



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Preparing to face new vulnerabilities

Preparing to face new vulnerabilities

GSEC Gold Certification

Author: Jacelyn Faucher, jacelyn.faucher@certaq.gouv.qc.ca

Adviser: Jim Purcell

Accepted: June 1, 2008

Table of contents

1	INTRODUCTION.....	3
2	MANAGEMENT OF THE CRISIS.....	4
3	GETTING THE INFORMATION.....	5
	External scanning.....	5
	Internal scanning.....	5
4	GETTING MANAGEMENT'S SUPPORT.....	6
5	CONNECTION REQUIREMENT.....	7
6	SETUP.....	8
	Description.....	9
	Credential.....	10
	Firewall rules.....	10
7	USING THE TOOLS TO GET PREPARED.....	11
	List of open port for each address visible from Internet.....	11
	12
	Nessus Linux scan with credentials from INT-SCANNER	13
	Is the Operating System up to date on FIREWALL?	14
	Is the SSH service up to date on FIREWALL?.....	18
	Is the NTP service up to date on FIREWALL?.....	21
	Is the Operating System up to date on LIN-TARGET?.....	24
	Is the SSH service up to date on LIN-TARGET?.....	27
	Is the HTTP service up to date on LIN-TARGET?.....	29
	Is the INT-SCANNER up to date?.....	33
	Is the Windows 2003 up to date?.....	34
	Scan summary.....	39
8	UPDATE ON NEW VULNERABILITIES COMMING OUT.....	40
9	CONCLUSION.....	40
10	REFERENCES.....	41

1 INTRODUCTION

This document illustrates the benefit of being prepared to deal with new vulnerabilities. We don't really know when that's going to happen, but it will. Let's look at a typical scenario: Monday morning, panic is in the air. The boss heard the existence of a big new vulnerability on the radio on his way to work.

The security person is under the spotlight. Management wants to know what the situation is. At this time, it is important to have answers quickly. Each time a new vulnerability is made public, one of the many roles of the security person is to find out if harm can be done to the IT infrastructure.

The information needed is simple. Is the vulnerable product running in our environment? Is it at risk? Is it accessible from the Internet? Of course, server administrators might possess that information, but at this stage, the security person has to deal with it.

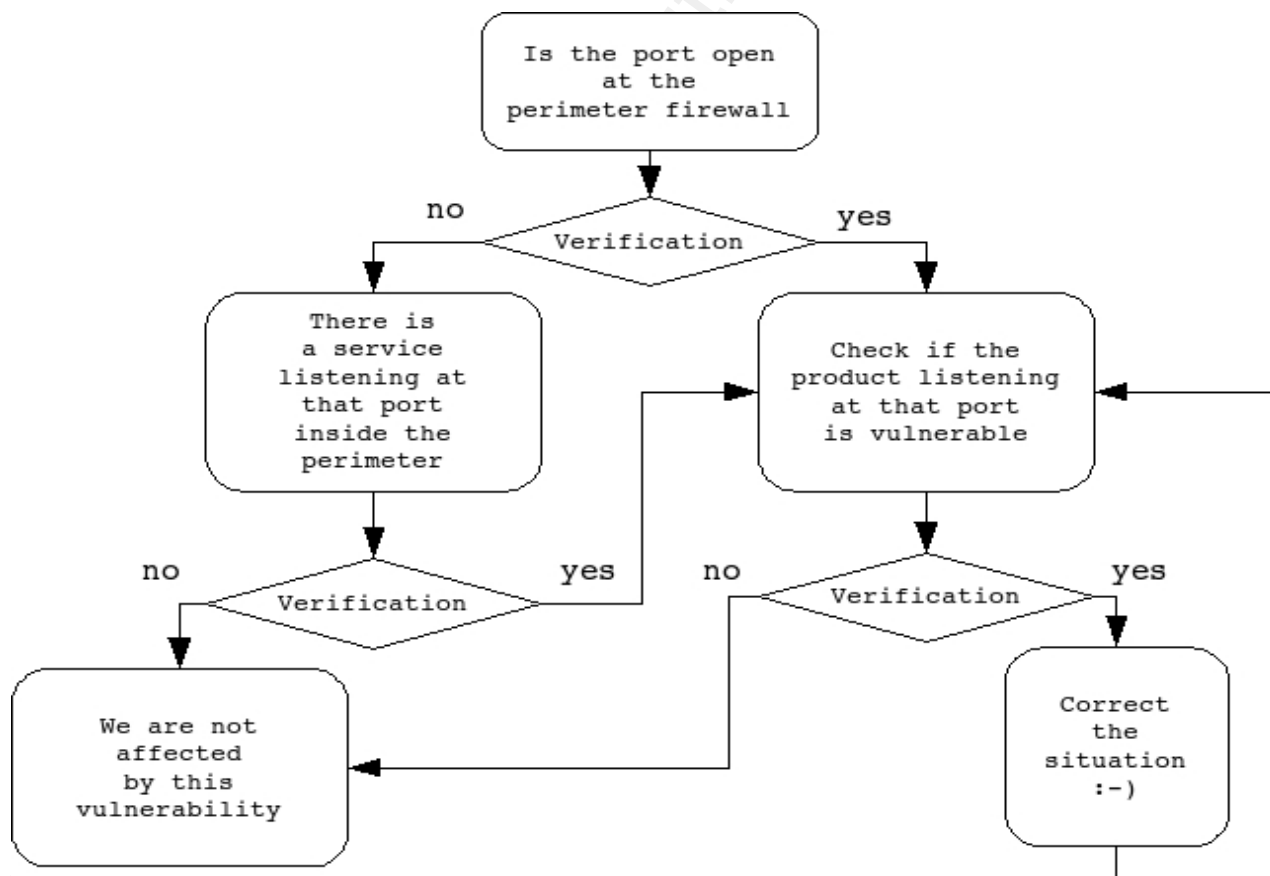
Server administrators are usually security minded, but they also have the responsibility to provide online services and sometimes, for all kinds of reasons, patches cannot be applied as they should. Also, lots of times, temporary solutions have to be put in place to preserve the continuity of the service. Sometimes, when a vulnerability is exploitable only on a local level, administrator have tendency to remain on the perimeter firewall. Administrators are reluctant to talk about these temporary solutions. They figure, the

Preparing to face new vulnerabilities

less people know about it, the better. But this can lead to a vulnerable network.

2 MANAGEMENT OF THE CRISIS

Back to our question: Is the vulnerability that just came out affecting us? How can we find out without spending lots of time to install software agents on the servers? The faster that question is answered, the better it is. Here is a flowchart detailing the process:



Flow chart of management of the crisis ***Server only***

3 GETTING THE INFORMATION

We need a picture of the network at a point in time with the following points: The list of allowed ports at the perimeter firewall, the actual versions of the products running on the machines listening on those ports and the actual patch level of each product.

External scanning

The tool NMAP will be used to scan from outside the firewall perimeter to see what is exposed. This will enumerate IP addresses and ports that can be accessed from the Internet. Of course, the scan has to be launched with a configuration to minimize the impact on the network. Not only will this tell you which ports are open, if done on a regular base, it will also notify you when a new port is opened or closed.

Internal scanning

By using credentials, the NESSUS tool can be granted local access to scan the target system without requiring an agent. That involves using an account with administrator privileges on each server. A NESSUS credential scan can quickly establish which systems are missing patches for UNIX and WINDOWS operating systems. Knowing the actual patch level of a system is the only way to be certain of the security state of a system. Of course, the system has to be configured correctly in the first place. For example, a system administrator may claim to have patched Apache 1.3, while they may have in fact simply disabled it. The NESSUS vulnerability scanner

Preparing to face new vulnerabilities

determines the difference between a quick fix and a fully mitigated security issue. This is especially important when a new vulnerability is published and management wants an answer regarding the impact on the organization.

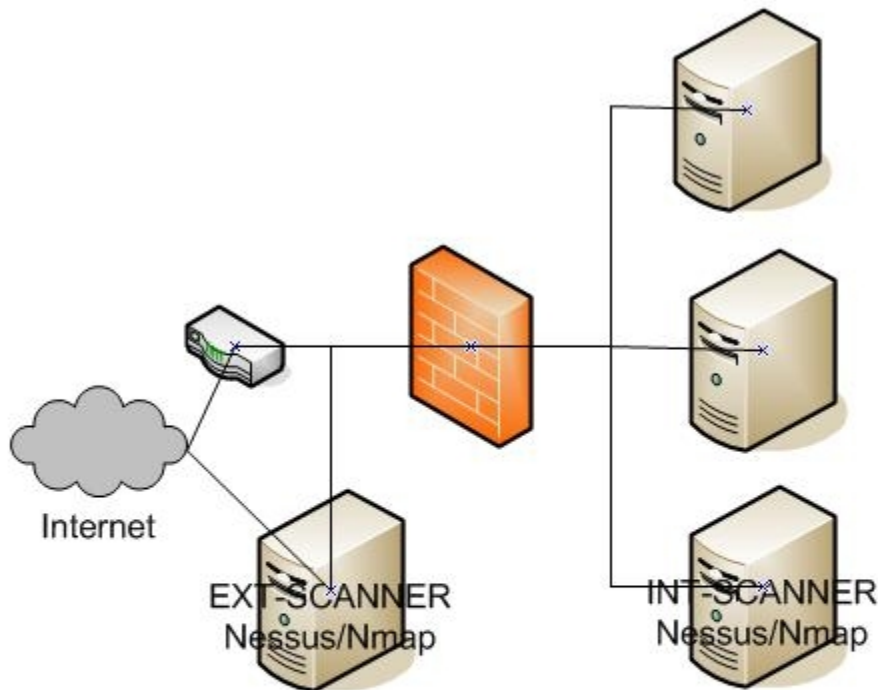
4 GETTING MANAGEMENT'S SUPPORT

This kind of project will definitely generate resistance to change. For many reasons, the server administrator may be reluctant to give 24/7 access to the servers to the security group. Furthermore, management need convincing regarding the necessity of collecting information using free tools to scan the private network and the perimeter firewall.

You definitely need their support. Be careful in the approach. You need to get a firm positive response. Find a ways to make them understand that the goal is to be able to know as soon as possible when a product, in the corporate environment, contains a vulnerability known to the public. This will greatly improve the process of correcting the situation and consequently, reducing the amount of time the vulnerability will be present. It doesn't take long to the underground world to write code exploiting any vulnerability after it is found. Furthermore, underline the fact that NISSUS supports the use of several secure approaches to solve the issue of providing privileged credentials. Once you have their approbation, involve them in the process of informing the server's administrators.

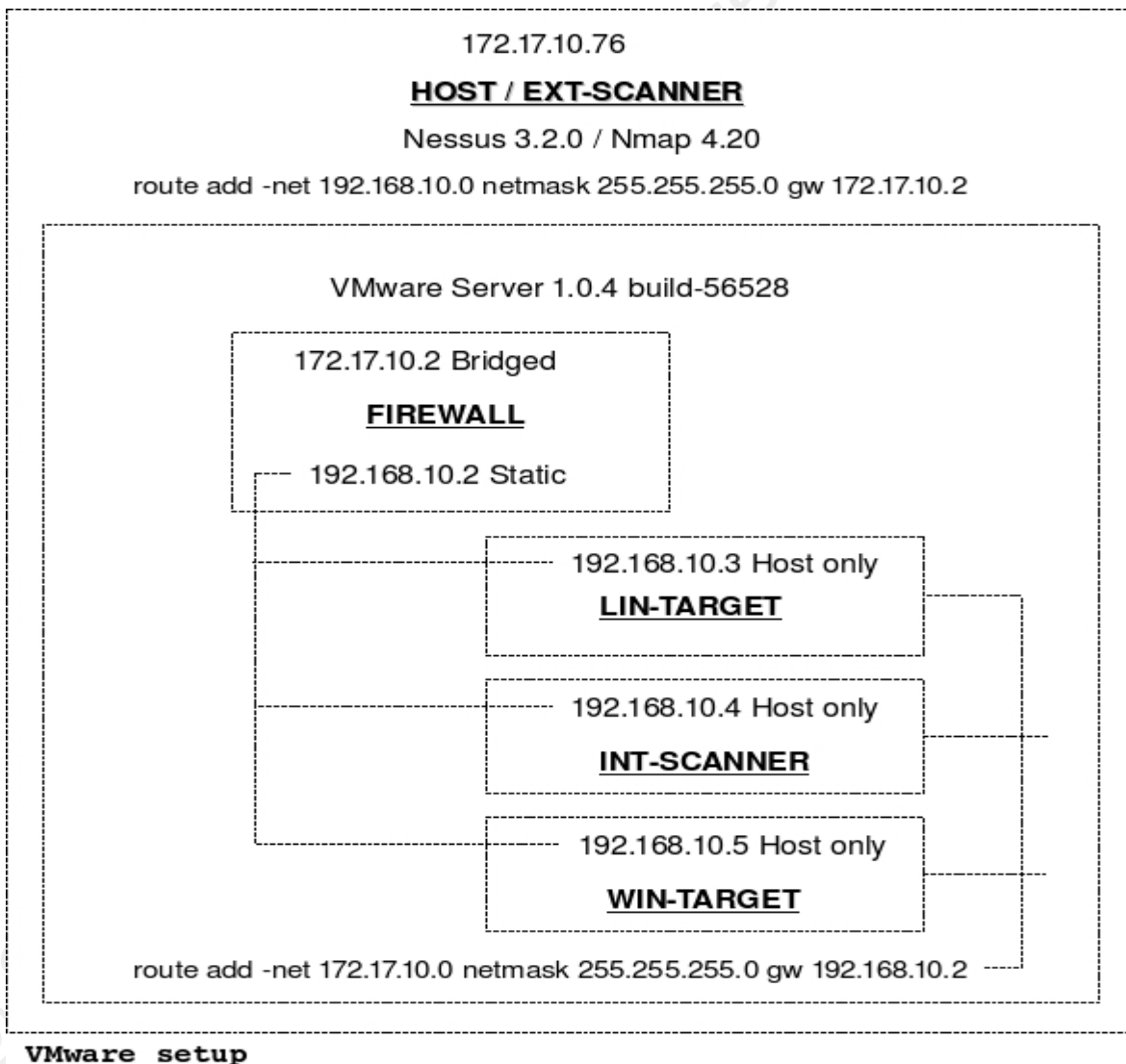
5 CONNECTION REQUIREMENT

You will need a connection outside of your firewall to perform scanning, from the internet. The ISP router might block some traffic and you might have to get their approbation. Choose the right place to get online. This will enable you to enumerate the open ports in the perimeter firewall. You will also need a second connection inside the perimeter to launch NESSUS Credential scans.



6 SETUP

For the purpose of this paper, the following setup has been installed in VMWARE on a Linux host. Take note that the choice of the machines names and users for this paper is not really a good choices. Appropriate server and account names should be used for production environments.



Description

The Debian 4.0 operating system have been installed with the “Hardening Debian 4.0 – Creating a simple and solid foundation for your applications” procedure found in the SANS Reading Room.

HOST(EXT-SCANNER)

Operating system: Ubuntu 7.10

VMware Server: VMware Server 1.0.4 build-56528

Nessus: Nessus 3.2.0

FIREWALL

Operating system: Debian 4.0

Firewall: Iptables 1.3.6

LIN-TARGET

Operating system: Debian 4.0

Firewall: Iptables 1.3.6

INT-PROBER

Operating system: Debian 4.0

Nessus: Nessus 3.2.0

Firewall: Iptables 1.3.6

WIN-TARGET

Operating system: Windows 2003 Service Pack 2

Firewall: Microsoft

Credential

According to NESSUS, user names and passwords are not recommended for authentication with SSH. "Man in the middle" and brute force attacks can be used with static passwords, especially when they have been in use for a long period of time.

Public/private keys will be used in order to allow NESSUS to launch authenticated network scans on the FIREWALL and the LIN-TARGET. This action will be performed from INT-SCANNER located inside the private network.

The "nessus" user with administrator privileges has been created on the FIREWALL, LIN-TARGET and WIN-TARGET servers. Permission to access the registry has been granted to the "nessus" user on WIN-TARGET.

An SSH private/public key pair has been created on INT-SCANNER. A copy of the SSH public key has been copied in the nessus user directory of the machine FIREWALL and LIN-TARGET.

Firewall rules

IPTABLES on FIREWALL and LIN-TARGET are configured to DROP everything except what is needed, and both ingress and egress filtering is activated. Also, three way hand-shake has to be complete with the correct flags enabled at the right moment in order to establish the connection. INT-SCANNER and EXT-SCANNER are configured to DROP everything inbound, except for the port needed to log the NESSUS server and SSH. They are wide opened for outbound. Finally, the WIN-TARGET is configured to DROP everything except for what is

Preparing to face new vulnerabilities

needed inbound and it is wide opened outbound.

7 USING THE TOOLS TO GET PREPARED

Now that the scanners are in place, let's get the information needed. First, let us take a picture of what is visible from the Internet.

List of open port for each address visible from Internet

The following NMAP scan has been launched on all TCP ports from EXT-SCANNER. The switch "-sT", TCP connect scan, accomplishes the three way hand-shake, the switch "-P0" assumes that the target is alive (No ICMP request) and the switch "-r" does a sequential port scan.

```
# nmap -sT -P0 -r -pl-65535 172.17.10.2 192.168.10.3 192.168.10.4
192.168.10.5
```

```
Starting Nmap 4.20 ( http://insecure.org ) at 2008-04-17 10:15 EDT
Interesting ports on firewall (172.17.10.2)(192.168.10.2):
Not shown: 1696 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
```

```
Interesting ports on lin-target (192.168.10.3):
Not shown: 1695 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Preparing to face new vulnerabilities

Interesting ports on int-scanner (192.168.10.4):

Not shown: 1695 filtered ports

PORT	STATE	SERVICE
------	-------	---------

22/tcp	open	ssh
--------	------	-----

1241/tcp	open	nessus
----------	------	--------

Interesting ports on win-target (192.168.10.5):

Not shown: 1696 filtered ports

PORT	STATE	SERVICE
------	-------	---------

80/tcp	open	http
--------	------	------

Nmap finished: 4 IP addresses (4 hosts up) scanned in 85.557 seconds

The four machines were scanned in 88.557 seconds. It took nearly twenty-two seconds for each IP address. Now, we have a picture of the opened TCP port visible from the Internet.

UDP port scanning across a firewall is another story; "icmp port unreachable" message have to be enabled in order for it to be effective.

We'll assume that all the servers and all the services where up at the time of the scan. We now have a good picture of the TCP ports listening at the other side of the firewall. The idea here is to find out if the port involved in the new vulnerability that just came out is listening at the perimeter.

Nessus Linux scan with credentials from INT-SCANNER

The scan has been launched from INT-SCANNER with the following configuration:

Options: Default

Credentials: Linux credentials

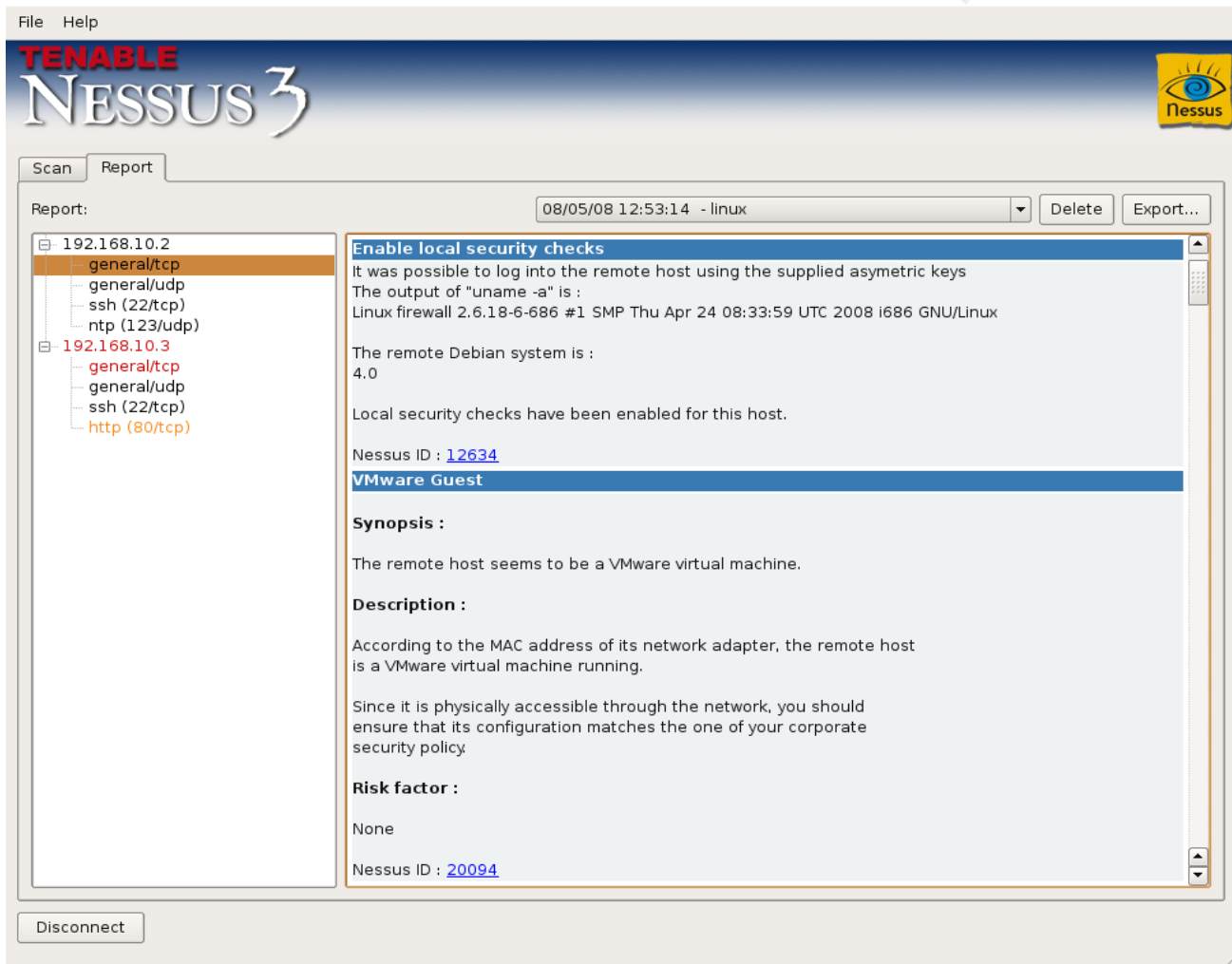
Plug-in Selection: Default

Network: Default

Advanced: Default

Is the Operating System up to date on FIREWALL?

Output 1, OS FIREWALL:

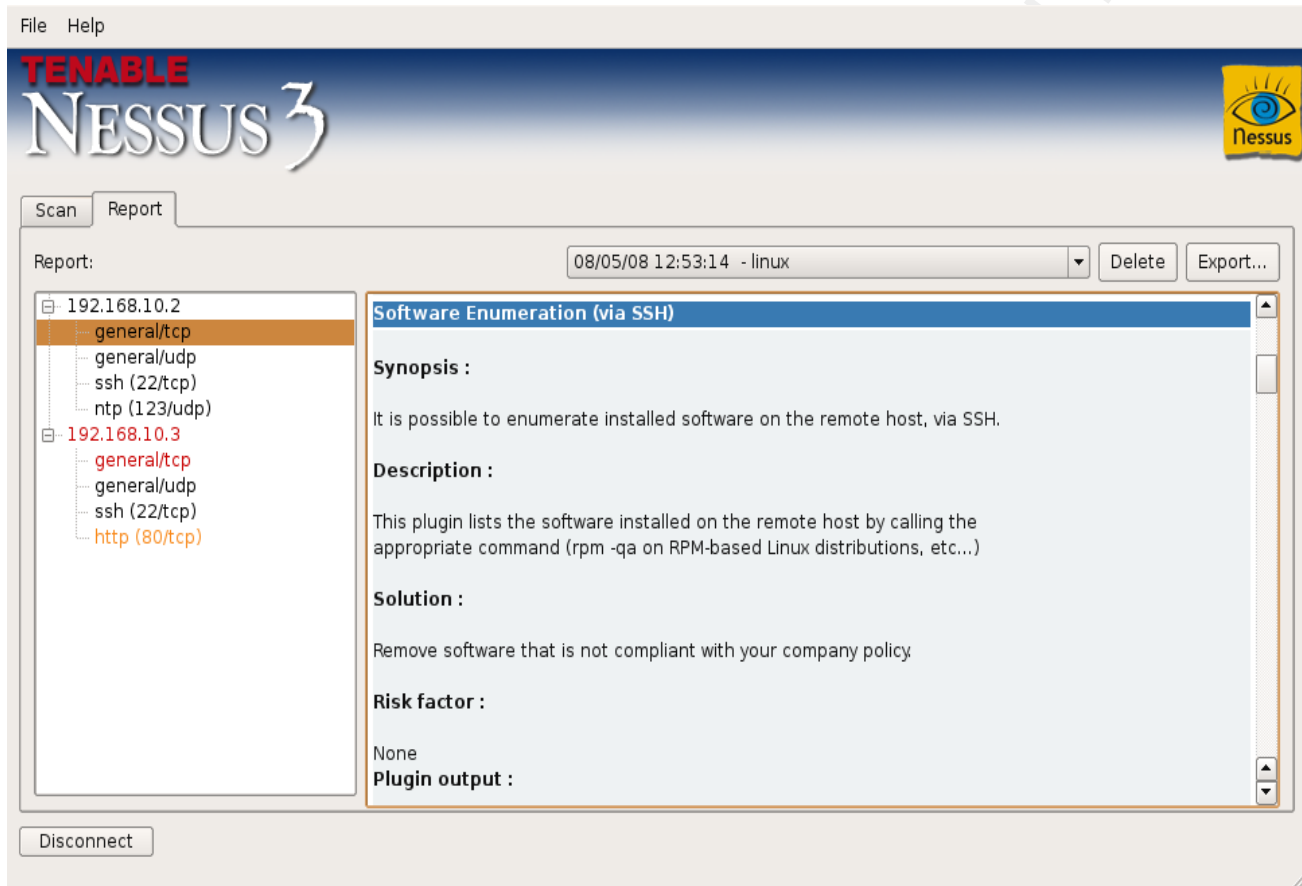


FIREWALL(172.17.10.2/192.168.10.2).

192.168.10.2 is the network interface facing the private network and 172.17.10.2 is the network interface facing the Internet. The NESSUS tool has logged into the remote host successfully.

Linux image: 2.6.18-6-686, April 24 2008

Output 2, OS FIREWALL:



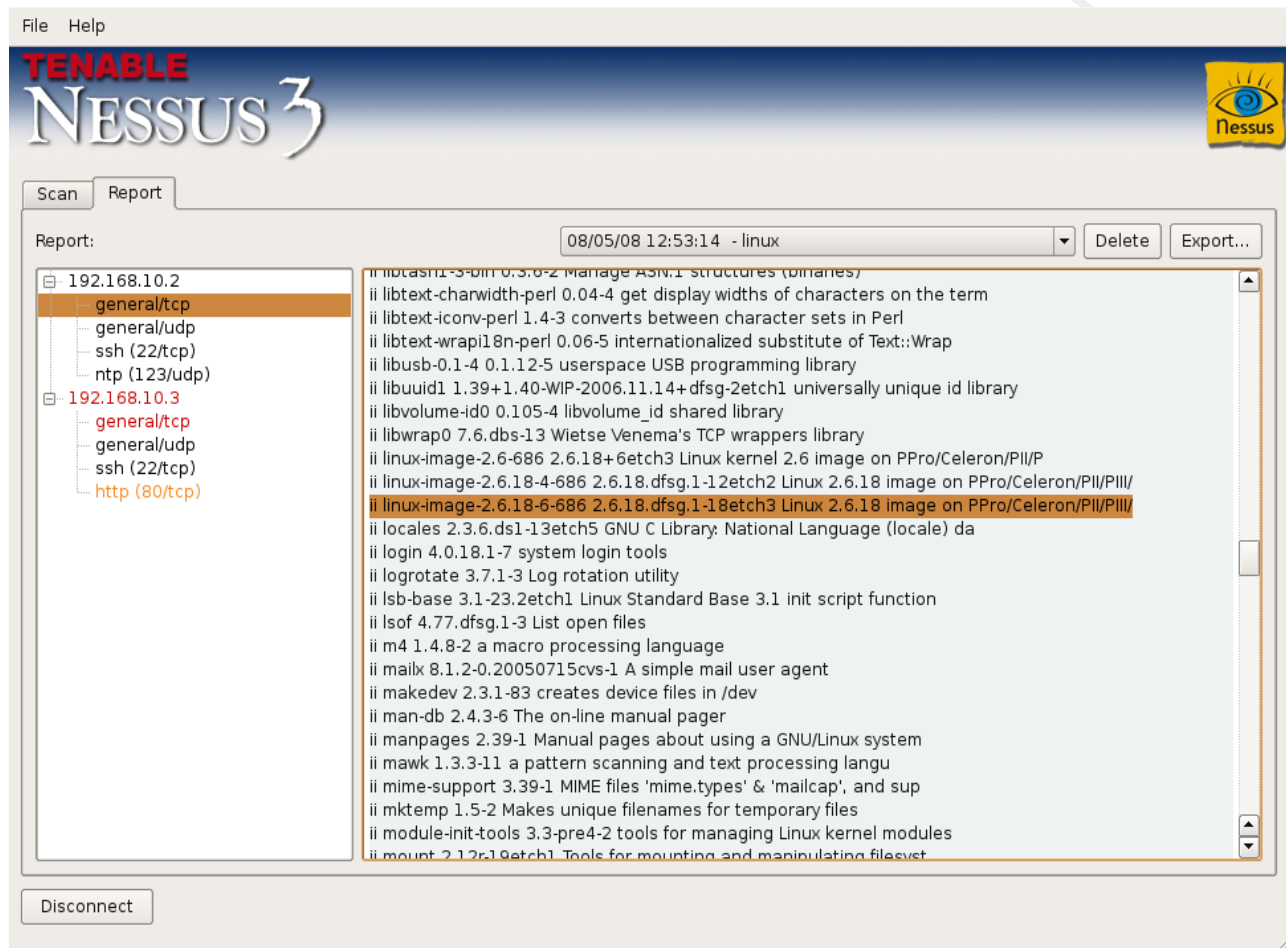
The Software Enumeration output uses the command "dpkg -l" to list the packages installed on FIREWALL via SSH.

Code of the Plugin:

<http://www.nessus.org/plugins/index.php?view=viewsrc&id=22869>

"Host/Debian/dpkg-l", "Linux",

Output 3, OS FIREWALL:



The Software Enumeration output indicate the version of the Linux image installed on the remote system. The output 1 indicate that the image is 2.6.18-6-686, April 24 2008.

OS: linux-image-2.6.18-6-686 2.6.18.dfsg.1-18etch3 Linux 2.6.18 image on Ppro/Celeron/PII/PIII/P4

Notice that the "/P4" is trunked in the NESSUS output.

Output 4, OS FIREWALL:

The screenshot shows the Debian website interface for the package **linux-headers-2.6-686**. The browser address bar shows <http://packages.debian.org/en/etch/linux-headers-2.6-686>. The page title is "Package: linux-headers-2.6-686 (2.6.18+6etch3)".

Header files for Linux 2.6 on PPro/Celeron/PII/PIII/P4

This package depends on the architecture-specific header files for the latest Linux kernel 2.6 on Pentium Pro/Celeron/Pentium II/Pentium III/Pentium 4 machines.

Tags: System Administration: [Kernel or Modules](#)

Other Packages Related to linux-headers-2.6-686

Legend: ● depends ◆ recommends ■ suggests

● [linux-headers-2.6.18-6-686](#)
Header files for Linux 2.6.18 on PPro/Celeron/PII/PIII/P4

Download linux-headers-2.6-686

Architecture	Package Size	Installed Size	Files
i386	2.3 kB	32 kB	[list of files]

Links for linux-headers-2.6-686

Debian Resources:

- [Bug Reports](#)
- [Developer Information \(PTS\)](#)
- [Debian Changelog](#)
- [Copyright File](#)

Download Source Package [linux-latest-2.6](#):

- [\[linux-latest-2.6_6etch3.dsc\]](#)
- [\[linux-latest-2.6_6etch3.tar.gz\]](#)

Maintainers:

- [Debian Kernel Team](#) (QA Page, Mail Archive)
- [Bastian Blank](#) (QA Page)
- [Frederik Schuler](#) (QA Page)

Similar packages:

- [linux-headers-2.6-686-bigmem](#)
- [linux-headers-2.6-vsserver-686](#)
- [linux-headers-2.6.18-4-686](#)
- [linux-headers-2.6.22-4-686](#)
- [linux-headers-2.6.18-6-686](#)
- [linux-headers-2.6.18-5-686](#)
- [linux-headers-2.6.22-3-686](#)
- [linux-headers-2.6.25-1-686](#)

Terminé

If we compare the informations obtained from the previous output with the output at the Debian web site. We can conclude that the kernel running on FIREWALL is up to date.

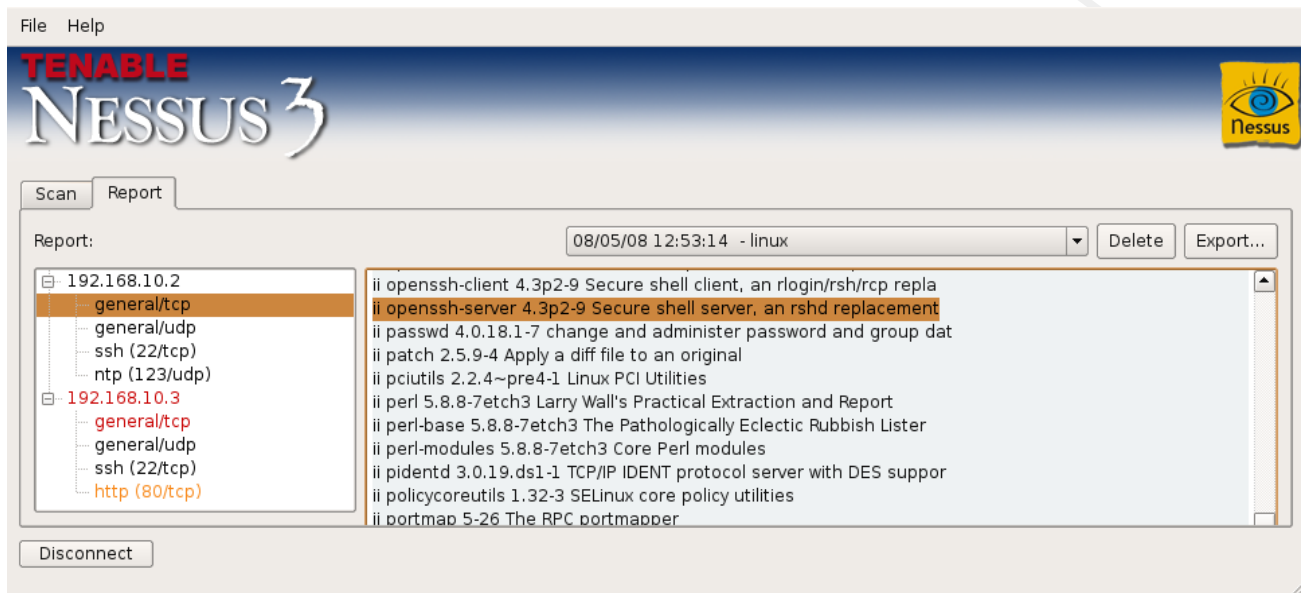
Is the SSH service up to date on FIREWALL?

Output 1, SSH on FIREWALL:



This output indicate that the SSH service is listening on port 22. Notice that password authentication is not permitted. Only public key authentication's.

Output 2, SSH on FIREWALL:



The information concerning the SSH service listening on port 22 has been obtained by the Software Enumeration output.

SSH: Version 4.3p2-9.

Output 3, SSH on FIREWALL:

The screenshot shows the Debian website interface for the `openssh-server` package. The browser address bar shows `http://packages.debian.org/en/etch/openssh-server`. The page title is "Debian -- Details of pac...". The Debian logo is visible. A search bar contains "package names". A navigation bar shows the path: `>> Debian >> Packages >> etch (stable) >> net >> openssh-server`. Below this, it says "[Source: [openssh](#)]" and "[[sarge-backports](#)] [[etch](#)] [[etch-m68k](#)] [[lenny](#)] [[sid](#)]".

Package: openssh-server (1:4.3p2-9)

Secure shell server, an rshd replacement

This is the portable version of OpenSSH, a free implementation of the Secure Shell protocol as specified by the IETF secsh working group.

Ssh (Secure Shell) is a program for logging into a remote machine and for executing commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. It is intended as a replacement for rlogin, rsh and rcp, and can be used to provide applications with a secure communication channel.

This package provides the sshd server.

In some countries it may be illegal to use any encryption at all without a special permit.

Tags: System Administration: [Login](#), User Interface: [Daemon](#), Networking: [Server](#), Network Protocol: [SSH](#), Role: [Program](#), Security: [Authentication](#), [Cryptography](#), Purpose: [Login](#), [Transmission](#)

Other Packages Related to openssh-server

depends recommends suggests

Links for openssh-server

Debian Resources:

- [Bug Reports](#)
- [Developer Information \(PTS\)](#)
- [Debian Changelog](#)
- [Copyright File](#)

Download Source Package [openssh](#):

- [\[openssh_4.3p2-9.dsc\]](#)
- [\[openssh_4.3p2.orig.tar.gz\]](#)
- [\[openssh_4.3p2-9.diff.gz\]](#)

Maintainers:

- [Matthew Vernon \(QA Page\)](#)
- [Colin Watson \(QA Page\)](#)

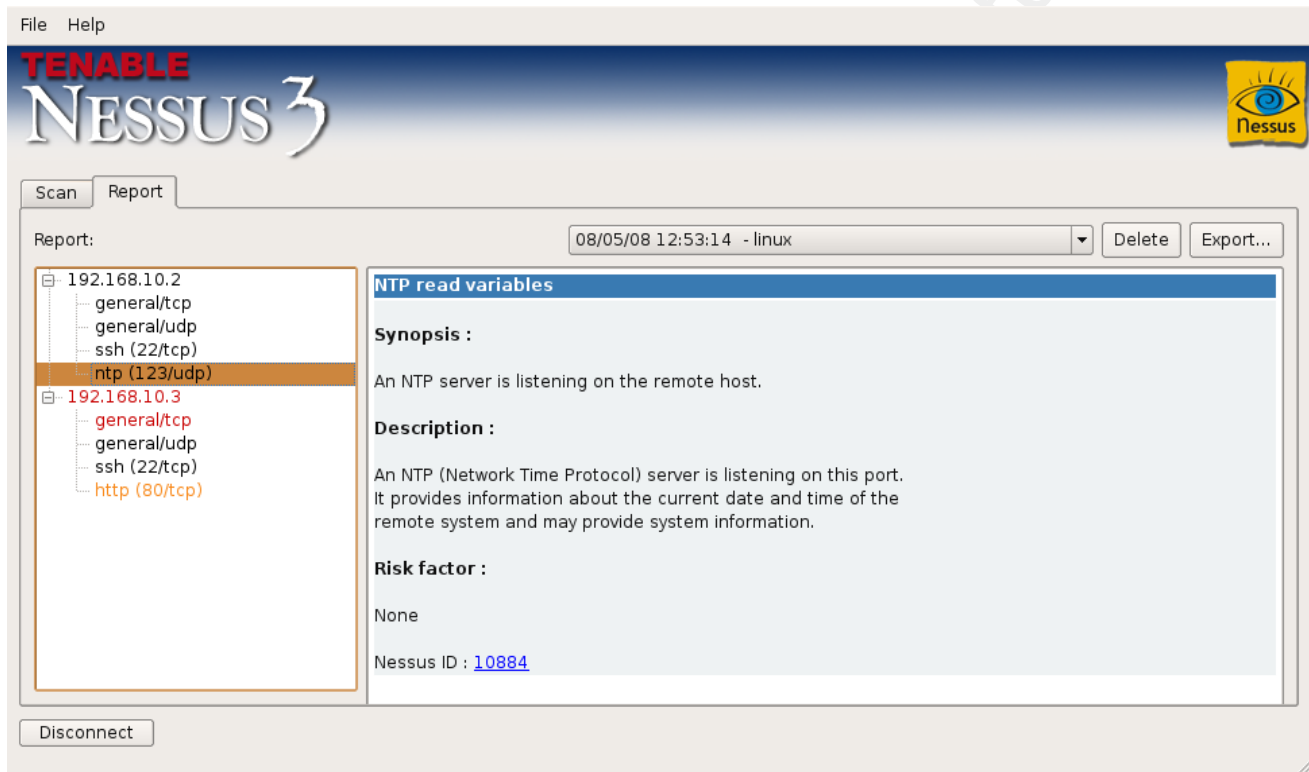
Similar packages:

- [ssh](#)
- [openssh-client](#)
- [ssh-krb5](#)
- [lsh-server](#)
- [lsh-client](#)
- [lsh-utils](#)
- [lsh-utils-doc](#)

If we compare the informations obtained from the previous output with the output at the Debian web site. We can conclude that the SSH service running on FIREWALL is up to date.

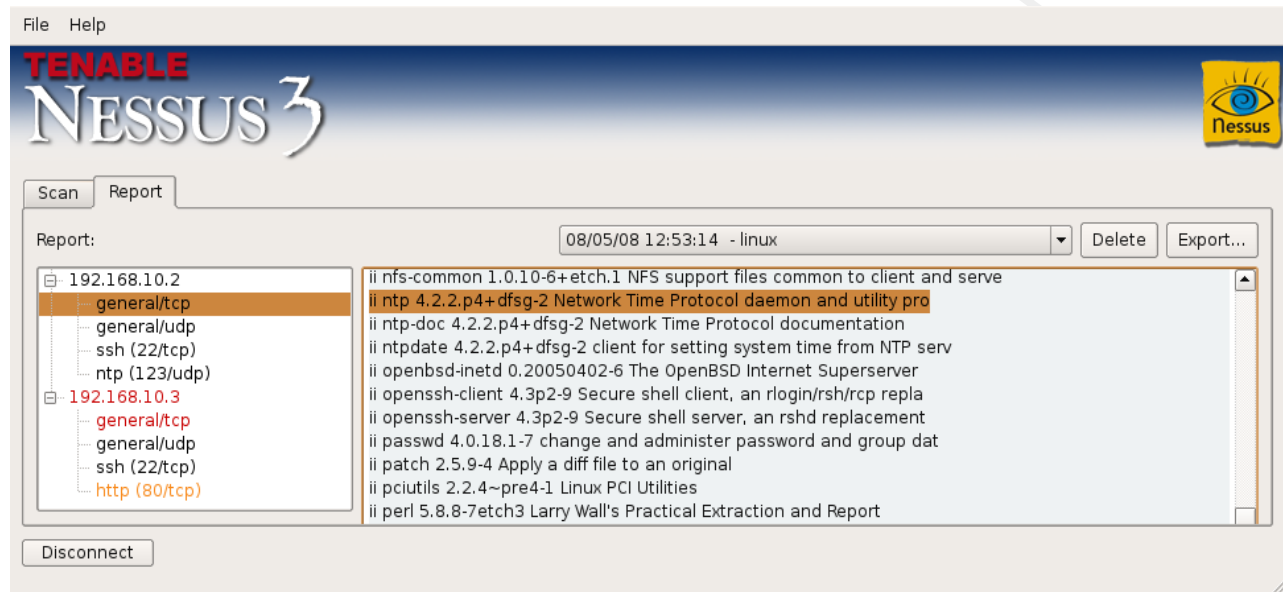
Is the NTP service up to date on FIREWALL?

Output 1, NTP on FIREWALL:



This output indicates that the NTP service is listening on port 123.

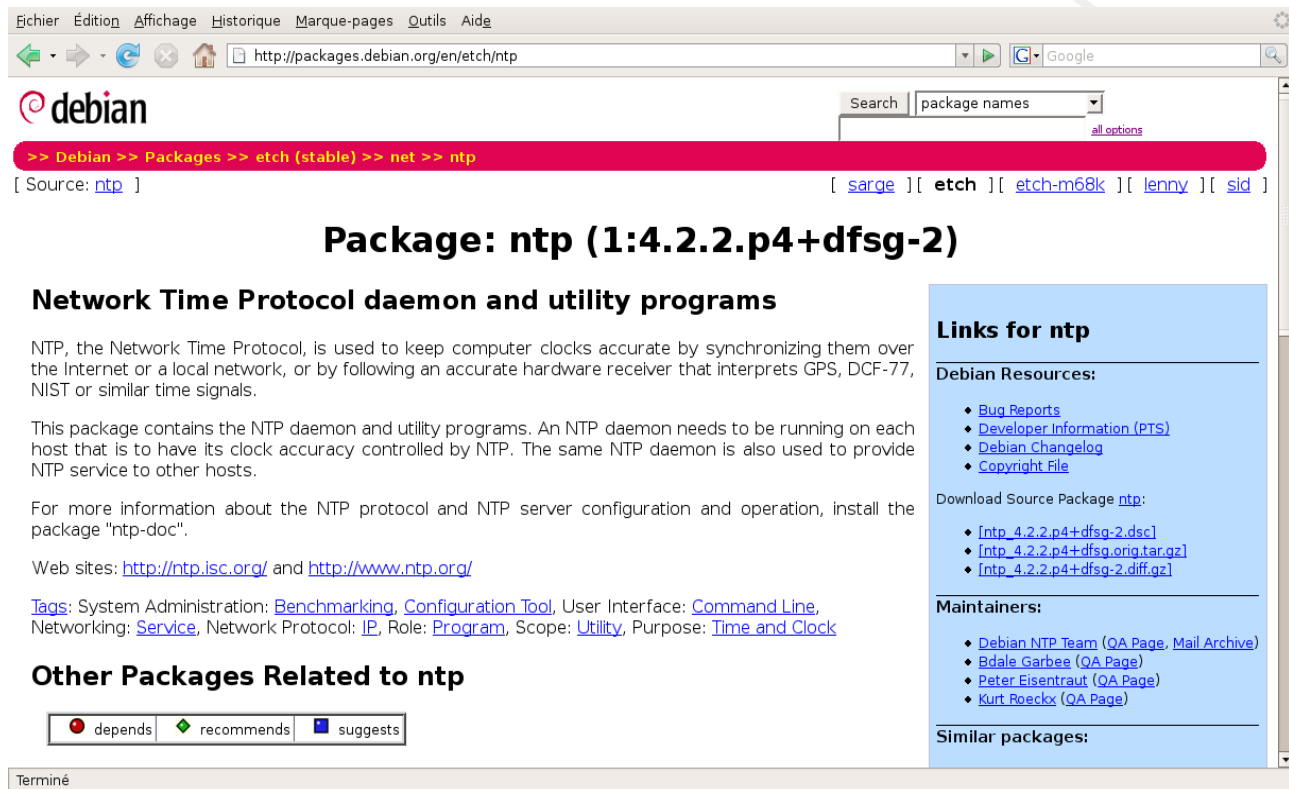
Output 2, NTP on FIREWALL:



The information concerning the NTP service listening on port 123 has been obtained by the Software Enumeration output. Note that the NTP server is answering at the request from the private network only. It is not a good practice to install the time server on a perimeter firewall. It was done in the context of the "VMware" test setup.

NTP: Version 4.2.2.p4+dfsg-2.

Output 3, NTP on FIREWALL:

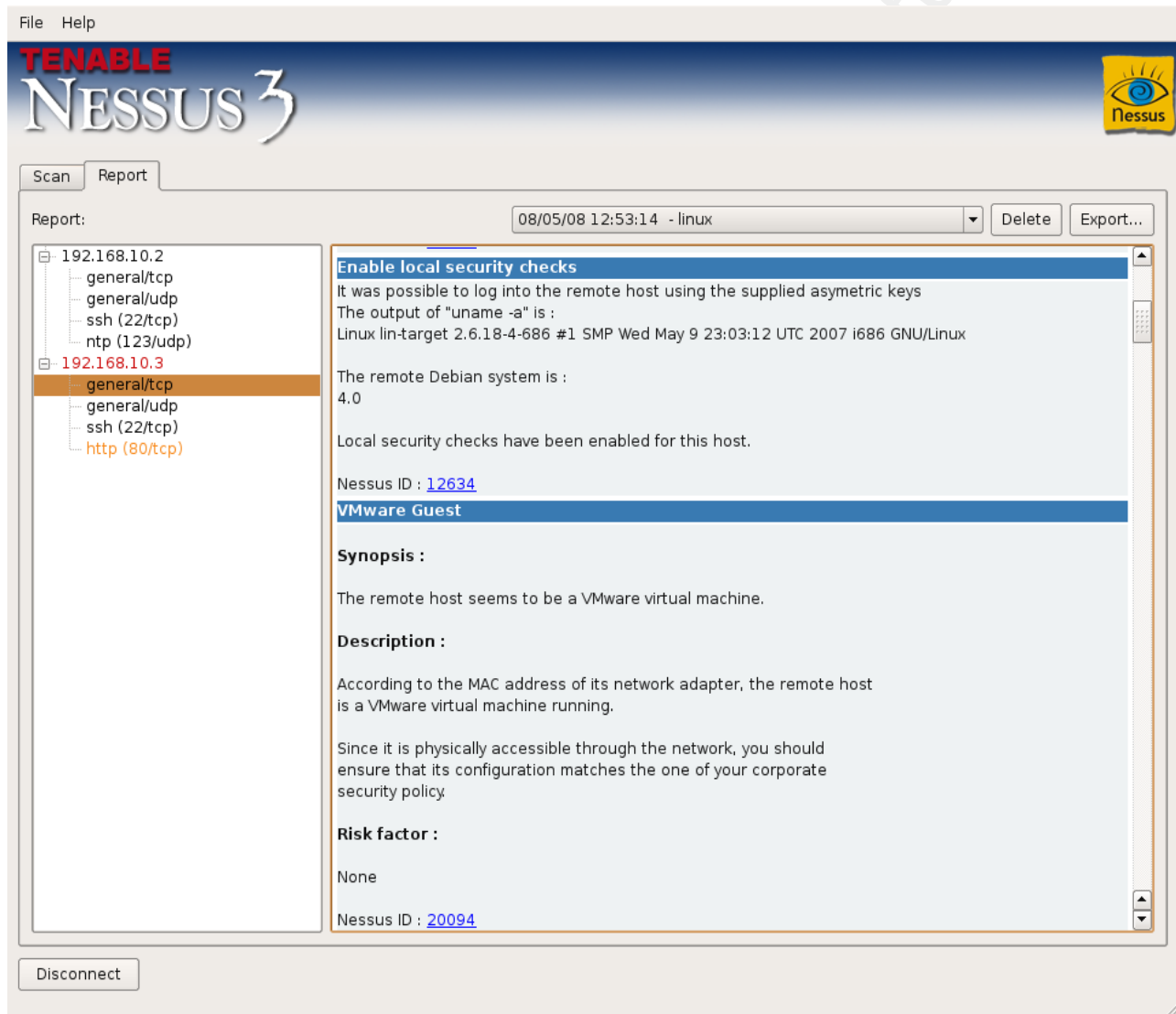


The screenshot shows the Debian package website for the **ntp** package (version 1:4.2.2.p4+dfsg-2). The page is titled "Package: ntp (1:4.2.2.p4+dfsg-2)" and describes it as the "Network Time Protocol daemon and utility programs". The description states that NTP is used to keep computer clocks accurate by synchronizing them over the Internet or a local network, or by following an accurate hardware receiver that interprets GPS, DCF-77, NIST or similar time signals. It also mentions that the package contains the NTP daemon and utility programs, and that an NTP daemon needs to be running on each host that is to have its clock accuracy controlled by NTP. The same NTP daemon is also used to provide NTP service to other hosts. For more information about the NTP protocol and NTP server configuration and operation, it suggests installing the package "ntp-doc". Web sites are listed as <http://ntp.isc.org/> and <http://www.ntp.org/>. Tags include System Administration, Benchmarking, Configuration Tool, User Interface, Command Line, Networking, Service, Network Protocol, IP, Role, Program, Scope, Utility, and Purpose, Time and Clock. The page also includes a section for "Other Packages Related to ntp" with buttons for "depends", "recommends", and "suggests". On the right side, there are sections for "Links for ntp", "Debian Resources" (including Bug Reports, Developer Information (PTS), Debian Changelog, and Copyright File), "Download Source Package ntp:" (with links for ntp_4.2.2.p4+dfsg-2.dsc, ntp_4.2.2.p4+dfsg.orig.tar.gz, and ntp_4.2.2.p4+dfsg-2.diff.gz), "Maintainers" (including Debian NTP Team, Bdale Garbee, Peter Eisentraut, and Kurt Roeckx), and "Similar packages:".

If we compare the informations obtained from the previous output with the output at the Debian web site. We can conclude that the NTP service running on FIREWALL is up to date.

Is the Operating System up to date on LIN-TARGET?

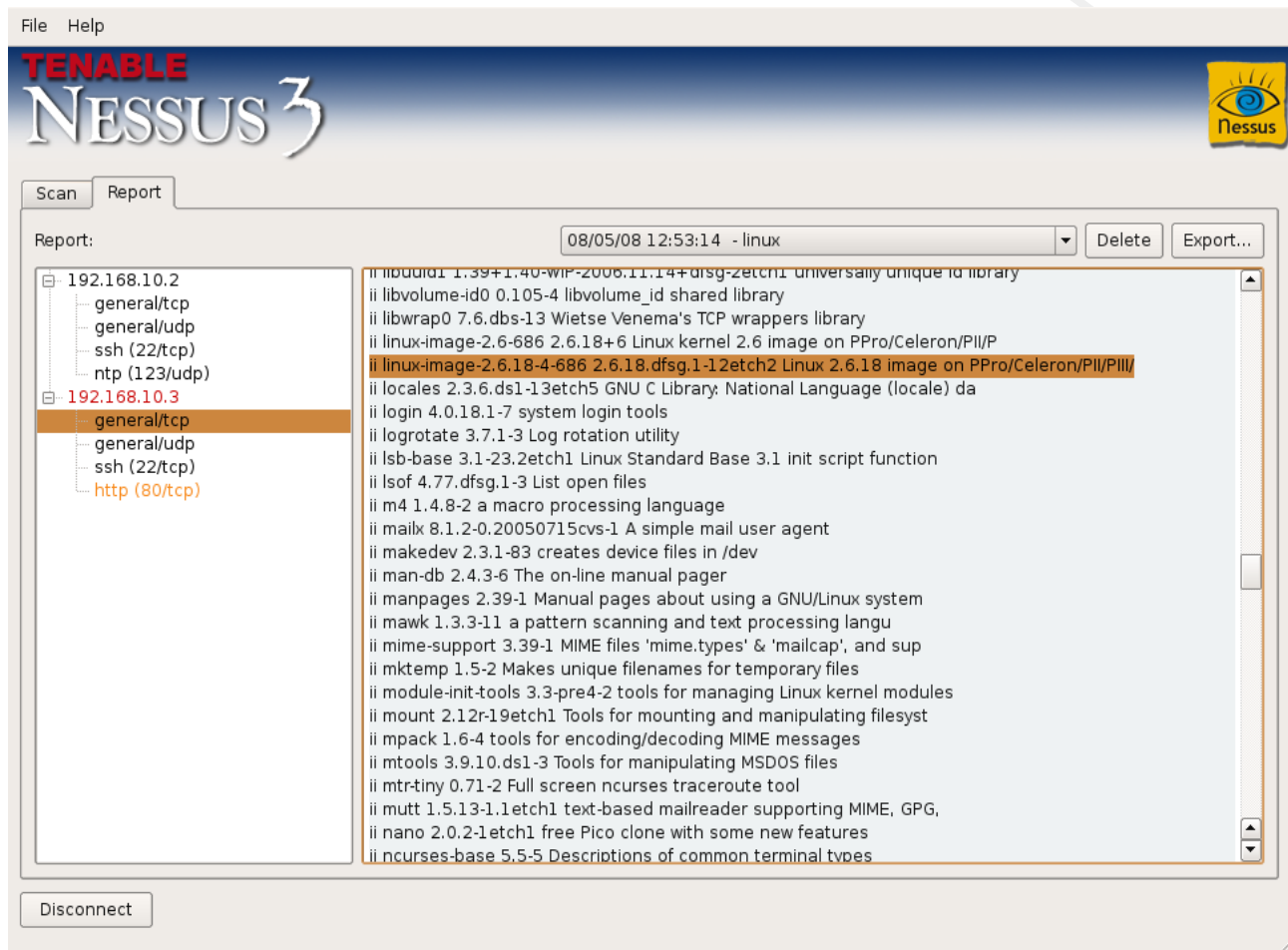
Output 1, OS on LIN-TARGET:



LIN-TARGET(192.168.10.3). The tool NESSUS has logged into the remote host successfully.

Linux image: 2.6.18-4-686, May 9 2007

Output 2, OS on LIN-TARGET:

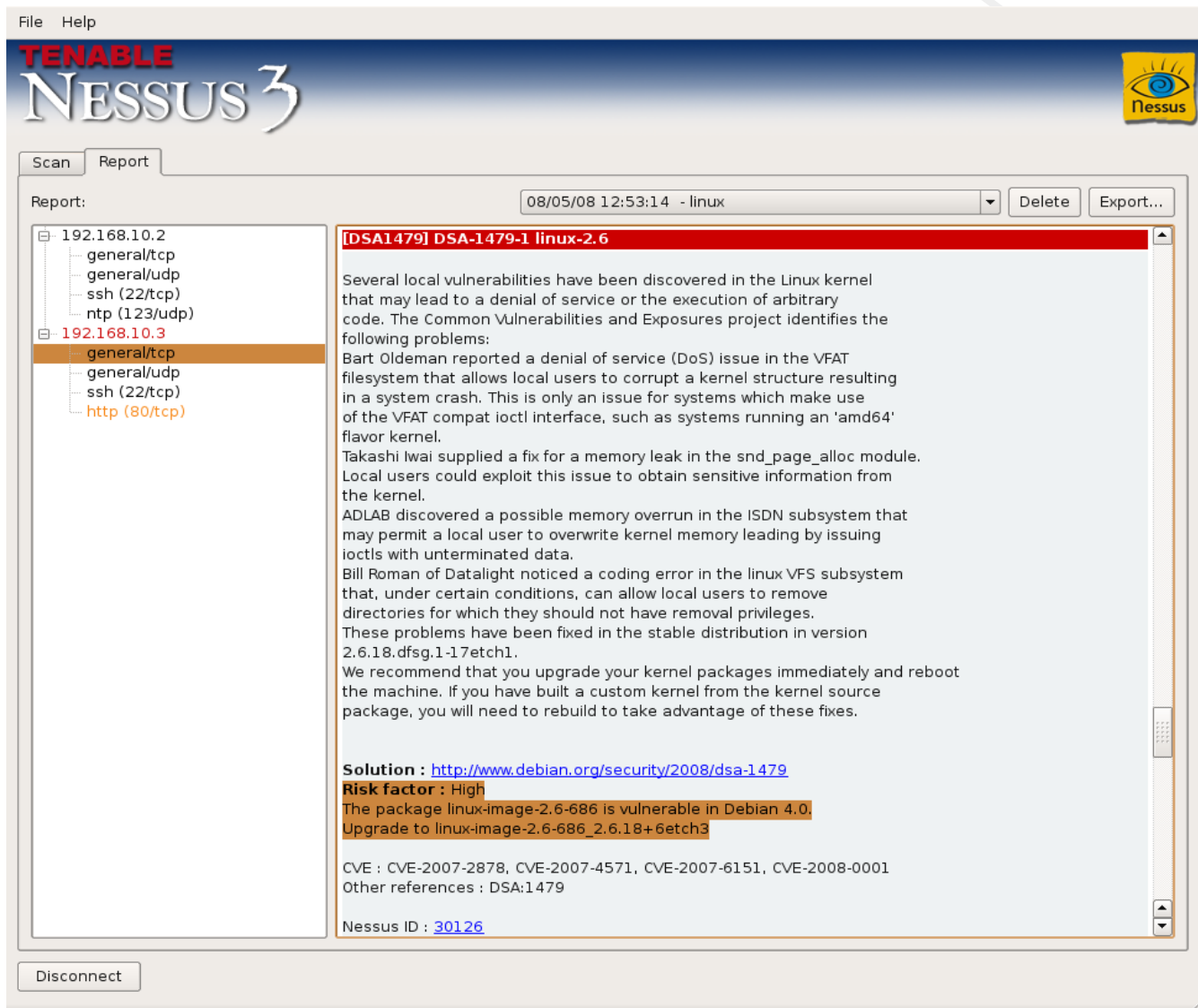


The Software Enumeration output indicates the version of the Linux image installed on the remote system. The previous output indicates that the image is 2.6.18-4-686, May 9 2007.

OS: linux-image-2.6.18-4-686 2.6.18.dfsg.1-12etch2 Linux 2.6.18 image on PPro/Celeron/PII/PIII/P4

Notice that the "/P4" is trunked in the NESSUS output.

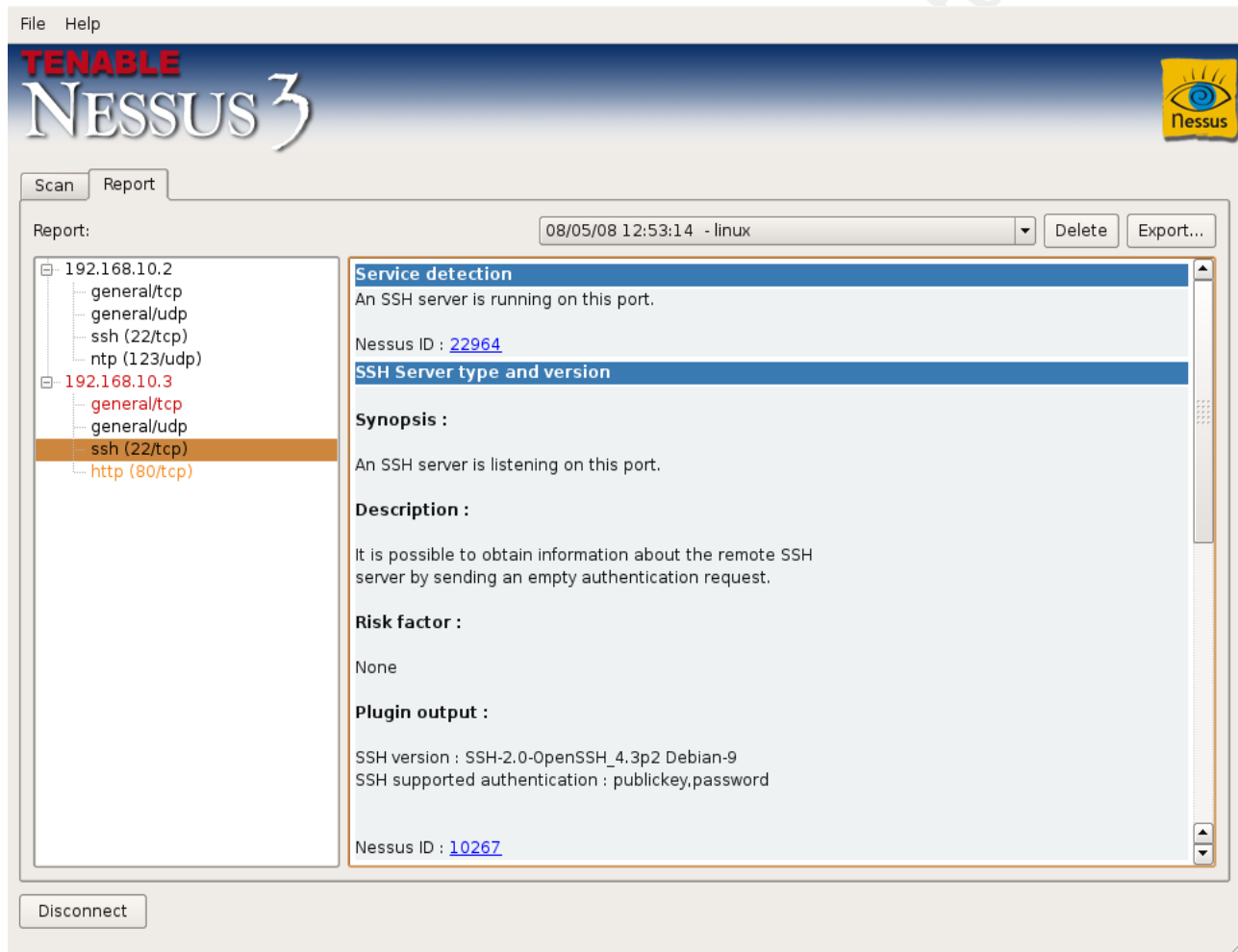
Output 3, OS on LIN-TARGET:



The tool indicates that the Linux image is vulnerable. The NISSUS output recommends an upgrade to the latest version linux-image-2.6-686_2.6.18+6etch3. According to that information, the Operating System on LIN-TARGET is vulnerable.

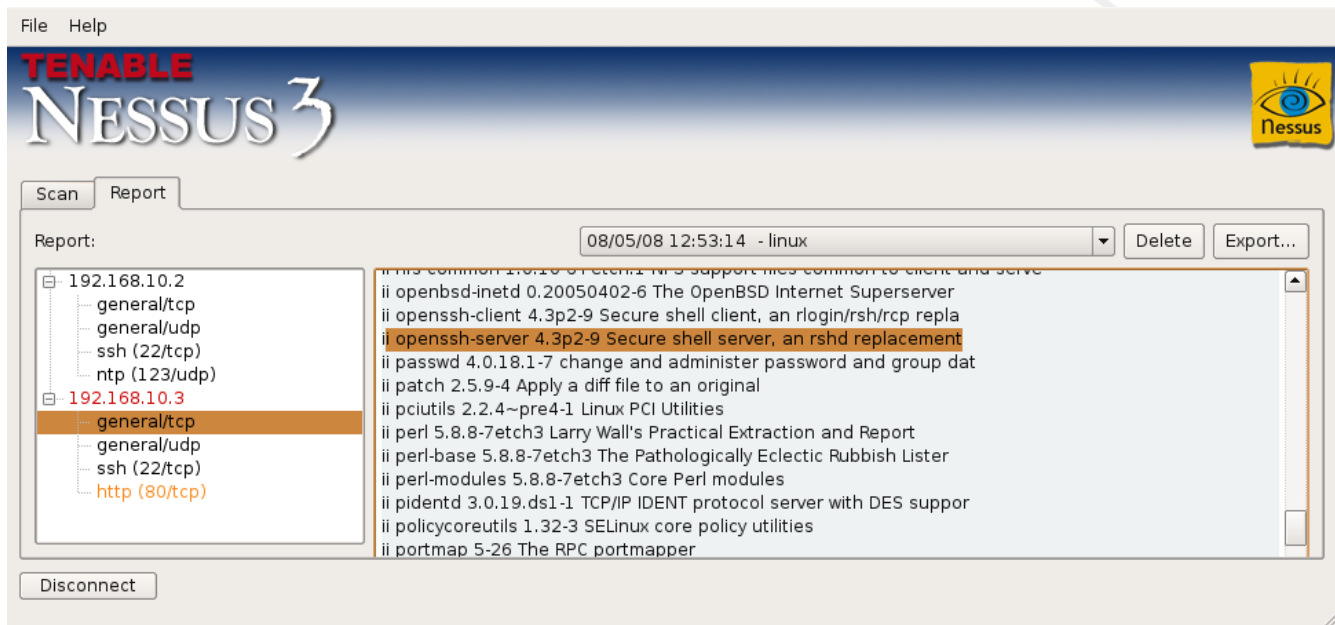
Is the SSH service up to date on LIN-TARGET?

Output 1, SSH on LIN-TARGET:



This output indicates that the service is listening on port 22. Notice that password and public key authentication are permitted.

Output 2, SSH on LIN-TARGET:

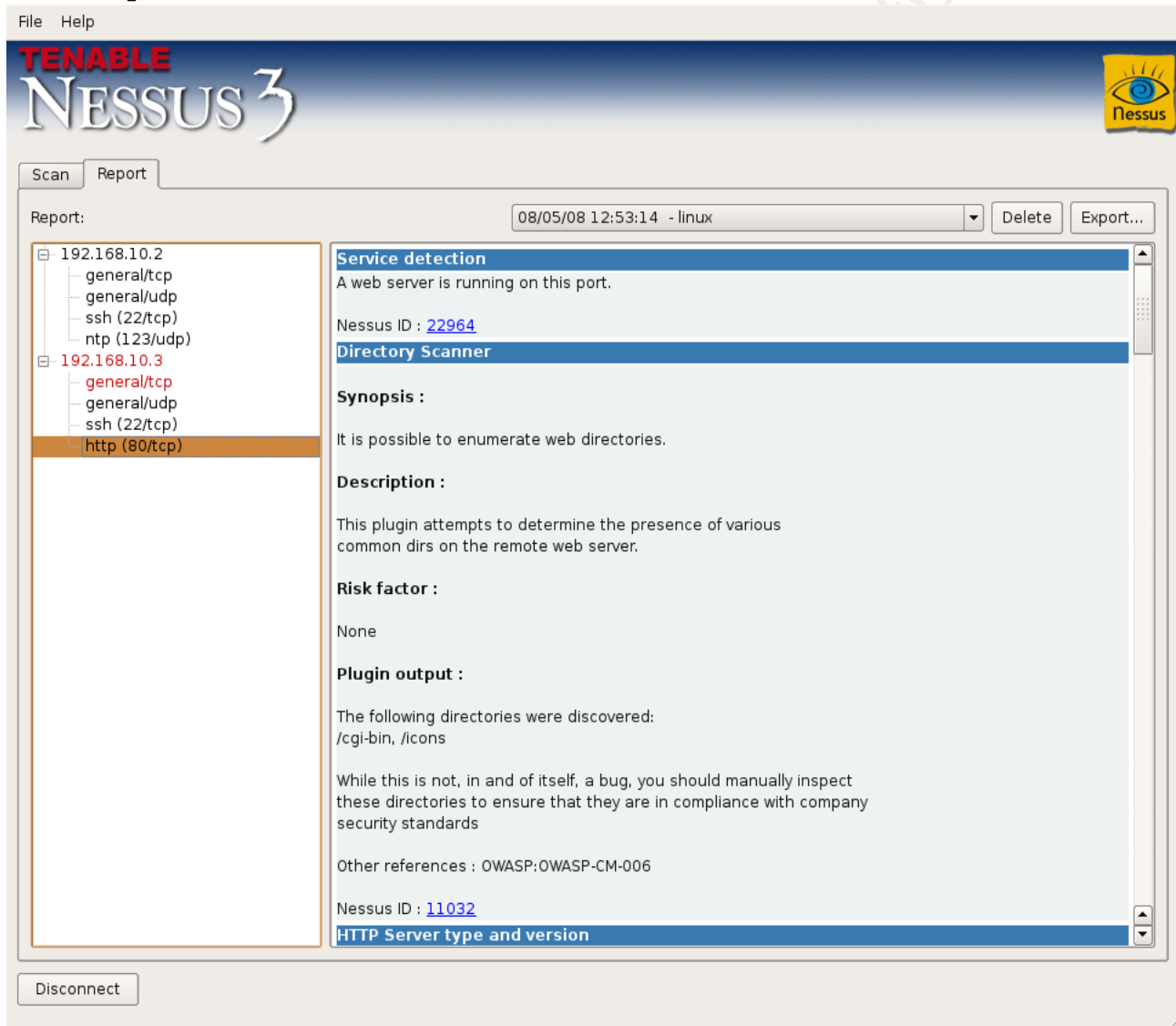


The information concerning the SSH service listening on port 22 has been obtained by the Software Enumeration output. According to the previous output, the service is up to date.

SSH: Version 4.3p2-9.

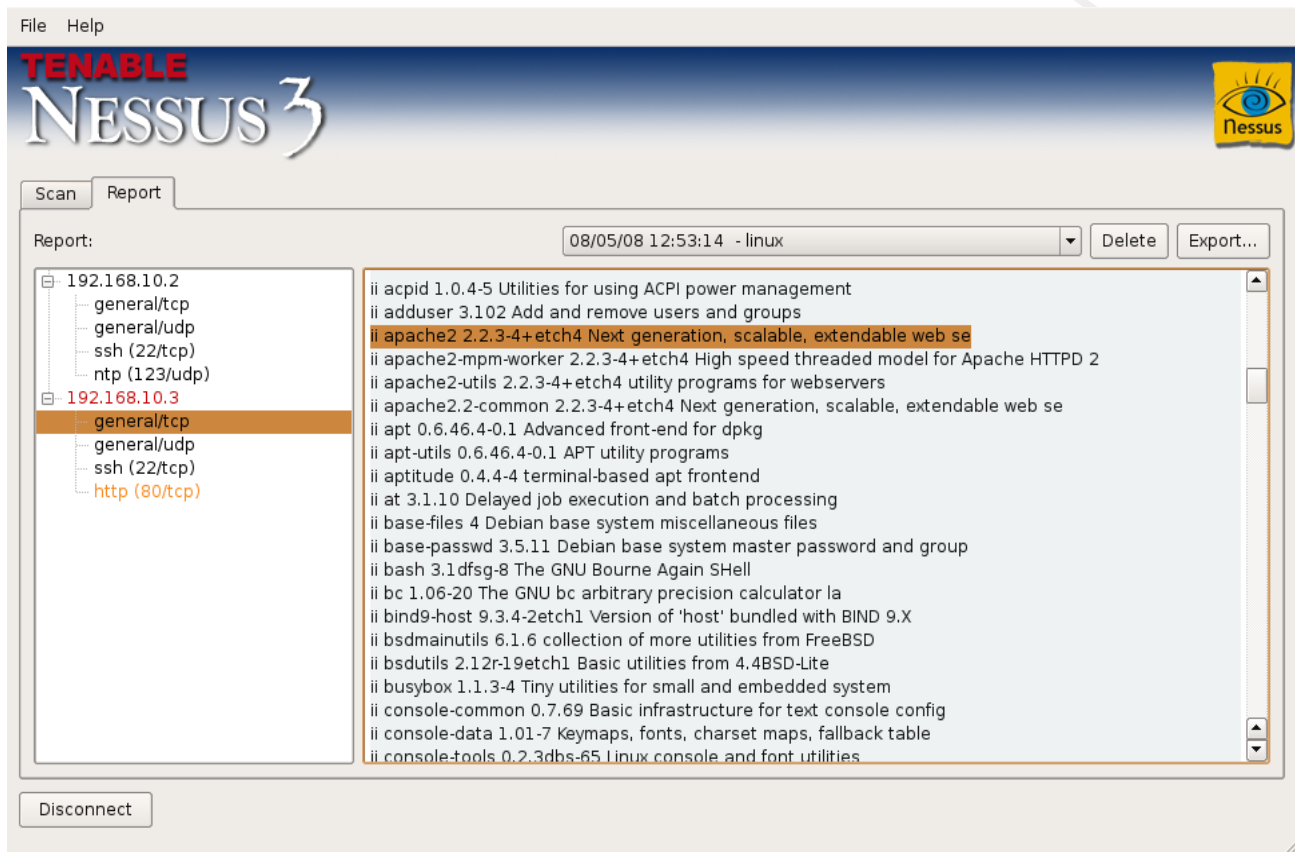
Is the HTTP service up to date on LIN-TARGET?

Output 1, HTTP on LIN-TARGET:



This output indicates that the HTTP service is listening on port 80.

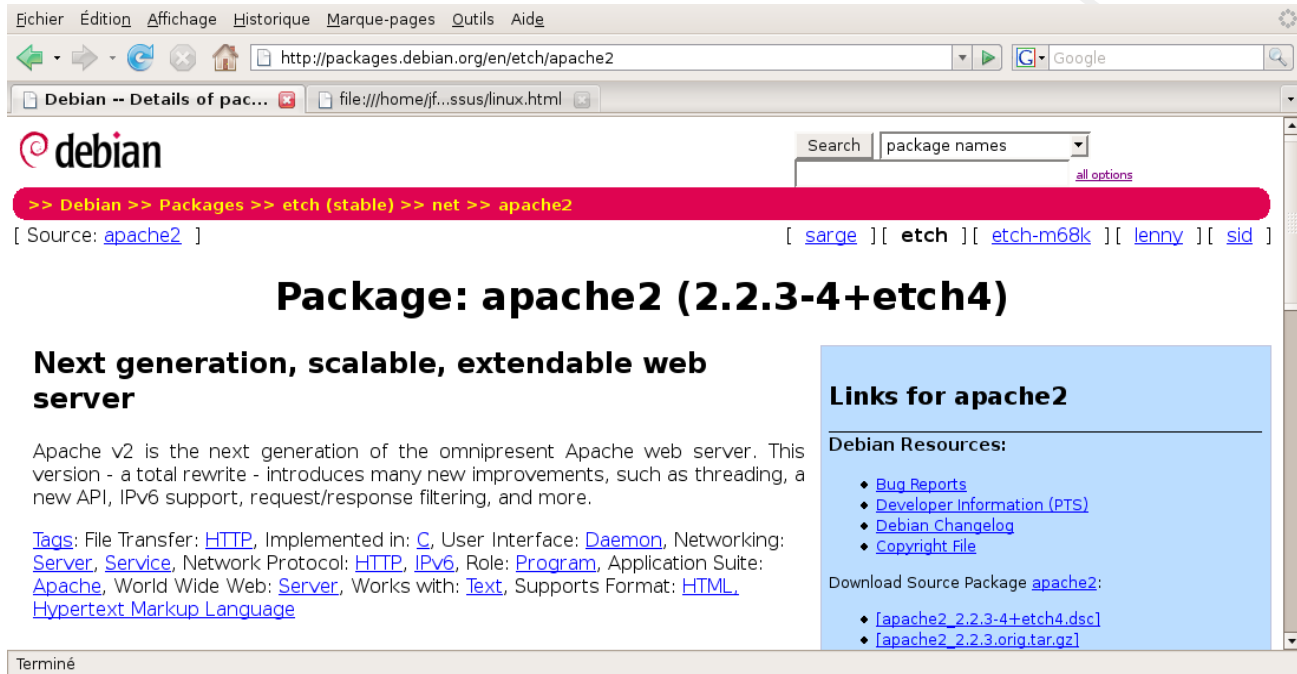
Output 2, HTTP on LIN-TARGET:



The information concerning the HTTP service listening on port 80 has been obtained by the Software Enumeration output.

apache2: Version 2 2.2.3-4+etch4

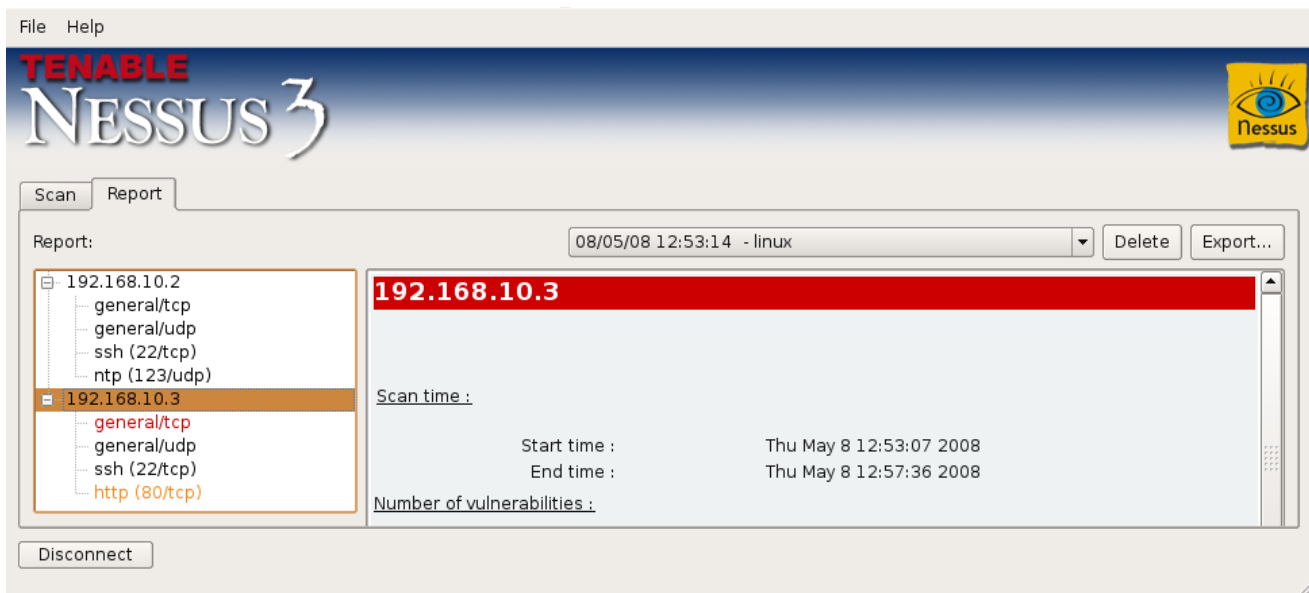
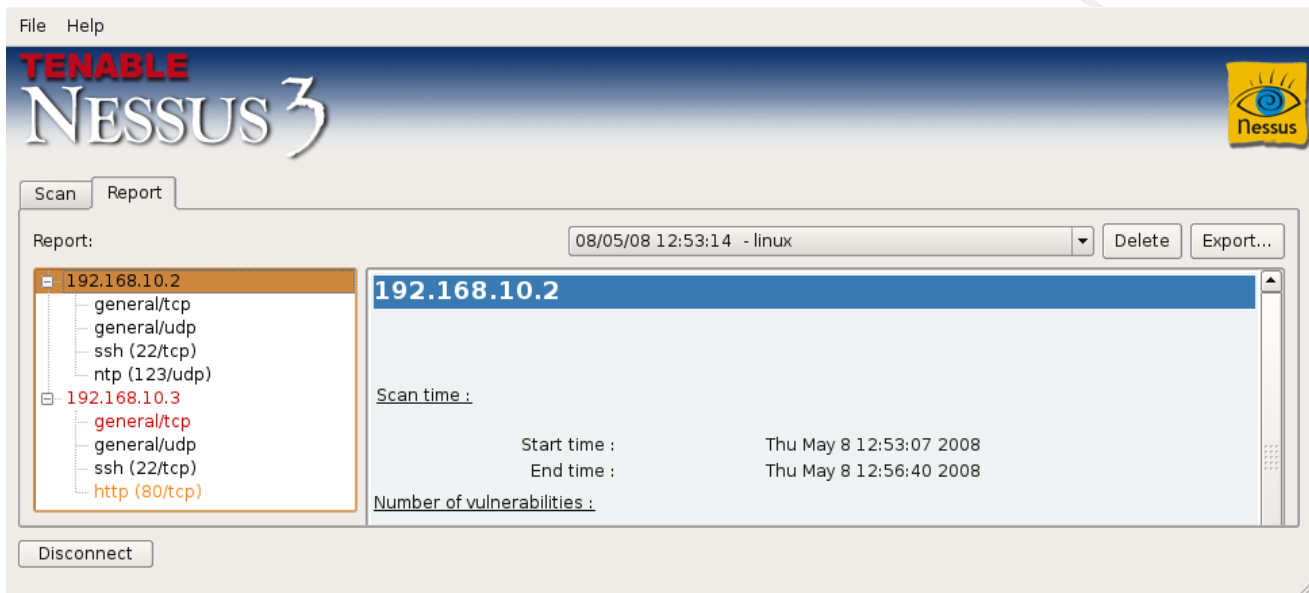
Output 3, HTTP on LIN-TARGET:



If we compare the informations obtained from the previous output with the output at the Debian web site. We can conclude that the HTTP service running on LIN-TARGET is up to date.

Preparing to face new vulnerabilities

Output scan duration Linux:



The scan duration for both addresses was 4 minutes 29 seconds.

Is the INT-SCANNER up to date?

Output INT-SCANNER:

INT-SCANNER(192.168.10.4)

This computer is the scanner that we have access. We can directly open a terminal via SSH to check the actual patch level by running command directly instead of using NISSUS.

```
# uname -a
```

```
Linux INT-SCANNER 2.6.18-6-686 #1 SMP Sun Feb 10 22:11:31 UTC  
2008 i686 GNU/Linux
```

```
# apt-get upgrade
```

```
Reading package lists... Done
```

```
Building dependency tree... Done
```

```
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
# ssh -V
```

```
OpenSSH_4.3p2 Debian-9
```

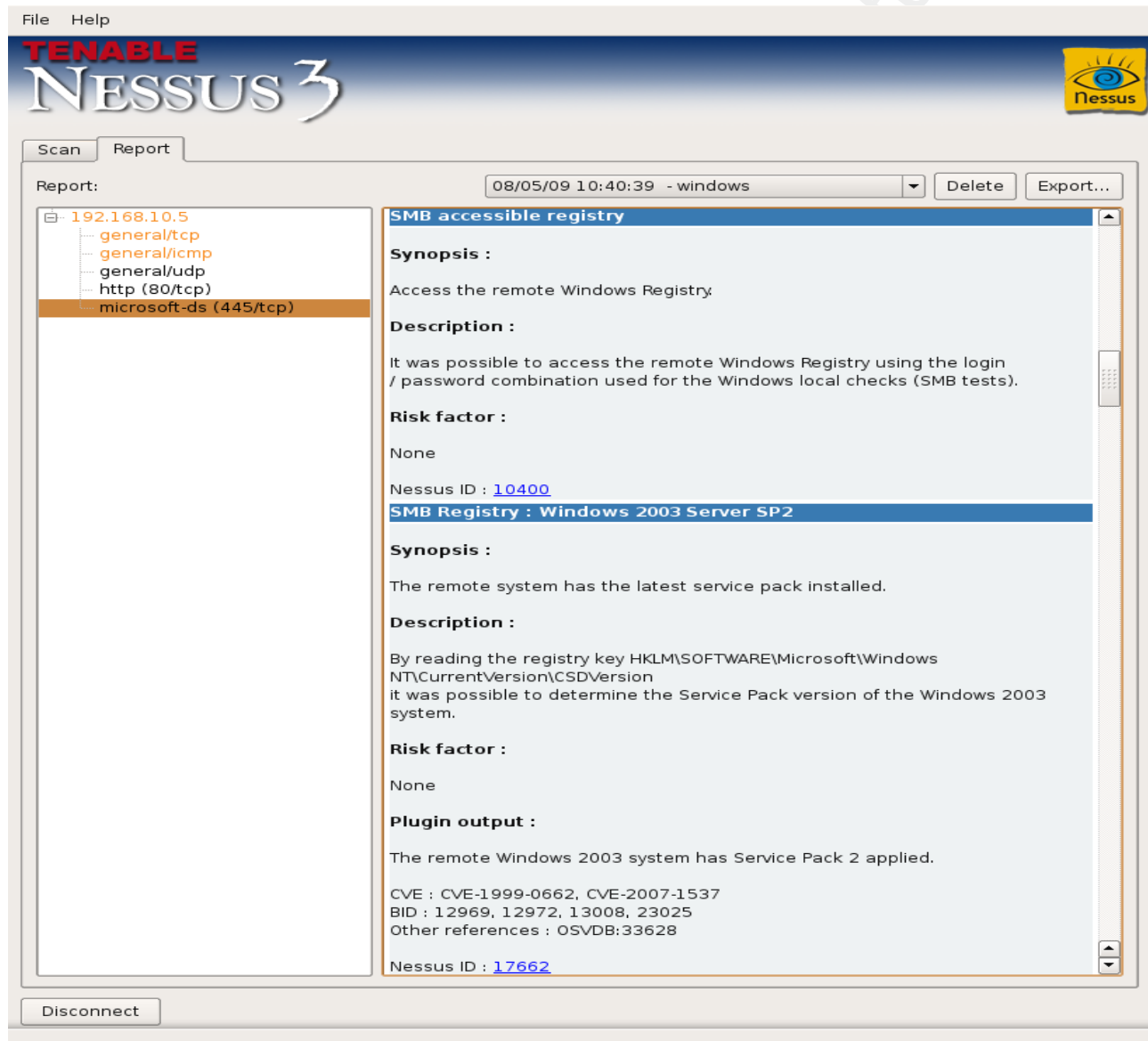
```
# /opt/nessus/sbin/nessusd -v
```

```
nessusd (Nessus) 3.2.0. [build A890] for Linux
```

```
1.1998 - 2008 Tenable Network Security, Inc.
```

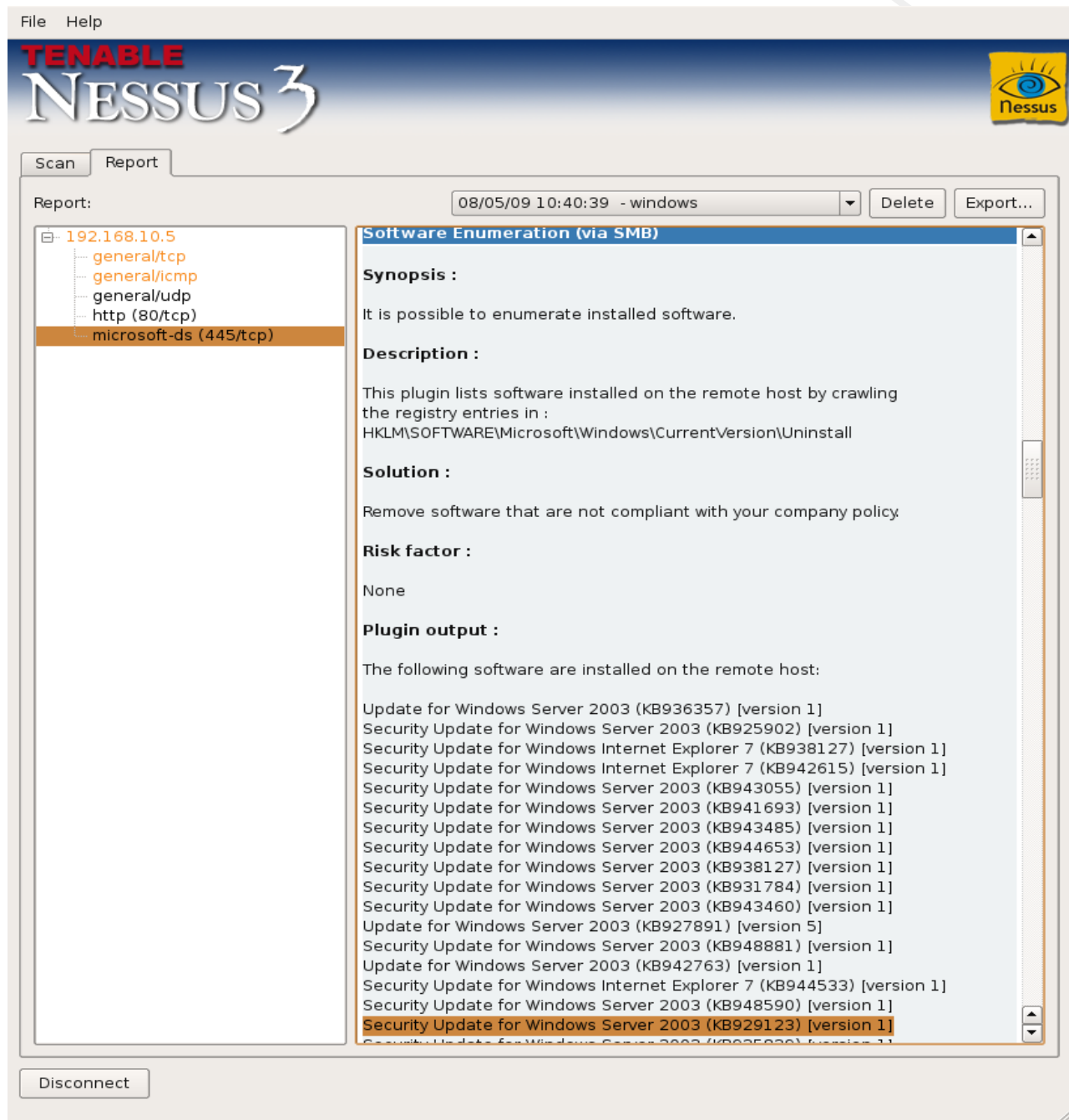
Is the Windows 2003 up to date?

Output 1, Windows 2003:

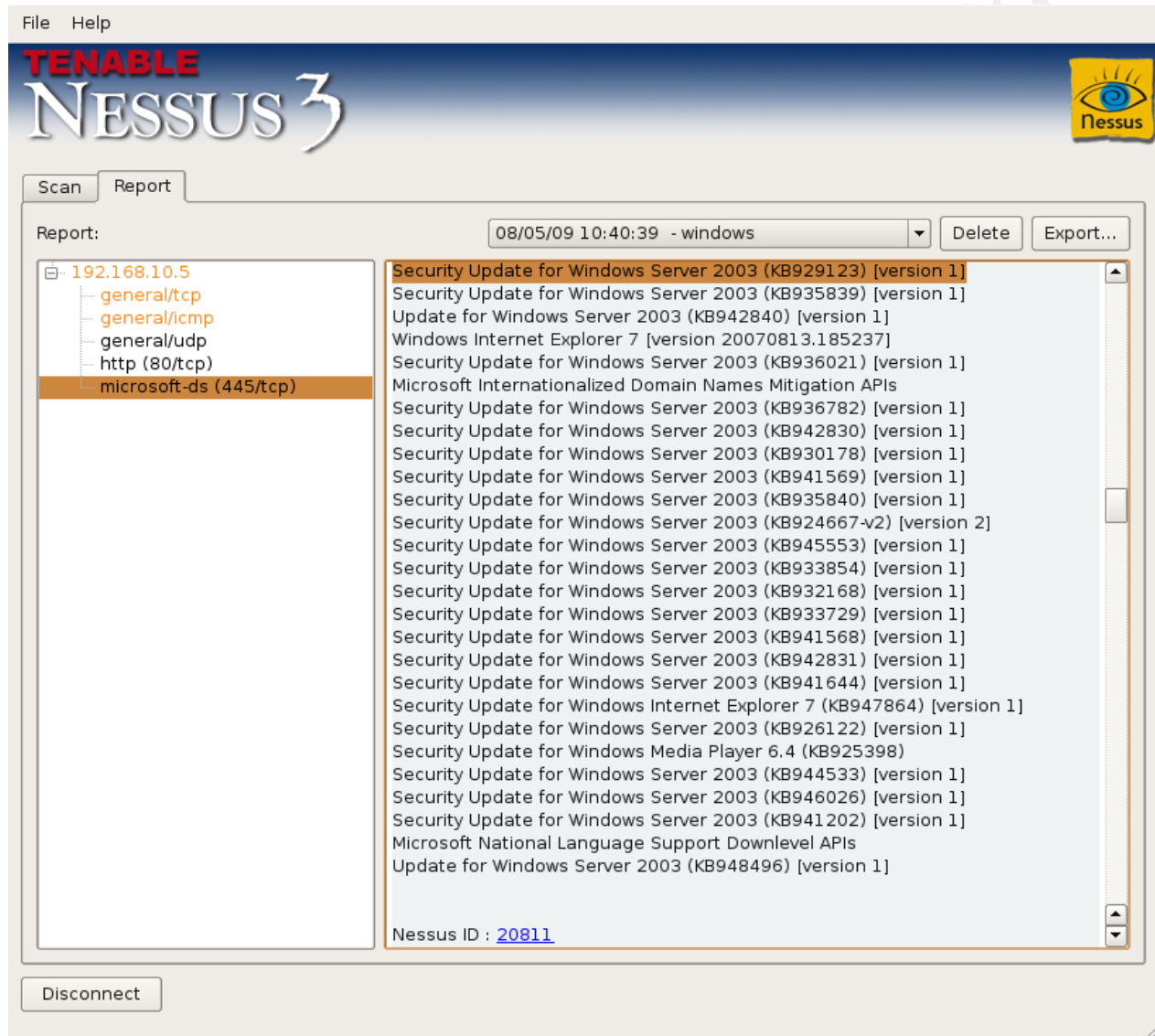


The access to the Windows registry was successful. The latest Service Pack is installed.

Output 2, Windows 2003:

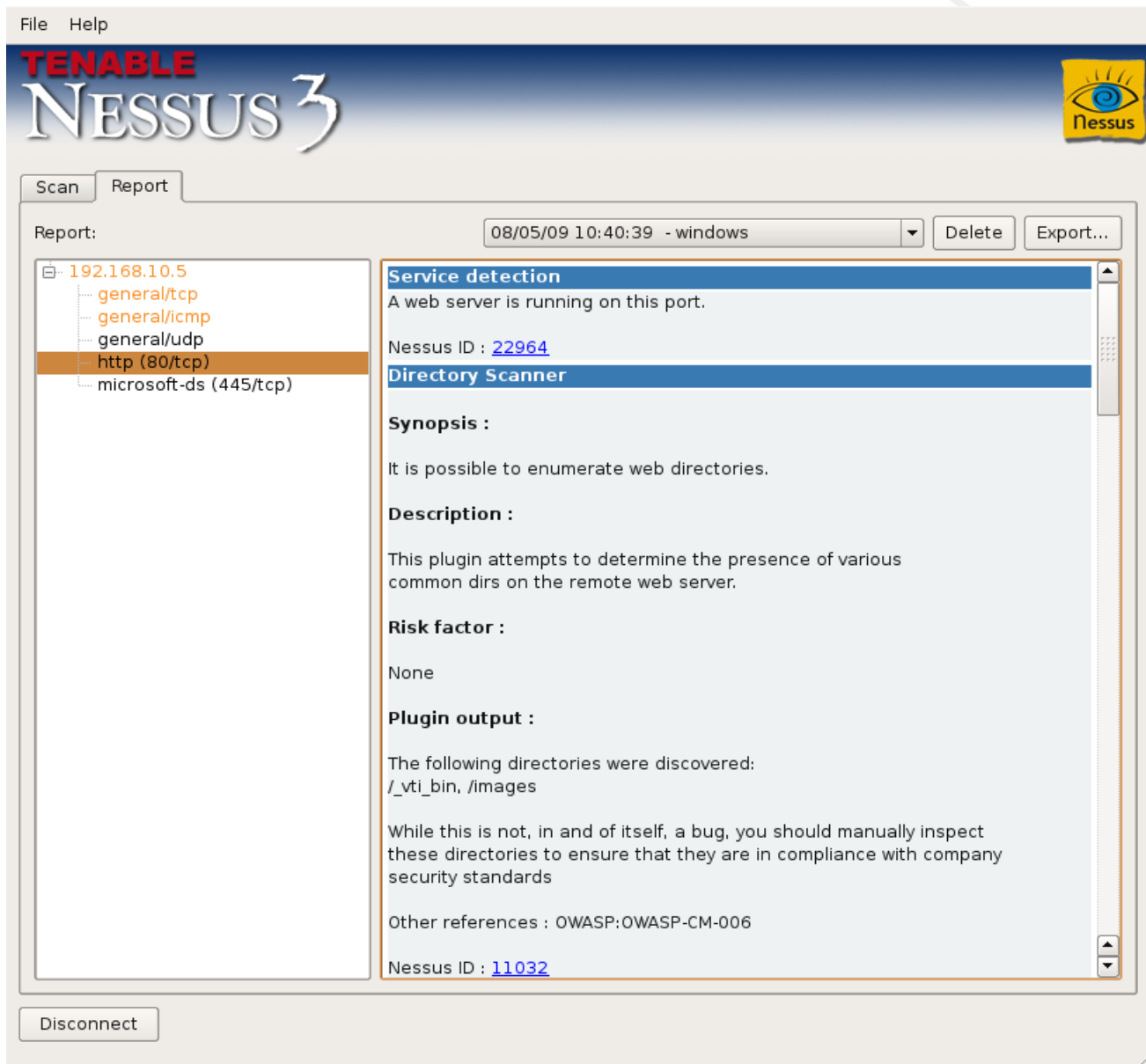


Preparing to face new vulnerabilities



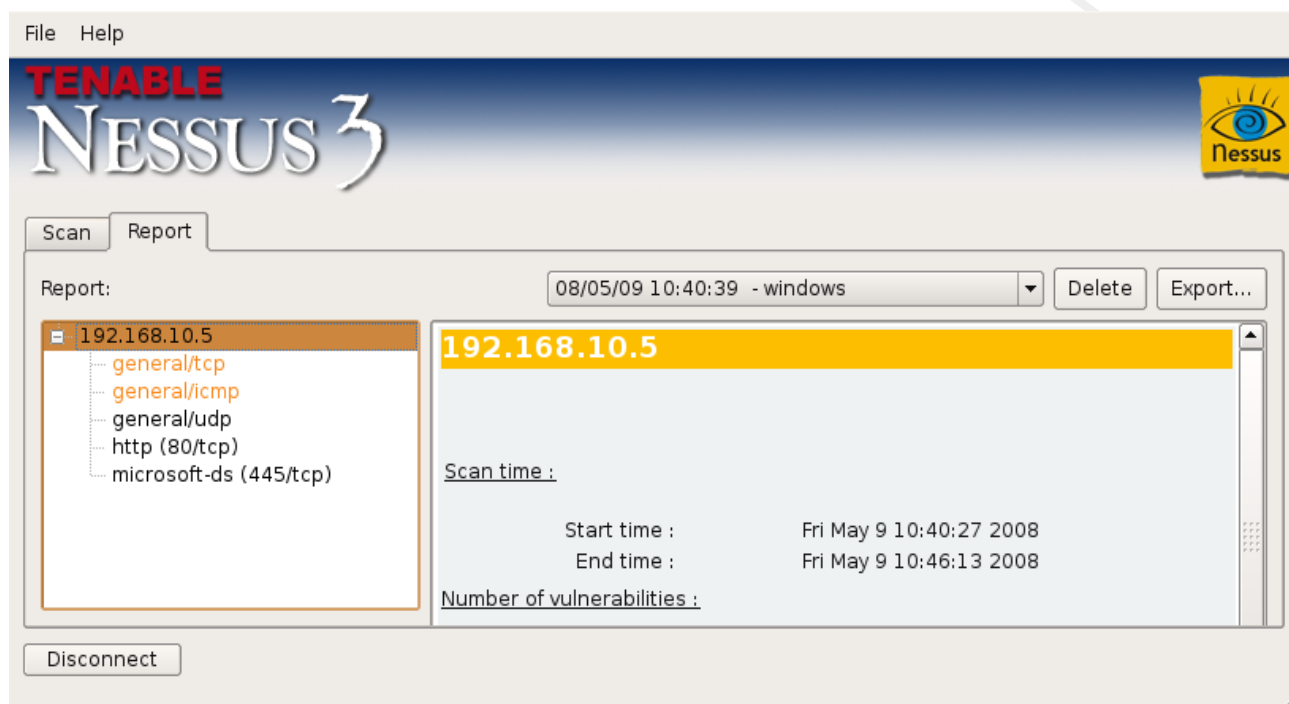
We can see all the patches installed on the server. Note that the information comes from Window's Registry.

Output 3, Windows 2003:



This output indicate that the HTTP service is listening on port 80.

Output 4, Windows 2003:



The scan duration for WIN-TARGET was 5 minutes 46 seconds.

Scan summary

IP	Port	Product/Version	Patched	Internet Access
172.17.10.2 192.168.10.2		OS: Linux 4.0 etch 2.6.18-6-686	Yes	
172.17.10.2 192.168.10.2	22	SSH, 4.3p2-9	Yes	Yes
192.168.10.2	123	NTP, 4.2.2.p4+dfsg-2	Yes	No
192.168.10.3		OS: Linux 4.0 etch 2.6.18-6-686	No	
192.168.10.3	22	SSH, 4.3p2-9	Yes	Yes
192.168.10.3	80	HTTP, apache2-rpm-prefork 2.2.3.4+etch	Yes	Yes
192.168.10.4		OS: Linux 4.0 etch 2.6.18-6-686	Yes	
192.168.10.4	22	SSH, 4.3p2-9	Yes	Yes
192.168.10.4	1243	NESSUS, 3.2.0 [build A890]	Yes	Yes*
192.168.10.5		OS: Windows 2003 Service Pack 2	Yes	
192.168.10.5	80	HTTP, Microsoft IIS 6.0	Yes	Yes
192.168.10.5	445	Microsoft-ds	Yes	No

Yes*: The internal scanner is reachable from outside the private network only for the purpose of this paper. In a production environment, it should be accessible only from the private network.

We have answered the question of the "**Flow chart of management of the crisis *Server only***".

8 UPDATE ON NEW VULNERABILITIES COMMING OUT

We definitely have to be informed before the executive management. We need to be informed as soon as the vulnerabilities are published.

There are many possibilities: You can subscribe to certain site to get them by e-mail. You can visit the web site of the purveyor of product manually on a daily basic. You can also use the RSS feed from various sources on the Internet to speed things up.

You can also visit site like:

<http://www.securityfocus.com/archive>

<http://isc.sans.org/>

<http://isc.sans.org/links.html>

<http://www.us-cert.gov/>

<http://www.microsoft.com/technet/security/current.aspx>

<http://www.us-cert.gov/>

9 CONCLUSION

The security group would definitely ameliorate their respond to vulnerabilities. They now have the possibility to get the exact informations when it is needed. They don't rely on servers administrators to get it.

Other tools can be added and deeper tests can be performed. It

Preparing to face new vulnerabilities depends on the amount of time you are willing to invest. Furthermore, besides gathering information for security purpose, the external scanner can be a great help for troubleshooting or testing new firewall rules. With this tools, you can do a lot of things, as long the process is under control and approved by management.

10 REFERENCES

<http://www.nessus.org/documentation/>

http://www.nessus.org/documentation/nessus_credential_check.pdf

http://www.nessus.org/products/pvs/index.php?view=blended_assessment

http://www.sans.org/reading_room/whitepapers/linux/

<http://packages.debian.org>