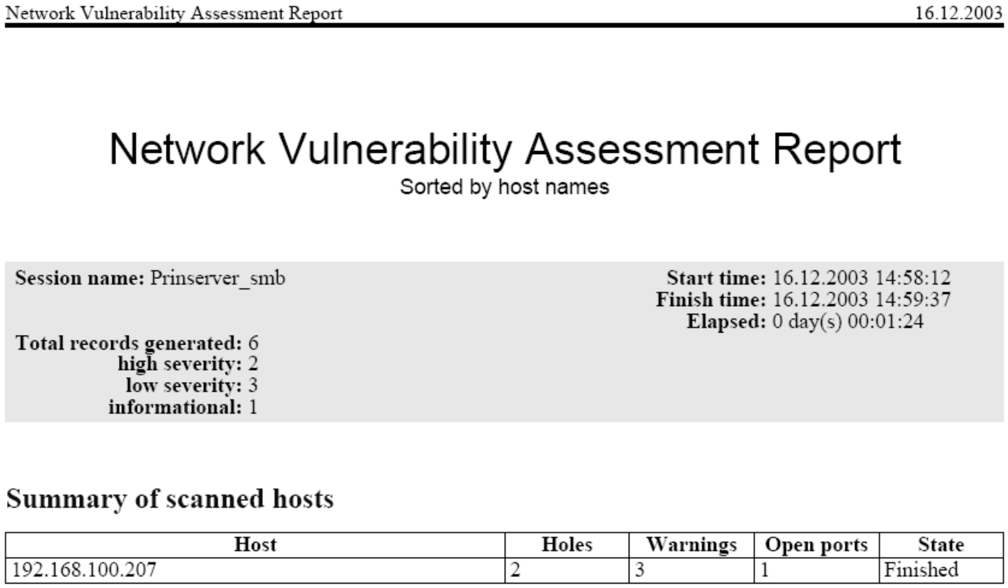
Test passes.

Compliance
Control No. 19 passes.

Control no. 20	**SMB2: Evaluate SMB server security**
Control objective: Use two up-to-date vulnerability scanners to check that no medium and high risk known vulnerabilities are detected for the SMB server	**Objective**

Test results

Test 1 (Nessus):



Network Vulnerability Assessment Report 16.12.2003

Network Vulnerability Assessment Report

Sorted by host names

Session name: Prinserver_smb

Start time: 16.12.2003 14:58:12
Finish time: 16.12.2003 14:59:37
Elapsed: 0 day(s) 00:01:24

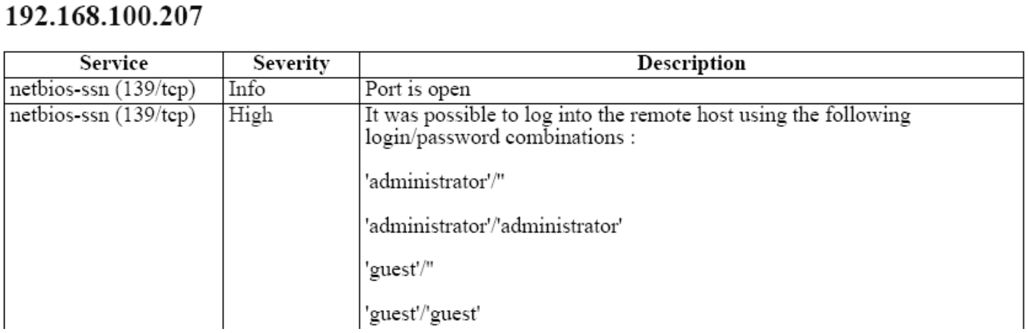
Total records generated: 6
high severity: 2
low severity: 3
informational: 1

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
192.168.100.207	2	3	1	Finished

Figure 44: Nessus SMB server vulnerability assessment report executive summary

The previous screen shot shows the summary of the vulnerabilities found by Nessus. Only one open port is seen as open because Nessus was tuned to look only for SMB vulnerabilities.

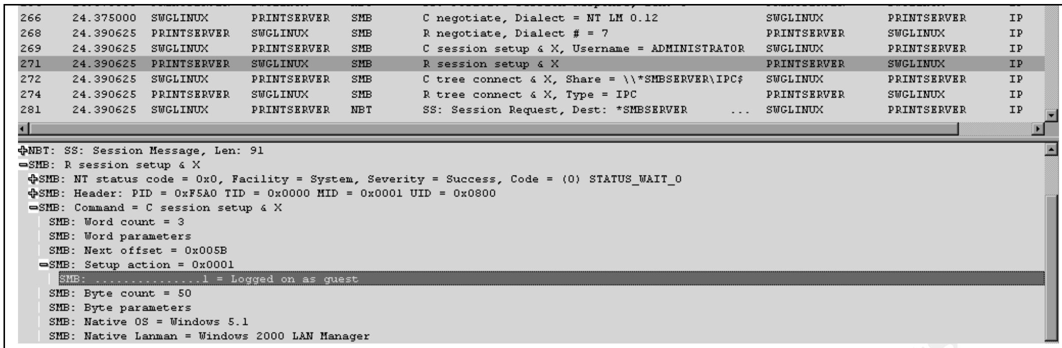


192.168.100.207

Service	Severity	Description
netbios-ssn (139/tcp)	Info	Port is open
netbios-ssn (139/tcp)	High	It was possible to log into the remote host using the following login/password combinations : 'administrator'/'' 'administrator'/'administrator' 'guest'/'' 'guest'/'guest'

Figure 45: Nesssus SMB server vulnerability assessment report

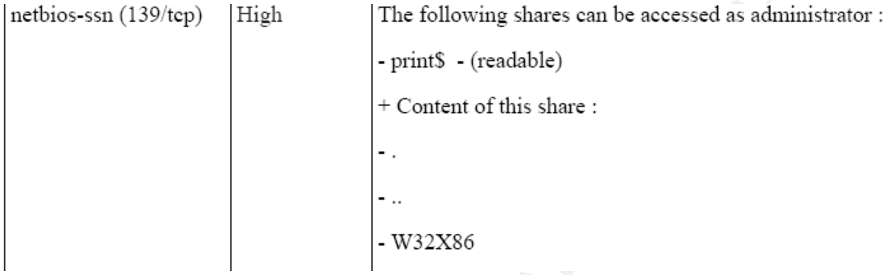
In the previous screen shot Nessus pretends to successfully logged in the SMB server using “guest” or a blank password for the guest account. This print server specification requires that everyone should be able to print so this server is correctly configured. Nessus pretends also a successful log in the administrator account using “administrator” or a blank password. This was unexpected so the network traffic during the SMB scan performed by Nessus was recorded.



```
266    24.375000  SWGLINUX     PRINTSERVER  SMB      C negotiate, Dialect = NT LM 0.12            SWGLINUX     PRINTSERVER  IP
268    24.390625  PRINTSERVER  SWGLINUX     SMB      R negotiate, Dialect # = 7                   PRINTSERVER  SWGLINUX     IP
269    24.390625  SWGLINUX     PRINTSERVER  SMB      C session setup & X, Username = ADMINISTRATOR SWGLINUX    PRINTSERVER  IP
271    24.390625  PRINTSERVER  SWGLINUX     SMB      R session setup & X                          PRINTSERVER  SWGLINUX     IP
272    24.390625  SWGLINUX     PRINTSERVER  SMB      C tree connect & X, Share = \\*SMBSERVER\IPC$ SWGLINUX    PRINTSERVER  IP
274    24.390625  PRINTSERVER  SWGLINUX     SMB      R tree connect & X, Type = IPC               PRINTSERVER  SWGLINUX     IP
281    24.390625  SWGLINUX     PRINTSERVER  NBT      SS: Session Request, Dest: *SMBSERVER     ... SWGLINUX    PRINTSERVER  IP

+NBT: SS: Session Message, Len: 91
-SMB: R session setup & X
  +SMB: NT status code = 0x0, Facility = System, Severity = Success, Code = (0) STATUS_WAIT_0
  +SMB: Header: PID = 0xF5A0 TID = 0x0000 MID = 0x0001 UID = 0x0800
  -SMB: Command = C session setup & X
    SMB: Word count = 3
    SMB: Word parameters
    SMB: Next offset = 0x005B
   -SMB: Setup action = 0x0001
      SMB: ...............1 = Logged on as guest
    SMB: Byte count = 50
    SMB: Byte parameters
    SMB: Native OS = Windows 5.1
    SMB: Native Lanman = Windows 2000 LAN Manager
```

Figure 46: Netmon log corresponding to Administrator login

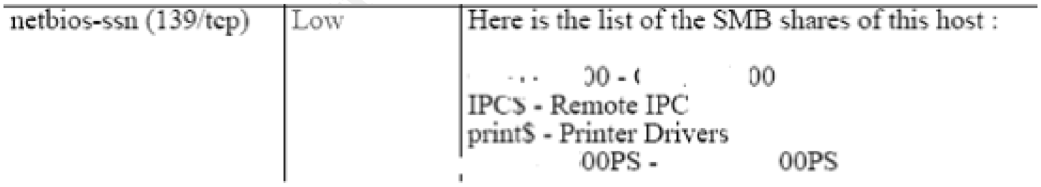
The previous screen shot shows that when Nessus pretended a successful connection using the "Administrator" account, it was in fact a successful connection but it was logged as "Guest" by the SMB server. Consequently this is not a security hole. The server is well configured and corresponds to the product specification.



netbios-ssn (139/tcp)	High	The following shares can be accessed as administrator : - print$ - (readable) + Content of this share : - . - .. - W32X86

Figure 47: Nessus SMB server vulnerability assessment report

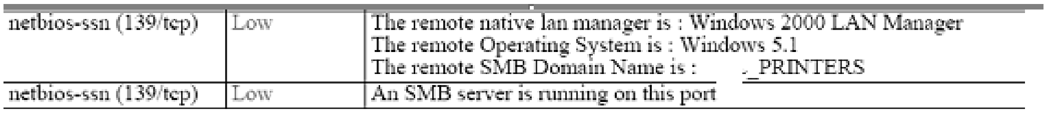
In the previous screen shot Nessus warns that "print$" share is readable. The product specification requires SMB printing and automatic driver download using "Point and Print" and for this "print$" read access is mandatory. Consequently this is not a security hole. The server is configured corresponding to the product specification.



netbios-ssn (139/tcp)	Low	Here is the list of the SMB shares of this host : 00 - (00 IPC$ - Remote IPC print$ - Printer Drivers 00PS - 00PS

Figure 48: Nessus SMB server vulnerability assessment report

The previous screen shot confirms the list of SMB share found using dumpsec.



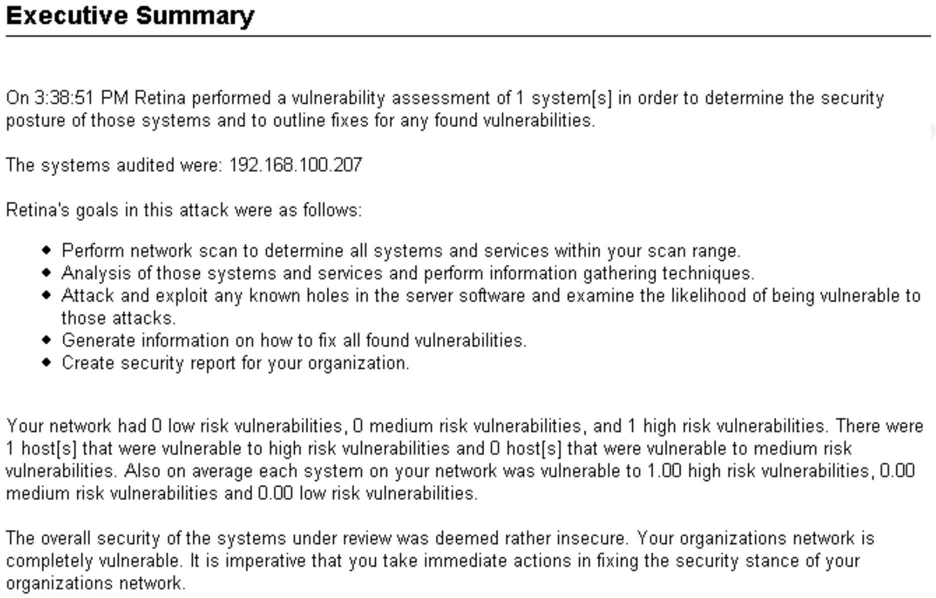
netbios-ssn (139/tcp)	Low	The remote native lan manager is : Windows 2000 LAN Manager The remote Operating System is : Windows 5.1 The remote SMB Domain Name is : _PRINTERS
netbios-ssn (139/tcp)	Low	An SMB server is running on this port

Figure 49: Nessus SMB server vulnerability assessment report

The previous screen shot shows the last two warnings produced by Nessus and

there are no security misconfigurations.
Test 1: Nessus SMB server vulnerabilities scan test passes.

Test 2 (Retina):
The Retina scanner version used for this test is 4.9.140, CVE Database Version 20030102.



Executive Summary

On 3:38:51 PM Retina performed a vulnerability assessment of 1 system[s] in order to determine the security posture of those systems and to outline fixes for any found vulnerabilities.

The systems audited were: 192.168.100.207

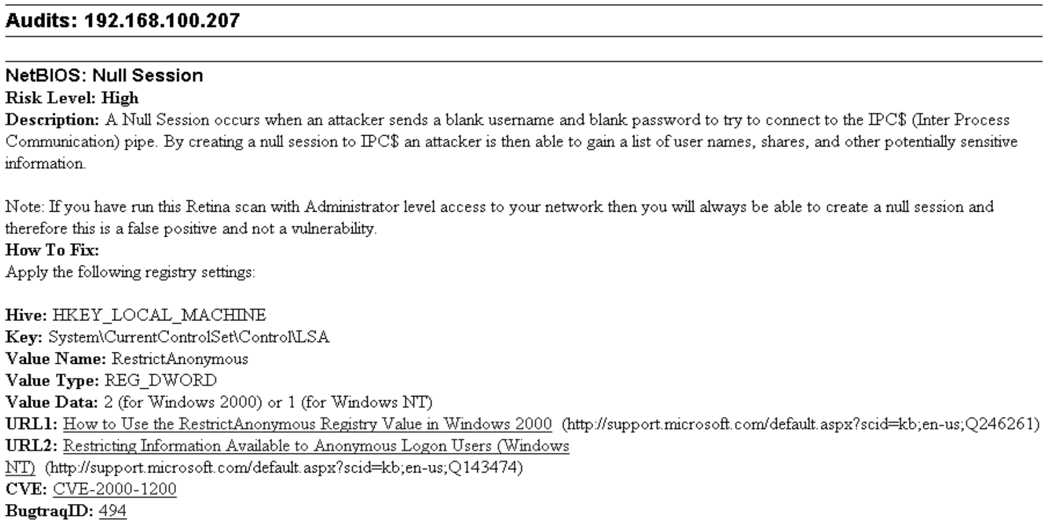
Retina's goals in this attack were as follows:

- Perform network scan to determine all systems and services within your scan range.
- Analysis of those systems and services and perform information gathering techniques.
- Attack and exploit any known holes in the server software and examine the likelihood of being vulnerable to those attacks.
- Generate information on how to fix all found vulnerabilities.
- Create security report for your organization.

Your network had 0 low risk vulnerabilities, 0 medium risk vulnerabilities, and 1 high risk vulnerabilities. There were 1 host[s] that were vulnerable to high risk vulnerabilities and 0 host[s] that were vulnerable to medium risk vulnerabilities. Also on average each system on your network was vulnerable to 1.00 high risk vulnerabilities, 0.00 medium risk vulnerabilities and 0.00 low risk vulnerabilities.

The overall security of the systems under review was deemed rather insecure. Your organizations network is completely vulnerable. It is imperative that you take immediate actions in fixing the security stance of your organizations network.

The previous screen shot shows the executive summary of the SMB vulnerabilities found by Retina. Retina found one high risk vulnerability.



Audits: 192.168.100.207

NetBIOS: Null Session
Risk Level: High
Description: A Null Session occurs when an attacker sends a blank username and blank password to try to connect to the IPC$ (Inter Process Communication) pipe. By creating a null session to IPC$ an attacker is then able to gain a list of user names, shares, and other potentially sensitive information.

Note: If you have run this Retina scan with Administrator level access to your network then you will always be able to create a null session and therefore this is a false positive and not a vulnerability.
How To Fix:
Apply the following registry settings:

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\LSA
Value Name: RestrictAnonymous
Value Type: REG_DWORD
Value Data: 2 (for Windows 2000) or 1 (for Windows NT)
URL1: How to Use the RestrictAnonymous Registry Value in Windows 2000 (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q246261)
URL2: Restricting Information Available to Anonymous Logon Users (Windows NT) (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q143474)
CVE: CVE-2000-1200
BugtraqID: 494

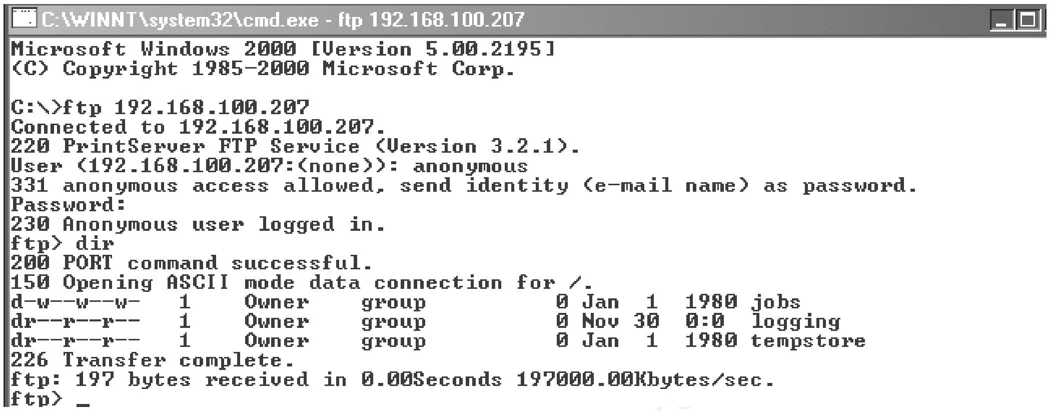
This vulnerability is related to one of the product specification (everyone and from any SMB client should be able to print by SMB). The settings mandatory for the server to follow the product specifications are excluded from the high risk vulnerabilities.
Test 2: Retina SMB server vulnerabilities scan test passes.

Compliance
Control No. 20 passes because all intermediary tests pass.

5.1.7 FTP server tests

Control no. 21	**FTP1: Check FTP server virtual directories ACLs**
Control objective: Verify that virtual directories have correct ACLs.	**Objective- stimulus response**

Test results

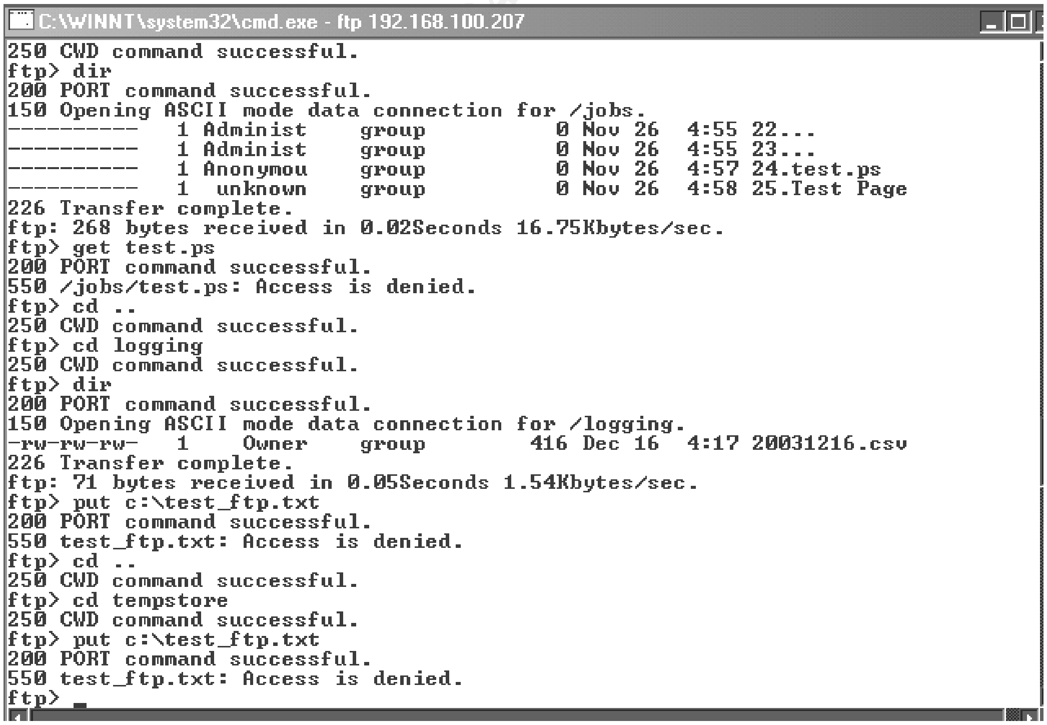


```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ftp 192.168.100.207
Connected to 192.168.100.207.
220 PrintServer FTP Service (Version 3.2.1).
User (192.168.100.207:(none)): anonymous
331 anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /.
d-w--w--w-   1    Owner    group          0 Jan  1  1980 jobs
dr--r--r--   1    Owner    group          0 Nov 30  0:0  logging
dr--r--r--   1    Owner    group          0 Jan  1  1980 tempstore
226 Transfer complete.
ftp: 197 bytes received in 0.00Seconds 197000.00Kbytes/sec.
ftp> _
```

Figure 50: Anonymous FTP connection

The previous screen shot shows an anonymous FTP connection from a remote FTP client to the print server. This server exposes three directories: jobs (only with write permission), logging and tempstore (only with read permission).

Test 1



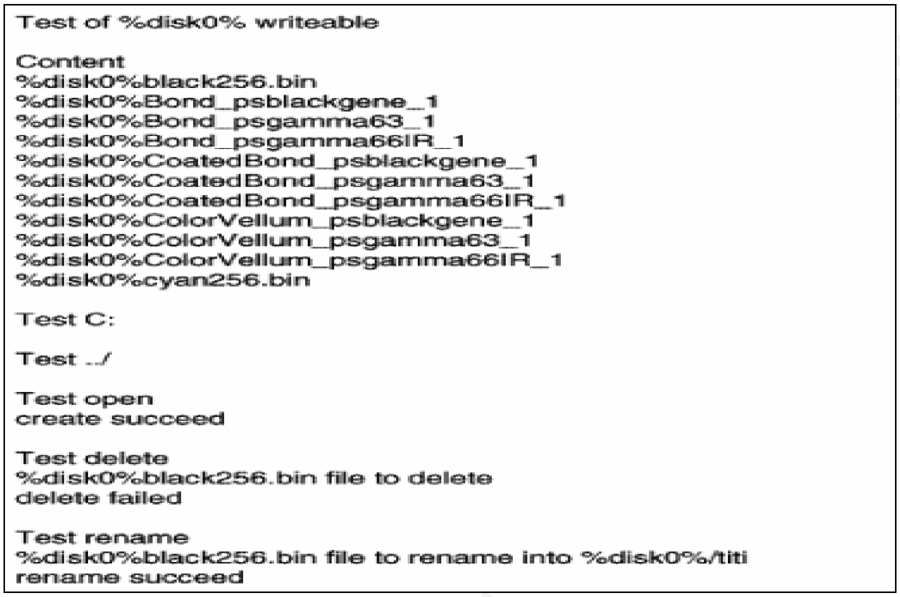
```
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /jobs.
----------   1 Administ    group          0 Nov 26   4:55 22...
----------   1 Administ    group          0 Nov 26   4:55 23...
----------   1 Anonymou    group          0 Nov 26   4:57 24.test.ps
----------   1  unknown    group          0 Nov 26   4:58 25.Test Page
226 Transfer complete.
ftp: 268 bytes received in 0.02Seconds 16.75Kbytes/sec.
ftp> get test.ps
200 PORT command successful.
550 /jobs/test.ps: Access is denied.
ftp> cd ..
250 CWD command successful.
ftp> cd logging
250 CWD command successful.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /logging.
-rw-rw-rw-   1    Owner    group        416 Dec 16   4:17 20031216.csv
226 Transfer complete.
ftp: 71 bytes received in 0.05Seconds 1.54Kbytes/sec.
ftp> put c:\test_ftp.txt
200 PORT command successful.
550 test_ftp.txt: Access is denied.
ftp> cd ..
250 CWD command successful.
ftp> cd tempstore
250 CWD command successful.
ftp> put c:\test_ftp.txt
200 PORT command successful.
550 test_ftp.txt: Access is denied.
ftp> _
```

Figure 51: Anonymous FTP connection

The previous screen shot shows that no file can be added in `logging` directory (readonly) and this is correct. No file can be added in `tempstore` (readonly) and this is correct. No OS dlls and executables are exposed in these directories and this is correct too. **Test 1 passes.** **Test 2** The previous screen shot shows that no file can be retrieved from jobs (writeonly) directory and this is correct. **Test 2 passes.**
Compliance **Control No. 21 passes because all intermediary tests pass.**

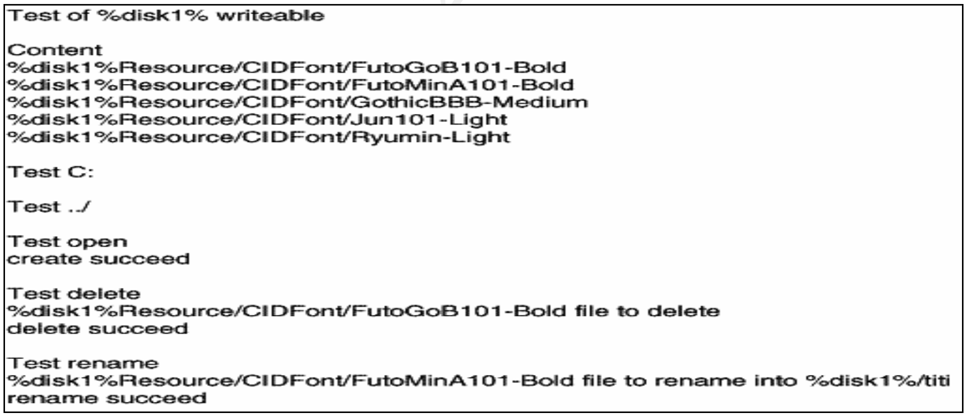
5.1.8 PostScript interpreter tests

The controls number 24, 25 and 26 use the same global PostScript file as stimulus. This PostScript file prints the results on a bitmap. The results for the three controls, for each PostScript interpreter disk, are output on the same page. The following figures show the results for three PostScript disks. The others three are included in Appendix 4 (Page 124).



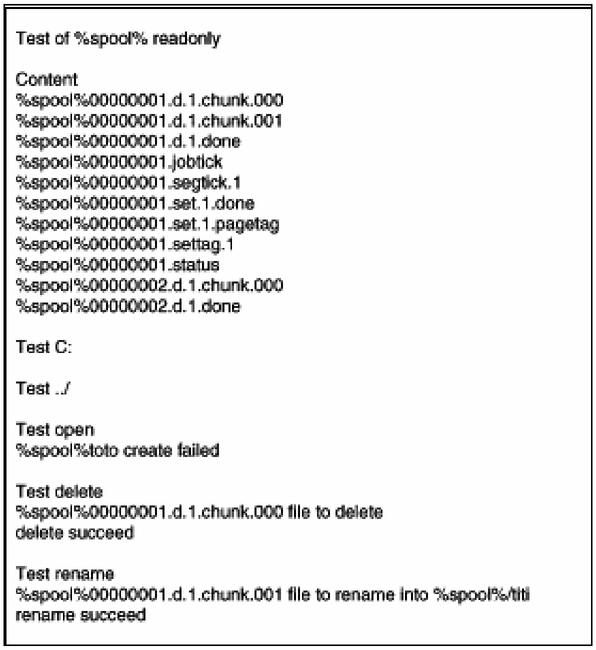
```
Test of %disk0% writeable

Content
%disk0%black256.bin
%disk0%Bond_psblackgene_1
%disk0%Bond_psgamma63_1
%disk0%Bond_psgamma66IR_1
%disk0%CoatedBond_psblackgene_1
%disk0%CoatedBond_psgamma63_1
%disk0%CoatedBond_psgamma66IR_1
%disk0%ColorVellum_psblackgene_1
%disk0%ColorVellum_psgamma63_1
%disk0%ColorVellum_psgamma66IR_1
%disk0%cyan256.bin

Test C:

Test ../

Test open
create succeed

Test delete
%disk0%black256.bin file to delete
delete failed

Test rename
%disk0%black256.bin file to rename into %disk0%/titi
rename succeed
```

Figure 52: PostScript generated bitmap for disk0



```
Test of %disk1% writeable

Content
%disk1%Resource/CIDFont/FutoGoB101-Bold
%disk1%Resource/CIDFont/FutoMinA101-Bold
%disk1%Resource/CIDFont/GothicBBB-Medium
%disk1%Resource/CIDFont/Jun101-Light
%disk1%Resource/CIDFont/Ryumin-Light

Test C:

Test ../

Test open
create succeed

Test delete
%disk1%Resource/CIDFont/FutoGoB101-Bold file to delete
delete succeed

Test rename
%disk1%Resource/CIDFont/FutoMinA101-Bold file to rename into %disk1%/titi
rename succeed
```

Figure 53: PostScript generated bitmap for disk 1



```
Test of %spool% readonly

Content
%spool%00000001.d.1.chunk.000
%spool%00000001.d.1.chunk.001
%spool%00000001.d.1.done
%spool%00000001.jobtick
%spool%00000001.segtick.1
%spool%00000001.set.1.done
%spool%00000001.set.1.pagetag
%spool%00000001.settag.1
%spool%00000001.status
%spool%00000002.d.1.chunk.000
%spool%00000002.d.1.done

Test C:

Test ../

Test open
%spool%toto create failed

Test delete
%spool%00000001.d.1.chunk.000 file to delete
delete succeed

Test rename
%spool%00000001.d.1.chunk.001 file to rename into %spool%/titi
rename succeed
```

54: PostScript generated bitmap

Control no. 24	**PS1: Check how the PostScript interpreter controls access to information**
Control objective: It should not be possible to retrieve information on file system partitions using a PostScript file	**Objective- stimulus response**
Test results In the all the pages generated by the PostScript file no OS sensitive files are exposed and the drive C: can't be browsed (please see the previous pages to have a snapshot of each PostScript generated pages). **Test passes.**	
Compliance **Control No. 24 passes.**	

Control no. 25	**PS2: Check PostScript directories ACLs**
Control objective: The access rights on PostScript file system should be set appropriately	**Objective- stimulus response**
Test passes For all the PostScript tests a global "ps" file was used and the screen shots are included either in page 91 or in Appendix 4 (Page124). On disk0 that is writable, no OS files are exposed. On this disk files can be created and renamed but can't be deleted. **Test passes.** The disks disk1, disk2, disk3 and disk10 are writable but no OS files are exposed. On these disks we can create, delete and rename files. **Tests pass.** On a private disk that is readonly, no OS files are exposed. On this disk files can't be deleted and renamed files. **Test passes.** On another readonly private disk called the "spool", no OS files are exposed. However, in this disk files can be deleted and renamed. **Test fails** because files from a readonly disk can be deleted and renamed files.	
Compliance **Control No. 25 fails because one intermediary test failed.**	

Control no. 26	**PS3: Check PostScript interpreter directory transversal access**	
Control objective: Parent relative access from the PostScript interpreter should be forbidden		**Objective- stimulus response**
Test results For all the PostScript tests a global “ps” file was used and the screen shots are included either in page 91 or in Appendix 4 (Page124). For all the disks seen by the PS interpreter it wasn’t possible to access the upper level directory (test flagged as Test ../). **All tests pass.**		
Compliance **Control No. 26 passes because all intermediary tests passed.**		

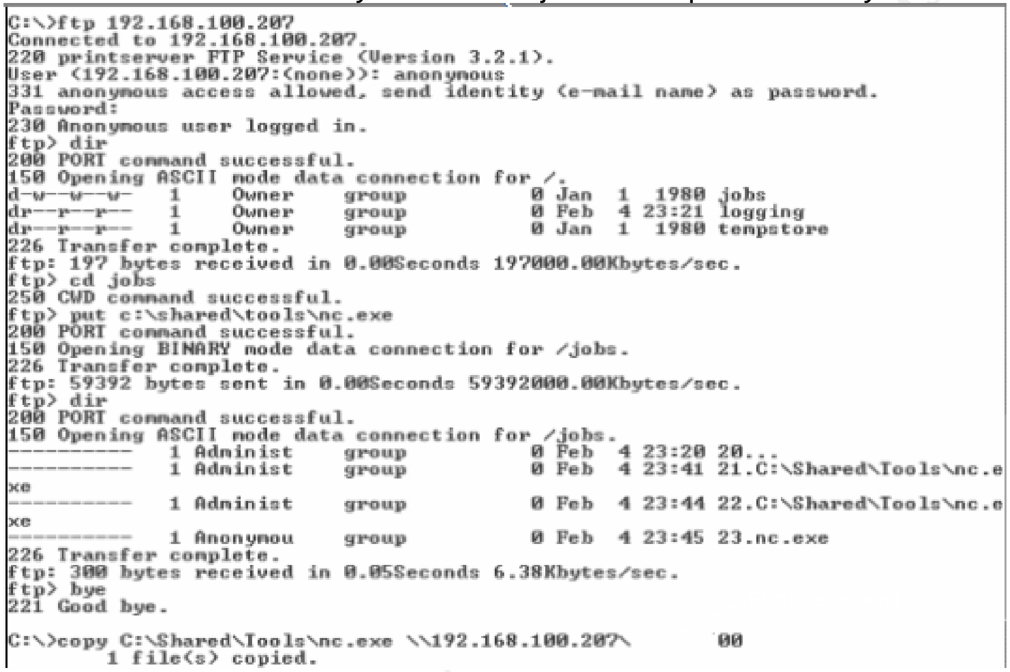
5.1.9 Malware execution checklist

Control no. 29	**MAL2: Check that in every writable directory exposed by the print server no code can be executed**
Control objective: The print server should not allow executing code in the exposed writable directories	**Objective- stimulus response**

Test results

Test SMB and FTP

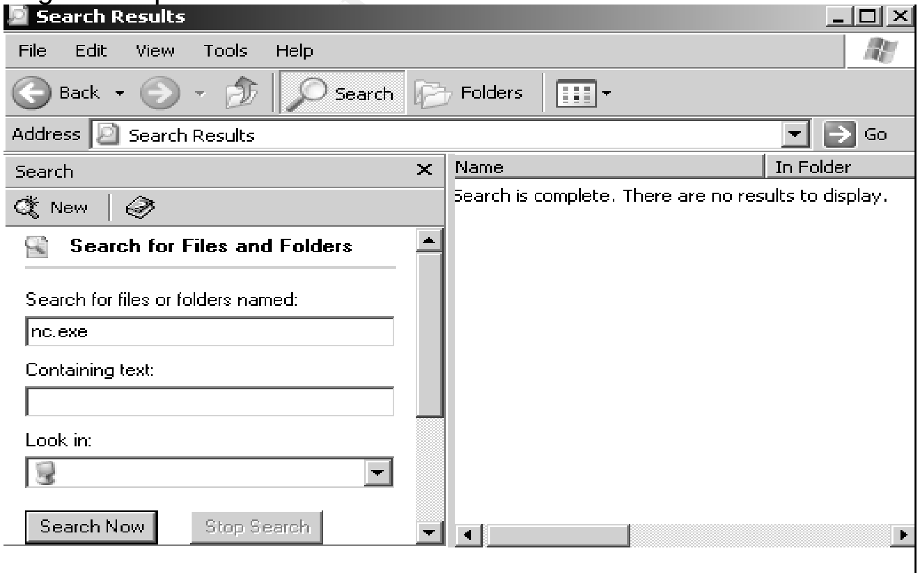
From a remote Windows system submit jobs to the print server by FTP and SMB.



```
C:\>ftp 192.168.100.207
Connected to 192.168.100.207.
220 printserver FTP Service (Version 3.2.1).
User (192.168.100.207:(none)): anonymous
331 anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /.
d-w--w--w-   1    Owner    group           0 Jan  1  1980 jobs
dr--r--r--   1    Owner    group           0 Feb  4 23:21 logging
dr--r--r--   1    Owner    group           0 Jan  1  1980 tempstore
226 Transfer complete.
ftp: 197 bytes received in 0.00Seconds 197000.00Kbytes/sec.
ftp> cd jobs
250 CWD command successful.
ftp> put c:\shared\tools\nc.exe
200 PORT command successful.
150 Opening BINARY mode data connection for /jobs.
226 Transfer complete.
ftp: 59392 bytes sent in 0.00Seconds 59392000.00Kbytes/sec.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /jobs.
----------   1 Administ    group           0 Feb  4 23:20 20...
----------   1 Administ    group           0 Feb  4 23:41 21.C:\Shared\Tools\nc.e
xe
----------   1 Administ    group           0 Feb  4 23:44 22.C:\Shared\Tools\nc.e
xe
----------   1 Anonymou    group           0 Feb  4 23:45 23.nc.exe
226 Transfer complete.
ftp: 300 bytes received in 0.05Seconds 6.38Kbytes/sec.
ftp> bye
221 Good bye.

C:\>copy C:\Shared\Tools\nc.exe \\192.168.100.207\       00
        1 file(s) copied.
```

Figure 55: Submit a file to the print server using FTP and then SMB

Log on the print server as administrator.



Search is complete. There are no results to display.

Search for files or folders named: nc.exe

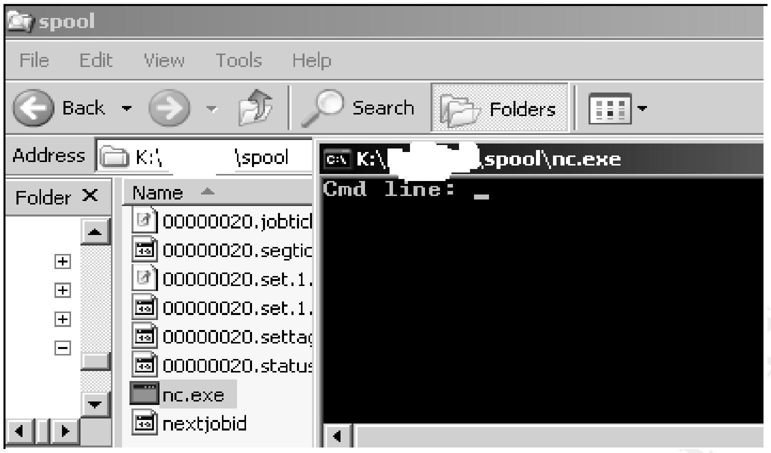
Containing text:

Look in:

Figure 56: Search for nc.exe on the print server

Search for `nc.exe` on all the system. `Nc.exe` can't be found. This is correct because the .exe files are not considered as graphic language jobs and are erased.
The FTP and SMB tests pass.

Test SPOOL



```
Cmd line: _
```

Figure 57: nc.exe can be executed in the spool directory

The auditor logged on the print server as administrator and put an `nc.exe` file in the spool directory. The previous screen shot shows `nc.exe` executing in the spool directory and this is not correct.
The SPOOL test fails.

Test PostScript
For all the PostScript disks the results are included in Appendix 5 (Page 125). Nc.exe can be executed in all the PostScript writable disks. This is not correct.
All the PostScript tests fail.

Compliance
Control No. 29 fails because several intermediary tests failed.

5.1.10 Controls Executive Summary

Control number	Short control description	Risks covered	Consequence	Likelihood	Pass or Fail?
1	P1: Check the OS of the system	R1.1, R1.5, R2.1, R2.2	H	H	Pass
2	P2: Check the Web server version	R1.4	M	M	Pass
3	P3: Check the remote Web server administration	R1.5	H	M	Pass
4	P4: Check the system remote SMB administration	R1.13	H	M	Pass
5	P5: Check the remote firewall administration	R1.14	H	M	Pass
6	F1: Check the firewall software patch level	R1.1, R2.1	H	L	Pass
7	F2: Check the firewall ruleset against the product specification	R1.1, R2.1	H	M	Pass
8	F3: Check what happens when the firewall is not running	R1.1, R2.1	H	M	Pass
9	F4: Check how the firewall protects the system from attacks with unexpected TCP flags	R1.1	M	M	Pass
10	F5: Check how the firewall protects the system from attacks on other IP protocols and on other protocols	R1.1	M	M	Pass
11	F6: Check if the firewall detects unauthorized network activities on the system	Best practice	L	M	Pass
12	W1: Check that the web server is minimizing services	R1.10	H	M	Pass
13	W2: Check the filesystem ACLs on web server directories	R1.10	H	M	Fail
14	W3: Check if Web server logging is appropriate	Best practice	L	M	Fail
15	W4: Evaluate the Web server with two CGI scanners	R1.4	H	M	Pass
16	W5: Evaluate the Web server with two vulnerability scanners	R1.4	H	H	Fail
17	W6: Check the Web server permissions	R1.4, R1.10	H	L	Pass
18	W7: Check the Java Virtual Machine patch level	R1.4	H	L	Pass
19	SMB1: Only PRINT$, IPC$ and PRINTQUEUE shares should be exposed and the appropriate ACLs should be set	R1.9	H	M	Pass

20	SMB2: Check the SMB server security with two vulnerability scanners	R1.5	H	H	Pass
21	FTP1: Check FTP server virtual directories ACLs.	R1.8	H	M	Pass
22	FTP2: Check FTP server has no well-known security vulnerabilities	R1.11	H	H	Pass
23	FTP3: Check the FTP server permissions	R1.8, R1.11	H	L	Fail
24	PS1: Check how the PostScript interpreter controls access to information	R1.7	M	M	Pass
25	PS2: Check PostScript devices/directoires ACLs	R1.7	H	M	Fail
26	PS3: Check PostScript interpreter directory traversal access	R1.12	H	M	Pass
27	PS4: Check PostScript interpreter permissions	R1.7, R1.12	H	L	Fail
28	MAL1: Check that no directories simultaneously writable and readable are exposed	R2.6	H	M	Pass
29	MAL2: Check that no code can be executed in every writable directory exposed by the print server	R2.2	M	L	Fail

5.2 Measure Residual Risk

The exposure - controls = residual risk.

5.2.1 Residual risk for the system integrity threat

Residual risk related to the exclusion of attacks targeting only in-house developed applications

Even protected by a firewall the attack surface of this product is large. In order to reduce the resources needed to audit the system, the auditor has excluded from the audit the attacks needing crafted packets targeting only in-house developed applications. Consequently, no controls were developed to verify potential weakness related to in-house developed applications. These applications may not be bug-free and a security error may still allow an attacker to take control over the system (Please see R1.2, R1.3 and R1.4 in the Security risk tables for more details). For the next step in order to increase the security level, the auditor is recommending a security audit targeted at these in-house developed applications.

Residual risk related to FTP server passive mode

The inbound traffic on TCP ports between 1024-65535 (required by FTP server data passive) will not be protected by the firewall because the FTP server uses any port from the dynamic range for data connections (Please see R1.6 in the Security risk tables for more details).

There are several possibilities to mitigate this risk:

1) Change the implementation of the current FTP server by limiting the range of the ports that may be used for data connections. This will allow limiting the range of the ports not protected by the firewall (the risk is reduced). Even if reducing the port range is not very difficult, only the development team can precisely estimate the workload to modify this.
2) Use another kind of firewall that can protect FTP servers in passive mode. The system owner may envisage the use of an application-proxy firewall (probably more expensive) or the Windows XP Internet Connection Firewall that can directly interact with the applications. Even if no additional fee will be needed for the second solution (the firewall is natively supplied by the OS used by the print server), the impact in terms of integration cost and the impact on the product functionalities should be estimated by the development team.
3) Decide to remove the support of FTP server data passive (the risk is eliminated). However, the customer's needs must be re-analysed because the FTP server passive connections are particularly useful when the client FTP system is protected by a packet filter firewall.

Only the system owner can choose between the three solutions. There is always a balance to be found between functionality, security and resources. However, from a security point of view it is not recommended to use a firewall to protect a system and to let so many ports unfiltered.

Residual risk related to the exclusion of the local interfaces

The company XYZ Inc. limited the audit scope to the network services. The local interfaces (floppy disk, USB, CDROM drive, keyboard and monitor) were excluded from the audit. However, the security audit for the physically accessible interfaces are mandatory in order to asses the global system security level.

5.2.2 Residual risk for the network integrity threat

If an intruder succeeds in installing a malware, the ports open for FTP, SMB, DNS or DHCP clients can be used to access the LAN (Please see R2.2 in the Security risk tables for more details). Furthermore, the outbound traffic originating from TCP ports between 1024-65535 (required by FTP client data passive and in-house developed FTP server data active) will not be protected by this kind of firewall configuration. The firewall used in this product can't protect against this risk because it is a packet filter (transport level firewall) that controls only ports. The auditor is strongly recommending the use of an application level firewall that will allow specifying the applications allowed to open dynamic ports.

Anyway, an exploit that gives administrative privilege to the attacker is most of the time lethal. Protecting the customer's network integrity even when the system integrity is compromised is an ambitious goal and can't be reached with only one level of protection. Employing the "defence in depth" principle can increase the difficulty for the attacker to achieve its goal.

There are several steps that can decrease the risk:
- prevent the malwares to enter the system:
    - by having all the controls specified in the audit checklists with a pass status
    - by choosing the appropriate firewall that mitigates the risks related to the FTP protocol
- prevent the malwares to execute on the system
    - by having all the controls related to malware propagation with a pass status
    - by employing a hardware platform that enforces the separation of application code and data ("preventing an application from executing program code that an attacking worm or virus inserted into a portion of memory marked for data only"- please see [REF_G7] "Windows XP Service Pack 2: A developer's view" for further details)
- detect the system integrity corruption
    - by using an integrity checking mechanism that verifies that no unexpected piece of software has been introduced in the system.

Combining several of the previous steps can significantly reduce this risk.

5.3 Is the system auditable?

The print server protected by a host-based firewall is an auditable system. Most of the controls are objective and the compliancy is always binary.

The system's role in the organization is very easy to define:
- allow printing and scanning jobs,
- allow print jobs monitoring and management.

However, the number of "security" relevant entities cooperating to fulfill its role is consequent:

- OS,
- firewall,
- web server,
- FTP server,
- LPD server,
- FTP, SMB clients
- DNS, DHCP clients,
- graphic language interpreters.

The main difficulty of the work was to establish a risk model and to create a reasonable number (no more than 30) of controls in order to asses the system security risks.

6 Assignment 4 –Audit report

6.1 Executive summary

The attack surface of the audited system is large. The auditor identified 21 possible vulnerabilities with high and medium impact on the identified threats (please see the section 3.2.4.3 on page 15 for more details). In order to reduce the resources needed to audit the system, the auditor has excluded from the audit the attacks needing crafted packets targeting only in-house developed applications.

6.1.1 Positive points

The print server is up-to-date according to the controls included in the checklist. Moreover, it passed all the controls related to the general company security policy. The auditor discovered a web directory traversal vulnerability that can be used to obtain sensitive information but not to corrupt system integrity. With the current level of knowledge of the OS and server vulnerabilities, this product doesn't contain security problems allowing system integrity corruption (threat 1).

6.1.2 Negative points

However, most of the preventive controls failed:

- the ACLs on web server directories are inappropriate
- the web server logging is inappropriate
- the controls related to running software with minimal privileges failed for the FTP server and PostScript interpreter.
- the print server exposes several directories writable via PostScript with execute permissions

Moreover, the web server has a directory traversal vulnerability that allows a remote user to retrieve any file on the print server if the attacker detects the OS version. Unfortunately this security error wasn't corrected by the current public version (2.2.3) of the web server and no security patch has been released yet. The auditor informed the owner of the system about this vulnerability and requested that the web server distributor be informed.

The auditor doesn't consider the VisNetic for workstation firewall appropriate for this print and scan server. The firewall doesn't fail any control. It is a stateful packet filter that fully fulfils its specifications. However, this product needs an application level firewall in order to cover the network integrity corruption threat (please see the paragraph 5.2.2 on page 100 for more details) because product specifications includes

1) an FTP passive mode server
2) several clients (FTP, SMB, DNS, DHCP)

6.2 Audit findings

During this audit the auditor had administrative privileges over the system but he is not the owner of the system.

For several failed controls, he has made recommendations on how the problems should be fixed and proved that after performing the steps suggested by the auditor, the associated control passes. However, it is the system owner's responsibility to validate the modifications and to decide if the correction will be applied before the product commercial release or in a future version.

For several failed controls, it was not feasible for the auditor to make a recommendation on how to correct the problem because the modifications required a re-design or modification of the print server code. In this case, the auditor described the risks of leaving the system unchanged and suggested that the system owner should perform further analysis in order to determine the cost of correcting the problem.

6.2.1 Failed controls

This paragraph contains the failed controls and the risks associated. The auditor proposed solutions to correct several failed controls.
Part of the failed controls can be only fixed in a future product release.
However, several proposed recommendations are considered as important by the auditor and seems easy to implement. The auditor is strongly recommending taking them into account before the commercial release.

Audit finding 1 **The ACLs on the web server directories are not correctly set (control number 13)**
Background/risk The audit proved that this vulnerability can not be remotely exploited; there is no known way to write to those directories (neither using product functionalities nor using known vulnerabilities). This vulnerability could be exploited by users with local console access. Even if the security audit of the system's physically accessible interfaces is out of the scope for this audit, the correction of this control was strongly recommended. If this control isn't corrected, everyone with physical access could change the configuration files, log directories, document root directories, could add new servlets and new code to the web server and this without the necessity of administrative privileges (because the audit proved that "everyone" has all the permissions required to modify files).
Root cause The root cause is the fact that the decision on how to launch the web application (server included) was based on the easiest way to do it and not the most secure one. A corrective control would be to have a new rule added to the company's security policy that will control the ACLs on the directories exposed by any network service.
Audit recommendation The auditor's proposal is to launch the web application (that includes the web server) as a service running on an account with limited privileges. Furthermore, all the web server directories ACLs were tuned to allow minimal rights.
Test results

This control initially failed but it is correctable.

Test 1

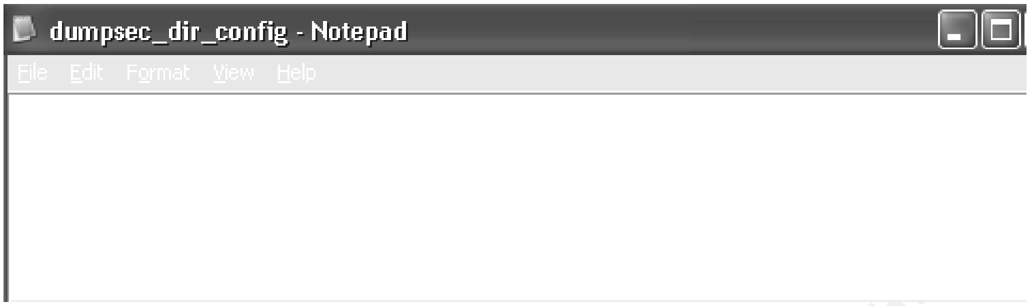
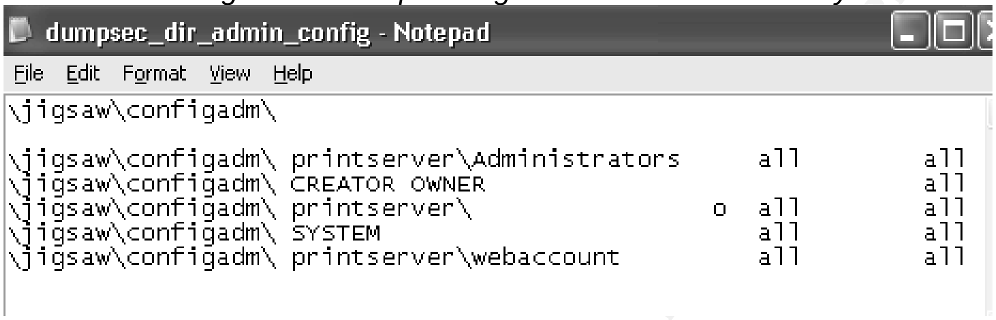


Figure 58: dumpsec log file for CONFIG directory


dumpsec_dir_admin_config - Notepad
File Edit Format View Help

```
\jigsaw\configadm\

\jigsaw\configadm\ printserver\Administrators     all        all
\jigsaw\configadm\ CREATOR OWNER                             all
\jigsaw\configadm\ printserver\               o  all        all
\jigsaw\configadm\ SYSTEM                        all        all
\jigsaw\configadm\ printserver\webaccount        all        all
```

Figure 59: dumpsec log file for CONFIG_ADMIN directory

The previous screen shots show that only the administrator account, web server account and the system have any rights on the web server configuration directories. The users aren't even mentioned because they were completely removed from the ACLs. This is correct.

This print server doesn't have two administrative accounts. The `DumpSec` generated file contains two lines (`printserver\Administrators` and `printserver\.....` because the administrator account has been renamed with a name that was masked by the auditor for confidentiality reasons.
Test 1 passes.

Test 2:
The tools and test methods used for this test are similar to those of the previous test. The screen shot can be found in Appendix 6 (Page 127).
The screen shot shows part of the `DumpSec` log file containing the permissions of the server log directories (DIR_LOGS). The screen shot shows that only the administrator account, web server account and the system have any rights on the web server log directory. This is correct. The users were completely removed from the ACLs.
Test 2 passes.

Test 3:
The screen shot can be found in Appendix 6 (Page 127).
The screen shot shows part of the file containing the permissions of directories containing GCI scripts. The users have only the right to read and execute. However, special permissions are mentioned for the users and the screen shot (named "*ACLs on cgi-bin folder*") shows that the users have no

right to write on this folder.

The screen shots containing the permissions for the directories containing servlets are included in Appendix 6 (Page 127). The users don't have the right to write to these folders and this is correct.

Test 3 passes.

Test 4

The screen shots can be found in Appendix 6 (Page127).

The screen shots show part of the `DumpSec` log file containing the permissions of the server document root directory. The users don't have the right to write in these folders and this is correct.

Test 4 passes

Test 5: not applicable because there are no aliases.

Test 6:

The screen shots can be found in Appendix 6 (Page 127).

The screen shots show part of the `DumpSec` log file containing the permissions of the directories included in the CLASSPATH environment variable. The users don't have the right to write in these folders and this is correct.

Test 6 passes

The control 13 passes because all the intermediary tests pass.

Costs

This problem is not difficult to solve technically (the auditor spent one day to do it). However, the modification may have an impact on the web application and only the system owner can evaluate the time needed to validate the web application.

Audit finding 2

Web server logging isn't appropriate (control number 14).

Background/risk

If the Web server log isn't enabled it will not be possible for the customer to detect or prove attacks against the server.

Root cause

The need to detect and prove an attack has not been included in the previous product specification. A preventive control can be to add this requirement by default for the new products.

Audit recommendation

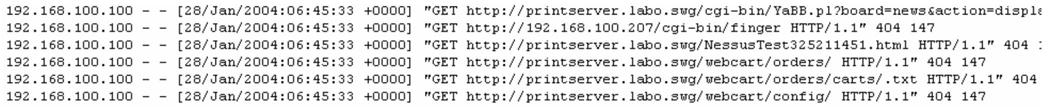
The auditor's recommendation is to activate the web server logs and to inform the customers to check these logs on regular bases.

Test results

This control initially fails but it is correctable.

In order to activate the logging process, add the following line in the web server configuration file http-server.conf :

```
org.w3c.jigsaw.logger=org.w3c.jigsaw.http.CommonLogger
```



```
192.168.100.100 - - [28/Jan/2004:06:45:33 +0000] "GET http://printserver.labo.swg/cgi-bin/YaBB.pl?board=news&action=displ
192.168.100.100 - - [28/Jan/2004:06:45:33 +0000] "GET http://192.168.100.207/cgi-bin/finger HTTP/1.1" 404 147
192.168.100.100 - - [28/Jan/2004:06:45:33 +0000] "GET http://printserver.labo.swg/NessusTest325211451.html HTTP/1.1" 404
192.168.100.100 - - [28/Jan/2004:06:45:33 +0000] "GET http://printserver.labo.swg/webcart/orders/ HTTP/1.1" 404 147
192.168.100.100 - - [28/Jan/2004:06:45:33 +0000] "GET http://printserver.labo.swg/webcart/orders/carts/.txt HTTP/1.1" 404
192.168.100.100 - - [28/Jan/2004:06:45:33 +0000] "GET http://printserver.labo.swg/webcart/config/ HTTP/1.1" 404 147
```

The previous screen shot shows parts of the web server log file during a Nessus vulnerability scan.
The IP address of the attacker, the date and time of the attack and requested URL can be identified.
The logging rotate frequency is done by:

`org.w3c.jigsaw.rotateLevel`

This property gives the frequency of log rotation used in the logger.

0 - log name is defined by `org.w3c.jigsaw.logger.logname`, no rotation done
1 - log name is as above with _yyyy added, rotation done every year on January 1st 00:00.
2 - log name as 0 with _yyyy_mm added, rotation done every month on the 1st at midnight.
3 - log name as 0 with _yyy_mm_dd added, rotation done every day at 00:00.

Costs
This problem is not difficult to solve technically (the auditor spent 2 hours do it). However, the real issue is to modify the user manual in order to advice the customers to review the logs on regular bases. Only the system owner can evaluate the time necessary to modify the user manual.

Audit finding 3
The web server has one high level security vulnerability discovered by Nessus scanner : directory traversal (control number 16)

Background/risk
Every remote user can see sensitive files on the print server.

Root cause
The web server has a security bug.
The last version of the Jigsaw web server isn't applied but this is acceptable: the last version was released on November 27th, 2003 and the product entered the consolidation test at the beginning of November (the product respects company policy rule). Furthermore, the distributor doesn't mention any security fixes in the release note for Jigsaw 2.2.3.
Consequently, this kind of problem can't be fixed by a new control. The system owner should verify the web server checklist before every new product release in order to detect the vulnerabilities and take corrective actions.

Audit recommendation
The auditor uploaded the version (2.2.3) of the Jigsaw web server. The same directory traversal error was encountered. The distributor was informed and quickly reacted by sending a security patch. This patch was directly sent to the system owner. The auditor installed and tested the correction.

However, at the date this report was submitted, this security patch is not yet published on www.w3c.org site. The distributor insured that this correction will be included in the next Jigsaw version (2.2.4) expected to come very soon.

Test results

The auditor used Nessus to scan for known security vulnerabilities (the scanner was set-up with the same options specified in the control number 16). The security patch corrected the directory traversal error. The results can be found in Appendix 8 (on page 134).

The control 16 passes.

Costs

This problem is not difficult to solve technically (the auditor spent 2 hours to do it). However, the modification may have an impact on the web application and only the system owner can evaluate the time needed to validate the web application.

Audit finding 4

FTP server runs with administrative privileges (control number 23).

Background/risk

Having the FTP server running with administrative privileges can cause two categories of problems:

Category 1: the server may be misconfigured or may have well known security flaws; the impact of these security flaws is proportional to the server privileges.

Category 2: if an attacker manages to produce a buffer overrun on the FTP server and if he can inject the appropriate command (for instance bind a command shell to the port of his choice), he can gain administrative privileges over the system.

The audit already proved that the ACLs of the FTP server's virtual directories are correctly set and that this server has no well-known vulnerabilities (consequently there are controls in place to mitigate the first risk category). Consequently, an attacker needs to craft special packets for this in-house developed FTP server in order to exploit the vulnerability of having the server running with administrative privileges (second risk category).

Root cause

During the product design the principle of running services with the least privileges was not applied. A preventive control would be to add by default the requirement that a service should run at the minimal privilege required to fulfil its function.

Audit recommendation

The system owner states that this problem can't be corrected with the current product design. The auditor has not in-depth knowledge of the product design and he can't propose a correction.

Test results

This control fails and can't be corrected with the current system design.

Compensating controls

The risk is mitigated by the fact that this is an in-house developed FTP server and crafting the appropriate command is too much of a pain for most of the hackers (it is not very likely that a skilled hacker will have access to this kind of print server and will spend his time with it).
The auditor checked that for the current release the FTP server is correctly configured and doesn't include any well-known high and medium risk vulnerabilities. However, security errors may appear in a future release. Consequently, the auditor recommends as a compensating control to verify the checklist related to the FTP server for every future product releases.
Another compensating control can be a security audit targeting this in-house developed application.

Audit finding 5
The PostScript interpreter allows writing files in a "readonly" directory (control number 25)

Background/risk
It is possible to delete and rename files that the print server needs. However, given the fact that no OS or print server sensitive files (executables and dlls) are exposed system integrity can't be impacted.

Root cause
The PostScript interpreter was not been previously tested for security errors. A preventive control would be to test every new version of the PostScript interpreter with the same kind of file the auditor used.

Audit recommendation
The system owner accepted to analyse this problem and to correct this issue for the next product release. The auditor has not in-depth knowledge of the product design and he can't propose a correction

Test results
This control failed but it is correctable. The owner of the system didn't provide the new version for validation. This control fails for the current release.

Compensating controls
The risk is mitigated by the fact that no OS files are exposed on the PostScript disks.
The auditor accepted that for the current release the PostScript interpreter has no security errors allowing system integrity corruption. However, there are some errors allowing denial of service attacks and these errors should be corrected even if they are out of the scope of this audit.
The auditor recommends as a compensating control to verify the checklist related to the PostScript interpreter for every future product releases.

Audit finding 6
PostScript interpreter runs with administrative privileges (control number 27).

Background/risk

Having the PostScript interpreter running with administrative privileges can cause two categories of problems:

Category 1: the interpreter may be misconfigured; the impact of these security flaws is proportional with the interpreter privileges

Category 2: if an attacker manages to produce a buffer overrun on the PostScript interpreter and if he can inject the appropriate command (for instance bind a command shell to the port of his choice), he can gain administrative privileges over the system

The audit already proved that the PostScript interpreter has no vulnerabilities related to access to OS files or to start-up folders (consequently there are controls in place to mitigate the first risk category).

An attacker needs to craft special commands targeting this in-house developed PostScript implementation in order to exploit the vulnerability of having the interpreter running with administrative privileges(second risk category).

Root cause

During the product design the principle of running services with the least privilege was not applied. A preventive control would be to add by default the requirement that a service should run at the minimal privilege required to fulfil its function.

Audit recommendation

The system owner states that this problem can't be corrected with the current product design. The auditor has not in-depth knowledge of the product design and he can't propose a correction.

Test results

This control fails and it is not correctable. The risk is mitigated by the fact that this interpreter is in-house developed application.

Compensating controls

Even if the security dangerous commands may be common to all the interpreters supporting PostScript, the impact on the system depends on how the file system access is implemented by each interpreter. Consequently, an attacker needs to have access to this in-house developed interpreter in order to prepare an exploit allowing system integrity corruption.

Crafting the appropriate command is too much of a pain for most of the hackers (it is not very likely that a skilled hacker will have access to this kind of print server and will spend his time with it).

The auditor accepted that for the current release the PostScript interpreter doesn't constitute a high risk item, especially if the control 25 is corrected. However, security errors may appear in the next releases. Consequently, the auditor recommends as a compensating control to verify the checklist related to the PostScript interpreter for every future product release.

Audit finding 7

The print server exposes writable directories that are executable (control number 29)

Background/risk

If another vulnerability allowing an attacker to execute code coexists, execute permissions on writable directories facilitate the attacker's work

Root cause

The root cause is the fact that the decision on how to install the system was based on the easiest way to do it and not the most secure one. A corrective control would be to have a new rule added to the company's security policy controlling the ACLs on the directories exposed by any network service.

Audit recommendation

There are at least two possibilities to correct this problem.

<u>The first solution:</u>

For each directory that can be accessed by a remote user, modify the ACLs on the physical directories by removing the execute rights.
Advantage: It is very easy to implement.
Disadvantage: It reduces the malware execution risk only on these directories.

<u>The second solution</u>:

Use the Software Restriction Policies to specify the binaries that are allowed to run on the system. If an attacker manages to put a binary in a remote accessible directory, it will not be possible to run it since this executable will not be in the list of allowed binaries.
Advantage: It reduces the malware execution risk on the entire system.
This solution is more difficult to set-up because the exhaustive list of all executables required for the system is needed.

The auditor recommends the second solution. However, only the system owner is able to implement the second solution.

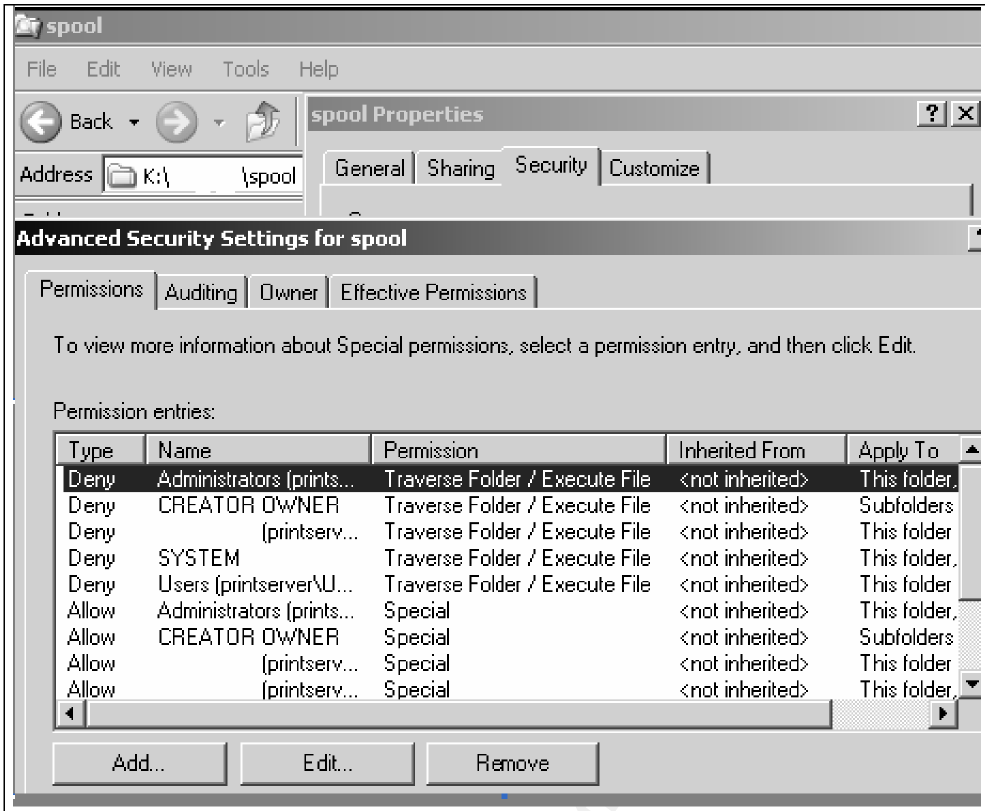
Test results

This control failed but it is correctable.

The results for the control 29 show that:

- FTP and SMB tests pass
- SPOOL and PostScript disks fail

In order to prove that control 29 is correctable, the auditor manually removed the execute rights of the physical directories corresponding to every SPOOL and writable PostScript disks.


spool
File Edit View Tools Help
Back
spool Properties
General Sharing Security Customize
Permissions Auditing Owner Effective Permissions
Add... Edit... Remove

Address K:\ \spool

Advanced Security Settings for spool

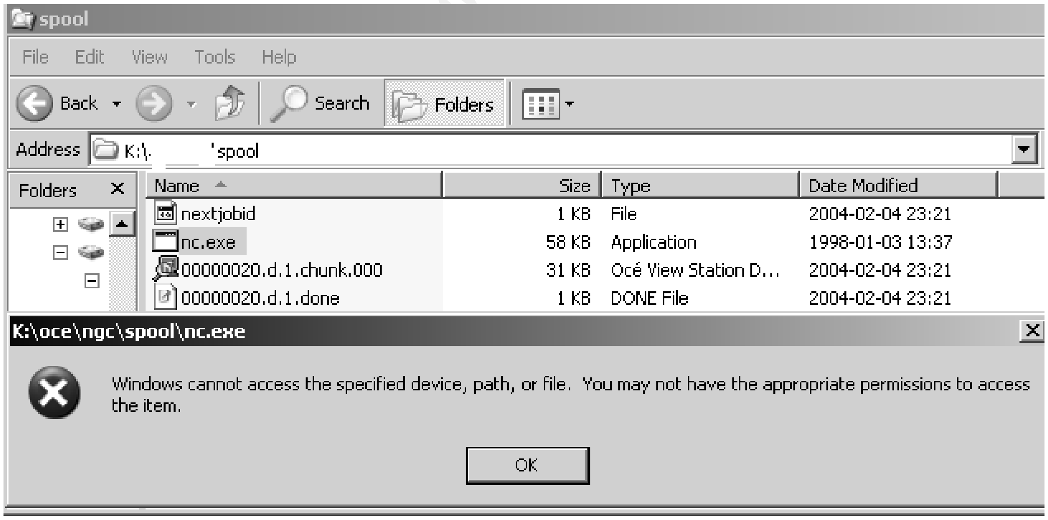
To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Deny	Administrators (prints...	Traverse Folder / Execute File	<not inherited>	This folder,
Deny	CREATOR OWNER	Traverse Folder / Execute File	<not inherited>	Subfolders
Deny	(printserv...	Traverse Folder / Execute File	<not inherited>	This folder
Deny	SYSTEM	Traverse Folder / Execute File	<not inherited>	This folder,
Deny	Users (printserver\U...	Traverse Folder / Execute File	<not inherited>	This folder
Allow	Administrators (prints...	Special	<not inherited>	This folder,
Allow	CREATOR OWNER	Special	<not inherited>	Subfolders
Allow	(printserv...	Special	<not inherited>	This folder
Allow	(printserv...	Special	<not inherited>	This folder,

Figure 60: Deny execute access to the SPOOL directory

The previous screen shot shows that even the administrative accounts don't have the privilege to execute files in the SPOOL directory.



Address K:\. 'spool

Name	Size	Type	Date Modified
nextjobid	1 KB	File	2004-02-04 23:21
nc.exe	58 KB	Application	1998-01-03 13:37
00000020.d.1.chunk.000	31 KB	Océ View Station D...	2004-02-04 23:21
00000020.d.1.done	1 KB	DONE File	2004-02-04 23:21

K:\oce\ngc\spool\nc.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

Figure 61: nc.exe can't run in the SPOOL directory

.

The previous screen shot shows that nc.exe can't be executed in this folder. **The SPOOL test passes.**

The screen shots included in Appendix 7 (Page 132) show that it is not possible to run nc.exe on the PostScript writable disks.

The PostScript disks tests pass. **Control 29 passes.**
Costs This problem is not difficult to solve technically (the auditor spent half a day to do it). However, these modifications may have an impact on the PostScript interpreter and the owner of the system should evaluate the time needed to validate the proposed solution.

6.2.2 Executive summary of failed controls and fixes

The following table summarizes the status of the previously failed controls after the modifications proposed by the auditor.

Control no.	Short control description	Pass or Fail?	Comments
13	W2: Check the filesystem ACLs on web server directories	Pass	The auditor prototyped the correction
14	W3: Check if Web server logging is appropriate	Pass	The auditor prototyped the correction but the owner of the system must modify the user manual to inform the customers to review the logs on regular basis.
16	W5: Evaluate the Web server with two vulnerability scanners	Pass	The auditor tested the correction. However, this control passes in the assumption that the distributor officially publishes the fix (or a new version) on the website in time for the upcoming product release.
23	FTP3: Check the FTP server permissions	Fail	The system owner will not correct this problem in the next release.
25	PS2: Check PostScript device/directory ACLs	Fail	The system owner accepted to analyze the problem and to estimate the cost of the correction.
27	PS4: Check PostScript interpreter permissions	Fail	The system owner will not correct this problem in the next release.
29	MAL2: Check that no code can be executed in every writable directory exposed by the print server	Pass	The auditor prototyped the correction

There are two preventive controls (23 and 27) that will not be corrected for the next release because the system owner has estimated that it costs too much regarding

the risk reduction. These preventive controls are related to in-house developed applications.
The system owner accepted to analyze and estimate the time needed to correct control 25.

6.3 Conclusion

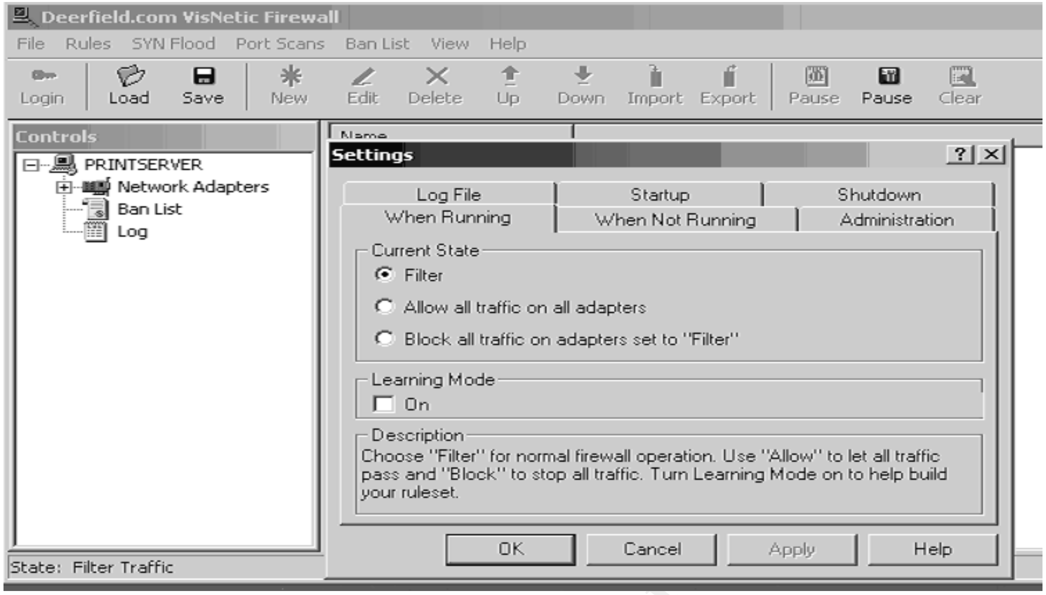
In the initial configuration, the print server had 22 controls with a “pass” status and 7 failed controls.
If the system owner takes into account the fixes proposed by the auditor, the system will have only 3 failed controls. The three failed controls are preventive controls.
With the current level of knowledge of the OS and server vulnerabilities, this product doesn’t contain security problems allowing system integrity corruption (threat 1), and the controls reducing the network integrity corruption threat have a pass status.
However, as the security is an ongoing process (new vulnerabilities can be found in current servers, new security flaws may be introduced in future releases), the auditor suggests verifying the controls included in this audit checklist for every future print server release.

The firewall used to protect the system it is not appropriate for this system and the auditor recommends replacing it with an application level firewall.

The auditor proposes several further recommendations to the system owner:

1) Incorporating the security requirements (like running software at low privilege) in new products from the specification phase. This will allow having the preventive controls included from the beginning. Security flaws in the product design are very costly to correct afterwards.
2) Adding a new rule to the company’s security policy controlling the ACLs on the directories exposed by the network services.
3) Modify the user manual to inform the customers to review the logs on regular bases.

7 Appendix 1: Visnetic firewall configuration screen shots



Current State

● Filter

○ Allow all traffic on all adapters

○ Block all traffic on adapters set to "Filter"

Learning Mode

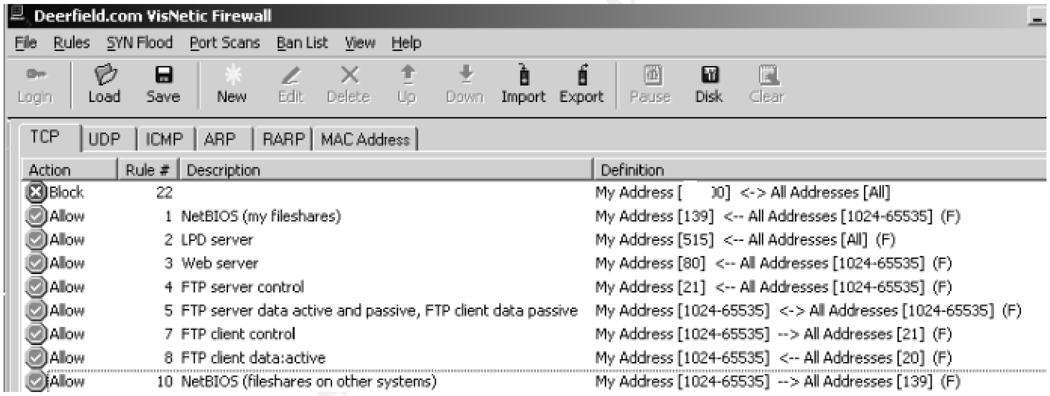
☐ On

Description

Choose "Filter" for normal firewall operation. Use "Allow" to let all traffic pass and "Block" to stop all traffic. Turn Learning Mode on to help build your ruleset.

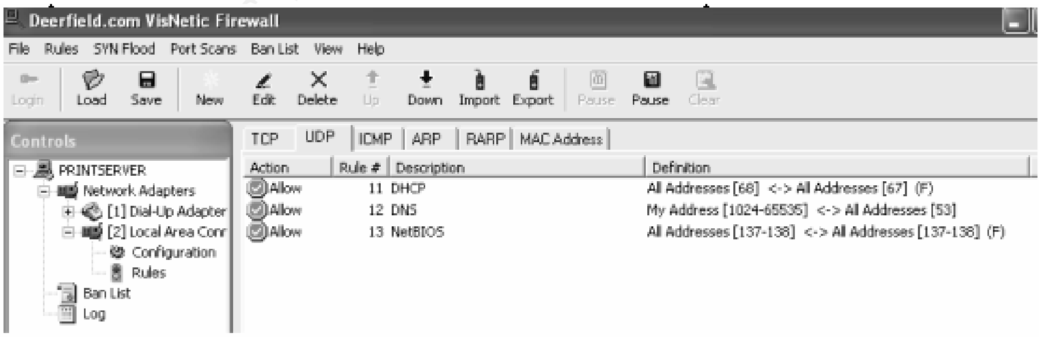
State: Filter Traffic

Figure 62: Firewall is set to actively filter traffic according to the loaded ruleset



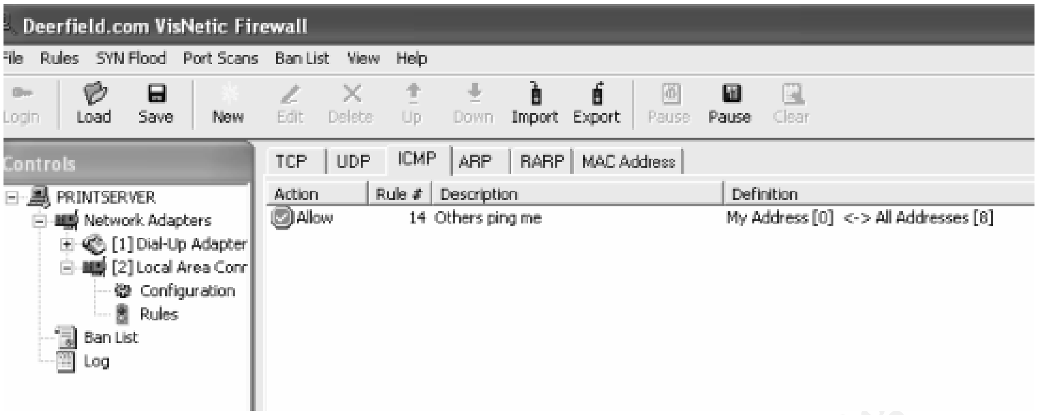
Action	Rule #	Description	Definition
Block	22		My Address [0] <-> All Addresses [All]
Allow	1	NetBIOS (my fileshares)	My Address [139] <-- All Addresses [1024-65535] (F)
Allow	2	LPD server	My Address [515] <-- All Addresses [All] (F)
Allow	3	Web server	My Address [80] <-- All Addresses [1024-65535] (F)
Allow	4	FTP server control	My Address [21] <-- All Addresses [1024-65535] (F)
Allow	5	FTP server data active and passive, FTP client data passive	My Address [1024-65535] <-> All Addresses [1024-65535] (F)
Allow	7	FTP client control	My Address [1024-65535] --> All Addresses [21] (F)
Allow	8	FTP client data:active	My Address [1024-65535] <-- All Addresses [20] (F)
Allow	10	NetBIOS (fileshares on other systems)	My Address [1024-65535] --> All Addresses [139] (F)

Figure 63: Firewall's TCP rules for the LAN adapter



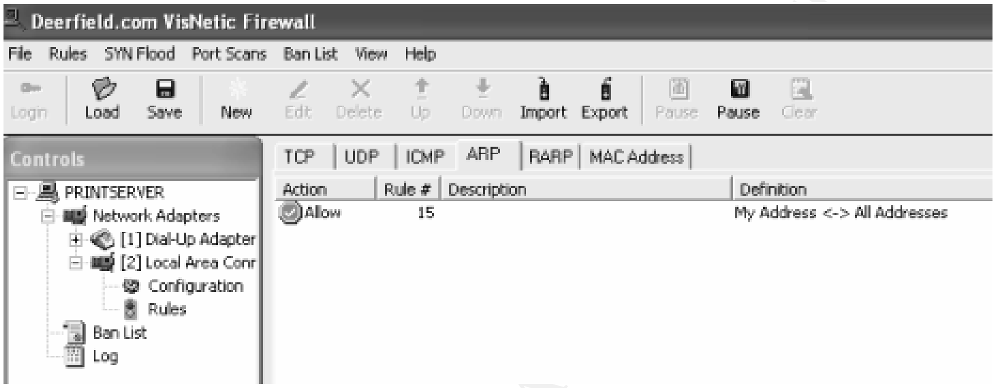
Action	Rule #	Description	Definition
Allow	11	DHCP	All Addresses [68] <-> All Addresses [67] (F)
Allow	12	DNS	My Address [1024-65535] <-> All Addresses [53]
Allow	13	NetBIOS	All Addresses [137-138] <-> All Addresses [137-138] (F)

Figure 64: Firewall's UDP rules for the LAN adapter


Deerfield.com VisNetic Firewall
File Rules SYN Flood Port Scans Ban List View Help
Login Load Save New Edit Delete Up Down Import Export Pause Pause Clear
Controls
PRINTSERVER
Network Adapters
[1] Dial-Up Adapter
[2] Local Area Conr
Configuration
Rules
Ban List
Log
TCP UDP ICMP ARP RARP MAC Address

Action	Rule #	Description	Definition
Allow	14	Others ping me	My Address [0] <-> All Addresses [8]

Figure 65: Firewall’s ICMP rule for the LAN adapter

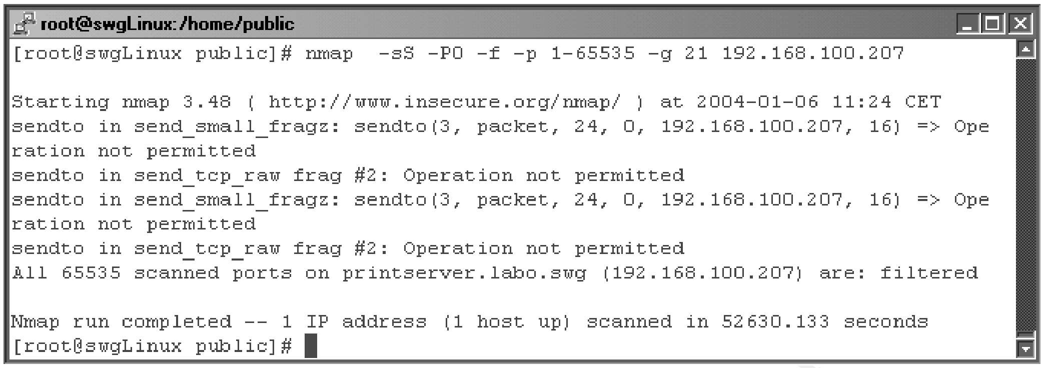

Deerfield.com VisNetic Firewall
File Rules SYN Flood Port Scans Ban List View Help
Login Load Save New Edit Delete Up Down Import Export Pause Pause Clear
Controls
PRINTSERVER
Network Adapters
[1] Dial-Up Adapter
[2] Local Area Conr
Configuration
Rules
Ban List
Log
TCP UDP ICMP ARP RARP MAC Address

Action	Rule #	Description	Definition
Allow	15		My Address <-> All Addresses

Figure 66: Firewall’s ARP rule for the LAN adapter

8 Appendix 2: Screen shots supporting Control No. 9

Test 2:

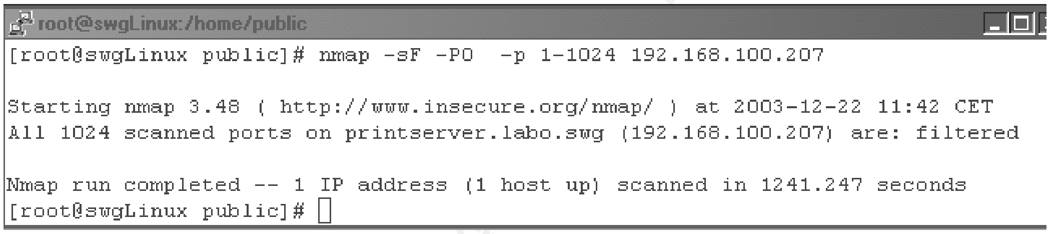


```
[root@swgLinux public]# nmap  -sS -P0 -f -p 1-65535 -g 21 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-01-06 11:24 CET
sendto in send_small_fragz: sendto(3, packet, 24, 0, 192.168.100.207, 16) => Ope
ration not permitted
sendto in send_tcp_raw frag #2: Operation not permitted
sendto in send_small_fragz: sendto(3, packet, 24, 0, 192.168.100.207, 16) => Ope
ration not permitted
sendto in send_tcp_raw frag #2: Operation not permitted
All 65535 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 52630.133 seconds
[root@swgLinux public]# 
```

Figure 67: nmap session on a remote system on the same LAN

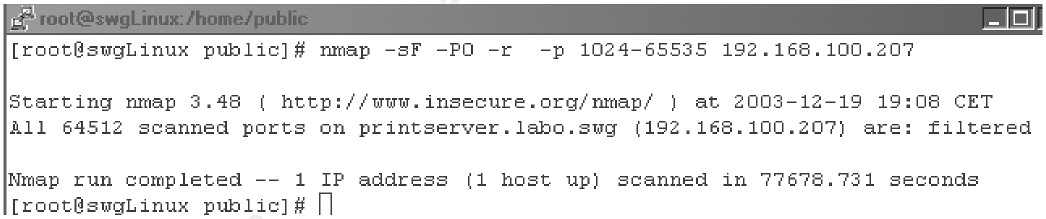
The previous screen shot shows that the system being audited does not respond to the nmap scan.

Test 3:



```
[root@swgLinux public]# nmap -sF -P0  -p 1-1024 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-22 11:42 CET
All 1024 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1241.247 seconds
[root@swgLinux public]# 
```

Figure 68: nmap session on a remote system on the same LAN

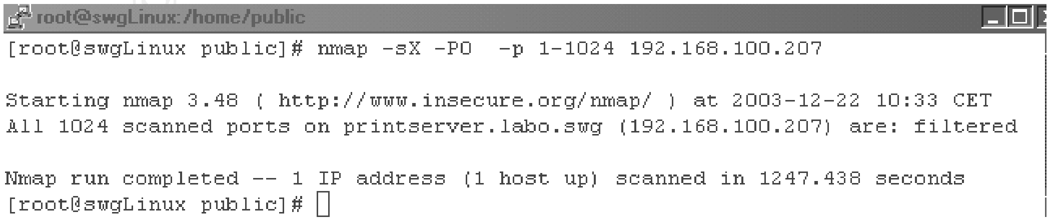


```
[root@swgLinux public]# nmap -sF -P0 -r  -p 1024-65535 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-19 19:08 CET
All 64512 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 77678.731 seconds
[root@swgLinux public]# 
```

Figure 69:nmap session on a remote system on the same LAN

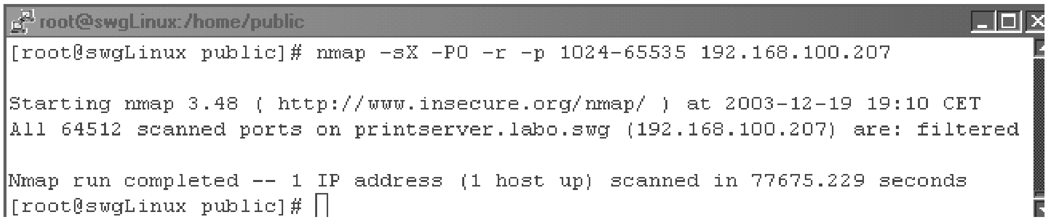
The previous screen shots show that nmap sees all ports as filtered.

Test 4:



```
[root@swgLinux public]# nmap -sX -P0  -p 1-1024 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-22 10:33 CET
All 1024 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1247.438 seconds
[root@swgLinux public]# 
```

Figure 70: nmap session on a remote system on the same LAN

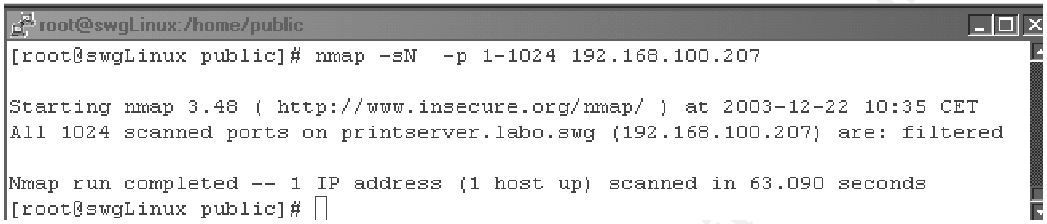


```
[root@swgLinux public]# nmap -sX -P0 -r -p 1024-65535 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-19 19:10 CET
All 64512 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 77675.229 seconds
[root@swgLinux public]#
```

Figure 71: nmap session on a remote system on the same LAN

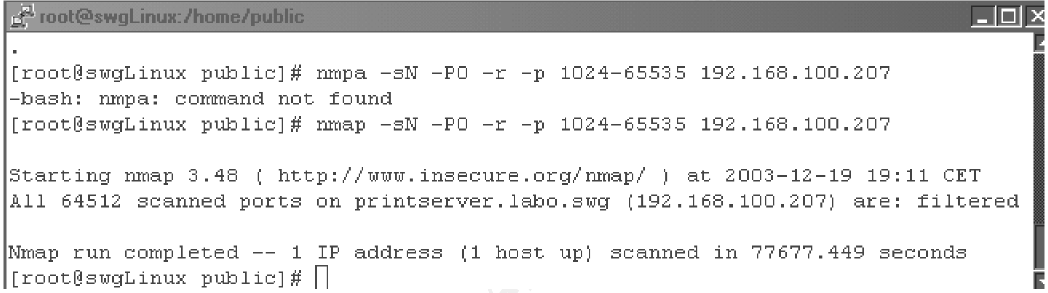
The previous screen shots show that nmap sees all ports as filtered.

Test 5:



```
[root@swgLinux public]# nmap -sN  -p 1-1024 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-22 10:35 CET
All 1024 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 63.090 seconds
[root@swgLinux public]#
```

Figure 72: nmap session on a remote system on the same LAN

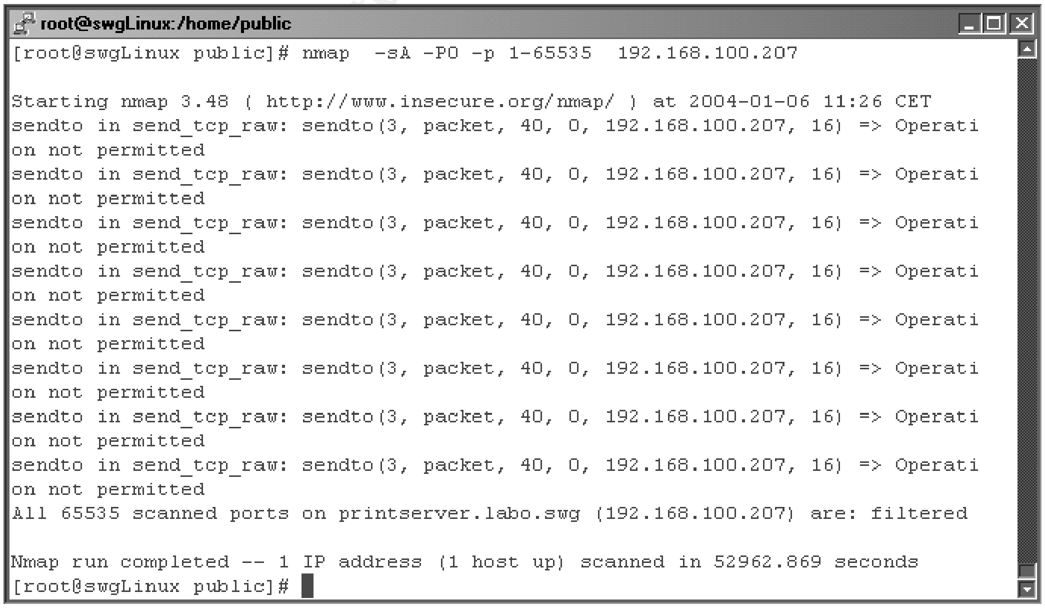


```
.
[root@swgLinux public]# nmpa -sN -P0 -r -p 1024-65535 192.168.100.207
-bash: nmpa: command not found
[root@swgLinux public]# nmap -sN -P0 -r -p 1024-65535 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-19 19:11 CET
All 64512 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 77677.449 seconds
[root@swgLinux public]#
```

Figure 73: nmap session on a remote system on the same LAN

The previous screen shots show that nmap sees all ports as filtered.

Test 6:

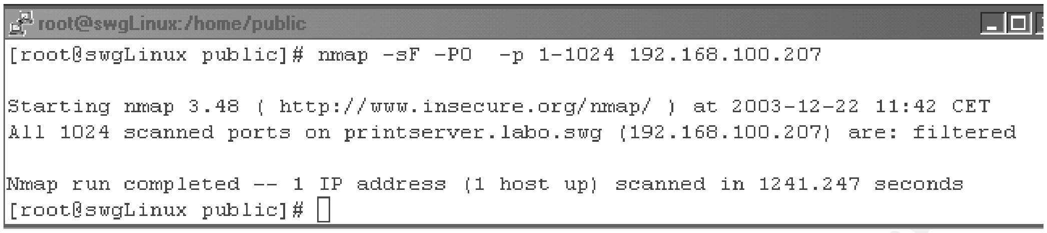


```
[root@swgLinux public]# nmap  -sA -P0 -p 1-65535  192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-01-06 11:26 CET
sendto in send_tcp_raw: sendto(3, packet, 40, 0, 192.168.100.207, 16) => Operati
on not permitted
sendto in send_tcp_raw: sendto(3, packet, 40, 0, 192.168.100.207, 16) => Operati
on not permitted
sendto in send_tcp_raw: sendto(3, packet, 40, 0, 192.168.100.207, 16) => Operati
on not permitted
sendto in send_tcp_raw: sendto(3, packet, 40, 0, 192.168.100.207, 16) => Operati
on not permitted
sendto in send_tcp_raw: sendto(3, packet, 40, 0, 192.168.100.207, 16) => Operati
on not permitted
sendto in send_tcp_raw: sendto(3, packet, 40, 0, 192.168.100.207, 16) => Operati
on not permitted
sendto in send_tcp_raw: sendto(3, packet, 40, 0, 192.168.100.207, 16) => Operati
on not permitted
sendto in send_tcp_raw: sendto(3, packet, 40, 0, 192.168.100.207, 16) => Operati
on not permitted
All 65535 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 52962.869 seconds
[root@swgLinux public]#
```

Figure 74: nmap session on a remote system on the same LAN

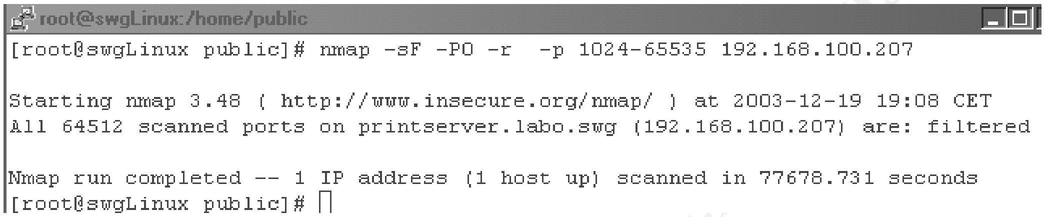
The previous screen shot shows that nmap sees all ports as filtered.

Test 7:



```
[root@swgLinux public]# nmap -sF -P0  -p 1-1024 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-22 11:42 CET
All 1024 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1241.247 seconds
[root@swgLinux public]# 
```

Figure 75: nmap session on a remote system on the same LAN

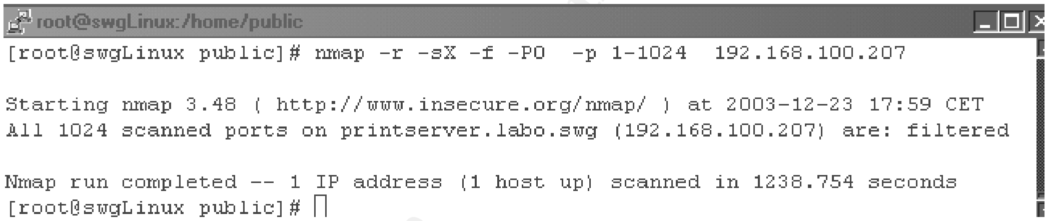


```
[root@swgLinux public]# nmap -sF -P0 -r  -p 1024-65535 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-19 19:08 CET
All 64512 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 77678.731 seconds
[root@swgLinux public]# 
```

Figure 76: nmap session on a remote system on the same LAN

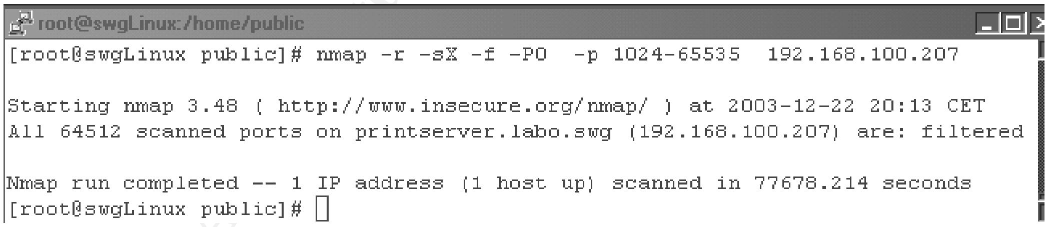
The previous screen shots show that nmap sees all ports as filtered.

Test 8:



```
[root@swgLinux public]# nmap -r -sX -f -P0  -p 1-1024  192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-23 17:59 CET
All 1024 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1238.754 seconds
[root@swgLinux public]# 
```

Figure 77: nmap session on a remote system on the same LAN

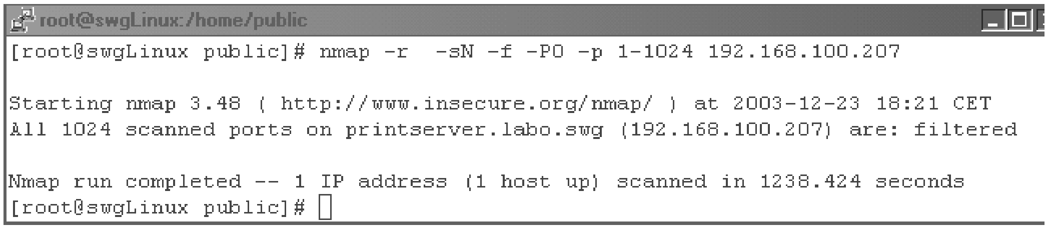


```
[root@swgLinux public]# nmap -r -sX -f -P0  -p 1024-65535  192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-22 20:13 CET
All 64512 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 77678.214 seconds
[root@swgLinux public]# 
```

Figure 78: nmap session on a remote system on the same LAN

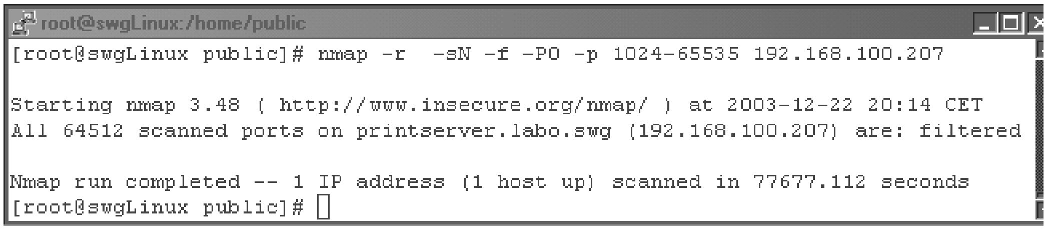
The previous screen shots show that nmap sees all ports as filtered.

Test 9:



```
[root@swgLinux public]# nmap -r  -sN -f -P0 -p 1-1024 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-23 18:21 CET
All 1024 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1238.424 seconds
[root@swgLinux public]# 
```

Figure 79: nmap session on a remote system on the same LAN

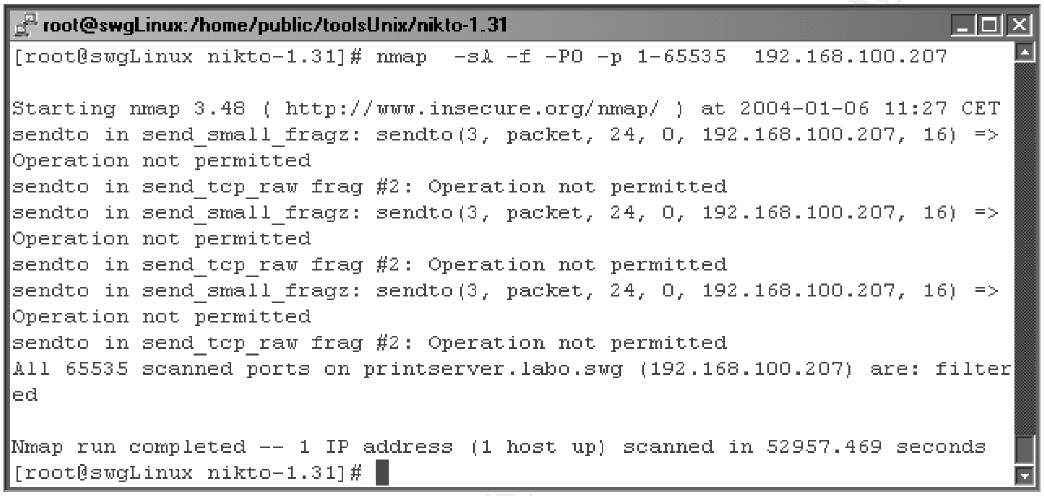


```
[root@swgLinux public]# nmap -r  -sN -f -P0 -p 1024-65535 192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-22 20:14 CET
All 64512 scanned ports on printserver.labo.swg (192.168.100.207) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 77677.112 seconds
[root@swgLinux public]# 
```

Figure 80: nmap session on a remote system on the same LAN

The previous screen shots show that nmap sees all ports as filtered.

Test 10:



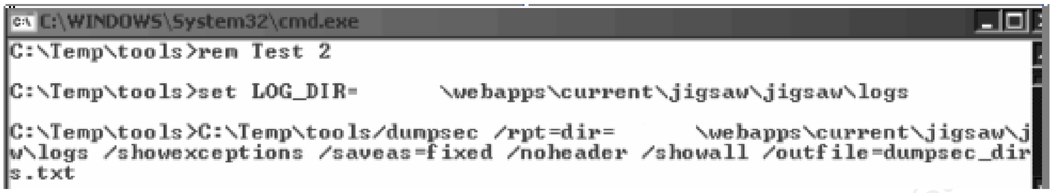
```
[root@swgLinux nikto-1.31]# nmap  -sA -f -P0 -p 1-65535  192.168.100.207

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-01-06 11:27 CET
sendto in send_small_fragz: sendto(3, packet, 24, 0, 192.168.100.207, 16) =>
Operation not permitted
sendto in send_tcp_raw frag #2: Operation not permitted
sendto in send_small_fragz: sendto(3, packet, 24, 0, 192.168.100.207, 16) =>
Operation not permitted
sendto in send_tcp_raw frag #2: Operation not permitted
sendto in send_small_fragz: sendto(3, packet, 24, 0, 192.168.100.207, 16) =>
Operation not permitted
sendto in send_tcp_raw frag #2: Operation not permitted
All 65535 scanned ports on printserver.labo.swg (192.168.100.207) are: filter
ed

Nmap run completed -- 1 IP address (1 host up) scanned in 52957.469 seconds
[root@swgLinux nikto-1.31]# 
```

Figure 81: nmap session on a remote system on the same LAN

The previous screen shot shows that nmap sees all ports as filtered.

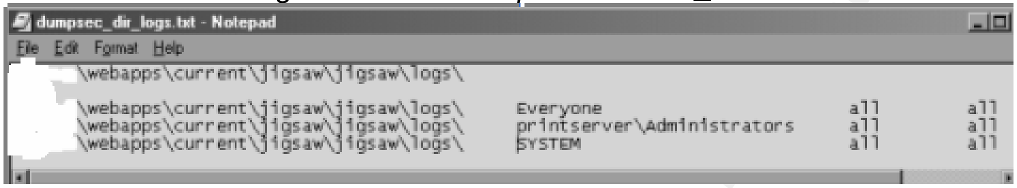
9 Appendix 3: Screen shots supporting Control No. 1 3

Test 2:



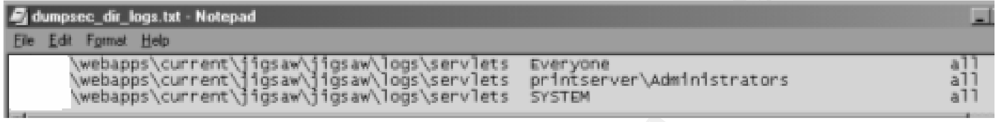
```
C:\Temp\tools>rem Test 2

C:\Temp\tools>set LOG_DIR=      \webapps\current\jigsaw\jigsaw\logs

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jigsaw\j
w\logs /showexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_dir
s.txt
```

Figure 82: Run dumpsec for LOG_DIR



```
      \webapps\current\jigsaw\jigsaw\logs\

      \webapps\current\jigsaw\jigsaw\logs\     Everyone                       all       all
      \webapps\current\jigsaw\jigsaw\logs\     printserver\Administrators     all       all
      \webapps\current\jigsaw\jigsaw\logs\     SYSTEM                         all       all
```

Figure 83: dumpsec logs for the LOG_DIR directory

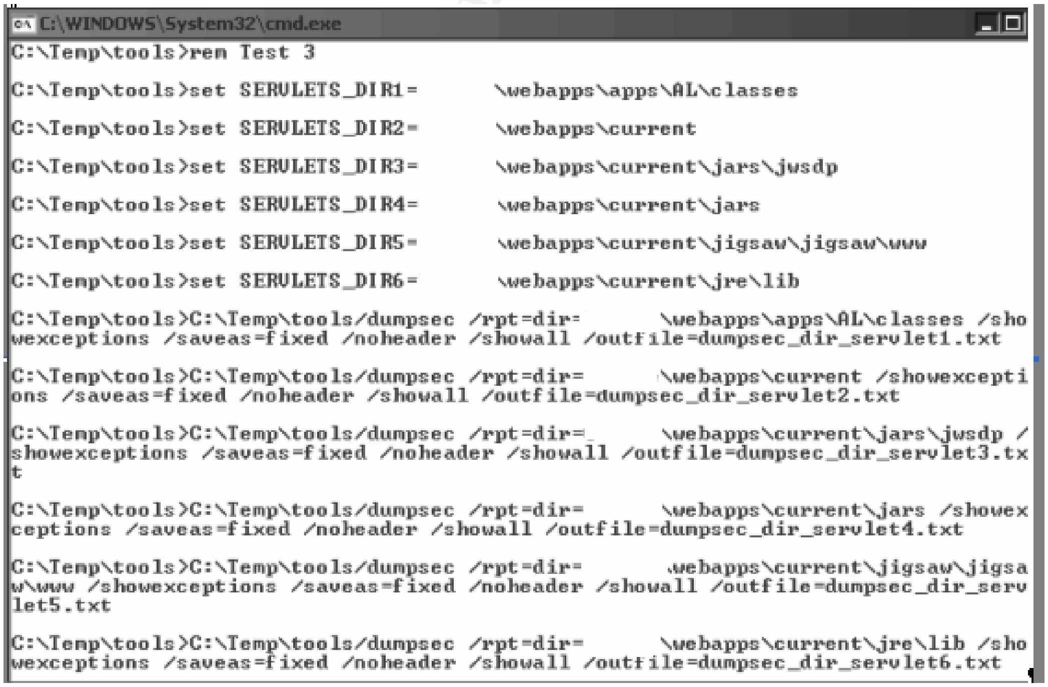


```
      \webapps\current\jigsaw\jigsaw\logs\servlets  Everyone                        all
      \webapps\current\jigsaw\jigsaw\logs\servlets  printserver\Administrators      all
      \webapps\current\jigsaw\jigsaw\logs\servlets  SYSTEM                          all
```

Figure 84: dumpsec logs for a log file

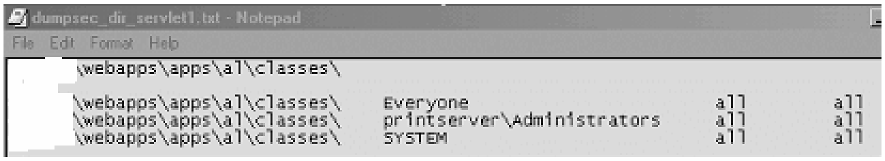
The previous screen shots show part of the file containing the permissions of the server log directories and an example of log file permissions. “Everyone “ has “all” permissions.

Test 3



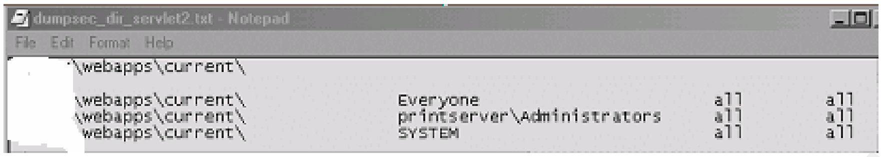
```
C:\Temp\tools>rem Test 3

C:\Temp\tools>set SERVLETS_DIR1=      \webapps\apps\AL\classes

C:\Temp\tools>set SERVLETS_DIR2=      \webapps\current

C:\Temp\tools>set SERVLETS_DIR3=      \webapps\current\jars\jwsdp

C:\Temp\tools>set SERVLETS_DIR4=      \webapps\current\jars

C:\Temp\tools>set SERVLETS_DIR5=      \webapps\current\jigsaw\jigsaw\www

C:\Temp\tools>set SERVLETS_DIR6=      \webapps\current\jre\lib

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\apps\AL\classes /sho
wexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_dir_servlet1.txt

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current /showexcepti
ons /saveas=fixed /noheader /showall /outfile=dumpsec_dir_servlet2.txt

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jars\jwsdp /
showexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_dir_servlet3.tx
t

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jars /showex
ceptions /saveas=fixed /noheader /showall /outfile=dumpsec_dir_servlet4.txt

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jigsaw\jigsa
w\www /showexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_dir_serv
let5.txt

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jre\lib /sho
wexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_dir_servlet6.txt
```

Figure 85: Run dumpsec for SERVLETS_DIRi



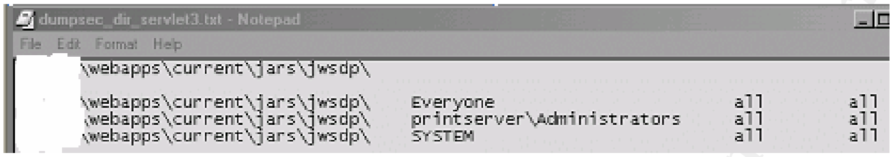
```
\webapps\apps\al\classes\

\webapps\apps\al\classes\    Everyone                        all         all
\webapps\apps\al\classes\    printserver\Administrators      all         all
\webapps\apps\al\classes\    SYSTEM                          all         all
```

Figure 86: dumpsec logs for the SERVLET_DIR1 directory



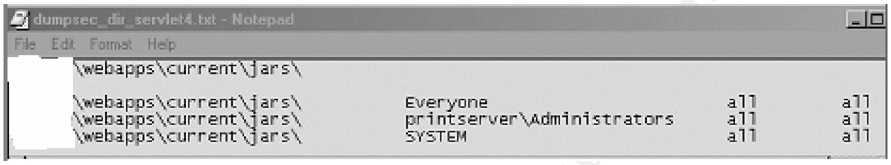
```
\webapps\current\

\webapps\current\              Everyone                      all        all
\webapps\current\              printserver\Administrators    all        all
 webapps\current\              SYSTEM                        all        all
```

Figure 87: dumpsec logs for the SERVLET_DIR2 directory



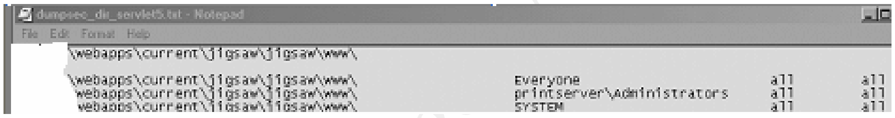
```
\webapps\current\jars\jwsdp\

\webapps\current\jars\jwsdp\    Everyone                      all        all
\webapps\current\jars\jwsdp\    printserver\Administrators    all        all
\webapps\current\jars\jwsdp\    SYSTEM                        all        all
```

Figure 88: dumpsec logs for the SERVLET_DIR3 directory



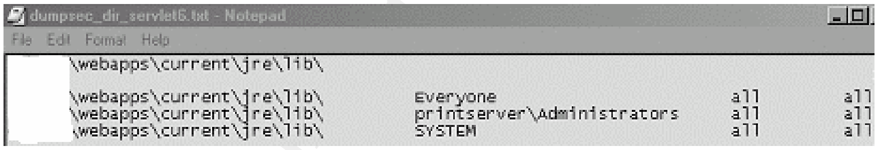
```
\webapps\current\jars\

\webapps\current\jars\          Everyone                      all        all
\webapps\current\jars\          printserver\Administrators    all        all
\webapps\current\jars\          SYSTEM                        all        all
```

Figure 89: dumpsec logs for the SERVLET_DIR4 directory



```
\webapps\current\jigsaw\jigsaw\www\

\webapps\current\jigsaw\jigsaw\www\                 Everyone                      all        all
 webapps\current\jigsaw\jigsaw\www\                 printserver\Administrators    all        all
  webapps\current\jigsaw\jigsaw\www\                SYSTEM                        all        all
```

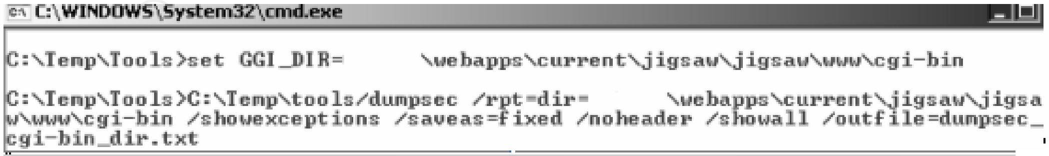
Figure 90: dumpsec logs for the SERVLET_DIR5 directory



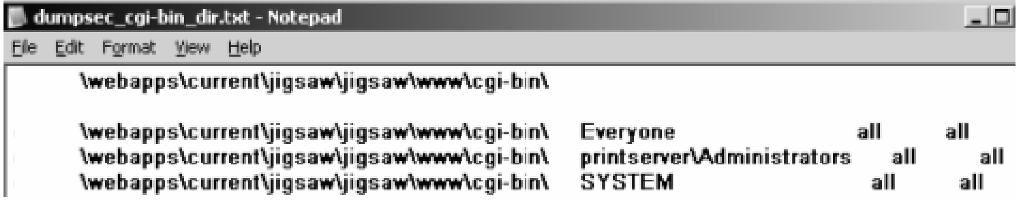
```
\webapps\current\jre\lib\

\webapps\current\jre\lib\       Everyone                      all        all
\webapps\current\jre\lib\       printserver\Administrators    all        all
\webapps\current\jre\lib\       SYSTEM                        all        all
```

Figure 91: dumpsec logs for the SERVLET_DIR6 directory

The previous screen shots show parts of the files containing the permissions of directories containing servlets. “Everyone “ has “all” permissions.



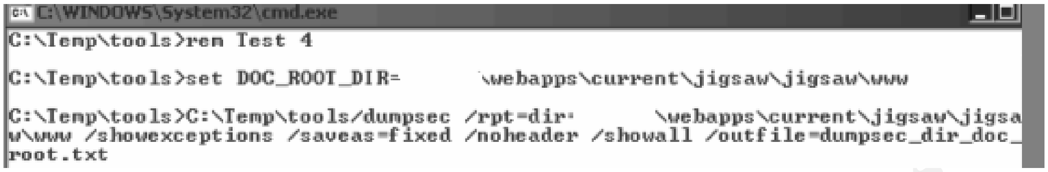
```
C:\Temp\Tools>set GGI_DIR=      \webapps\current\jigsaw\jigsaw\www\cgi-bin

C:\Temp\Tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jigsaw\jigsa
w\www\cgi-bin /showexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_
cgi-bin_dir.txt
```



```
\webapps\current\jigsaw\jigsaw\www\cgi-bin\

\webapps\current\jigsaw\jigsaw\www\cgi-bin\    Everyone                      all      all
\webapps\current\jigsaw\jigsaw\www\cgi-bin\    printserver\Administrators    all      all
\webapps\current\jigsaw\jigsaw\www\cgi-bin\    SYSTEM                        all      all
```

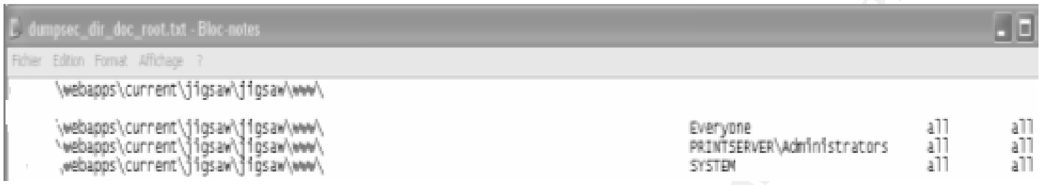
The previous screen shots show parts of the files containing the permissions of directories containing cgi scripts. “Everyone “ has “all” permissions.

Test 4



```
C:\Temp\tools>rem Test 4

C:\Temp\tools>set DOC_ROOT_DIR=      \webapps\current\jigsaw\jigsaw\www

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=       \webapps\current\jigsaw\jigsa
w\www /showexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_dir_doc_
root.txt
```

Figure 92: Run dumpsec for DOC_ROOT_DIR



dumpsec_dir_doc_root.txt - Bloc-notes
Fichier Edition Format Affichage ?

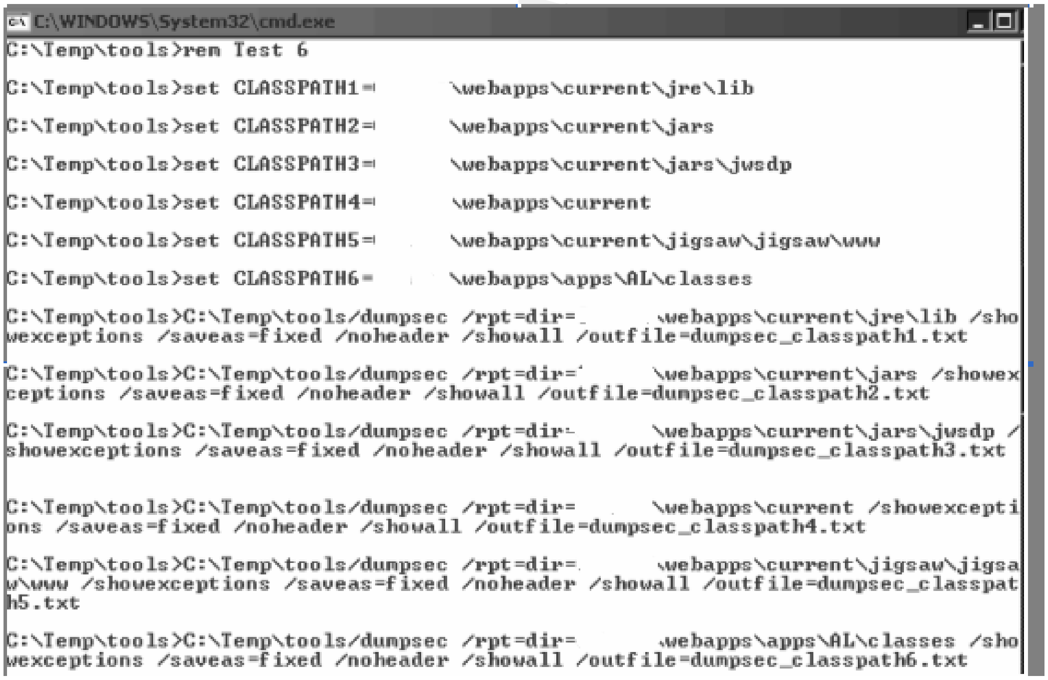
```
     \webapps\current\jigsaw\jigsaw\www\

     \webapps\current\jigsaw\jigsaw\www\                            Everyone                    all      all
     \webapps\current\jigsaw\jigsaw\www\                            PRINTSERVER\Administrators  all      all
     \webapps\current\jigsaw\jigsaw\www\                            SYSTEM                      all      all
```

Figure 93: dumpsec logs for the DOC_ROOT_DIR directory

The previous screen shots show part of the file containing the permissions of the server configuration directory. “Everyone “ has “all” permissions.

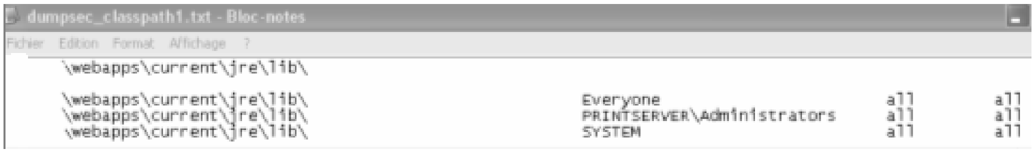
Test 5: not applicable because there are no symbolic links.

Test 6:



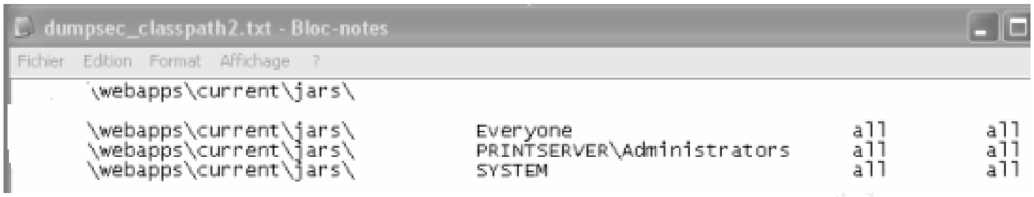
```
C:\Temp\tools>rem Test 6

C:\Temp\tools>set CLASSPATH1=      \webapps\current\jre\lib

C:\Temp\tools>set CLASSPATH2=      \webapps\current\jars

C:\Temp\tools>set CLASSPATH3=      \webapps\current\jars\jwsdp

C:\Temp\tools>set CLASSPATH4=      \webapps\current

C:\Temp\tools>set CLASSPATH5=      \webapps\current\jigsaw\jigsaw\www

C:\Temp\tools>set CLASSPATH6=      \webapps\apps\AL\classes

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jre\lib /sho
wexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_classpath1.txt

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jars /showex
ceptions /saveas=fixed /noheader /showall /outfile=dumpsec_classpath2.txt

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jars\jwsdp /
showexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_classpath3.txt


C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current /showexcepti
ons /saveas=fixed /noheader /showall /outfile=dumpsec_classpath4.txt

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\current\jigsaw\jigsa
w\www /showexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_classpat
h5.txt

C:\Temp\tools>C:\Temp\tools/dumpsec /rpt=dir=      \webapps\apps\AL\classes /sho
wexceptions /saveas=fixed /noheader /showall /outfile=dumpsec_classpath6.txt
```

Figure 94: Run dumpsec for CLASSPATHi directories


dumpsec_classpath1.txt - Bloc-notes
Fichier Edition Format Affichage ?

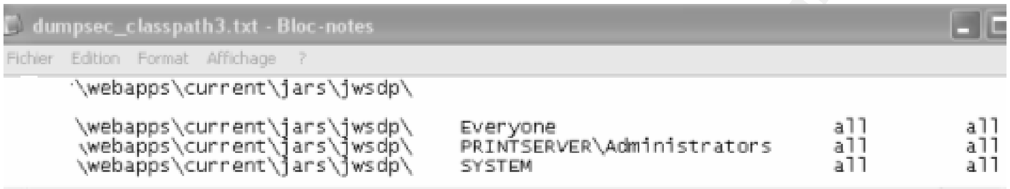
```
\webapps\current\jre\lib\

\webapps\current\jre\lib\                                          Everyone                         all        all
\webapps\current\jre\lib\                                          PRINTSERVER\Administrators       all        all
\webapps\current\jre\lib\                                          SYSTEM                           all        all
```

Figure 95: dumpsec logs for the CLASSPATH1 directory


dumpsec_classpath2.txt - Bloc-notes
Fichier Edition Format Affichage ?

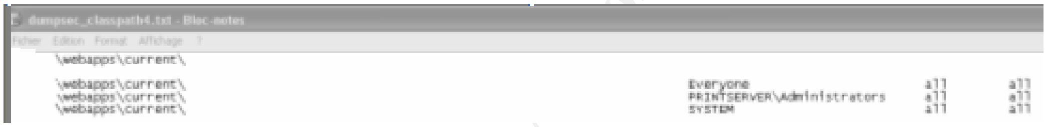
```
\webapps\current\jars\

\webapps\current\jars\          Everyone                       all        all
\webapps\current\jars\          PRINTSERVER\Administrators     all        all
\webapps\current\jars\          SYSTEM                         all        all
```

Figure 96: dumpsec logs for the CLASSPATH2 directory


dumpsec_classpath3.txt - Bloc-notes
Fichier Edition Format Affichage ?

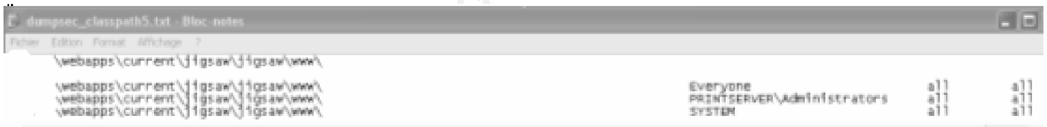
```
\webapps\current\jars\jwsdp\

\webapps\current\jars\jwsdp\    Everyone                       all        all
\webapps\current\jars\jwsdp\    PRINTSERVER\Administrators     all        all
\webapps\current\jars\jwsdp\    SYSTEM                         all        all
```

Figure 97: dumpsec logs for the CLASSPATH3 directory


dumpsec_classpath4.txt - Bloc-notes
Fichier Edition Format Affichage ?

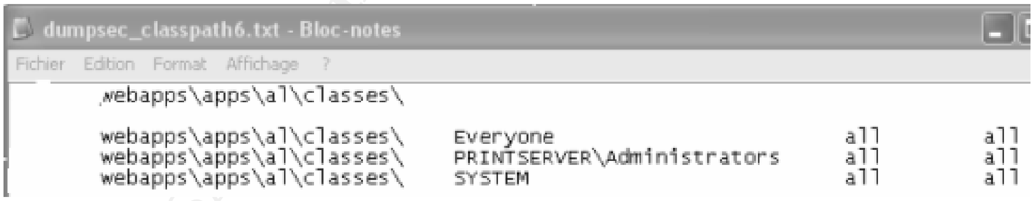
```
\webapps\current\

\webapps\current\                                                        Everyone                      all        all
\webapps\current\                                                        PRINTSERVER\Administrators    all        all
\webapps\current\                                                        SYSTEM                        all        all
```

Figure 98: dumpsec logs for the CLASSPATH4 directory


dumpsec_classpath5.txt - Bloc-notes
Fichier Edition Format Affichage ?

```
\webapps\current\jigsaw\jigsaw\www\

\webapps\current\jigsaw\jigsaw\www\                                      Everyone                      all        all
\webapps\current\jigsaw\jigsaw\www\                                      PRINTSERVER\Administrators    all        all
\webapps\current\jigsaw\jigsaw\www\                                      SYSTEM                        all        all
```

Figure 99: dumpsec logs for the CLASSPATH5 directory

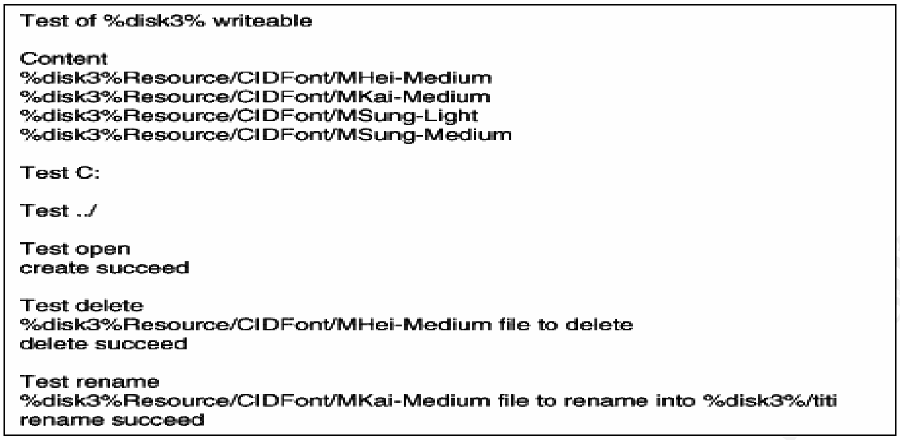

dumpsec_classpath6.txt - Bloc-notes
Fichier Edition Format Affichage ?

```
webapps\apps\al\classes\

webapps\apps\al\classes\     Everyone                       all        all
webapps\apps\al\classes\     PRINTSERVER\Administrators     all        all
webapps\apps\al\classes\     SYSTEM                         all        all
```

Figure 100: dumpsec logs for the CLASSPATH6 directory

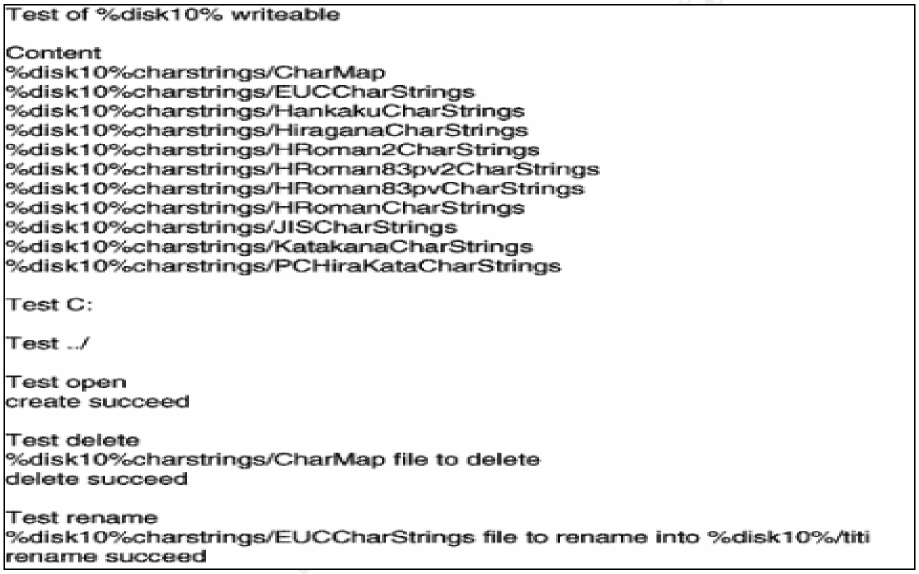
The previous screen shots show parts of the files containing the permissions of the directories included in the CLASSPATH environment variable. “Everyone “ has “all” permissions.

10 Appendix 4: Screen shots supporting Control No. 24, 25, 26



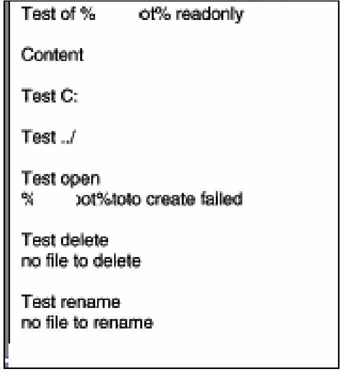
```
Test of %disk3% writeable

Content
%disk3%Resource/CIDFont/MHei-Medium
%disk3%Resource/CIDFont/MKai-Medium
%disk3%Resource/CIDFont/MSung-Light
%disk3%Resource/CIDFont/MSung-Medium

Test C:

Test ../

Test open
create succeed

Test delete
%disk3%Resource/CIDFont/MHei-Medium file to delete
delete succeed

Test rename
%disk3%Resource/CIDFont/MKai-Medium file to rename into %disk3%/titi
rename succeed
```

Figure 101: PostScript generated bitmap for disk3



```
Test of %disk10% writeable

Content
%disk10%charstrings/CharMap
%disk10%charstrings/EUCCharStrings
%disk10%charstrings/HankakuCharStrings
%disk10%charstrings/HiraganaCharStrings
%disk10%charstrings/HRoman2CharStrings
%disk10%charstrings/HRoman83pv2CharStrings
%disk10%charstrings/HRoman83pvCharStrings
%disk10%charstrings/HRomanCharStrings
%disk10%charstrings/JISCharStrings
%disk10%charstrings/KatakanaCharStrings
%disk10%charstrings/PCHiraKataCharStrings

Test C:

Test ../

Test open
create succeed

Test delete
%disk10%charstrings/CharMap file to delete
delete succeed

Test rename
%disk10%charstrings/EUCCharStrings file to rename into %disk10%/titi
rename succeed
```

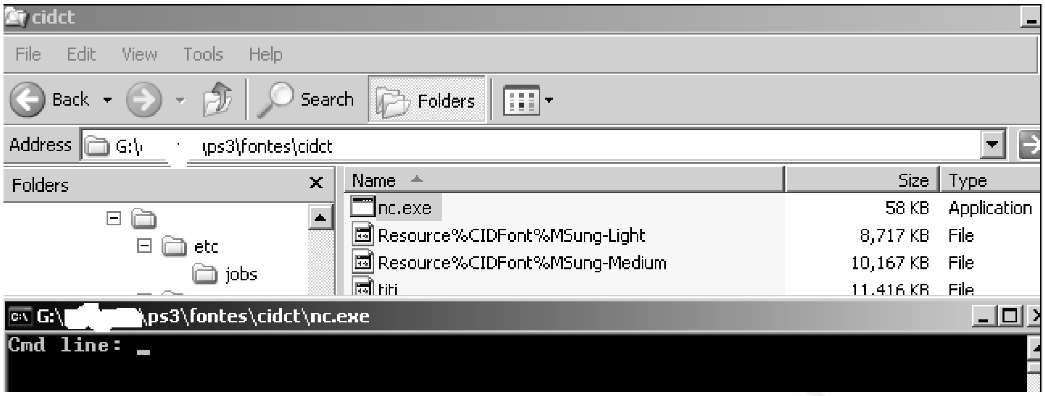
Figure 102: PostScript generated bitmap for disk10



```
Test of %        ot% readonly

Content

Test C:

Test ../

Test open
%        ot%toto create failed

Test delete
no file to delete

Test rename
no file to rename
```

Figure 103: PostScript generated bitmap

11 Appendix 5: Screen shots supporting the Control No. 29

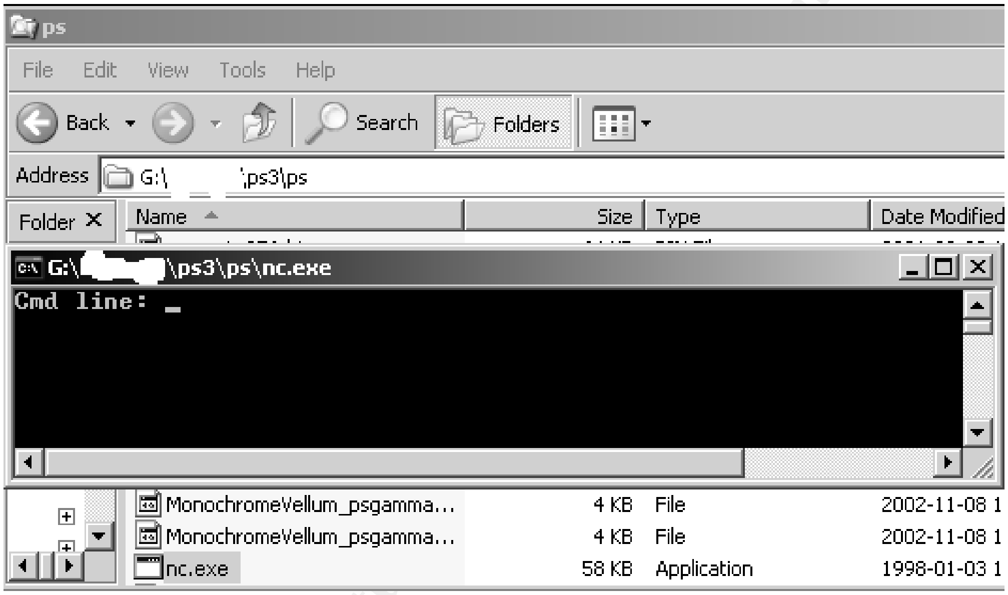


Address: G:\[redacted]\ps3\fontes\cidct

Name	Size	Type
nc.exe	58 KB	Application
Resource%CIDFont%MSung-Light	8,717 KB	File
Resource%CIDFont%MSung-Medium	10,167 KB	File
titi	11,416 KB	File

G:\[redacted]\ps3\fontes\cidct\nc.exe

```
Cmd line: _
```

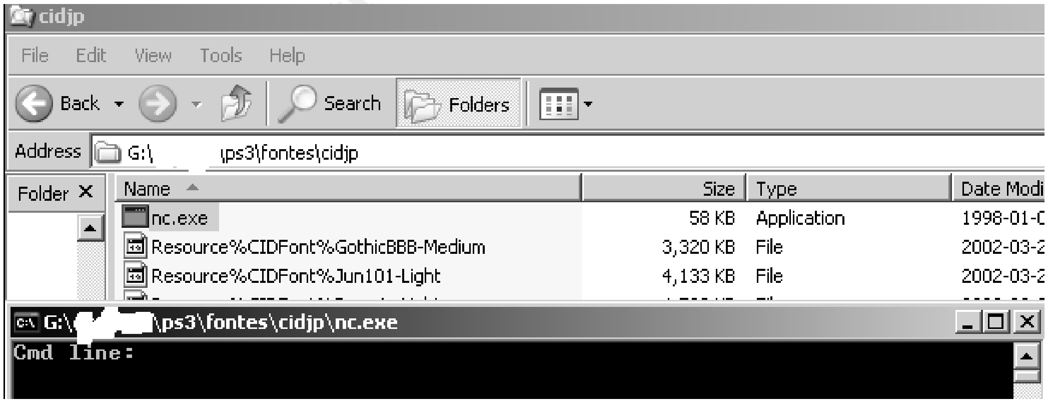


Address: G:\[redacted]\ps3\ps

G:\[redacted]\ps3\ps\nc.exe

```
Cmd line: _
```

Name	Size	Type	Date Modified
MonochromeVellum_psgamma...	4 KB	File	2002-11-08 1
MonochromeVellum_psgamma...	4 KB	File	2002-11-08 1
nc.exe	58 KB	Application	1998-01-03 1

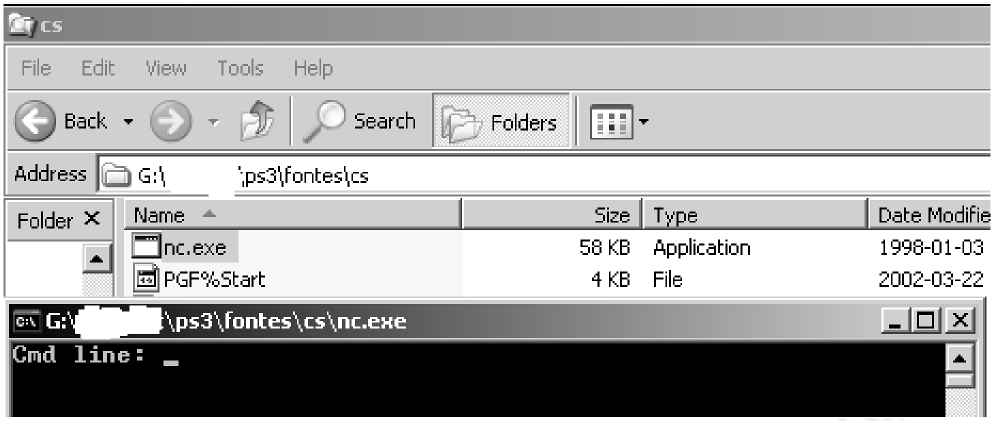


Address: G:\[redacted]\ps3\fontes\cidjp

Name	Size	Type	Date Modi
nc.exe	58 KB	Application	1998-01-0
Resource%CIDFont%GothicBBB-Medium	3,320 KB	File	2002-03-2
Resource%CIDFont%Jun101-Light	4,133 KB	File	2002-03-2

G:\[redacted]\ps3\fontes\cidjp\nc.exe

```
Cmd line:
```



Address: G:\[redacted]\ps3\fontes\cs

Name	Size	Type	Date Modifie
nc.exe	58 KB	Application	1998-01-03
PGF%Start	4 KB	File	2002-03-22

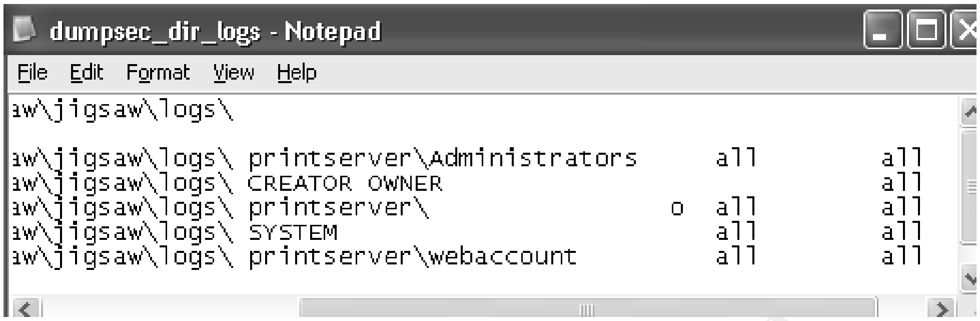
G:\[redacted]\ps3\fontes\cs\nc.exe

```
Cmd line: _
```

The previous screen shots show that nc.exe can be executed in every writable PostScript disk.

12 Appendix 6: Screen shots supporting the correction for Control No. 13

Test 2:

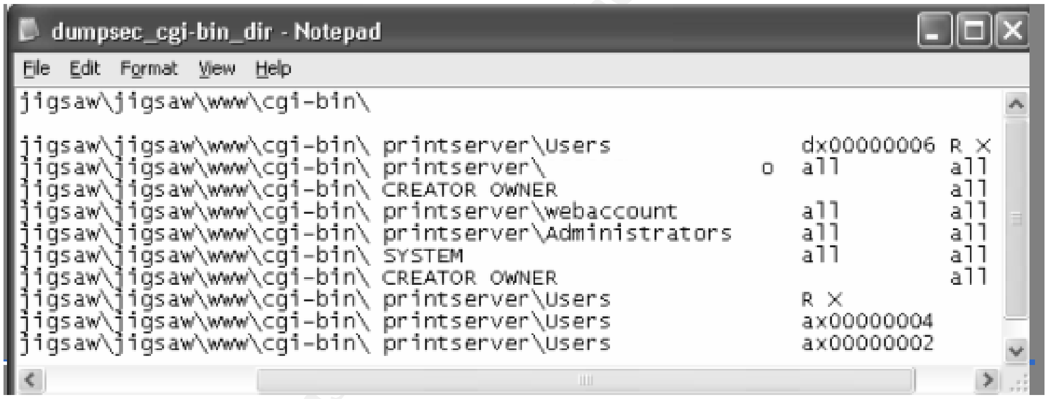


```
aw\jigsaw\logs\

aw\jigsaw\logs\ printserver\Administrators     all        all
aw\jigsaw\logs\ CREATOR OWNER                             all
aw\jigsaw\logs\ printserver\                o  all        all
aw\jigsaw\logs\ SYSTEM                         all        all
aw\jigsaw\logs\ printserver\webaccount         all        all
```

Figure 104: dumpsec log file for DIR_LOGS directory

The previous screen shot shows that the only the administrator account, web server account and the system have any rights on the web server log directory. The users were completely removed from the accounts having any rights on this directory.

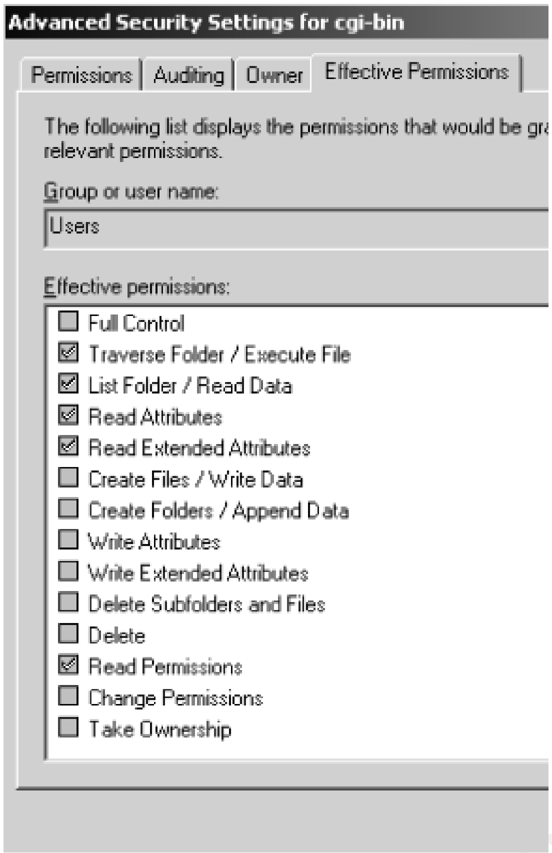
Test 3:



```
jigsaw\jigsaw\www\cgi-bin\

jigsaw\jigsaw\www\cgi-bin\ printserver\Users              dx00000006 R X
jigsaw\jigsaw\www\cgi-bin\ printserver\                o  all        all
jigsaw\jigsaw\www\cgi-bin\ CREATOR OWNER                             all
jigsaw\jigsaw\www\cgi-bin\ printserver\webaccount         all        all
jigsaw\jigsaw\www\cgi-bin\ printserver\Administrators     all        all
jigsaw\jigsaw\www\cgi-bin\ SYSTEM                         all        all
jigsaw\jigsaw\www\cgi-bin\ CREATOR OWNER                             all
jigsaw\jigsaw\www\cgi-bin\ printserver\Users              R X
jigsaw\jigsaw\www\cgi-bin\ printserver\Users              ax00000004
jigsaw\jigsaw\www\cgi-bin\ printserver\Users              ax00000002
```

Figure 105: dumpsec log file for CGI-BIN directory

The screen shot shows part of the file containing the permissions of directories containing GCI scripts. The users have only the rights to read and execute. However, specials permissions are mentioned for the users and the following screen shot shows that the users have no right to write on this folder.



The following list displays the permissions that would be gr
relevant permissions.

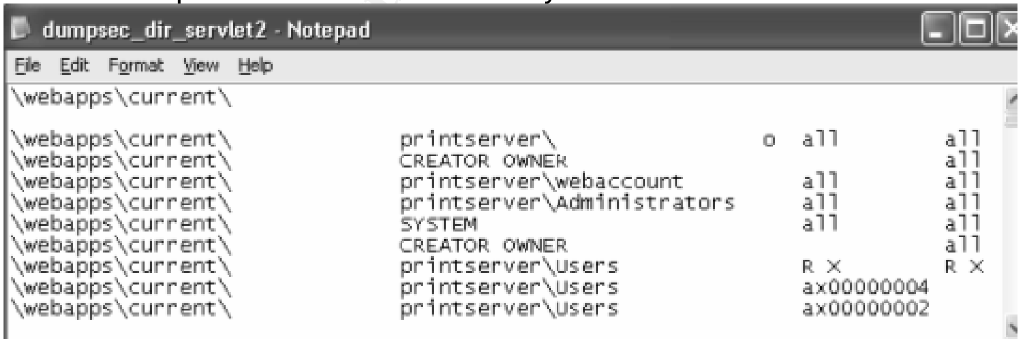
Group or user name:
Users

Effective permissions:

- ☐ Full Control
- ☑ Traverse Folder / Execute File
- ☑ List Folder / Read Data
- ☑ Read Attributes
- ☑ Read Extended Attributes
- ☐ Create Files / Write Data
- ☐ Create Folders / Append Data
- ☐ Write Attributes
- ☐ Write Extended Attributes
- ☐ Delete Subfolders and Files
- ☐ Delete
- ☑ Read Permissions
- ☐ Change Permissions
- ☐ Take Ownership

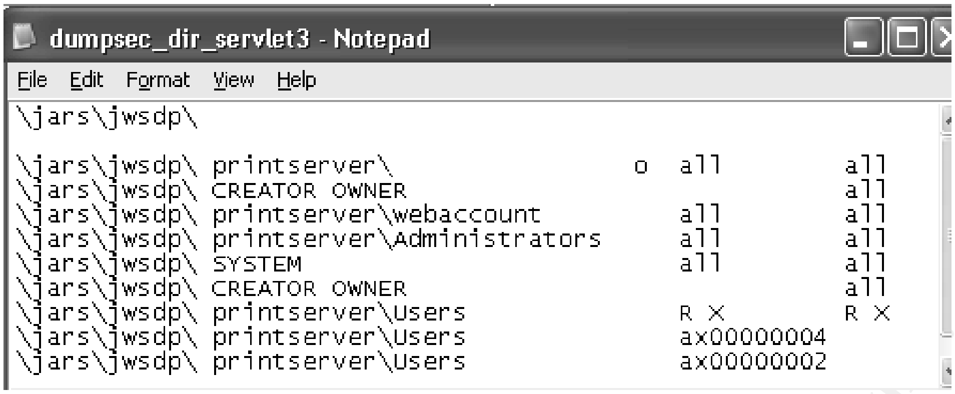
Figure 106: ACLs on cgi-bin folder

The system owner included DIR_SERVLET1 directory in the DOC_SERVERS_DIRS_USERS. The auditor searched the “servlet” pattern in this directory and it didn’t find it. The system owner accepted that this directory was erroneously included in the documentation. Consequently, the auditor doesn’t modified the permissions for this directory.



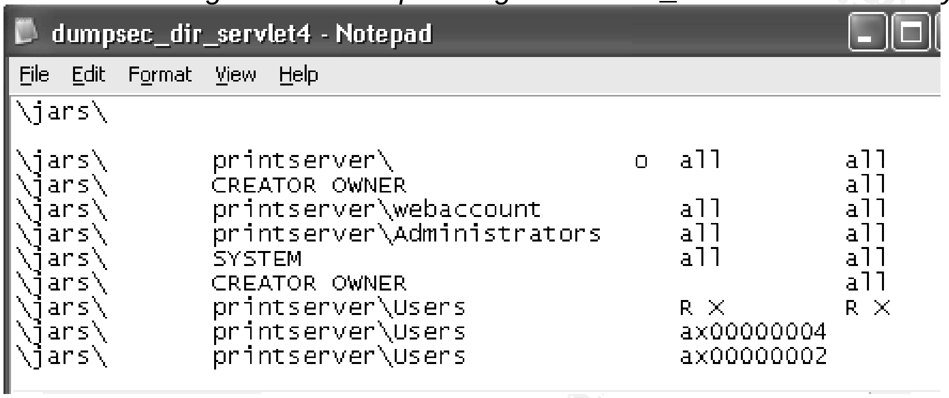
```
\webapps\current\

\webapps\current\             printserver\                o  all        all
\webapps\current\             CREATOR OWNER                             all
\webapps\current\             printserver\webaccount         all        all
\webapps\current\             printserver\Administrators     all        all
\webapps\current\             SYSTEM                         all        all
\webapps\current\             CREATOR OWNER                             all
\webapps\current\             printserver\Users              R X        R X
\webapps\current\             printserver\Users              ax00000004
\webapps\current\             printserver\Users              ax00000002
```

Figure 107: dumpsec log file for DIR_SERVLET2 directory



```
\jars\jwsdp\

\jars\jwsdp\ printserver\                 o  all         all
\jars\jwsdp\ CREATOR OWNER                               all
\jars\jwsdp\ printserver\webaccount          all         all
\jars\jwsdp\ printserver\Administrators      all         all
\jars\jwsdp\ SYSTEM                          all         all
\jars\jwsdp\ CREATOR OWNER                               all
\jars\jwsdp\ printserver\Users               R X         R X
\jars\jwsdp\ printserver\Users               ax00000004
\jars\jwsdp\ printserver\Users               ax00000002
```

Figure 108: dumpsec log file for DIR_SERVLET3 directory



```
\jars\

\jars\       printserver\                 o  all         all
\jars\       CREATOR OWNER                               all
\jars\       printserver\webaccount          all         all
\jars\       printserver\Administrators      all         all
\jars\       SYSTEM                          all         all
\jars\       CREATOR OWNER                               all
\jars\       printserver\Users               R X         R X
\jars\       printserver\Users               ax00000004
\jars\       printserver\Users               ax00000002
```

Figure 109: dumpsec log file for DIR_SERVLET4 directory

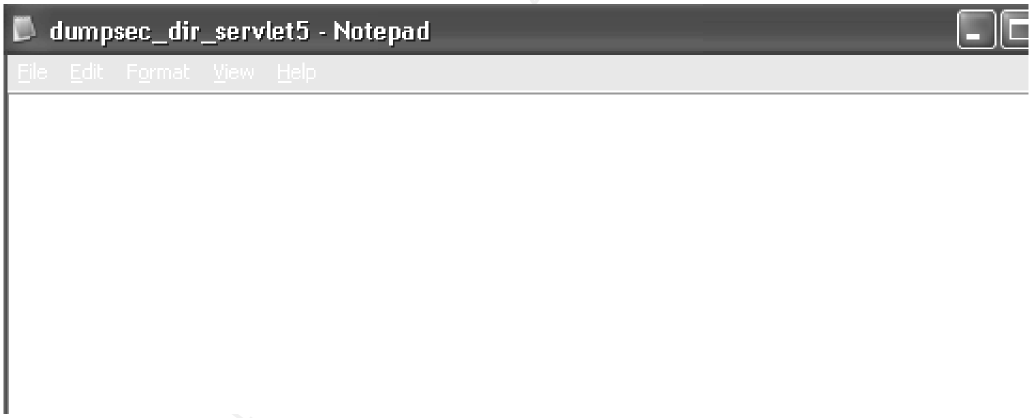
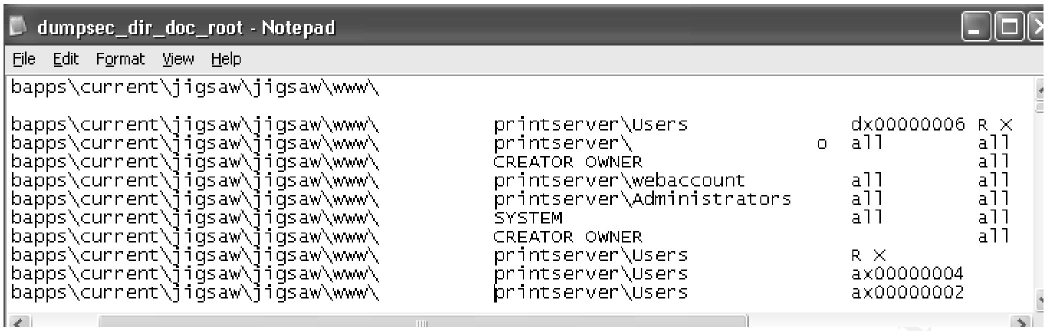


Figure 110: dumpsec log file for DIR_SERVLET5 directory

The previous screen shots show that the users have no rights to write on the folders containing servlets.

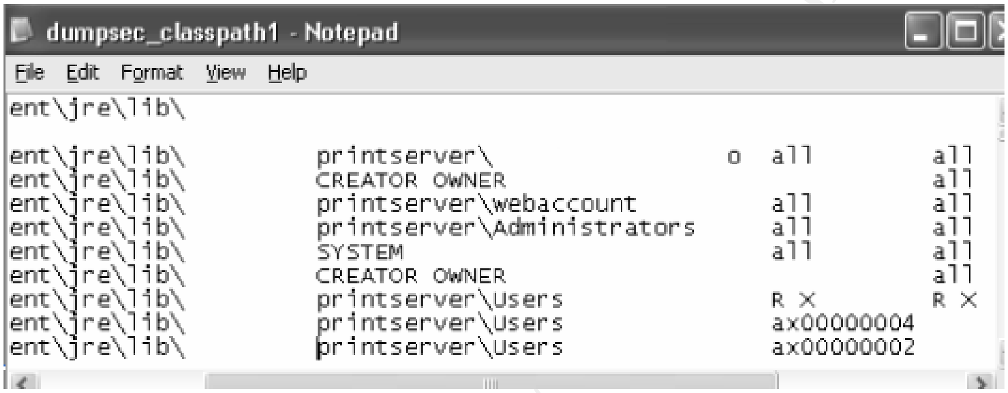
Test 4:



```
bapps\current\jigsaw\jigsaw\www\

bapps\current\jigsaw\jigsaw\www\          printserver\Users                 dx00000006 R X
bapps\current\jigsaw\jigsaw\www\          printserver\                   o  all        all
bapps\current\jigsaw\jigsaw\www\          CREATOR OWNER                                all
bapps\current\jigsaw\jigsaw\www\          printserver\webaccount            all        all
bapps\current\jigsaw\jigsaw\www\          printserver\Administrators        all        all
bapps\current\jigsaw\jigsaw\www\          SYSTEM                            all        all
bapps\current\jigsaw\jigsaw\www\          CREATOR OWNER                                all
bapps\current\jigsaw\jigsaw\www\          printserver\Users                 R X
bapps\current\jigsaw\jigsaw\www\          printserver\Users                 ax00000004
bapps\current\jigsaw\jigsaw\www\          printserver\Users                 ax00000002
```

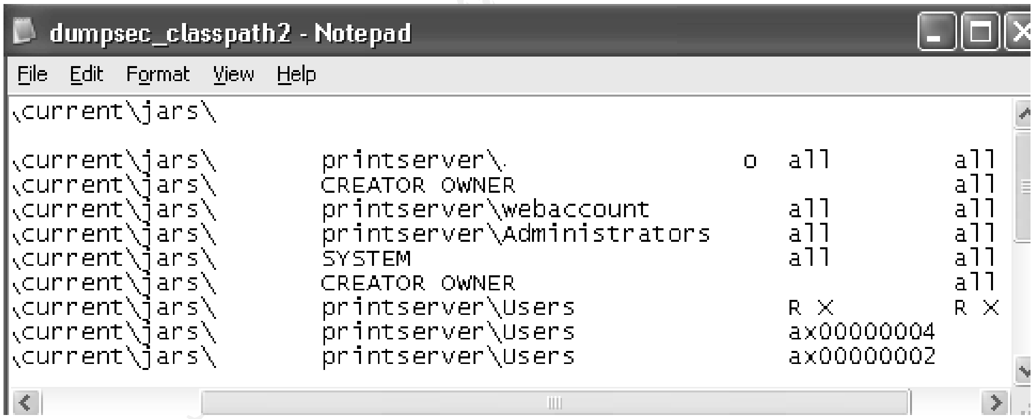
Figure 111: dumpsec log file for DOC_ROOT directory

The previous screen shot shows that the users have no rights to write in the web server document root.



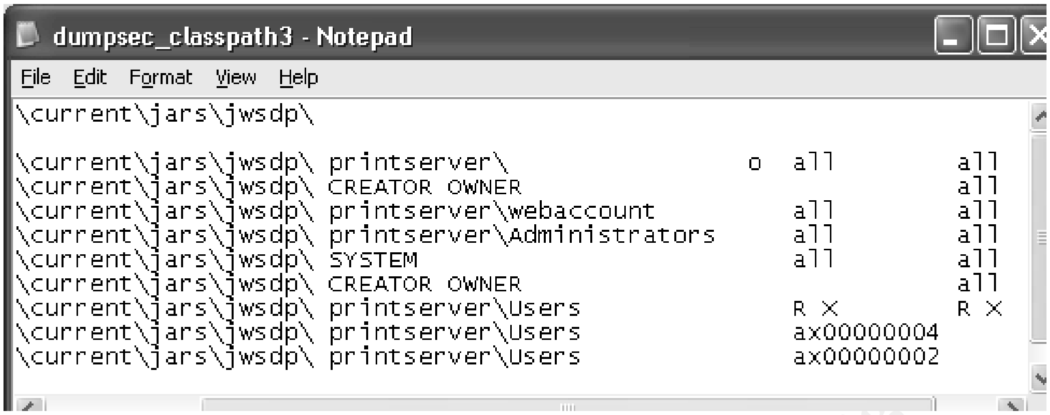
```
ent\jre\lib\

ent\jre\lib\        printserver\                o  all        all
ent\jre\lib\        CREATOR OWNER                             all
ent\jre\lib\        printserver\webaccount         all        all
ent\jre\lib\        printserver\Administrators     all        all
ent\jre\lib\        SYSTEM                         all        all
ent\jre\lib\        CREATOR OWNER                             all
ent\jre\lib\        printserver\Users              R X        R X
ent\jre\lib\        printserver\Users              ax00000004
ent\jre\lib\        printserver\Users              ax00000002
```

Figure 112: dumpsec log file for CLASSPATH1 directory



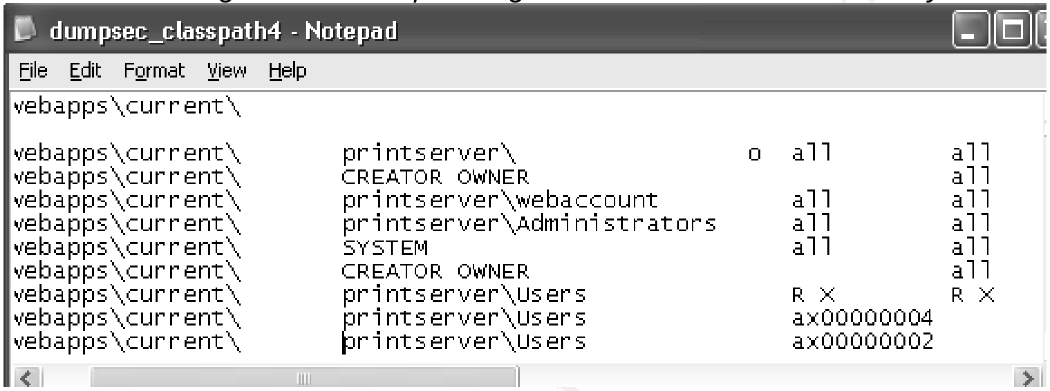
```
\current\jars\

\current\jars\       printserver\                o  all        all
\current\jars\       CREATOR OWNER                             all
\current\jars\       printserver\webaccount         all        all
\current\jars\       printserver\Administrators     all        all
\current\jars\       SYSTEM                         all        all
\current\jars\       CREATOR OWNER                             all
\current\jars\       printserver\Users              R X        R X
\current\jars\       printserver\Users              ax00000004
\current\jars\       printserver\Users              ax00000002
```

Figure 113: dumpsec log file for CLASSPAT2 directory



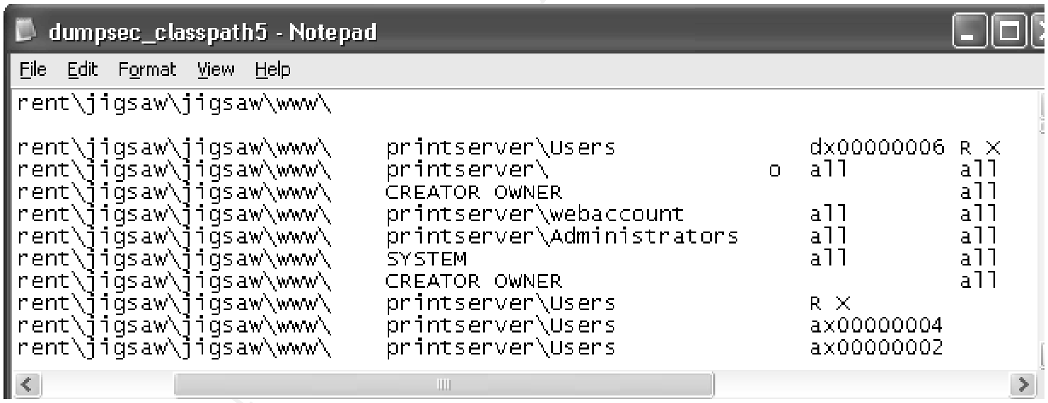
```
\current\jars\jwsdp\

\current\jars\jwsdp\ printserver\                  o  all        all
\current\jars\jwsdp\ CREATOR OWNER                               all
\current\jars\jwsdp\ printserver\webaccount           all        all
\current\jars\jwsdp\ printserver\Administrators        all        all
\current\jars\jwsdp\ SYSTEM                           all        all
\current\jars\jwsdp\ CREATOR OWNER                               all
\current\jars\jwsdp\ printserver\Users                R X        R X
\current\jars\jwsdp\ printserver\Users                ax00000004
\current\jars\jwsdp\ printserver\Users                ax00000002
```

Figure 114: dumpsec log file for CLASSPATH3 directory



```
vebapps\current\

vebapps\current\       printserver\                  o  all        all
vebapps\current\       CREATOR OWNER                               all
vebapps\current\       printserver\webaccount           all        all
vebapps\current\       printserver\Administrators       all        all
vebapps\current\       SYSTEM                           all        all
vebapps\current\       CREATOR OWNER                               all
vebapps\current\       printserver\Users                R X        R X
vebapps\current\       printserver\Users                ax00000004
vebapps\current\       printserver\Users                ax00000002
```

Figure 115: dumpsec log file for CLASSPATH4 directory

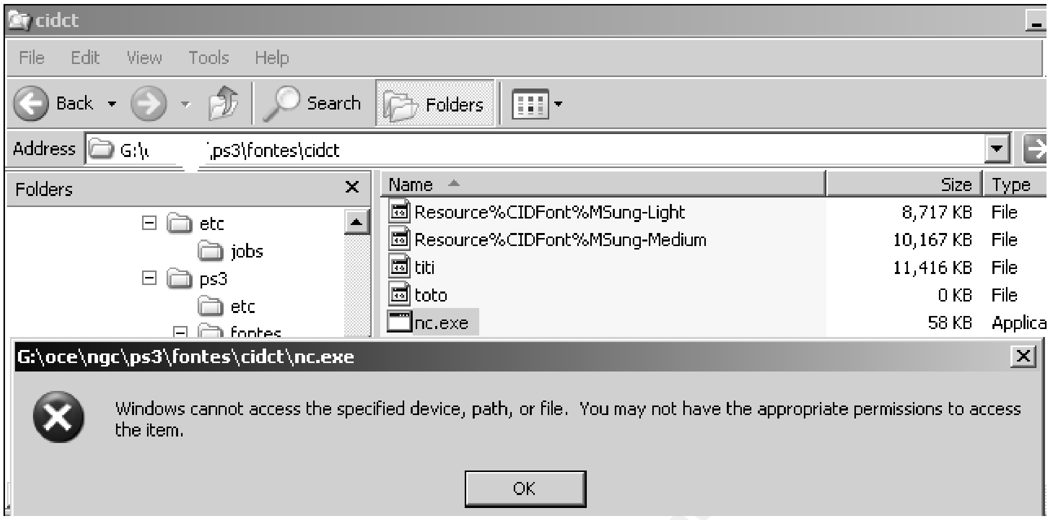


```
rent\jigsaw\jigsaw\www\

rent\jigsaw\jigsaw\www\    printserver\Users                dx00000006 R X
rent\jigsaw\jigsaw\www\    printserver\                  o  all        all
rent\jigsaw\jigsaw\www\    CREATOR OWNER                               all
rent\jigsaw\jigsaw\www\    printserver\webaccount           all        all
rent\jigsaw\jigsaw\www\    printserver\Administrators       all        all
rent\jigsaw\jigsaw\www\    SYSTEM                           all        all
rent\jigsaw\jigsaw\www\    CREATOR OWNER                               all
rent\jigsaw\jigsaw\www\    printserver\Users                R X
rent\jigsaw\jigsaw\www\    printserver\Users                ax00000004
rent\jigsaw\jigsaw\www\    printserver\Users                ax00000002
```

Figure 116: dumpsec log file for CLASSPATH5 directory

The previous screen shots show that the users have no rights to write in the folders contained in the CLASSPATH environment variable.

13 Appendix 7: Screen shots supporting the correction for Control No. 29

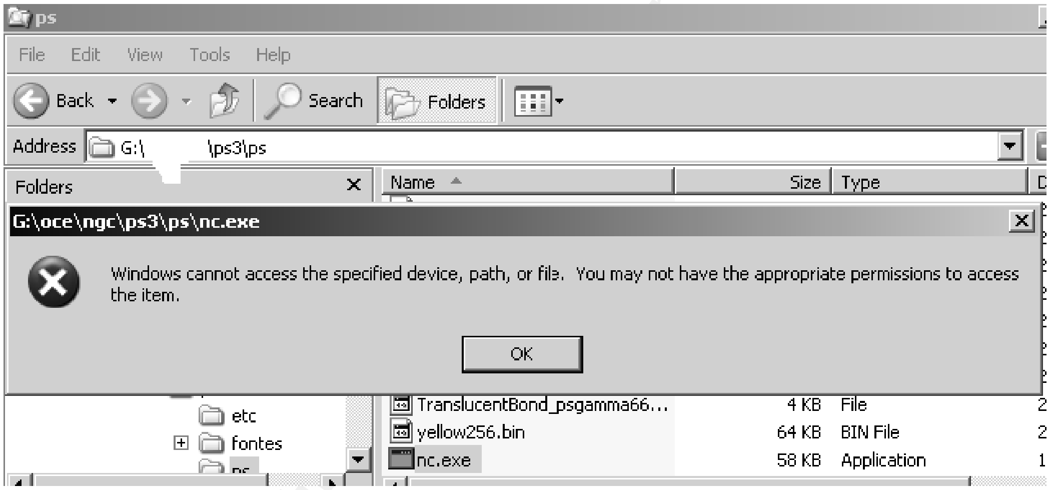


Name	Size	Type
Resource%CIDFont%MSung-Light	8,717 KB	File
Resource%CIDFont%MSung-Medium	10,167 KB	File
titi	11,416 KB	File
toto	0 KB	File
nc.exe	58 KB	Applica

G:\oce\ngc\ps3\fontes\cidct\nc.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

OK

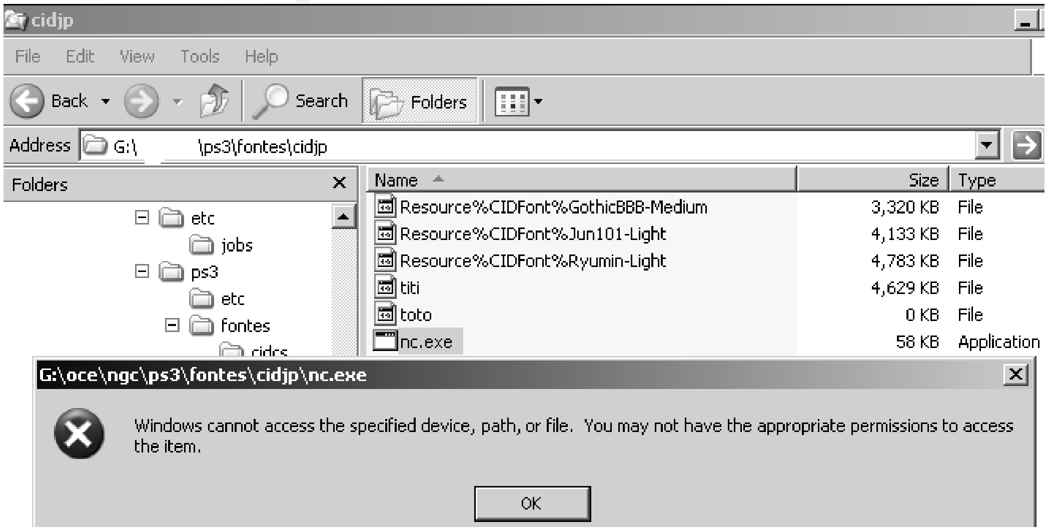


Name	Size	Type
TranslucentBond_psgamma66...	4 KB	File
yellow256.bin	64 KB	BIN File
nc.exe	58 KB	Application

G:\oce\ngc\ps3\ps\nc.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

OK

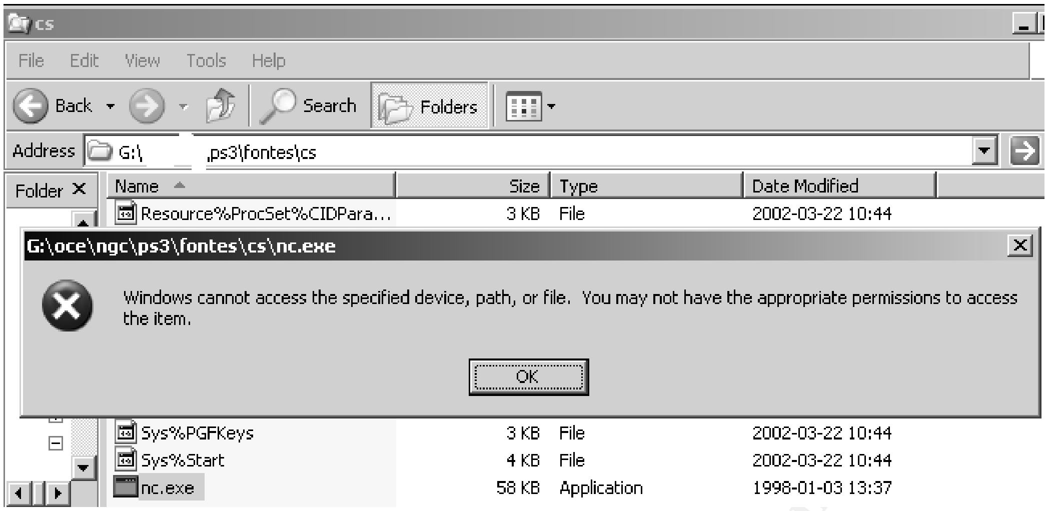


Name	Size	Type
Resource%CIDFont%GothicBBB-Medium	3,320 KB	File
Resource%CIDFont%Jun101-Light	4,133 KB	File
Resource%CIDFont%Ryumin-Light	4,783 KB	File
titi	4,629 KB	File
toto	0 KB	File
nc.exe	58 KB	Application

G:\oce\ngc\ps3\fontes\cidjp\nc.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

OK



G:\[redacted],ps3\fontes\cs

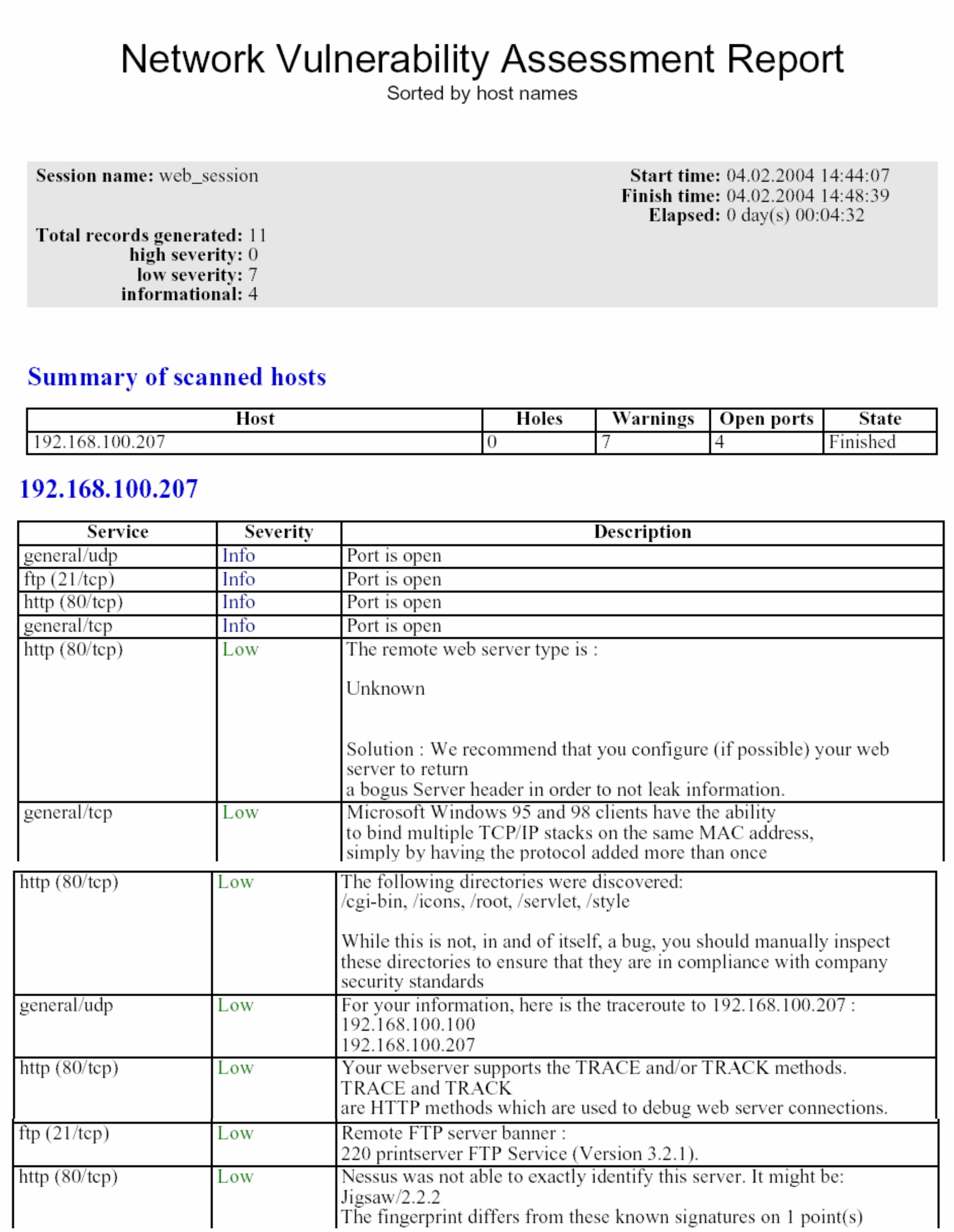
Name	Size	Type	Date Modified
Resource%ProcSet%CIDPara...	3 KB	File	2002-03-22 10:44
Sys%PGFKeys	3 KB	File	2002-03-22 10:44
Sys%Start	4 KB	File	2002-03-22 10:44
nc.exe	58 KB	Application	1998-01-03 13:37

G:\oce\ngc\ps3\fontes\cs\nc.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

The previous screen shots show that it is not possible to run nc.exe in the PostScript writable disks.

14 Appendix 8: Screen shots supporting the correction for Control No. 16



Network Vulnerability Assessment Report

Sorted by host names

Session name: web_session

Start time: 04.02.2004 14:44:07
Finish time: 04.02.2004 14:48:39
Elapsed: 0 day(s) 00:04:32

Total records generated: 11
high severity: 0
low severity: 7
informational: 4

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
192.168.100.207	0	7	4	Finished

192.168.100.207

Service	Severity	Description
general/udp	Info	Port is open
ftp (21/tcp)	Info	Port is open
http (80/tcp)	Info	Port is open
general/tcp	Info	Port is open
http (80/tcp)	Low	The remote web server type is : Unknown Solution : We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.
general/tcp	Low	Microsoft Windows 95 and 98 clients have the ability to bind multiple TCP/IP stacks on the same MAC address, simply by having the protocol added more than once
http (80/tcp)	Low	The following directories were discovered: /cgi-bin, /icons, /root, /servlet, /style While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards
general/udp	Low	For your information, here is the traceroute to 192.168.100.207 : 192.168.100.100 192.168.100.207
http (80/tcp)	Low	Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
ftp (21/tcp)	Low	Remote FTP server banner : 220 printserver FTP Service (Version 3.2.1).
http (80/tcp)	Low	Nessus was not able to exactly identify this server. It might be: Jigsaw/2.2.2 The fingerprint differs from these known signatures on 1 point(s)

The previous screen shots show that the Nessus scanner didn't find any high or medium level security vulnerabilities.

15 References

Security in general

[REF_G1] "Hacking exposed"-Third Edition- by Stuart McClure, Joel Scambray and George Kurtz (McGraw-Hill/Osborne

[REF_G2] "Writing secure code" by Michael Howard and David LeBlanc (Microsoft Press)

[REF_G3] http://razor.bindview.com/publish/presentations/nullsess.html

[REF_G4] PostScript Language Reference – Adobe Systems Incorporated

[REF_G5] Don Lancaster – Adobe Acrobat Security Flaws (http://www.tinaja.com/text/insecure.html)

[REF_G6] Gary Stonebumer, Alice Goguen, Alice, and Alex Feringa, NIST: Risk Management Guide for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

[REF_G7]: Windows XP Service Pack 2: A developer's view (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwxp/html/securityinxpsp2.asp)

Firewalls checklists references

[REF_F1] John Wack, Ken Cutler, Jamie Pole -NIST: Guidelines on Firealls and Firewall Policy (http://www.ffiec.gov/ffiecinfobase/resources/info_sec/nis-guide_on_firewall_and_firewall_pol_800_41.pdf)

[REF_F2] Horace B. Jones - Administratively Auditing the Security Provided by Norton Personal Firewall 2002 (http://www.giac.org/GSNA_0100.php)

[REF_F3] Egil Andresen, "Auditing Perimeter defenses in Home Office Environment with D-LINK Broadband Router and Kerio Personal Firewall" (http://www.giac.org/practical/GSNA/Egil_Andresen_GSNA.pdf)

[REF_F4] Mount Ararat Blossom- Firewall penetration testing (http://wittys.com/files/mab/fwpentesting.html)

[REF_F5] Ofir Arkin - ICMP Usage in Scanning. The Complete Know-How (http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf)

Web server checklists references

[REF_W1] The World Wide Web Security FAQ (http://www.w3.org/Security/Faq/wwwsf3.html)

[REF_W2] David P. Boswell - Writing Web Services for Jigsaw (http://www.wutka.com/hackingjava/ch25.htm)

[REF_W3] Publishing Pages with PUT (http://www.apacheweek.com/features/put)

[REF_W4] Winie HTTP/1.1 PUT Tool. (http://jigsaw.w3.org/Winie/)

[REF_W5] http://www.w3.org/Jigsaw/Doc/User/publication.html

[REF_W6] Internet Holes: 50 Ways to Attack Your Web Systems (http://agressor.times.lv/Articles/dirivweb.html)

[REF_W7] Hans Bergsten- An introduction to java servlets (http://webdevelopersjournal.com/articles/intro_to_servlets.html)

[REF_W8] David Hopwood – A comparison between Java and ActiveX Security (http://www.cgisecurity.com/lib/compsec97.html)

[REF_W9] Artur Maj - Securing Apache: Step-by-Step (http://www.securityfocus.com/infocus/1694)