



Information Assurance & Auditing

4th Year – 1st Semester

Assignment

Student Registration Number	Student Name with Initials
IT 17 0437 24	Nalaka B.W.N.S.

Submitted to

Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the
Bachelor of Science Special Honors Degree in Information Technology

08th May 2020

Declaration

I certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of my knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

Table of Contents

Page

Declaration.....	i
Table of Content.....	ii
List of Figures.....	iii
List of Tables.....	iv
1 Introduction	1
2 Audit Scope	5
3 The Process of Auditing Windows 7 Box	6
3.1 Scanning Using Nmap.....	8
3.1.1 Scanning connected hosts	9
3.1.2 Scanning open TCP ports	9
3.1.3 Scanning UDP ports	10
3.1.4 Operating System Detection on Target Host	10
3.2 Vulnerably Assessment Using Nessus	12
4 Conclusion.....	26
References.....	27

List of Figures

Figure 2.1:Creating two virtual machines.....	6
Figure 2.2:Network adapter settings in Kali Linux VM	6
Figure 2.3: Network adapter settings in Windows 7 VM	6
Figure 2.4:IP Address of the Windows 7 VM.....	7
Figure 2.5:ping from Kali Linux VM to Windows 7 VM.....	7
Figure 2.6:All the commands available for using under nmap	8
Figure 2.7:Finding the IP address of the machine which have been connected to Kali.....	9
Figure 2.8:Scanning open TCP ports.....	10
Figure 2.9:Scanning UDP ports between 130 and 140	10
Figure 2.10:2. Operating System Detection on Target Host	11
Figure 2.11:Starting Nessus Service.....	12
Figure 2.12:Accessing Nessus GUI.....	12
Figure 2.13:Going to Policies.....	13
Figure 2.14:Policies section	13
Figure 2.15:Selecting Advanced Scan Policy Templates	14
Figure 2.16:Settings tab in Advanced Scan Policy Template	14
Figure 2.17:Credentials tab in Advanced Scan Policy Template	15
Figure 2.18:Plugging tab in Advanced Scan Policy Template.....	16
Figure 2.19:Enabled or disabled according to the Audit.....	17
Figure 2.20:Created Policy saved under Policies	17
Figure 2.21:After creating the policy, the target can be scanned	18
Figure 2.22:Selecting Scan Templates.....	18
Figure 2.23:Selecting User Defined Scan Templates	19
Figure 2.24:Giving name and target for new scan.....	19
Figure 2.25:Scanning the vulnerability.....	20
Figure 2.26:Scan will be completed	20
Figure 2.27:The status of the scan will be shown in a bar	21
Figure 2.28:Available vulnerabilities	21
Figure 2.29:Windows Terminal Services Enabled	22
Figure 2.30:Critical Vulnerabilities	22
Figure 2.31: Critical Vulnerability 01 - Microsoft RDP RCE.....	23
Figure 2.32:Critical Vulnerability 02 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution	23
Figure 2.33:Critical Vulnerability 03 - Unsupported Windows OS (remote).....	24

List of Tables

Table 2.1:Summary of critical vulnerability.....	25
--	----

1 Introduction

In today's world usage of computers is more prominent. Computer has become a more important asset in all sectors. As a result of that, numerous problems have been risen in computer and information technology industry. The most serious situation is the cybercrimes. When comes to the business industry, without considering the size of the organization, it can gain a crucial insight to the overall computing functionality, potential security risks, and potential solutions for them. Within the organizations and businesses, information technology plays a very big role. Therefore, IT audits are very essential for the organizations and businesses and organizations can gain the values for them by performing audits.

Information systems of the organization can be evaluated and safeguard by IT audits. Web applications, software applications, networks, and operating systems can be covered by IT audits. The importance of audits towards the organizations and businesses should be realized, in order to gain the benefits of performing audits. Therefore, this report is aimed to describe the importance of the audits, how to do a computer audit for Windows 7 box and explain the Nmap and Nessus to which are used to audit Windows 7 box. Then it will further explain the processes of auditing Windows 7 box.

What is computer auditing?

Computer auditing is a systematic and logical procedure, with the intend of identifying the detailed information technology processes, activities and controls of an information system [1]. A risk-based procedure is followed for this. Computer auditing process also checks whether that, the organizational goals, and objectives are achievable by the information system auditing. Computer auditing process can be described as a field of specialization in auditing. Following areas can be mentioned as needed specializations in computer auditing [4].

- Computer Assisted Audit Techniques
- IT governance
- Information system and risk control
- Information security
- Disaster recovery
- Information system continuity

Data processing in a business can be facilitated with the special attention to targeted operations by the computer auditing. Programmers and analysts can review the data by the tools used for computer auditing. Therefore, the frustration, money and time can be saved. Safety measuring for the business can be done by computer auditing [4].

There are three types of IT auditing. First type is IT performance. Then the second type is compliance to applicable laws, policies and standards [1]. Third type of audit is, final statement audits. Checking whether the inefficiencies and inaccuracies is the main objective of performing audits. Therefore, the importance of performing IT audits can be mentioned as follows [4].

- Risks of the organization can be reduced.
- Frauds can be detected and prevented.
- Security of data can be improved.
- IT governance is enhanced.
- Susceptibility to threat is checked.
- System is evaluated.
- Integrity of the system can be ensured.

Tools for Audit Windows 7 Box

- Nmap
- Nessus

Nmap

Nmap stands for Network mapper and it is a number of computers probing features are provided by the Nmap. Detection of operating systems, service and host discovery are included for Nmap. Scripts extensible the features of Nmap and an advanced service detection, a detection for vulnerability, and many other features are provided by these scripts. Adopting for network conditions such as latency, congestion is enabling for Nmap. Various features of Nmap can be mentioned as follows [2].

- Discovering hosts
- Scanning ports
- Detecting operating systems

Further details on DNSs, devices, targets and MAC addresses can be gained by Nmap tool. Some typical uses of Nmap tool can be mentioned as follows [2].

- Security devices or firewalls can be audited to identify the network connections.
- Open ports of a target host can be identified.
- Network maintenance and network mapping.
- Security condition of a network can be audited with the identification of new servers.
- The traffic on a network can be generated.
- Exploiting vulnerabilities and attacks of a network can be identified.

Nessus

Nessus can be mentioned as a remote security scanning tool. A given computer can be scanned using Nessus and it will raise an alert when it discovers that there is any vulnerability which gives the access to malicious hackers to connect your computer. Nessus runs more than 1200 checks for a given particular computer to discover the vulnerabilities. There, it checks that if the computer can be harmed or broken by malicious attacks. Administrators who are in charge of computers which are connected to the internet, can use Nessus for protecting their domains from vulnerabilities. However, Nessus cannot be used as a complete solution for security and it can be used as a part of strategic security mechanism [3]. Attacks cannot be prevented actively by Nessus and computer is checked by Nessus for finding vulnerabilities. Therefore, it is the responsibility of administrators for patching the vulnerabilities that have been detected by Nessus. Some of the vulnerabilities that can be detected by Nessus can be mentioned as follows [3].

- Vulnerabilities which allow for unauthorized access and control for sensitive data.
- Vulnerabilities of Denials of service.
- Misconfigurations

Operating systems, databases, network devices, and web servers can be scanned by Nessus resulting a report in plain text format or HTML or XML or LaTeX. The compliance audits, configuration audits, and SCADA audits also can be supported by Nessus. In addition to the testing vulnerabilities, Nessus can be used for examining the patch levels using windows credentials. For

the Nessus scan for Windows operating system there are some requirements that should be fulfilled [3].

- Enable WMI service on target.
- Enable remote registry service.
- Enable file and printer sharing service in target's firewall.
- Open port 139 and port 445.
- Allow bidirectional traffic between auditor's IP and target's IP in the firewall.
- Down system firewall during scanning process.
- Disable Network Threat Detection related antivirus feature.
- Low the user access control settings.

Benefits of Nessus

Comparing with other tools, followings are the benefits that can be gained by using Nessus for vulnerability scanning [3].

- Not making the assumptions about the server configuration which can be caused for missing vulnerabilities.
- Extensible and provides scripting language to write specific tests which are specific to the system.
- Provides virus and vulnerability detected free plug-ins.
- Gets update on latest attacks and vulnerabilities.
- Open source and free to modify.
- Assistance for patching.
- Suggesting the best and most suitable way for mitigating a vulnerability.
- Easy policy creation and requiring a less effort to scan a whole network.

2 **Audit Scope**

The overall objective of auditing Windows 7 box is to, ensure that the system is controlled respect to the pre-defined policies and administrations and to check the Common Vulnerability Exposures for Windows 7 [5].

Checklist

- Win32k Elevation of Privilege Vulnerability
- Windows GDI Information Disclosure Vulnerability'
- Win32k Elevation of Privilege Vulnerability
- Microsoft Graphics Components Information Disclosure Vulnerability
- Jet Database Engine Remote Code Execution Vulnerability
- Jet Database Engine Remote Code Execution Vulnerability
- Windows Denial of Service Vulnerability
- Windows Code Integrity Module Information Disclosure Vulnerability
- Windows Error Reporting Manager Elevation of Privilege Vulnerability
- Windows Power Service Elevation of Privilege Vulnerability
- Windows Error Reporting Manager Elevation of Privilege Vulnerability
- Windows NTLM Security Feature Bypass Vulnerability
- Windows Kernel Information Disclosure Vulnerability
- Remote Desktop Client Remote Code Execution Vulnerability
- Windows Imaging API Remote Code Execution Vulnerability
- Remote Desktop Client Remote Code Execution Vulnerability
- LNK Remote Code Execution Vulnerability

3 The Process of Auditing Windows 7 Box

Create two virtual machines for Kali Linux and Windows 7, using Oracle VM VirtualBox software. Then when the VirtualBox is started, created virtual machines will be displayed as shown in following figure.

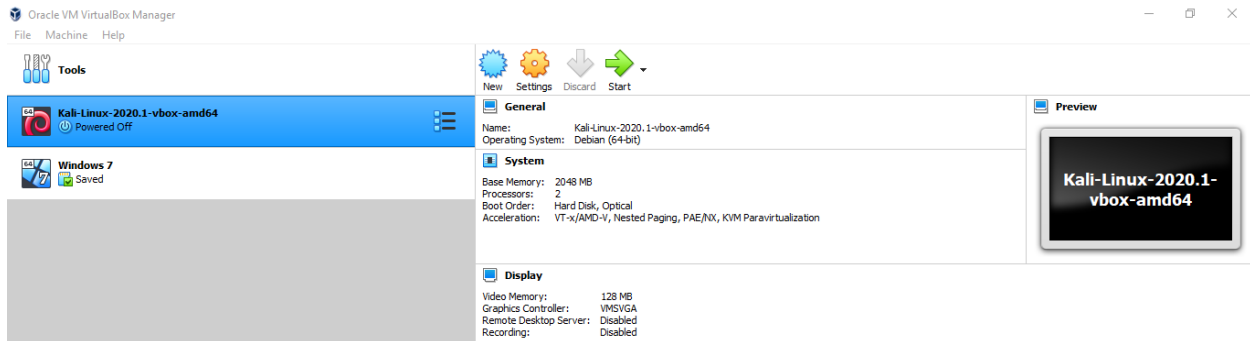


Figure 3.1: Creating two virtual machines

Then both virtual machines are attached to the same network.

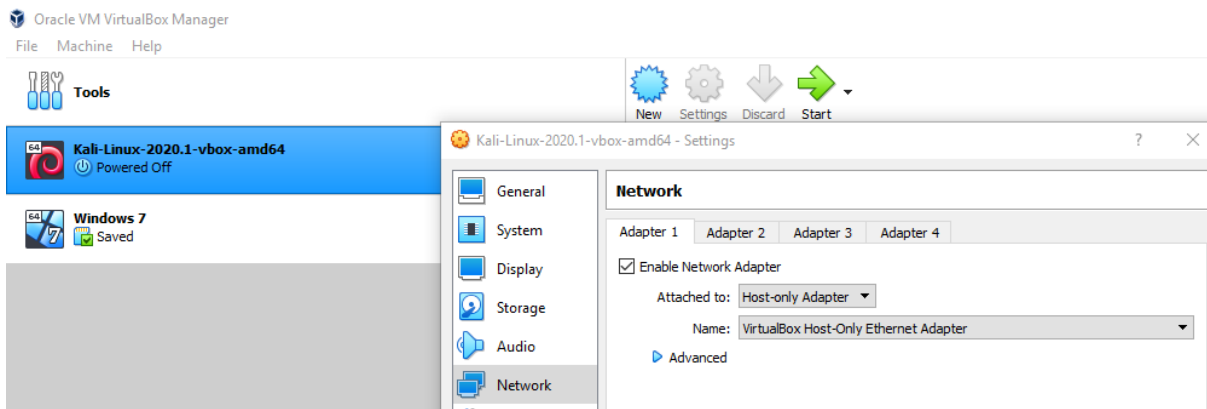


Figure 3.2: Network adapter settings in Kali Linux VM

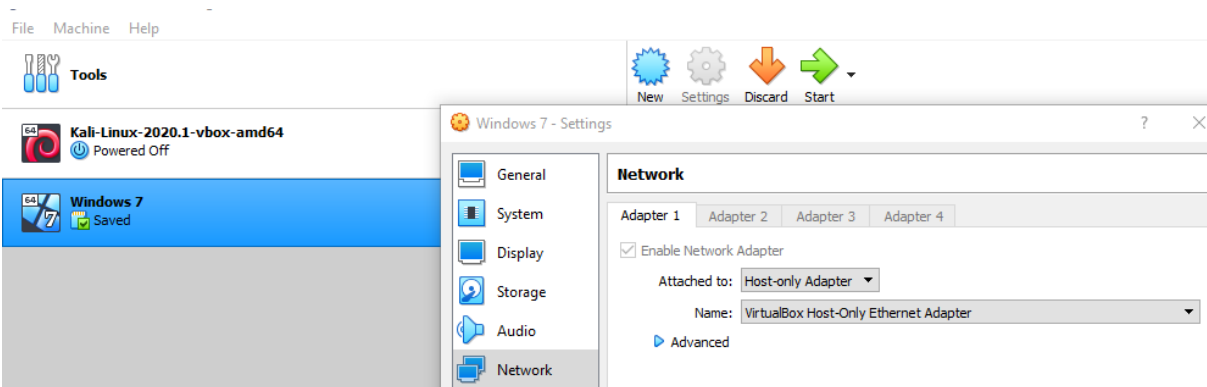


Figure 3.3: Network adapter settings in Windows 7 VM

Check whether that both virtual machines have been connected to the network successfully. For that we have to ping from the Kali Linux virtual machine to Windows 7. There, the IP addresses for two virtual machines should be known.

Issue the command “ipconfig” on the command prompt of Windows 7 machine to get the IP address. According to the following figure, the IP address of Windows 7 machine (target) is 192.168.56.101

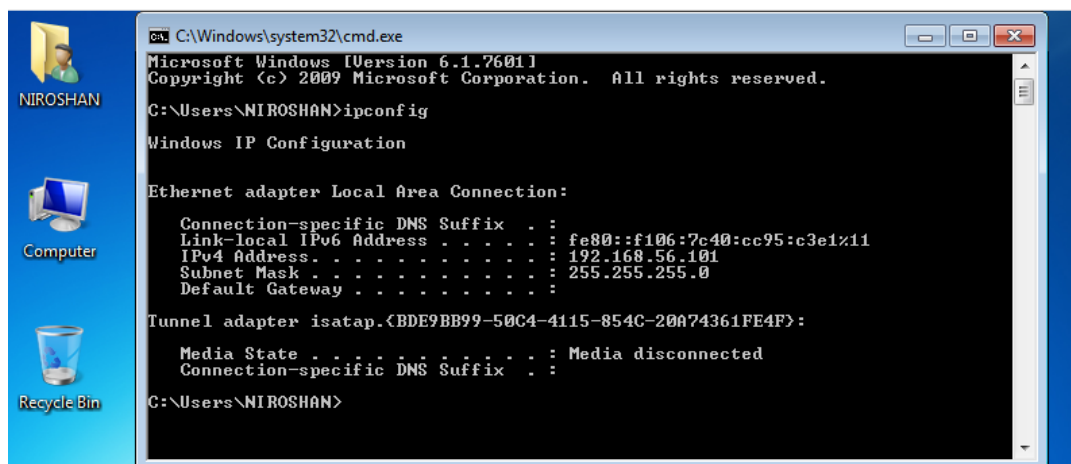


Figure 3.4:IP Address of the Windows 7 VM

From Kali Linux machine, Issue the following command to check the connectivity of two virtual machines.

ping 192.168.56.101

Then the ping will be successful as mentioned in following figure.

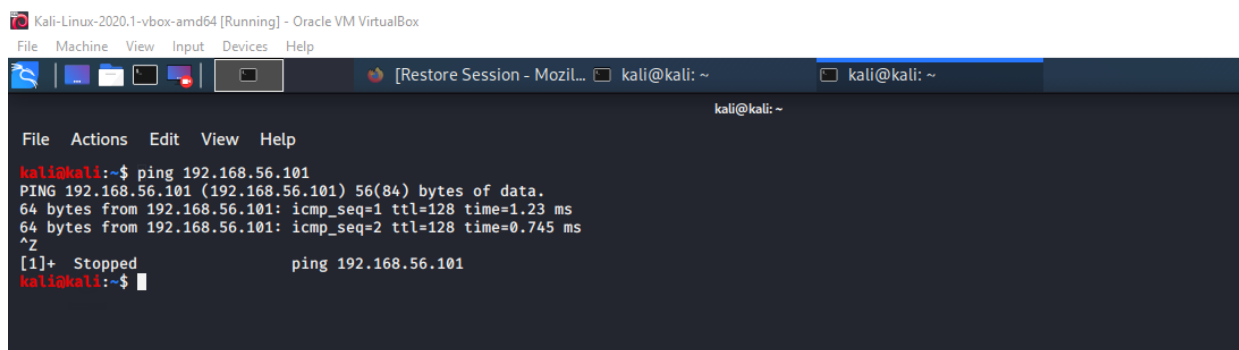
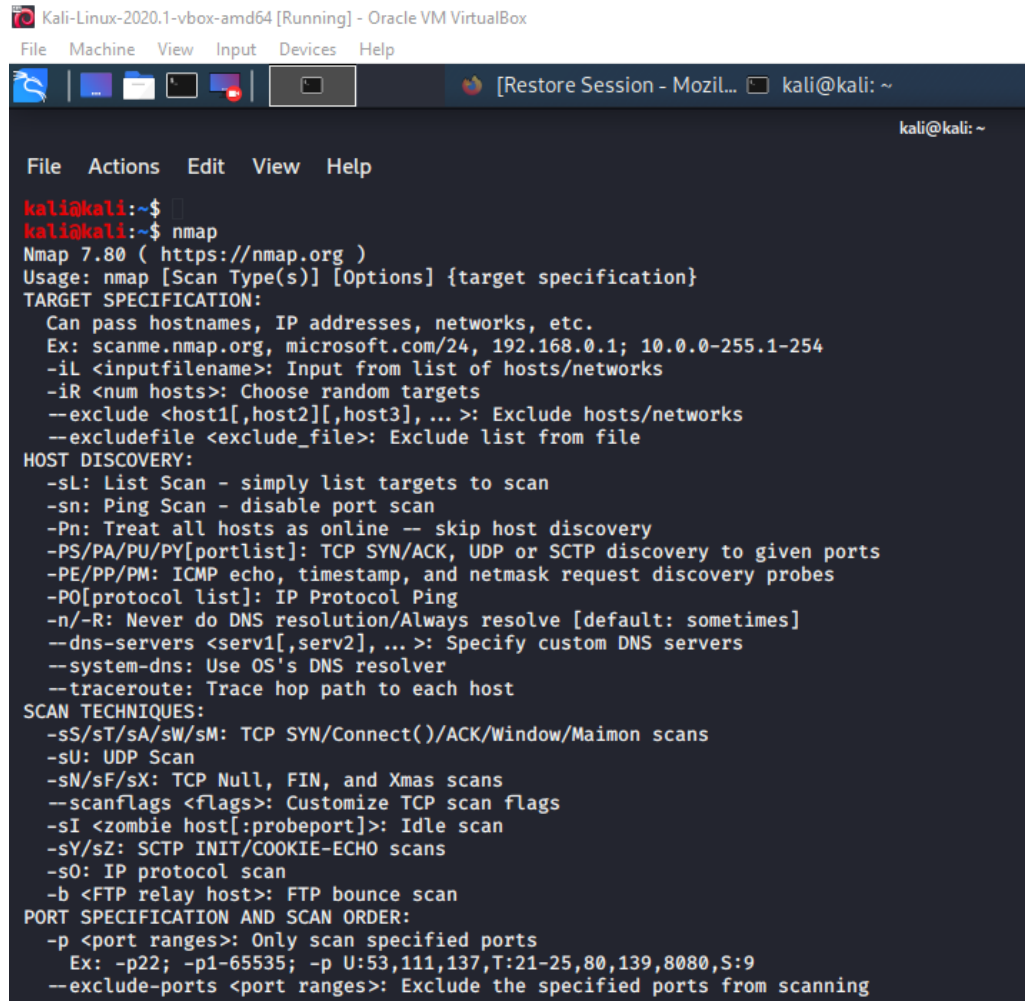


Figure 3.5:ping from Kali Linux VM to Windows 7 VM

3.1 Scanning Using Nmap

After checking the connectivity, information on connected host IP, operating system and ports can be gained using Nmap.

Issue the following command to view all the commands available for using under nmap. Then all the commands will be displayed as shown in following figure.



```
Kali-Linux-2020.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Restore Session - Mozil... kali@kali: ~
kali@kali: ~
File Actions Edit View Help
kali@kali:~$ 
kali@kali:~$ nmap
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ... >: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ... >: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
```

Figure 3.6: All the commands available for using under nmap

3.1.1 Scanning connected hosts

Issue the following command to know the IP address of the machine which have been connected to Kali Linux virtual machine.

`nmap -sP <IP address of Kali Linux VM>`

```
root@kali:~#  
root@kali:~#  
root@kali:~# nmap -sP 192.168.56.102/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-08 01:56 EDT  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid  
Nmap scan report for 192.168.56.1  
Host is up (0.00046s latency).  
MAC Address: 0A:00:27:00:00:11 (Unknown)  
Nmap scan report for 192.168.56.100  
Host is up (0.00056s latency).  
MAC Address: 08:00:27:4B:AF:10 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.56.101  
Host is up (0.00023s latency).  
MAC Address: 08:00:27:D5:43:6D (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.56.102  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.77 seconds  
root@kali:~#
```

Figure 3.7: Finding the IP address of the machine which have been connected to Kali

3.1.2 Scanning open TCP ports

Issue the following command to view open TCP ports on target host.

`nmap -sS <IP address of target host>`

```
root@kali:~# nmap -sS 192.168.56.101/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-08 06:22 EDT  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid  
Nmap scan report for 192.168.56.1  
Host is up (0.00039s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE  
12000/tcp open  cce4x  
MAC Address: 0A:00:27:00:00:11 (Unknown)  
Nmap scan report for 192.168.56.100  
Host is up (0.00032s latency).  
All 1000 scanned ports on 192.168.56.100 are filtered  
MAC Address: 08:00:27:E4:B3:43 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.56.101  
Host is up (0.00075s latency).  
Not shown: 986 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
554/tcp   open  rtsp  
2869/tcp  open  icslap  
3389/tcp  open  ms-wbt-server  
5357/tcp  open  wsdaapi  
10243/tcp open  unknown  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown
```

```

MAC Address: 08:00:27:D5:43:6D (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.56.102 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 7.51 seconds
root@kali:~#

```

Figure 3.8: Scanning open TCP ports

3.1.3 Scanning UDP ports

Issue the following command to view UDP ports on target host.

nmap -sU <IP address of target host>

Issue the following command to view UDP ports between 130 and 140.

nmap -sU -p U:130-140 <IP address of target host>

```

root@kali:~#
root@kali:~# nmap -sU -p U:130-140 192.168.56.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-08 06:42 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid :
Nmap scan report for 192.168.56.101
Host is up (0.0011s latency).
PORT      STATE SERVICE
130/udp   closed  cisco-fna
131/udp   closed  cisco-tna
132/udp   closed  cisco-sys
133/udp   closed  statsrv
134/udp   closed  ingres-net
135/udp   closed  msrpc
136/udp   closed  profile
137/udp   open    netbios-ns
138/udp   open|filtered netbios-dgm
139/udp   closed  netbios-ssn
140/udp   closed  emfis-data
MAC Address: 08:00:27:D5:43:6D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.07 seconds

```

Figure 3.9: Scanning UDP ports between 130 and 140

3.1.4 Operating System Detection on Target Host

Issue the following command to operating system detection on target host.

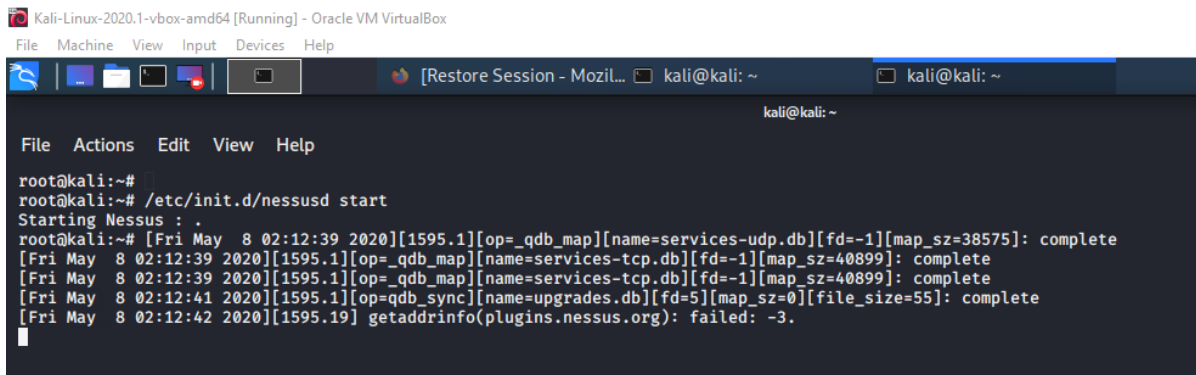
nmap -O <IP address of target host>



3.2 Vulnerability Assessment Using Nessus

Vulnerability scan for Windows 7 can be started after having the information from Nmap. In order to start the Nessus, issue the below command on the Kali terminal.

/etc/init.d/nessusd start



```
Kali-Linux-2020.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
root@kali:~#
root@kali:~# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:~# [Fri May 8 02:12:39 2020][1595.1][op=qdb_map][name=services-udp.db][fd=-1][map_sz=38575]: complete
[Fri May 8 02:12:39 2020][1595.1][op=qdb_map][name=services-tcp.db][fd=-1][map_sz=40899]: complete
[Fri May 8 02:12:39 2020][1595.1][op=qdb_map][name=services-tcp.db][fd=-1][map_sz=40899]: complete
[Fri May 8 02:12:41 2020][1595.1][op=qdb_sync][name=upgrades.db][fd=5][map_sz=0][file_size=55]: complete
[Fri May 8 02:12:42 2020][1595.19] getaddrinfo(plugin.nessus.org): failed: -3.
```

Figure 3.11: Starting Nessus Service

Type <https://localhost:8834> on the web browser and then it will be automatically redirected to the Nessus GUI as shown in following figure. Then click on “Sign in”.

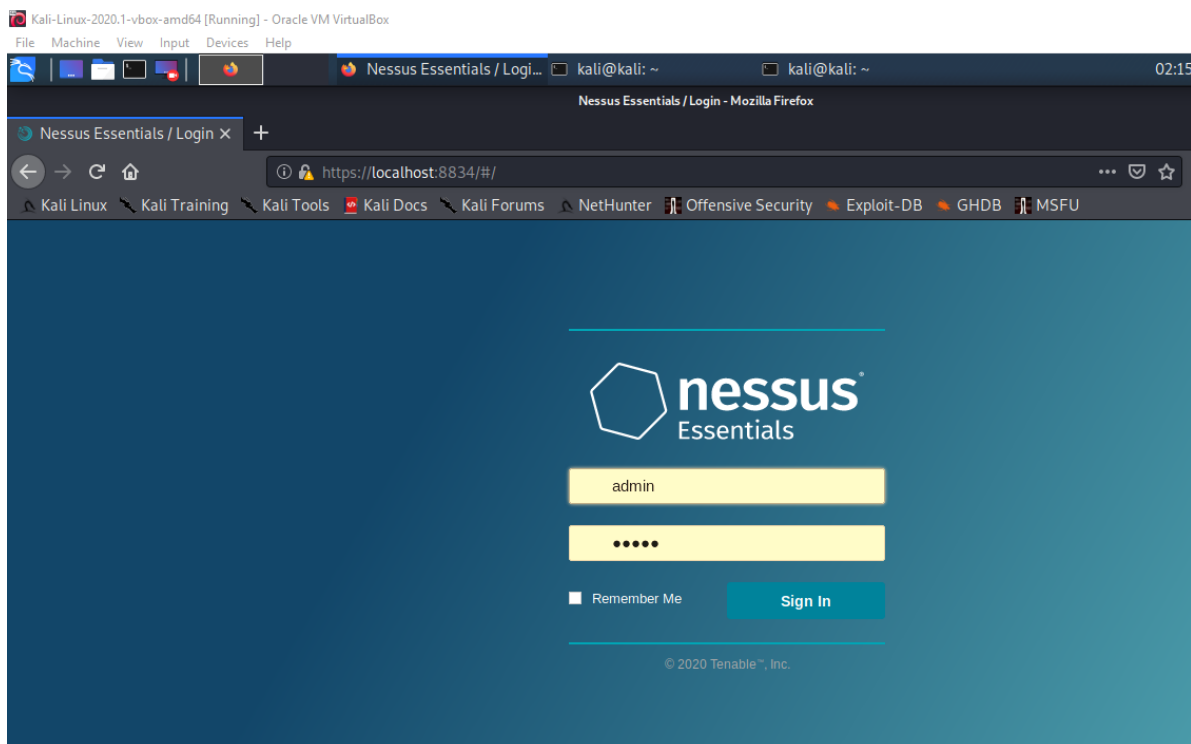


Figure 3.12: Accessing Nessus GUI

Before starting the vulnerability scan, a policy should be created. Therefore, click on “Policies”.

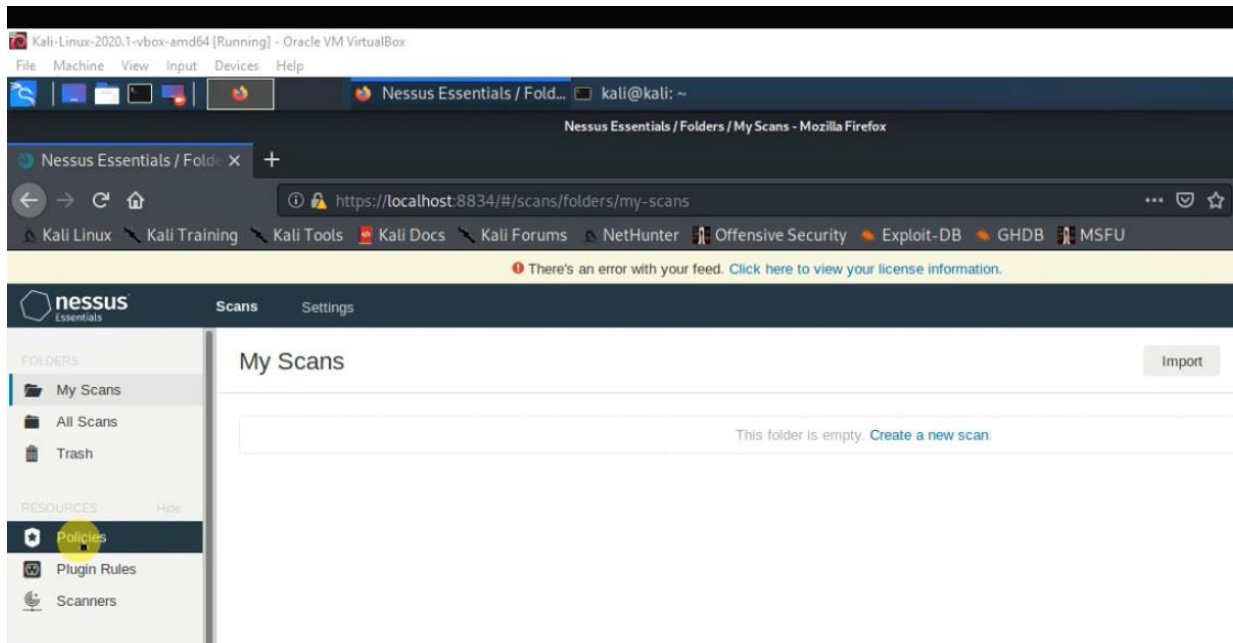


Figure 3.13: Going to Policies

After clicking on “Policies”, it will be displayed as following. There, click on “New Policy”.

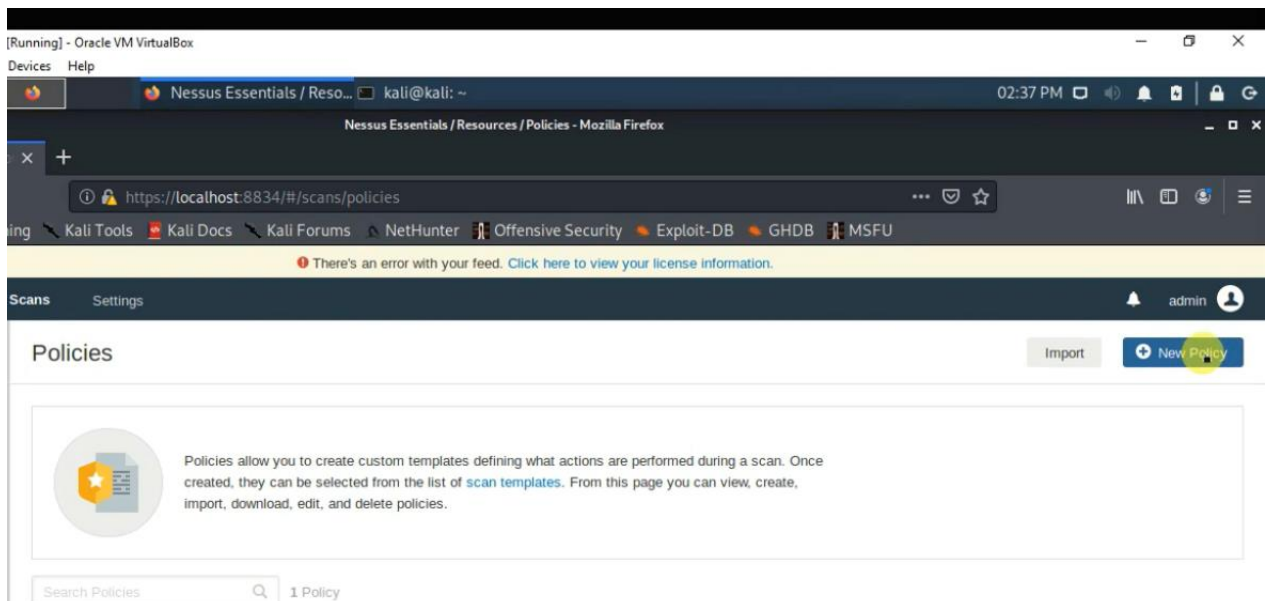


Figure 3.14: Policies section

Then you will be redirected to “Policy Templates” as shown in following figure. There, it will display all the available options to create a policy.

When doing the vulnerability scan for Windows 7, a policy is created for “Advanced Scan”. Therefore, click on “Advanced Scan”.

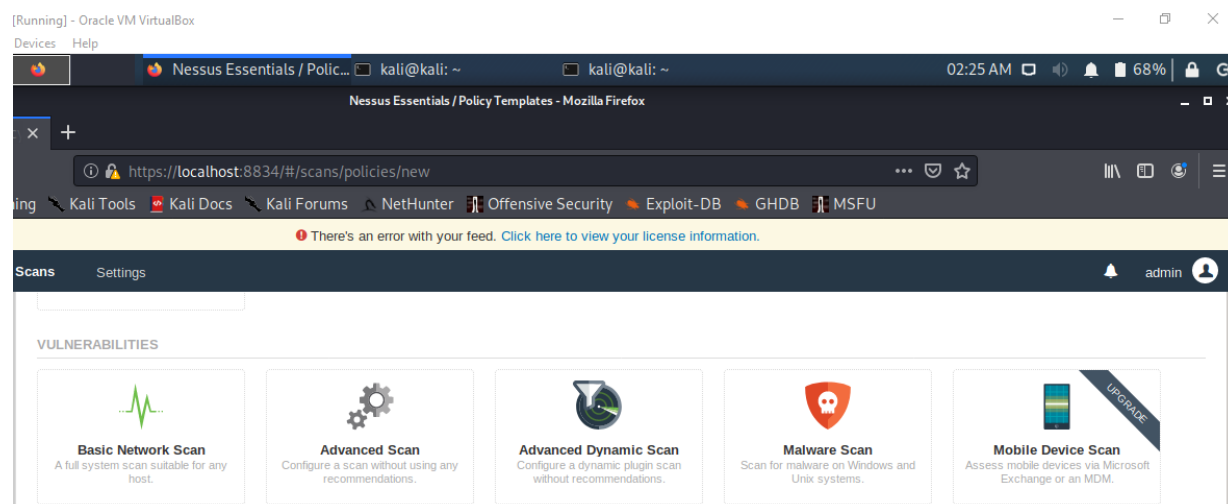


Figure 3.15: Selecting Advanced Scan Policy Templates

Then it will give “New Policy / Advanced Scan”. There, the information should be given under three sections Settings, Credentials, Plugins. Under the Settings, give a name.

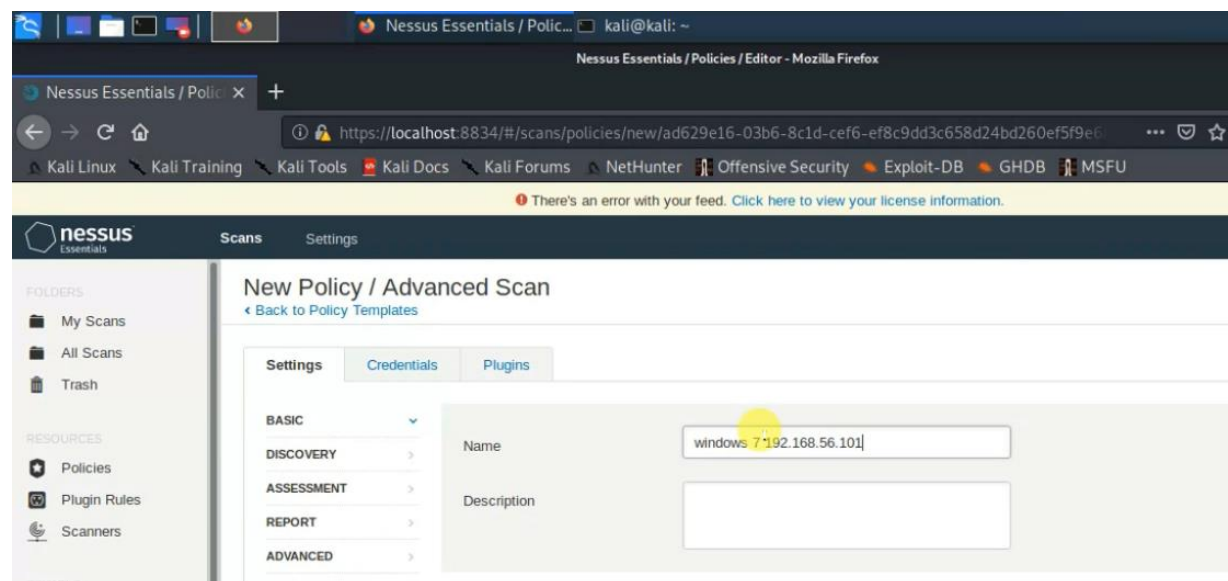


Figure 3.16: Settings tab in Advanced Scan Policy Template

Then go to “Credentials” and click on “Windows” Then it will show four fields, under “Windows’
There, select “Password” as the “Authentication Method” from the drop-down list. Then give a username and a password.

Under “Global Configuration Settings”, there are four options that should be enabled. Tick on all four options.

Then click on “Plugins”.

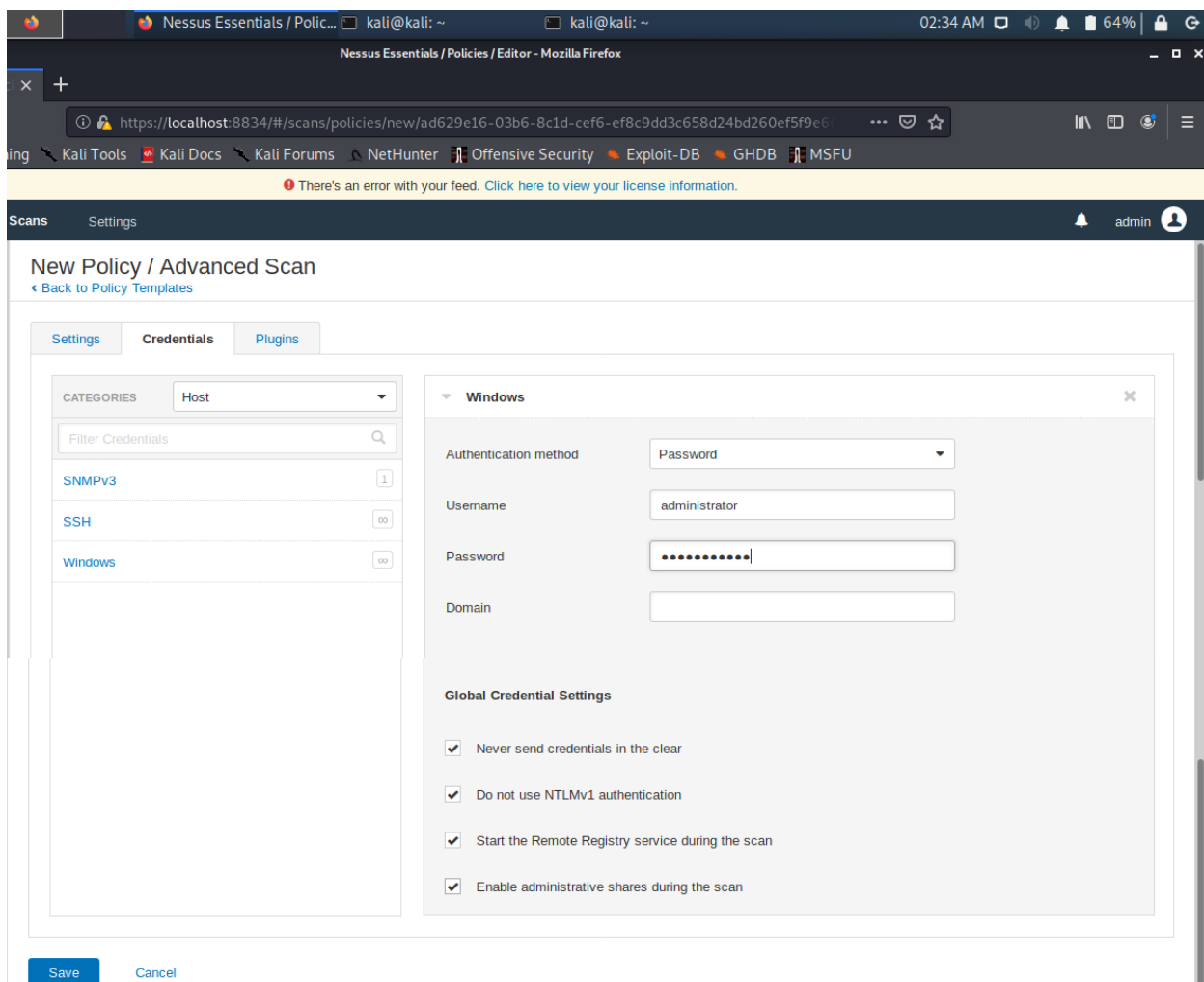


Figure 3.17: Credentials tab in Advanced Scan Policy Template

Then there will be many plugins as shown in following figure.

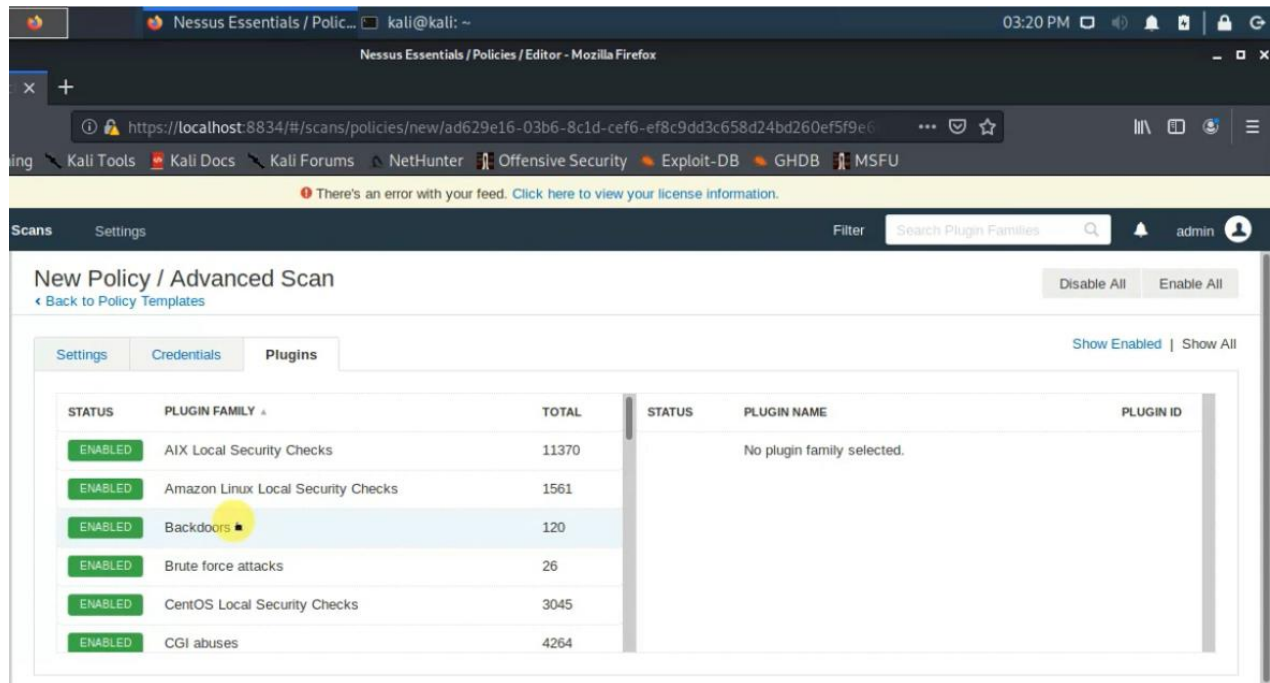


Figure 3.18:Plugging tab in Advanced Scan Policy Template

Among the available plugins, they can be enabled or disabled according to the audit going to be done.

Following plugging are enabled

- Backdoors
- CGI abuses
- CGI abuses: XSS
- Database
- DNS, Firewalls
- FTP
- Peer-To-Peer File Sharing
- Policy Compliance
- Service detection Settings
- SMTP problem
- SNMP
- Web Servers
- Windows
- Windows: Microsoft Bulletins
- Windows: User management

Then click on “Save”.

STATUS	PLUGIN NAME	PLUGIN ID
DISABLED	Solaris Local Security Checks	3711
DISABLED	SuSE Local Security Checks	14925
DISABLED	Ubuntu Local Security Checks	4909
DISABLED	Virtuozzo Local Security Checks	294
DISABLED	VMware ESX Local Security Checks	132
ENABLED	Web Servers	1215
ENABLED	Windows	4541

[Save](#) [Cancel](#)

Figure 3.19:Enabled or disabled according to the Audit

Then the created policy will be saved under Policies.

The screenshot shows the Nessus Essentials web interface in a browser window. The address bar shows the URL `https://localhost:8834/#/scans/policies`. The interface has a dark sidebar on the left with the following sections:

- FOLDERS**: My Scans, All Scans, Trash
- RESOURCES**: Policies (selected), Plugin Rules, Scanners
- TENABLE**: Community, Research

The main content area is titled "Policies" and includes an "Import" button and a "New Policy" button. Below this is a descriptive text box about policies. A search bar shows "1 Policy". The policy list table is as follows:

<input type="checkbox"/>	Name ▲	Template	Last Modified	
<input type="checkbox"/>	windows 7 - 192.168.56.101	Advanced Scan	May 6 at 4:21 PM	⬇️ ✕

Figure 3.20:Created Policy saved under Policies

After creating the policy, the target can be scanned. Therefore, click on “My Scans” and then click on “New Scan”.

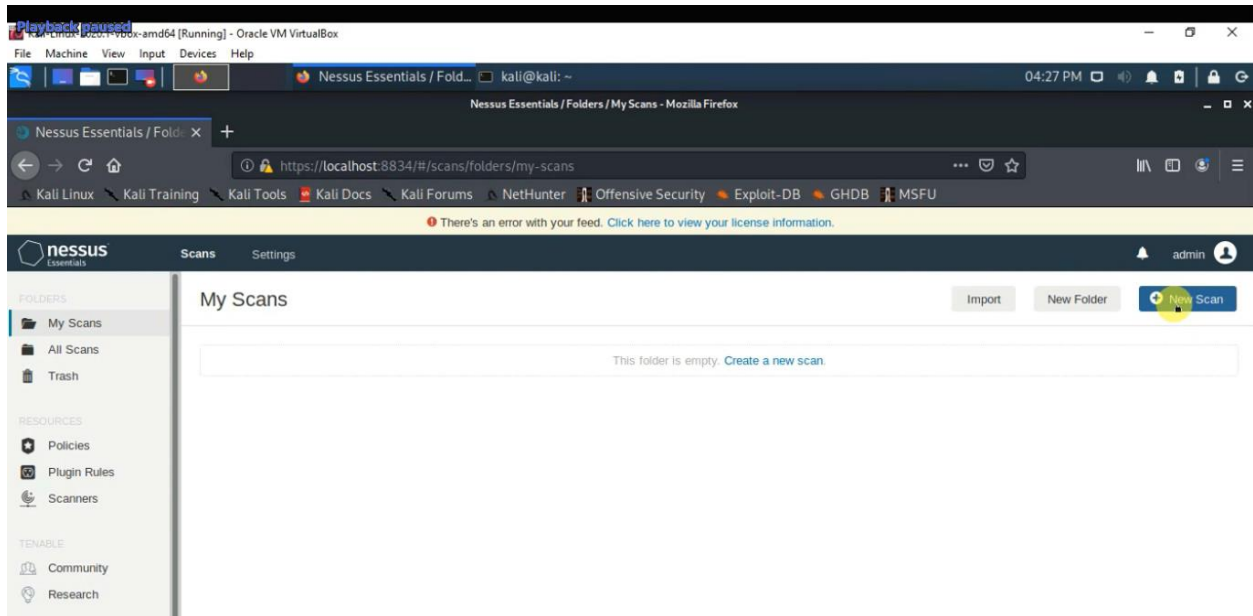


Figure 3.21: After creating the policy, the target can be scanned

Then it will open a page as shown in following figure and click on “User Defined”.

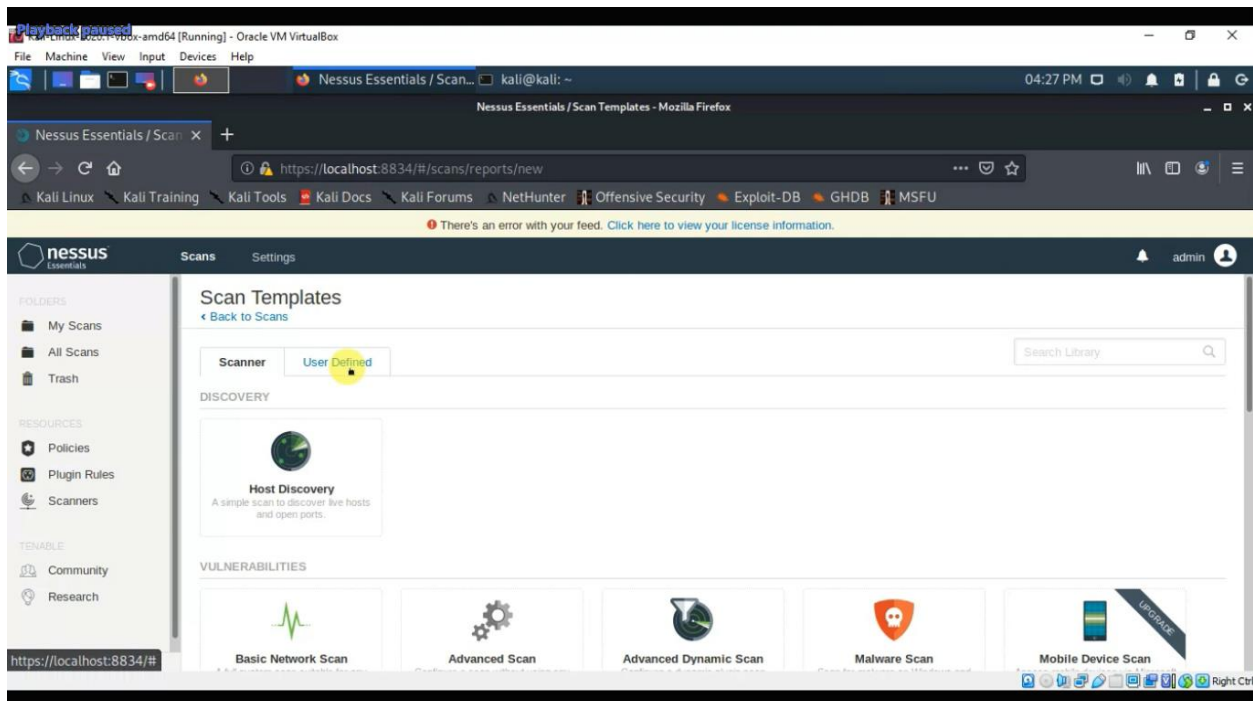


Figure 3.22: Selecting Scan Templates

Then it will display the created policy as mentioned following figure and click on that policy.

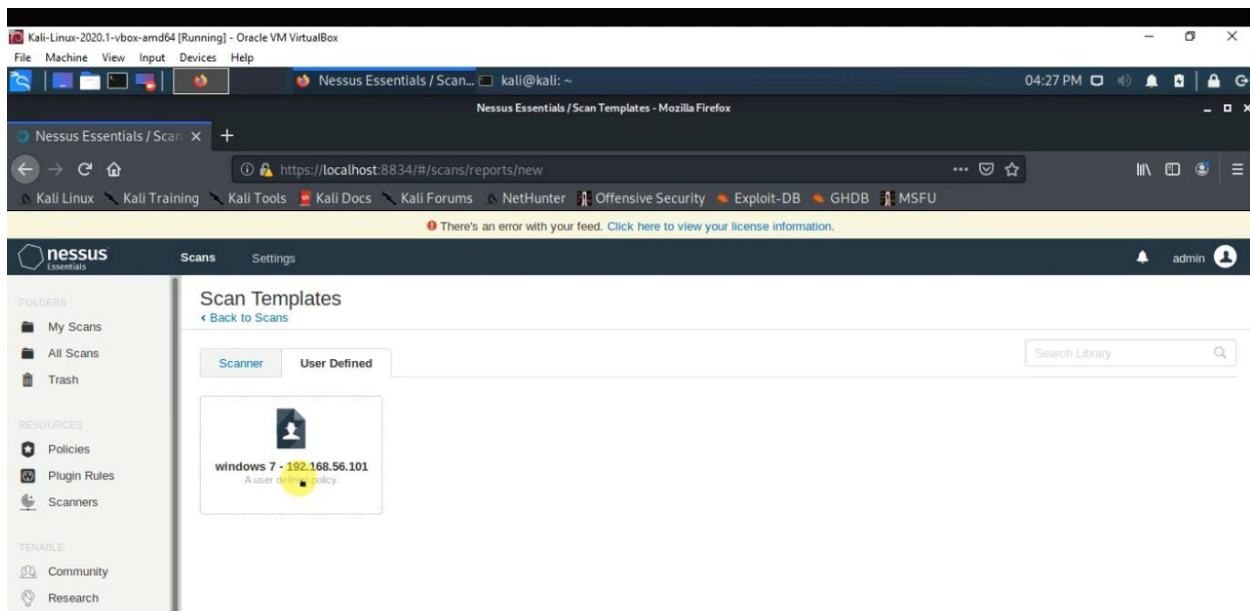


Figure 3.23: Selecting User Defined Scan Templates

There are some fields under general settings that should be filled. Give a meaningful name for the scan. Give the IP address of target. In this case give the IP address of Windows 7 virtual machine and click on “Launch”.

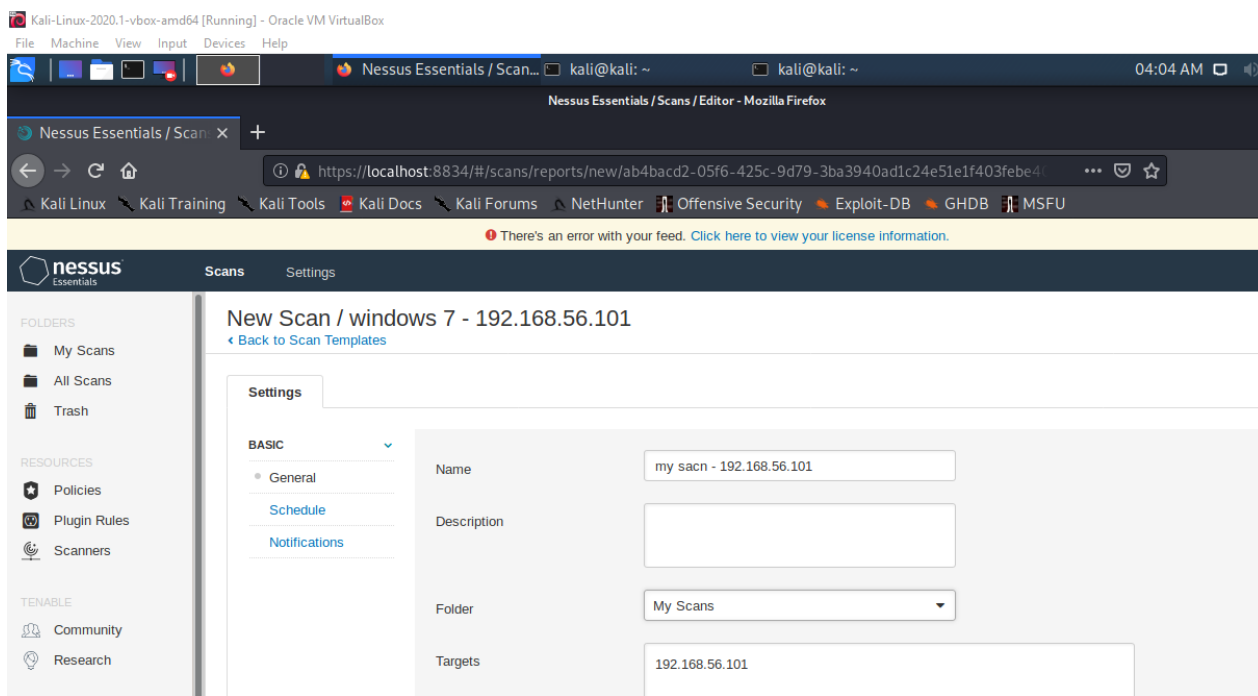


Figure 3.24: Giving name and target for new scan

Then the scan will be saved and launched successfully. Then the scan will be running as shown in following figure.

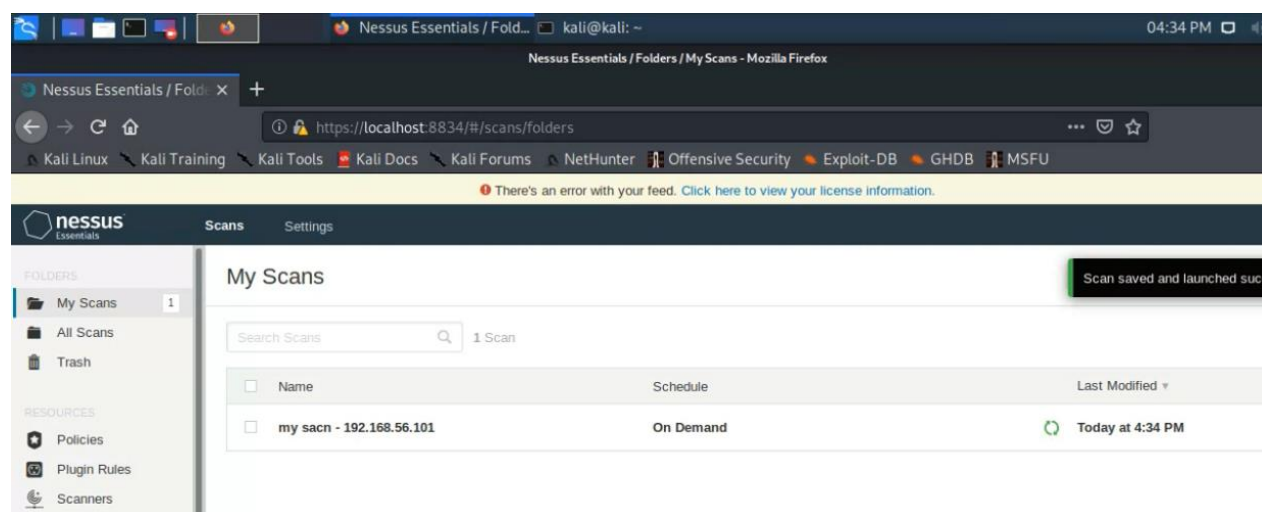


Figure 3.25: Scanning the vulnerability

The scan will be running for few minutes and then the scan will be completed. Then click on the name of the scan.

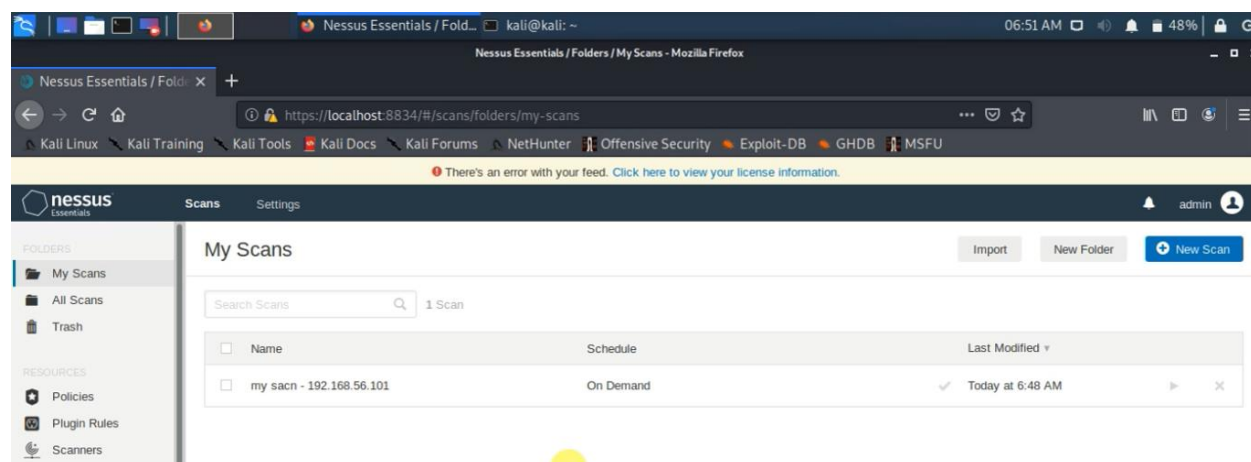


Figure 3.26: Scan will be completed

Then the status of the scan will be shown in a bar as shown in following figure and it will display the status of the scan under “Scan Details”. According to that 6 minutes have been taken to complete the scan.

The nature of the vulnerabilities will be displayed by a pie chart whether they are critical vulnerabilities, high, medium, low or just the information.

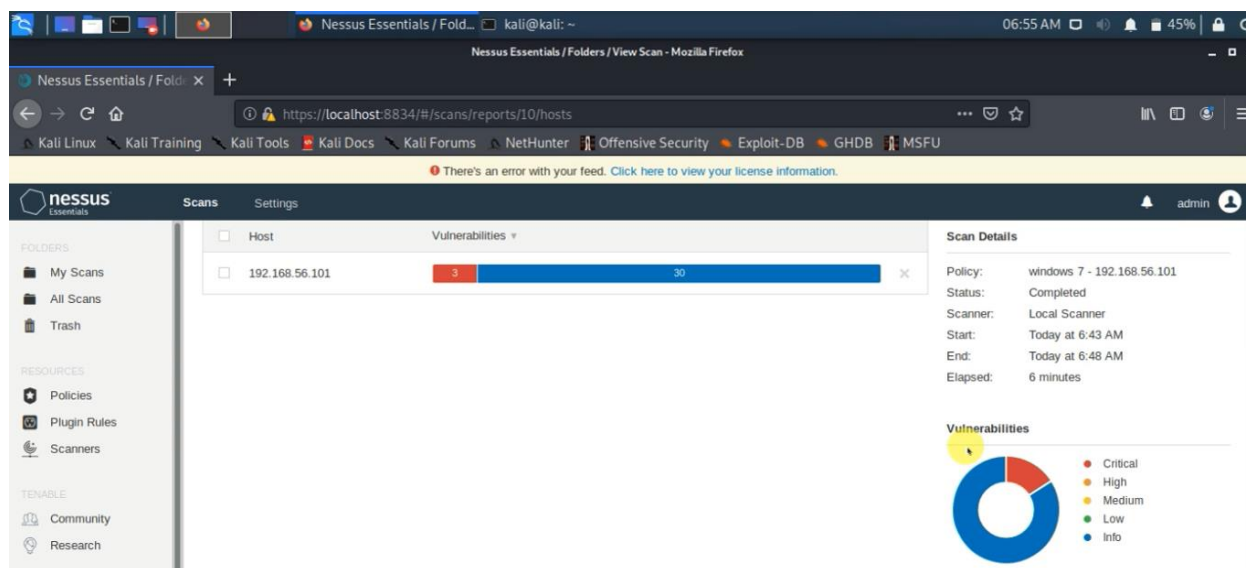


Figure 3.27: The status of the scan will be shown in a bar

When click on the vulnerabilities bar, it will display the available vulnerabilities.

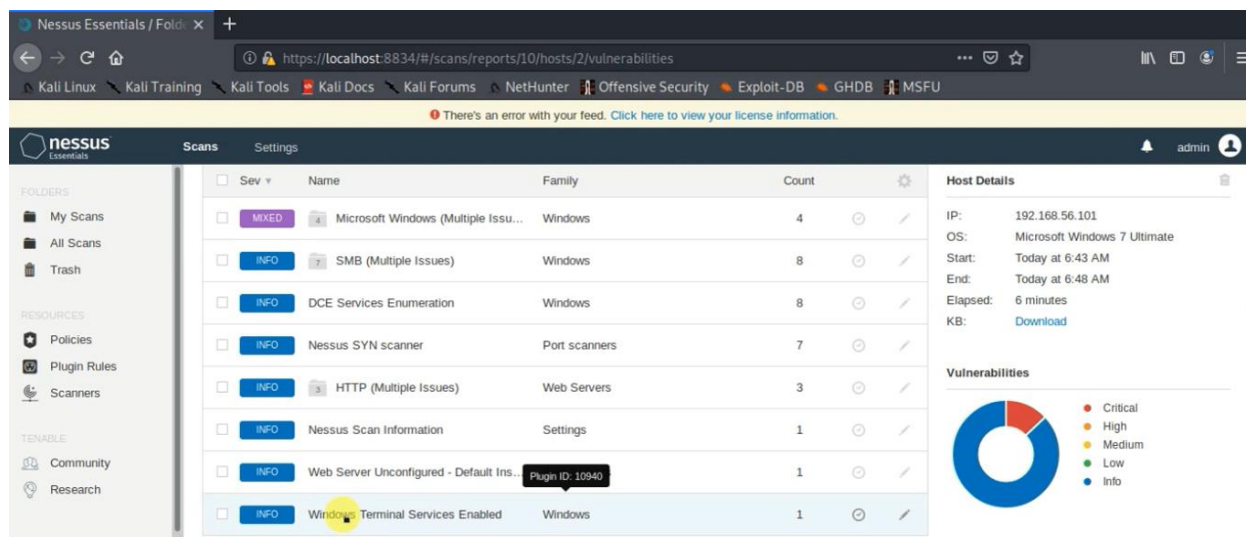


Figure 3.28: Available vulnerabilities

We can click on a vulnerability and then it will display the description of that and the solution for that. Therefore, click on “Windows Services Terminal Enabled”.

According to the given description, terminal services allows a Windows user to remotely obtain a graphical login. The solution for that is, disabling terminal services if you do not use it and do not allow this service to run across the internet.

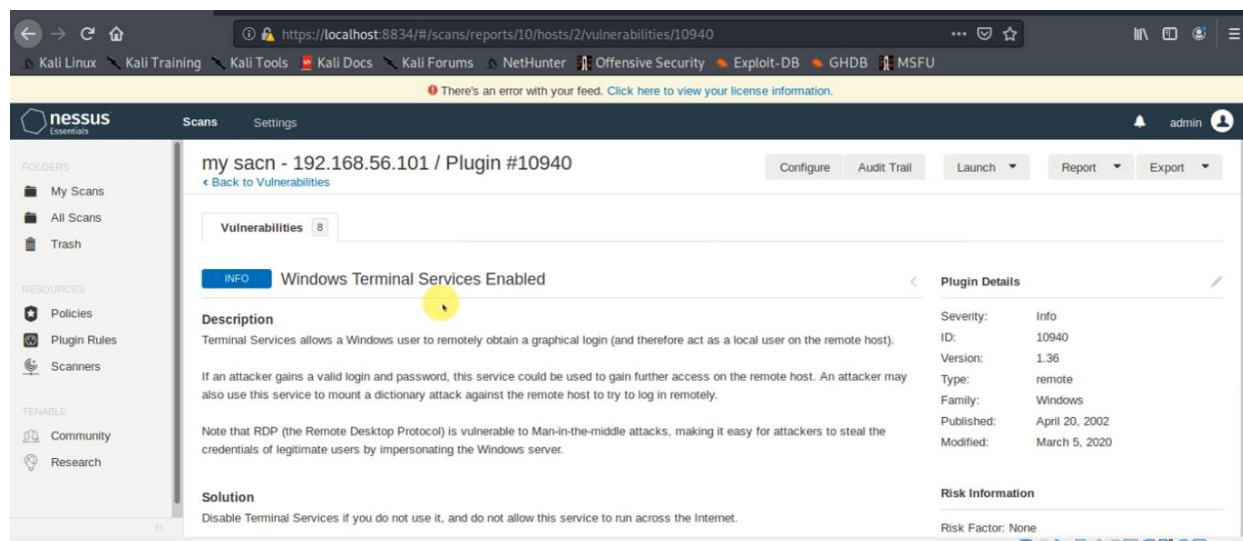


Figure 3.29: Windows Terminal Services Enabled

Then go back to the vulnerability list and click on “Mixed”. Then it will list down the critical vulnerabilities that are there.

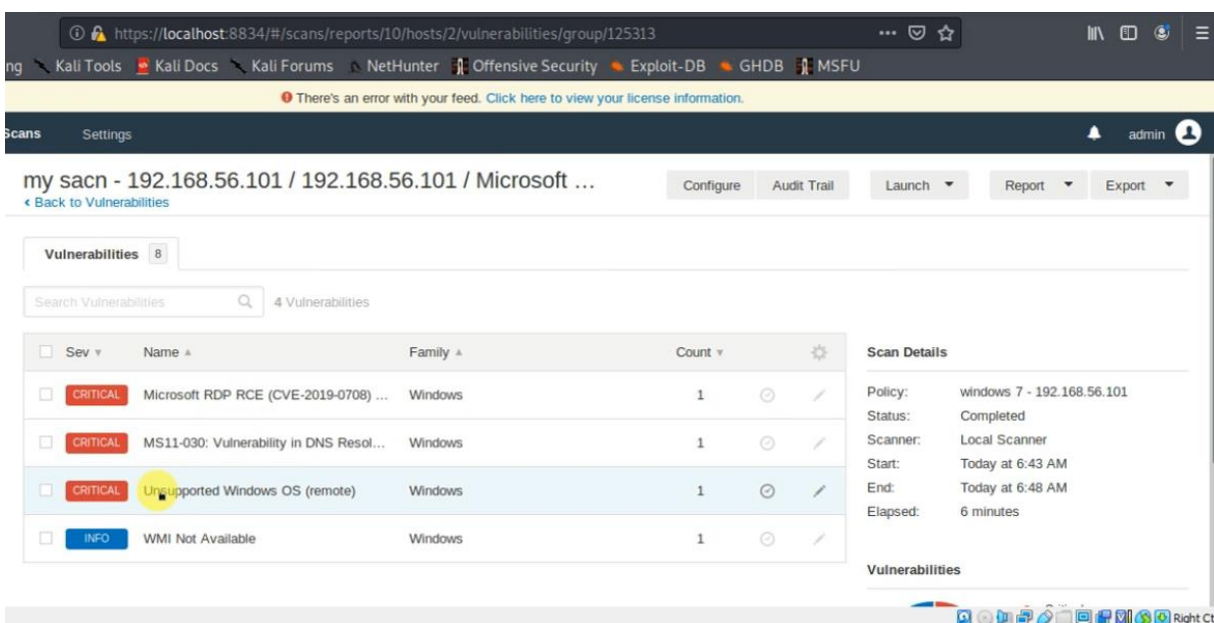


Figure 3.30: Critical Vulnerabilities

If we click on a vulnerability, it will show a description of that vulnerability and the solution for that.

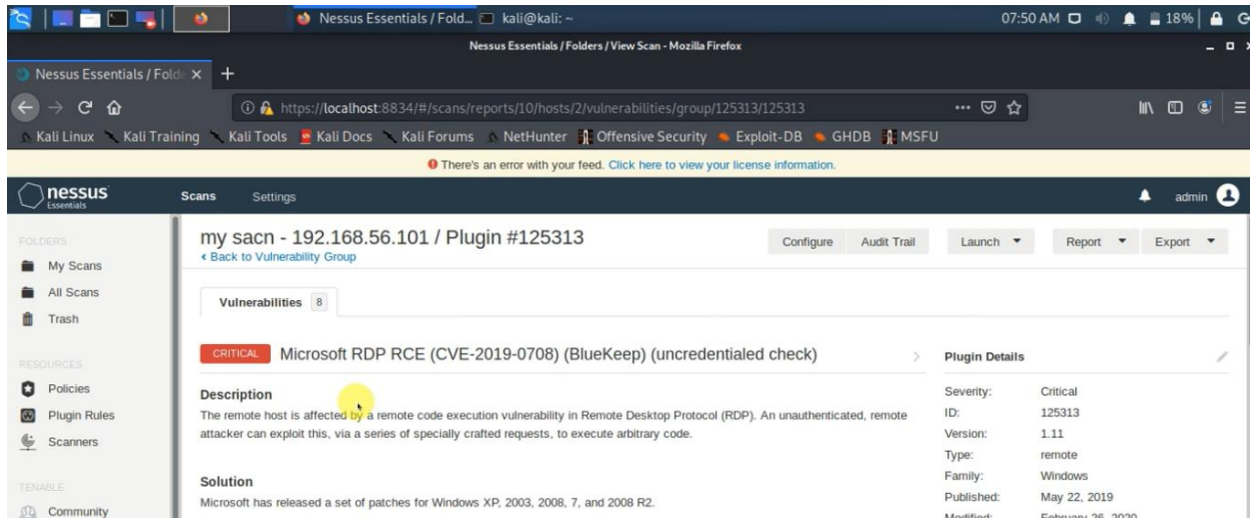


Figure 3.31: Critical Vulnerability 01 - Microsoft RDP RCE

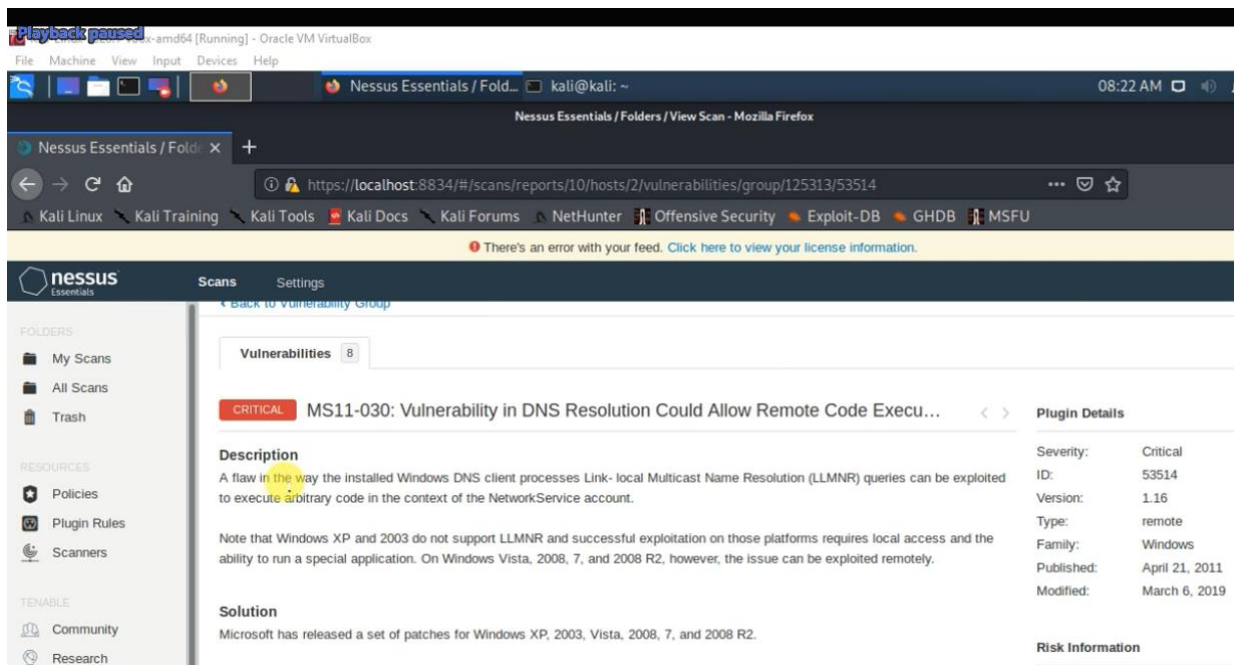


Figure 3.32: Critical Vulnerability 02 - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution

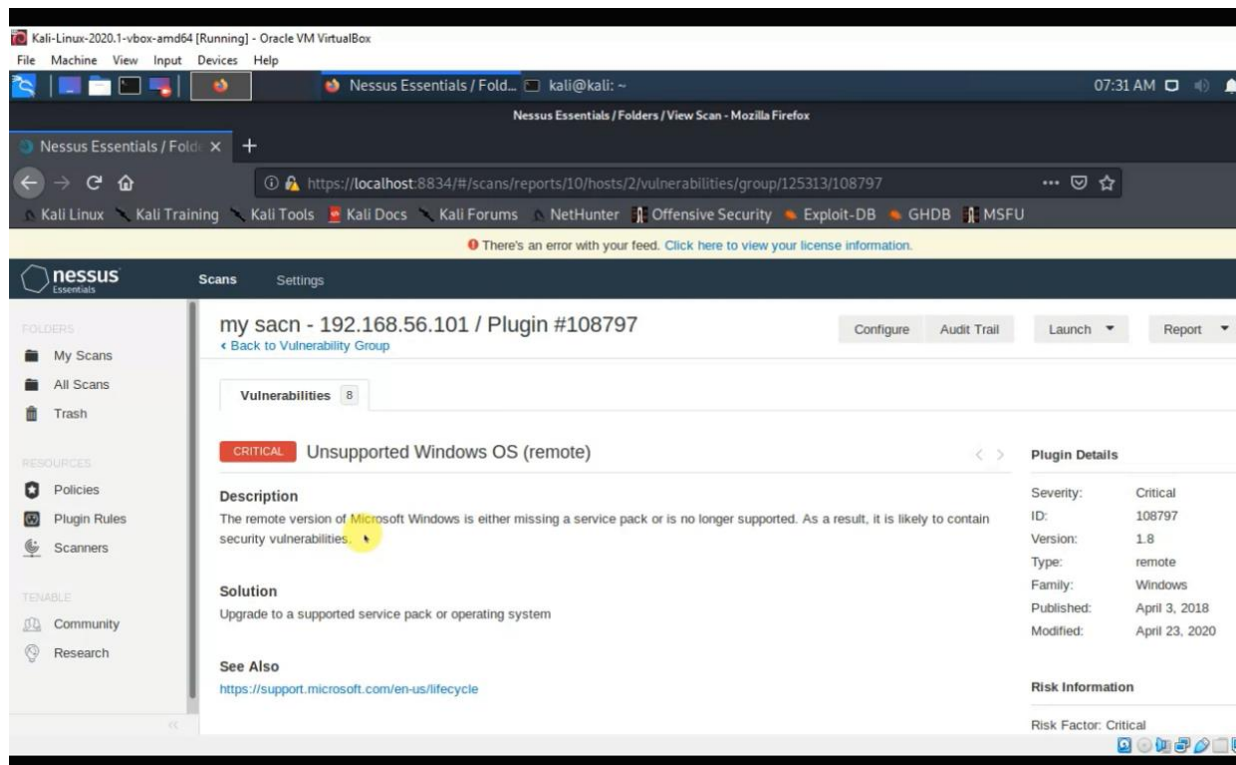


Figure 3.33: Critical Vulnerability 03 - Unsupported Windows OS (remote)

According to the vulnerability scan there are three critical issues.

Table 3.1: Summary of critical vulnerability

Critical Vulnerability	Description	Solution
MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution	A flaw in the way the installed Windows DNS client processes Link-local Multicast Name Resolution (LLMNR) queries can be exploited to execute arbitrary code in the context of the Network Service account.	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7 and 2008R2
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check)	The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP).	Microsoft has released a set of patches for Windows XP, 2003, 7 and 2008 R2
Unsupported Windows OS (remote)	The remote version of Microsoft Windows is either missing a service pack or is no longer supported.	Upgrade to a supported service pack or operating system

4 Conclusion

Based on the Windows 7 box auditing which was done according to the audit check list, which was discussed under audit scope, followings are the critical vulnerabilities.

1. Unsupported Windows OS (remote)
2. Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
3. MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution

Therefore, the operating system should be updated to the latest version.

References

- [1] "Computer auditing", *Unisa.ac.za*, 2020. [Online]. Available: <https://www.unisa.ac.za/sites/corporate/default/Colleges/Accounting-Sciences/Schools,-departments-&-centre/School-of-Accountancy/Department-of-Auditing/Fields-of-study/Computer-auditing>. [Accessed: 28- April- 2020].
- [2] "Nmap", *En.wikipedia.org*, 2020. [Online]. Available: <https://en.wikipedia.org/wiki/Nmap>. [Accessed: 01- May- 2020].
- [3] "Nessus", *Cs.cmu.edu*, 2020. [Online]. Available: <https://www.cs.cmu.edu/~dwendlan/personal/nessus.html>. [Accessed: 26- Apr- 2020].
- [4] "Computer Auditing", *Readyratios.com*, 2020. [Online]. Available: https://www.readyratios.com/reference/audit/computer_auditing.html. [Accessed: 23- Apr- 2020].
- [5] "Microsoft Windows 7 : List of security vulnerabilities", *Cvedetails.com*. [Online]. Available: <https://www.cvedetails.com/>. [Accessed: 10- May- 2020].