
# Information Assurance & Auditing – IE4040

MID-TERM ASSIGNMENT

Year 4, Semester 1, 2020

**Thaha M.S.M.S - IT 17 1310 70**

Bachelor of Science Special (Honors) Degree in Computer Systems & Network Engineering

Department of Information Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka.

May 2020.

# *Windows Server 2008 R2 Audit Report*

# DECLARATION

I declare that this is my own work and this report does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

*Shiraz Safwan.*

# Table of Contents

# List of Figures

# 1. INTRODUCTION

Today each and every organizations, be it large or small, depends on information technology for some or most of its functions; comes with information security [1]. The majority of small and medium sized organizations and even large companies do not identify the problem of IT security and thus mostly ignore it. These problems lead to a lack of security and eventually costs more in the form of data loss and the handling cases. Within the field of information security, it is often easier to follow a proactive approach than a reactive one.

Windows operating systems are among the world's most used and exploited OS [2]. The ease of deployment and use has made them common not only among ordinary people but also a soft target for the attackers.

In this report I am going to discuss the windows server 2008 R2 vulnerability assessment [3] utilizing OpenVAS tool and so that the right people define the vulnerabilities using this tool and at the right time to prevent security breaches. This tool was deliberately chosen so that someone with basic technical knowledge could use them, so that even a small or large business, system or network administrator could use them to generate report and results and take necessary actions.

This vulnerability assessment is a part of computer audit. This may be undertaken to check the status and of the computer and turn up with any violations and vulnerabilities. The most basic part of computer audit is asset management inventory in an organization. Another aspect of computer audit is a security review, knowing and checking the computer to make sure they are safe not.

## 2. BENEFITS OF AUDIT [4]

- **Security**- Scan the OS and find the vulnerabilities and at the right time can take necessary actions.
- **Cost** - Audit helps in the budgeting and repair of equipment on schedule. It greatly decreases the guesswork in designing the correct capital expenditure budget.
- **Time** – Using OpenVAS tool is reducing time to audit.
- **Avoid and reduce risk** - Such as theft, fire and security attacks.
- **Integrity -** The audit will help the organization create a more efficient running system.
- **Mitigate threats -** The way an organization manages data will always pose risks. So, with an audit, it would ensure businesses operate at the lowest possible risk. In addition, high-risk areas will be defined, which will enable businesses to establish a strategy to resolve or fix certain risks and minimize potential threats.

# 3. HOW TO PERFORM AUDIT USING OPENVAS TOOL

## 3.1 Open Vulnerability Assessment Tool

The Open Vulnerability Assessment System (OpenVAS) is an open source platform of a series of tools and services [5]. These tools and services work together to scan multiple computers, identify known vulnerabilities on these computers, and provide a collection of resources to monitor and manage identified vulnerabilities mitigation. Many vulnerability assessors, auditors, penetration testers, and hackers utilize OpenVAS to look for security vulnerabilities. The OpenVAS framework is free to use and has the functionality of paid or commercial editions or commercial alternatives that exist out there like Nessus, is frequently updated to identify the latest vulnerabilities. We can use OpenVAS to scan many computers, including those running Microsoft and non-Microsoft operating systems. It's similar to Nessus but completely free. The framework is very good at identifying the underlying operating system for any target and then tailoring the scans for that operating system.

OpenVAS is intended to be an all-in-one vulnerability scanner with a variety of built-in tests and a Web interface designed to quickly and easily set up and run vulnerability scans while providing a high user configurability level.

## 3.2 OpenVAS installation [6]

### Step-01 (Setup the virtual machines in virtual box)

Here I used OpenVAS for scan the windows server 2008 R2 machine and to do the vulnerability assessment. I have two virtual machines running on virtual box in same network. One is kali Linux and other one is windows server 2008 R2. OpenVAS is the system running on kali Linux. Windows server 2008 R2 is fresh installed.

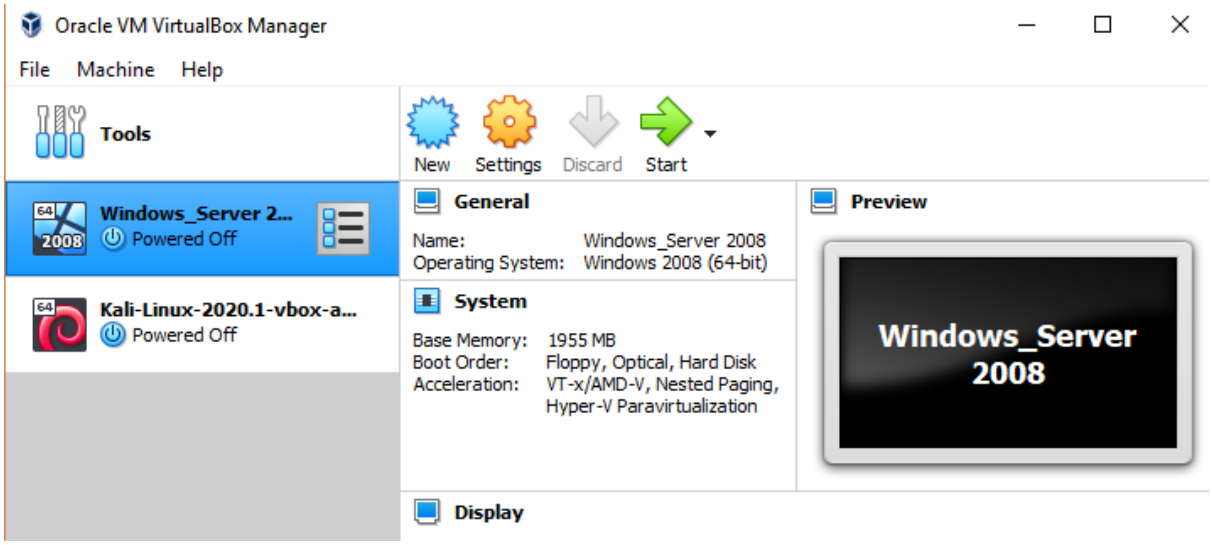


*Figure 3.2.1:2 Virtual machines*

### Step-02 (Install the OpenVAS in kali Linux)

The installation process is easy to do. First need to update the system. its dependencies on our Kali Linux system we simply have to run the following command.

```
root@kali:~# sudo apt-get update -y
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Packages [16.5 MB]
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:4 http://kali.cs.nctu.edu.tw/kali kali-rolling/contrib amd64 Packages [97.6 kB]
Fetched 16.8 MB in 50s (334 kB/s)
```

*Figure 3.2.2: Update the kali Linux*

After the reboot has completed. Need to open the terminal and install the OpenVAS package using following command.

```
root@kali:~# sudo apt-get install openvas -y
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
  cryptsetup cryptsetup-initramfs doc-base dvisvgm fonts-droid-fallback fonts-lmodern fonts-noto-mono fonts-texgyre
  fonts-urw-base35 gcc-10-base gnutls-bin greenbone-security-assistant greenbone-security-assistant-common libapache-pom-java
  libcommons-logging-java libcommons-parent-java libfontbox-java libgcc-s1 libgnutls-dane0 libgnutls30 libgs9 libgs9-common
  libhiredis0.14 libijs-0.35 libjbig2dec0 libjemalloc2 libkpathsea6 liblua5.1-0 liblzf1 libopenvas9 libpdfbox-java libptexenc1
  libradcli4 libsynctex2 libteckit0 libtexlua53 libtexluajit2 libunbound8 libuuid-perl libyaml-tiny-perl libzzip-0-13 lmodern
  lua-bitop lua-cjson openvas-cli openvas-manager openvas-manager-common openvas-scanner preview-latex-style redis-server
  redis-tools t1utils tcl tex-common tex-gyre texlive-base texlive-binaries texlive-fonts-recommended texlive-latex-base
  texlive-latex-extra texlive-latex-recommended texlive-pictures texlive-plain-generic tipa tk tk8.6
Suggested packages:
```

*Figure 3.2.3: Installing the OpenVAS package*

After the installation is finished, need to run OpenVAS-setup using following command. This will take a lot of time because it will download a lot of CVE, sync NVT's, vulnerabilities etc. at this stage. Also, this method creates an HTTPS login certificate to OpenVAS gui.

```
root@kali:~# sudo openvas-setup

[>] Updating OpenVAS feeds
[*] [1/3] Updating: NVT
--2020-05-07 19:35:00--  http://dl.greenbone.net/community-nvt-feed-current.tar.bz2
Resolving dl.greenbone.net (dl.greenbone.net) ... 2a01:130:2000:127::d1, 89.146.224.58
Connecting to dl.greenbone.net (dl.greenbone.net)|2a01:130:2000:127::d1|:80 ...
```

*Figure 3.2.4: OpenVAS setup*

Using the following command and configure the OpenVAS databases.

```
root@kali:~# sudo openvas-check-setup
openvas-check-setup 2.3.7
  Test completeness and readiness of OpenVAS-9
  (add '--v6' or '--v7' or '--v8'
   if you want to check for another OpenVAS version)

  Please report us any non-detected problems and
  help us to improve this check routine:
  http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
```

```
root@kali:~# sudo greenbone-scapdata-sync
```

```
root@kali:~# sudo greenbone-certdata-sync
```

*Figure 3.2.5: Configuring the OpenVAS database*

Finally, start the OpenVAS services using following command.

```
root@kali:~# sudo openvas-start
[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

*Figure 3.2.6: Start the OpenVAS service 1*

Now open the browser and type https://127.0.0.1:9392, accept the self-signed SSL certificate and plugin the credentials for the admin user. The admin password was generated during the setup phase. Login the OpenVAS GUI using the username and password.

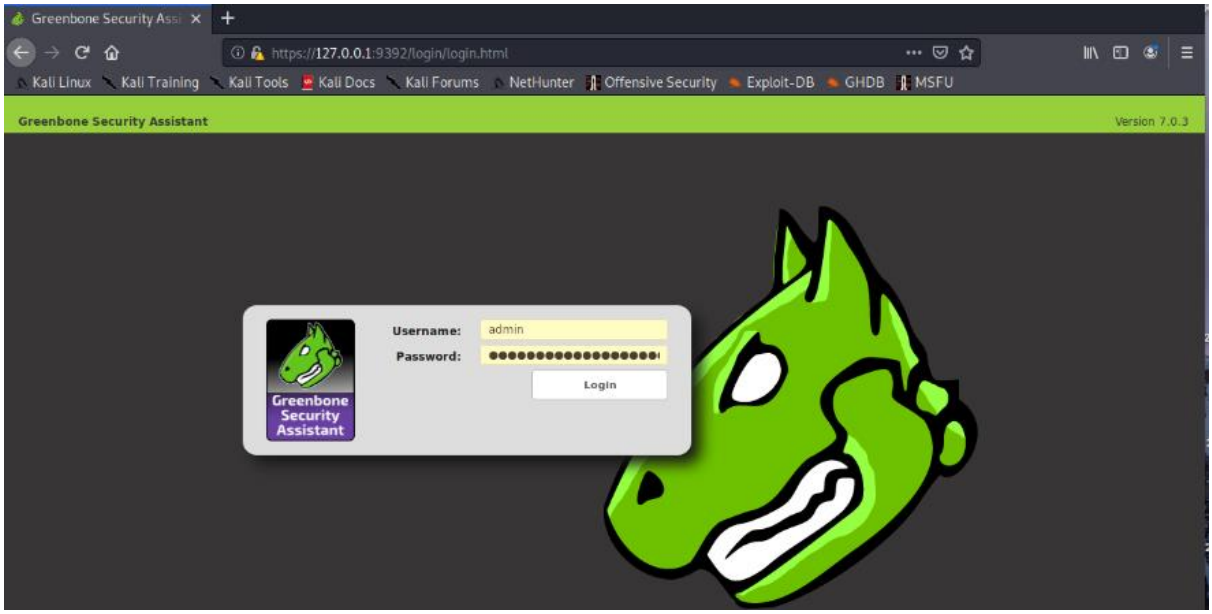


*Figure 3.2.7: OpenVAS Login page*

After the login. It shows the dashboard of the OpenVAS. It is user friendly web interface.

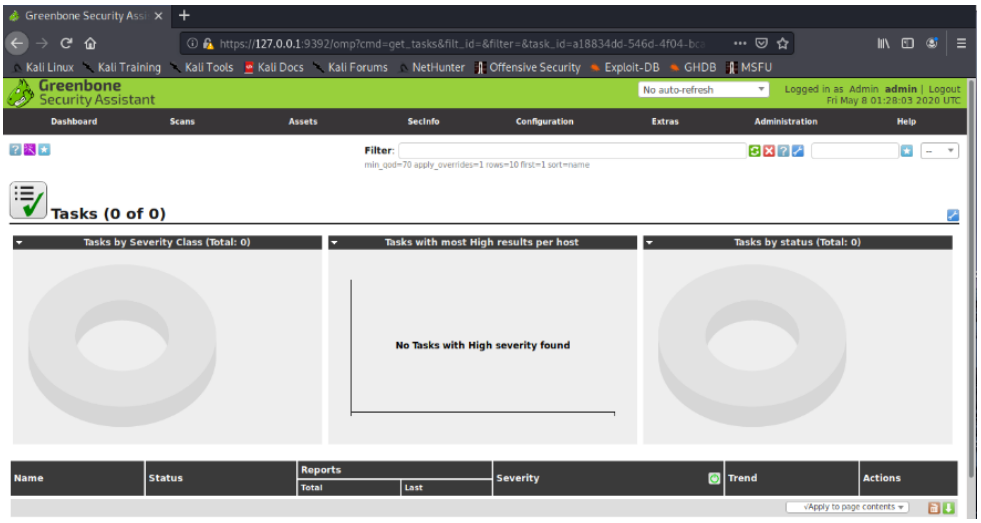


*Figure 3.2.8: OpenVAS dashboard*

## 3.3 Scan the target machine [7]

**Step-03 (check the communication between 2 virtual machines)**

OpenVAS is not able ping it so didn't find anything because windows server 2008 R2 system, the firewall is enabled. Let's disable the firewall and check the communication.

```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.8.107  netmask 255.255.255.0  broadcast 192.168.8.255
        inet6 fe80::a00:27ff:fefc:1760  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:fc:17:60  txqueuelen 1000  (Ethernet)
        RX packets 124  bytes 12932 (12.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74  bytes 10119 (9.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

*Figure 3.3.1: Kali Linux IP address*

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1c46:a486:47c7:4f27%11
   IPv4 Address. . . . . . . . . . . : 192.168.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{529EBD7D-6CCC-4C76-B323-4C798036325F}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>
```

*Figure 3.3.2: Windows Server 2008 R2 IP address*

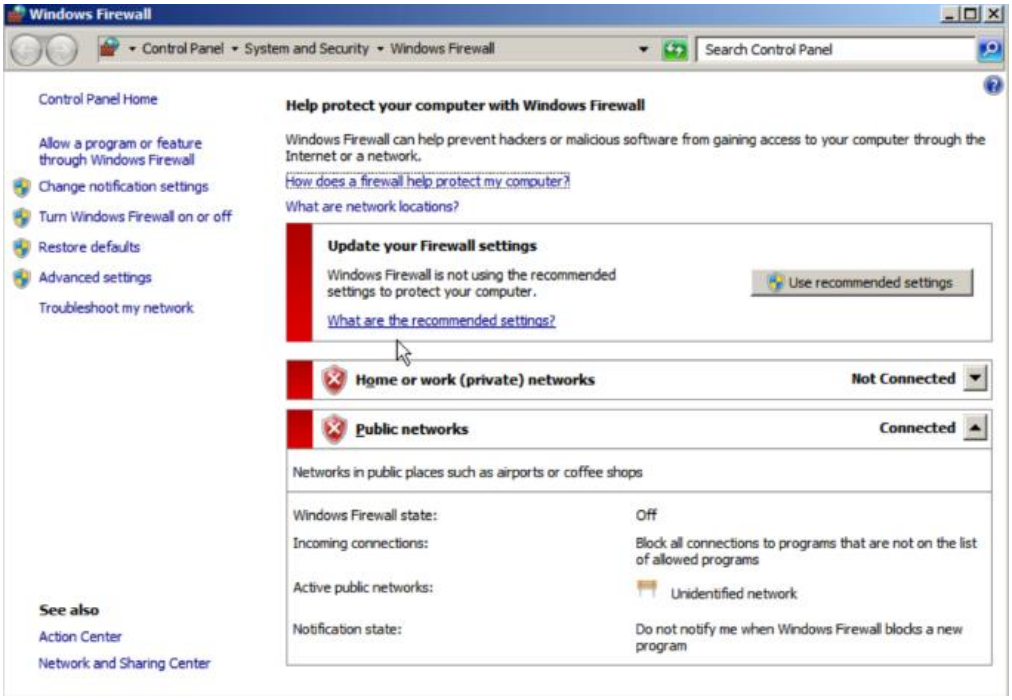


*Figure 3.3.3: Disable the firewall*

**Step-04 (scan on the target machine)**

When logging into the web GUI and by clicking the task wizard to scan a system using the wizard directly it is enough to enter the IP address of the target machine and click start scan button to start the scan. We can edit the task as well. Here my target machine IP is 192.168.10.2 and task name is Windows_Server_R2 Scan.

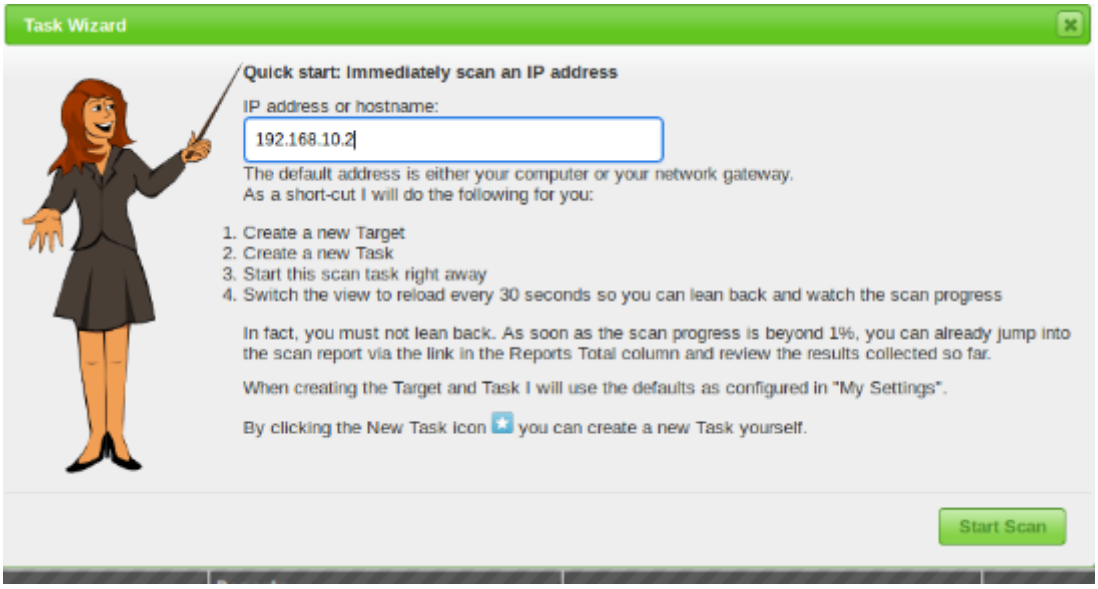


*Figure 3.3.4: Target machine IP & Task wizard*

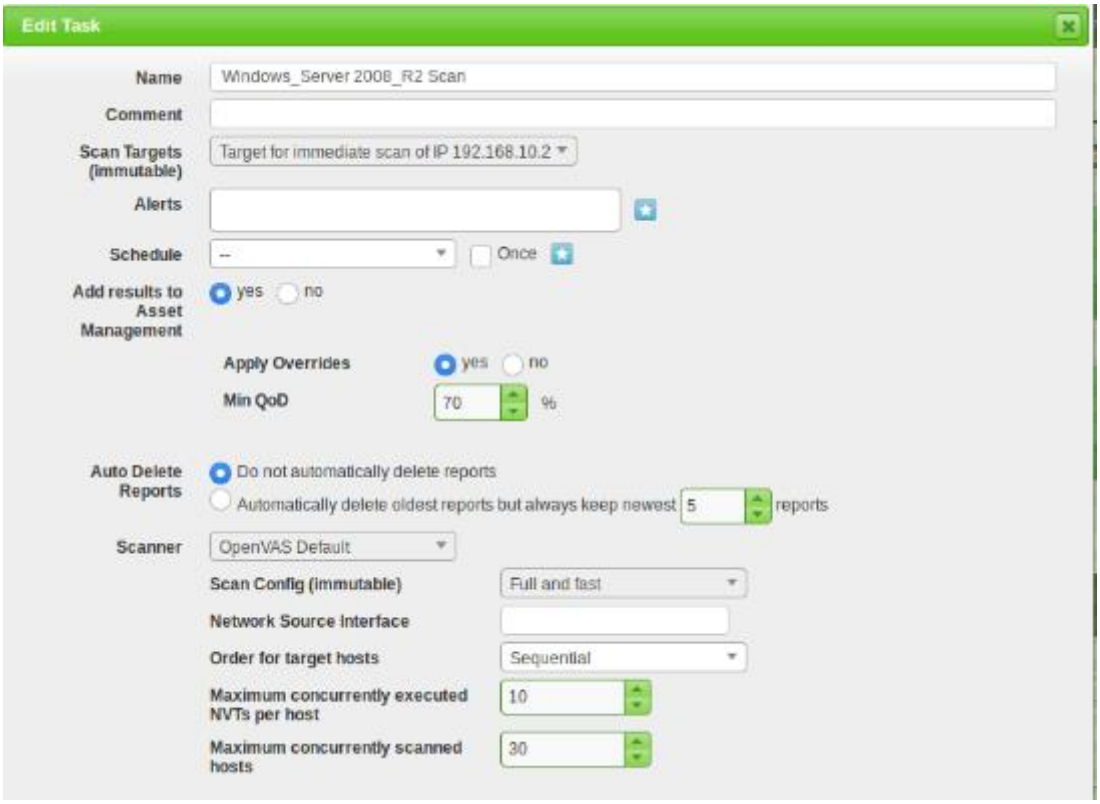


*Figure 3.3.5: Edit the Scan Name*

After the task is started the progress can be monitored. The Green bone Security Assistant displays the overview page. The scan be taking several minutes to complete and wait for this to complete 100%. Colors and the status bar fill level inform about the scan status.

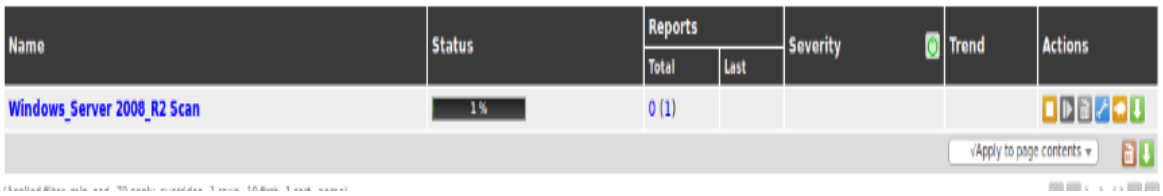


*Figure 3.3.6: Scan progress*


*Figure 3.3.7: Status bar of the progress*

**Step-05 (Review the vulnerabilities and solutions)**

When the scan is completed, the scan navigation > results notify the all vulnerability detections and the scan navigation > report notify the high-risk detections. The Severity column notifies about the criticality of the vulnerabilities detected. The prior column shows the severity, topology, status and NVTs etc.

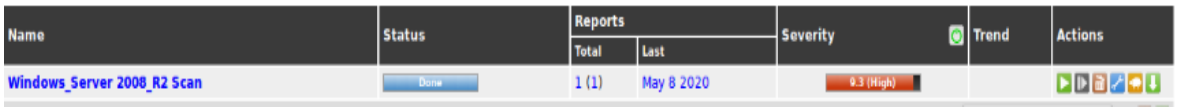


*Figure 3.3.8: Scan complete*

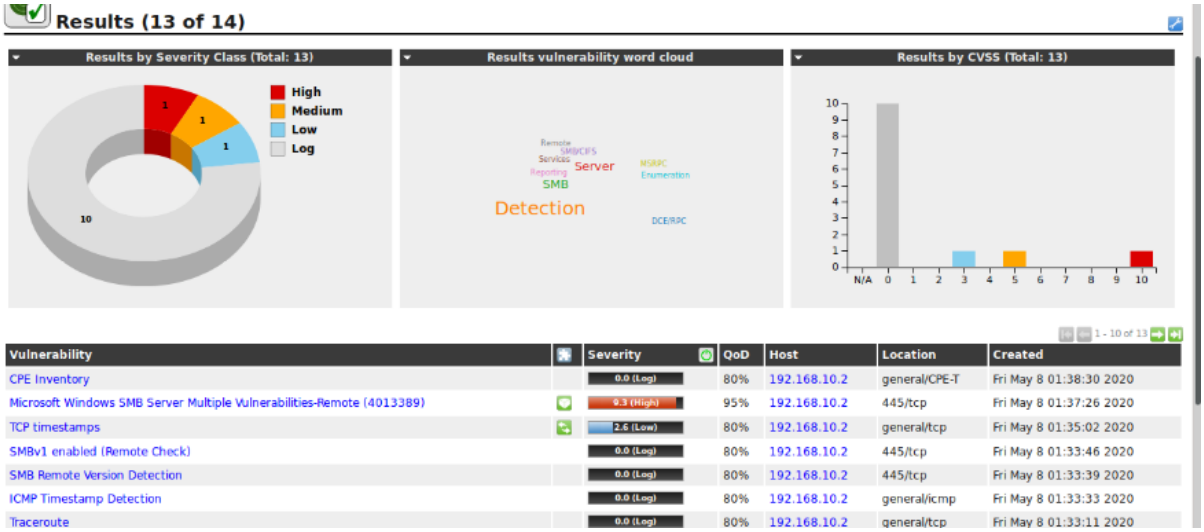


*Figure 3.3.9: Vulnerabilities*


*Figure 3.3.10: 3 High risks*

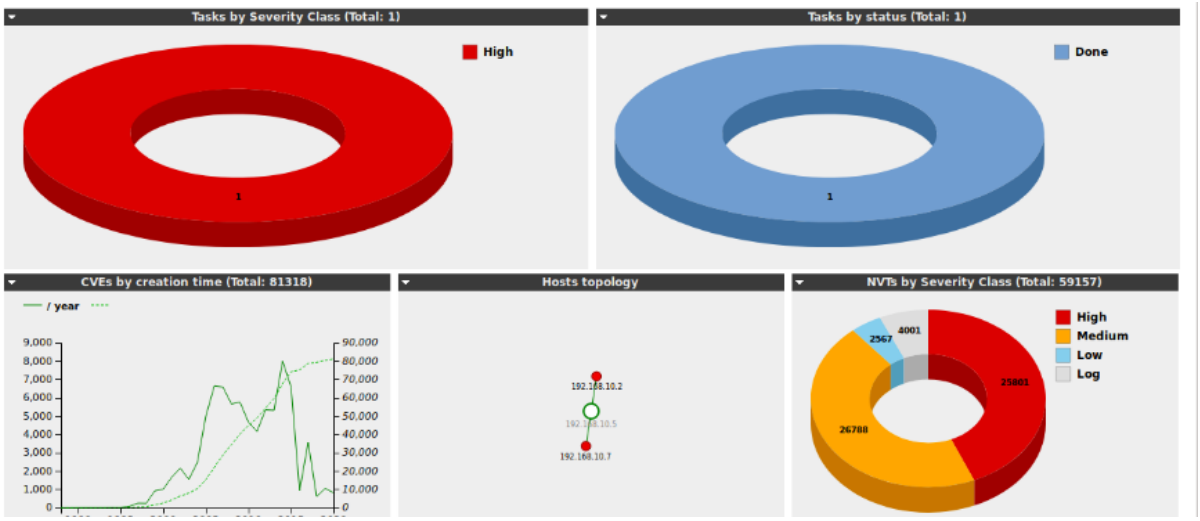


*Figure 3.3.11: Severity, NVTs, Task Status, Topology and CVEs*

### Step-06 (Download the reports)

report summarizes the results of a scan. Reports can be accessed via a browser and downloaded from different formats. Here I am downloaded pdf format. If the summary of the results found so far has been started a scan can be viewed. Upon completion of a scan the status is updated to ***DONE***.

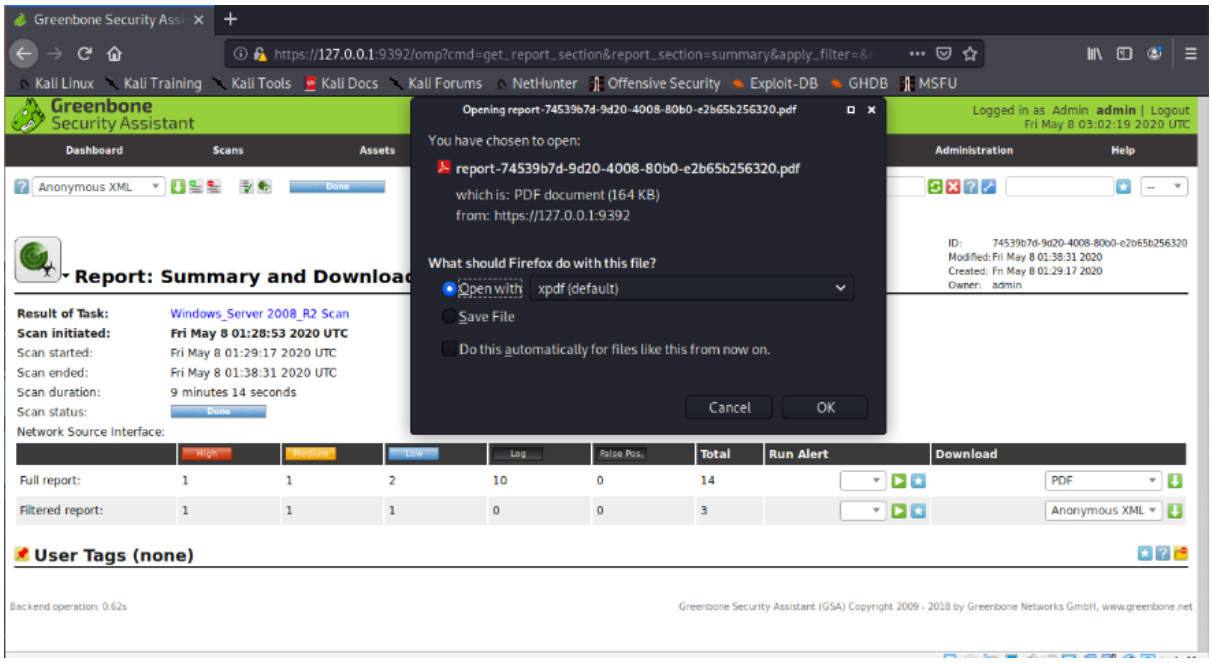


*Figure 3.3.12: Downloaded from pdf format*

WE are able to download the report category wise such as Hosts, Ports, and CVEs etc.

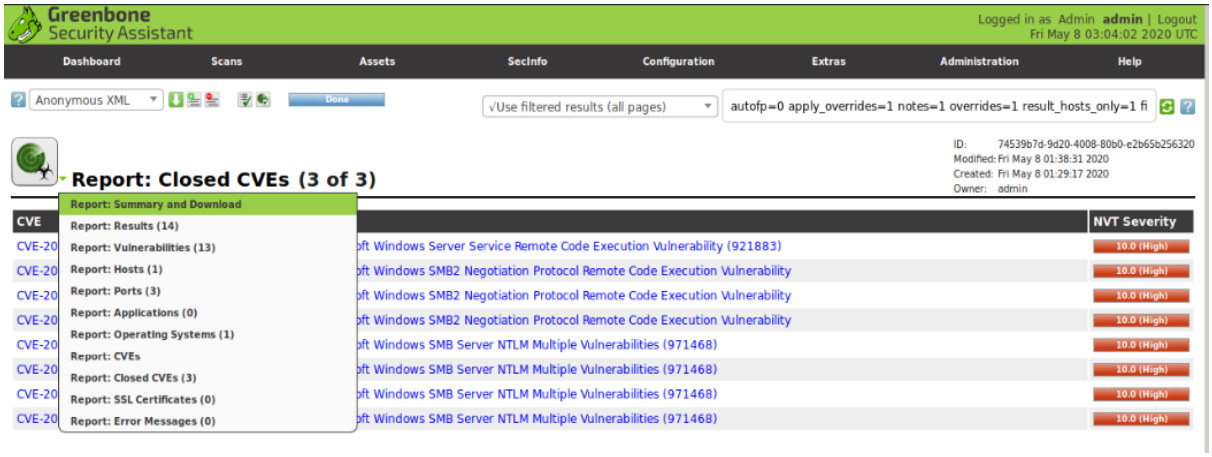


*Figure 3.3.13: Report category*

## 3.4 Scan Report Overview

## Windows Server 2008 R2 (Fresh Installed) full report overview

This document reports on the results of an automatic security scan. This report contains all 14 results selected by the filtering described above. Before filtering there were 14 results.

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 192.168.10.2 | 1 | 1 | 2 | 10 | 0 |
| Total: 1 | 1 | 1 | 2 | 10 | 0 |

*Figure 3.4.1: Filtering Results*

Risk level as shown in below figure 3.4.2

| Service (Port) | Threat Level |
|---|---|
| 445/tcp | High |
| 135/tcp | Medium |
| general/tcp | Low |
| 139/tcp | Log |
| general/CPE-T | Log |
| general/tcp | Log |
| general/icmp | Log |
| 445/tcp | Log |
| 135/tcp | Log |

*Figure 3.4.2: Risk level*

Here, below figure shown high, medium and low-level threats overview of may target machine.

**High 445 / tcp**

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

**Summary**
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Impact**
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

**Solution**
**Solution type:** VendorFix
The vendor has released updates. Please see the references for more information.

**Affected Software/OS**
- Microsoft Windows 10 x32/x64 Edition
- Microsoft Windows Server 2012 Edition
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64 Edition
- Microsoft Windows Server 2012 R2 Edition
- Microsoft Windows 7 x32/x64 Edition Service Pack 1
- Microsoft Windows Vista x32/x64 Edition Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

**Vulnerability Insight**
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

**Vulnerability Detection Method**
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: 2019-12-20T12:42:55+0000

**References**
CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147,
↪CVE-2017-0148
BID:96703, 96704, 96705, 96707, 96709, 96706
Other:
URL:https://support.microsoft.com/en-in/kb/4013078
URL:https://technet.microsoft.com/library/security/MS17-010
URL:https://github.com/rapid7/metasploit-framework/pull/8167/files

*Figure 3.4.3: High risk*

**Medium 135 / tcp**

**Summary**

Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

**Vulnerability Detection Result**

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49152]
Port: 49153/tcp
      UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49153]
      Annotation: NRP server endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49153]
      Annotation: DHCP Client LRPC Endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49153]
      Annotation: DHCPv6 Client LRPC Endpoint
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49153]
      Annotation: Event log TCPIP
Port: 49154/tcp
      UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49154]
      Annotation: IP Transition Configuration endpoint
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49154]
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49154]
      Annotation: XactSrv service
      UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49154]
      Annotation: IKE/Authip API
Port: 49155/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.10.2[49155]
Port: 49156/tcp
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49156]
      Annotation: IPSec Policy agent endpoint
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
```

Continued from previous page….

```
      Description : Spooler service
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49156]
      Annotation: Remote Fw APIs
Port: 49157/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.10.2[49157]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.
```

**Impact**
An attacker may use this fact to gain more knowledge about the remote host.

**Solution**
**Solution type:** Mitigation
Filter incoming traffic to this ports.

**Vulnerability Detection Method**
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: $Revision: 6319 $

*Figure 3.4.4: Medium risk*

## Low general / tcp

Low (CVSS: 2.6)
NVT: Relative IP Identification number change

**Summary**
The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

**Vulnerability Detection Result**
The target host was found to be vulnerable

**Impact**
An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are:
1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network.

Continued from previous page....

2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines.
3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.

**Solution**
**Solution type:** VendorFix
Contact your vendor for a patch

**Vulnerability Detection Method**
Details: `Relative IP Identification number change`
OID:1.3.6.1.4.1.25623.1.0.10201
Version used: 2020-03-21T13:23:23+0000

*Figure 3.4.5: Low risk*

Low (CVSS: 2.6)
NVT: TCP timestamps

**Summary**
The remote host implements TCP timestamps and therefore allows to compute the uptime.

**Vulnerability Detection Result**
```
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 102371
Packet 2: 102479
```

**Impact**
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**Solution**
**Solution type:** Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

**Affected Software/OS**
TCP/IPv4 implementations that implement RFC1323.

**Vulnerability Insight**

Continued from previous page....

The remote host implements TCP timestamps, as defined by RFC1323.

**Vulnerability Detection Method**

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: `TCP timestamps`

OID:1.3.6.1.4.1.25623.1.0.80091

Version used: 2020-03-21T13:23:23+0000

**References**

Other:

URL:http://www.ietf.org/rfc/rfc1323.txt

URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152

*Figure 3.4.6: Low risk 2*

After reviewing the vulnerability assessment report, we can analyze the vulnerability of the target machine and take necessary actions at the right time using the right way.

# 4. CONCLUSION

This report conducted a vulnerability assessment for a windows server 2008 R2 using the OpenVAS tool with the aim of analyzing its vulnerability findings and solutions. Among the likely vulnerabilities that the target machine is exposed to include vulnerabilities of critical security updates, remote host attacks and effect of uptime of the remote host. The report then suggested solutions and recommendations. This document be performed in order to ensure the overall security of the windows server 2008 R2.

# 5. REFERENCES

[1] L. . Constantin, "Critical vulnerability in Group Policy puts Windows computers at risk," , . [Online]. Available: http://www.csoonline.com/article/2882566/application-security/critical-vulnerability-in-group-policy-puts-windows-computers-at-risk.html. [Accessed 8 5 2020].

[2] D. Palmer, "Security", Top ten security vulnerabilities most exploited by hackers, 2019.

[3] Michener, "Common Permissions in Microsoft Windows Server 2008 and Windows Vista", IEEE Security & Privacy Magazine, vol. 6, no. 3, pp. 63-67, 2008. Available: 10.1109/msp.2008.59 [Accessed 7 May 2020].

[4] Computer audit", 2-small-business.com, 2020. [Online]. Available: http://www.2-small-business.com/computer_audit.shtml#.XrVCr2gzbIU. [Accessed: 08- May- 2020].

[5] OpenVAS - OpenVAS - Open Vulnerability Assessment Scanner", Openvas.org, 2020. [Online]. Available: https://www.openvas.org/. [Accessed: 05- May- 2020].

[6] "Install, setup, configure and run OpenVAS on Kali Linux", blackMORE Ops, 2018. [Online]. Available: https://www.blackmoreops.com/2018/10/02/install-setup-configure-and-run-openvas-on-kali-linux/. [Accessed: 04- May- 2020].

[7] "Vulnerability Scanning with OpenVAS 9 part 3: Scanning the Network - Hacking Tutorials", Hacking Tutorials, 2018. [Online]. Available: https://www.hackingtutorials.org/scanning-tutorials/vulnerability-scanning-with-openvas-9-scanning-the-network/. [Accessed: 05- May- 2020].