SLIIT

COMPUTING | BUSINESS | ENGINEERING

Information Assurance & Auditing (IE4040)

4th Year, 1st Semester

Assignment

IAA Mini Project

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

<<8th May 2020>>

Student Name	- K.H.M.I.N. Jayawardhana
Registration Nu:	- IT17378994
Batch	- CSNE-WE

TABLE OF CONTENTS

Page

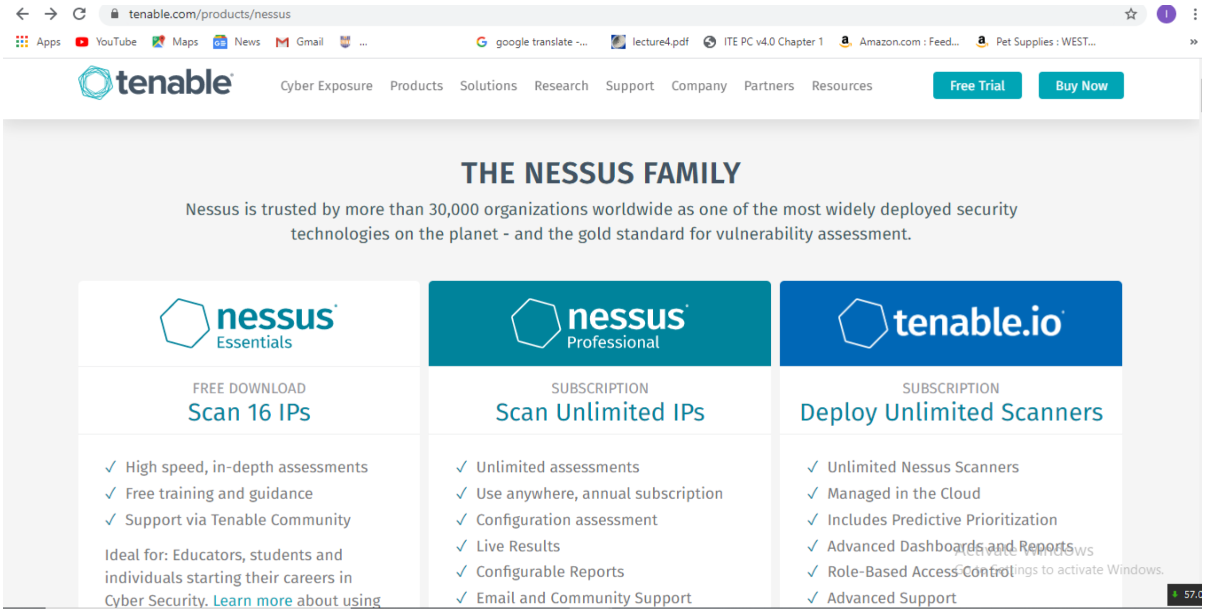
LIST OF FIGURES

1. INTRODUCTION

In the war against cybercrime, the hackers appear to be winning since as of every day we hear news of a massive data breach that was discovered only after millions of peoples' financial information was stolen and then likely bought or sold to an underground black market. These attacks can be carried out by both internal and external communities in order to gain personal economic benefits. To avert these risks, it is first important to define the term information security Audit. An information security audit is an audit on the level of information security in an organization [1] .security auditing is an essential task for modern enterprises that involves auditing organizations IT assets and policies. An audit can be helpful in exposing potential vulnerabilities as well as it provides a high-order overview of the network which can be useful when trying to solve specific problems. Audits can also give us an understanding of how protected our organization is against known security threats. Also An security audit can be helpful to Identify potential risks and threats that are most likely to affect the organization, to prevent security breaches and reduce impact of breaches, Keep technology up-to-date, Keep sensitive data protected, Keep compliance programs up to date, Keep the organization on top of current and new security practice, Keep the organization on top of current and new security practices…etc are some benefits of doing regular audits [2]. There are many different types of security audits. Some audits are specifically designed to make sure that the organization is legally compliant and others are focus on recognizing potential vulnerabilities in the organizational IT infrastructure. Risk assessment, Vulnerability assessment, Penetration test and Compliance audit are the main four types of security audits we should regularly conduct to keep our business running in excellent order [3]. Most of the organizations use several type of security auditing tools for their auditing purposes. Nessus, Metasploit**,** OpenVAS, ManageEngine AdAudit Plus, Network Inventory Advisor, Kaseya VSA, Acunetix, Netwrix Auditor and Wireshark are some best network security auditing tools that use in most of organizations in the world. In this assessment we are going to scan vulnerabilities in windows 10 machine using Nessus vulnerability scanner and the kali Linux operating system in virtual box environment.

2. NESSUS VULNERABILITY SCANNER

Nessus is a proprietary vulnerability assessment tool developed by Tenable, Inc. Nessus can be used for auditing**,** configuration management**,** patch management purposes and it supports variety of operating systems and platforms including Mac, Linux, and Windows. Nessus is trusted by thousands of organizations worldwide as one of the most widely deployed security technologies on the planet and the gold standard for vulnerability assessment [4]. Nessus supports over 450 different configuration templates and that variety makes it easy to find the vulnerabilities we need**.** Basic network scan, Advanced scan, Advanced dynamic scan, Malware Scan, Host discovery, Mobile device scan, Web application test, Credentialed patch audit, Badlock detection…etc. are some examples for configuration templates. Nessus Essentials version is available for free and can scan up to 16 IPs. Paid versions named Nessus professional and Tenable.io comes with yearly subscriptions and unlimited IPs and scanners. After scan we can also generate Hosts executive summary report or Custom report and can see how many hosts are categorized as Critical, High, Medium, Low, and Informational vulnerabilities. These Reports can be created in HTML, CSV or PDF as we prefer [5]. In this assessment we are going to scan vulnerabilities in windows 10 machine using Nessus vulnerability scanner and the kali Linux operating system in virtual box environment.



THE NESSUS FAMILY

Nessus is trusted by more than 30,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.

FREE DOWNLOAD
Scan 16 IPs

- ✓ High speed, in-depth assessments
- ✓ Free training and guidance
- ✓ Support via Tenable Community

Ideal for: Educators, students and individuals starting their careers in Cyber Security. Learn more about using

SUBSCRIPTION
Scan Unlimited IPs

- ✓ Unlimited assessments
- ✓ Use anywhere, annual subscription
- ✓ Configuration assessment
- ✓ Live Results
- ✓ Configurable Reports
- ✓ Email and Community Support

SUBSCRIPTION
Deploy Unlimited Scanners

- ✓ Unlimited Nessus Scanners
- ✓ Managed in the Cloud
- ✓ Includes Predictive Prioritization
- ✓ Advanced Dashboards and Reports
- ✓ Role-Based Access Control
- ✓ Advanced Support

Figure 2.1: Nessus vulnerability scanner

3. AUDITING / SCANNING PROCESS

- ❖ Here we are going to scan vulnerabilities in windows 10 machine using Nessus vulnerability scanner and the kali Linux operating system in virtual box environment.

1. In first, we have to install Windows 10 & Kali Linux into two oracle virtual boxes and after that the Nessus vulnerability scanner should be download and install into the kali Linux operating system. In this task we are using Nessus Essentials version is available for free and can scan up to 16 IPs.

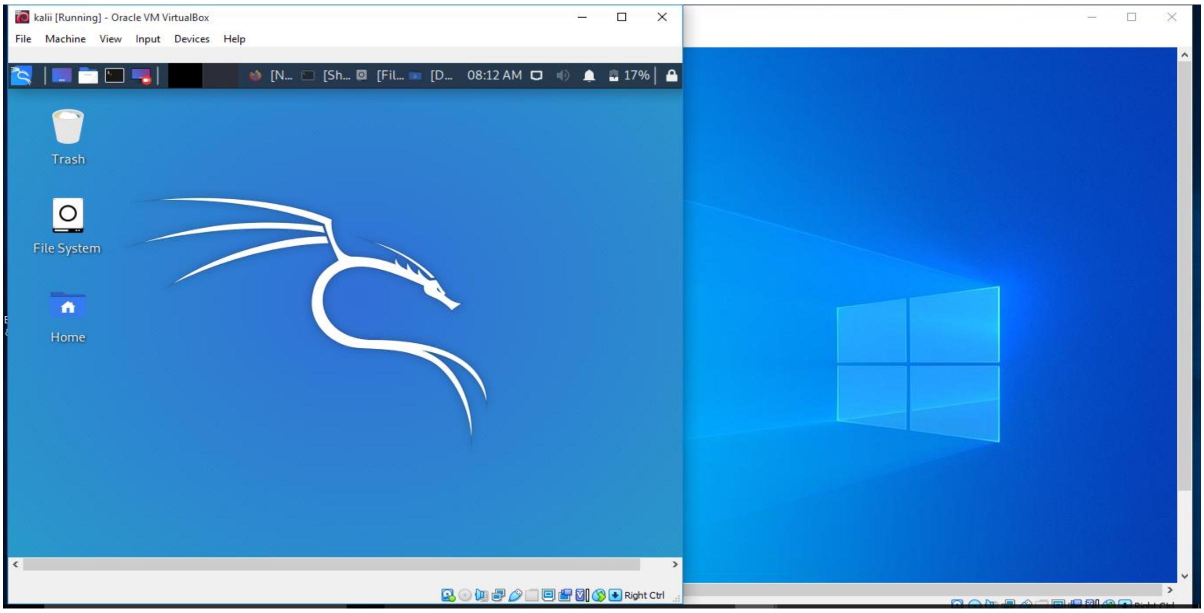
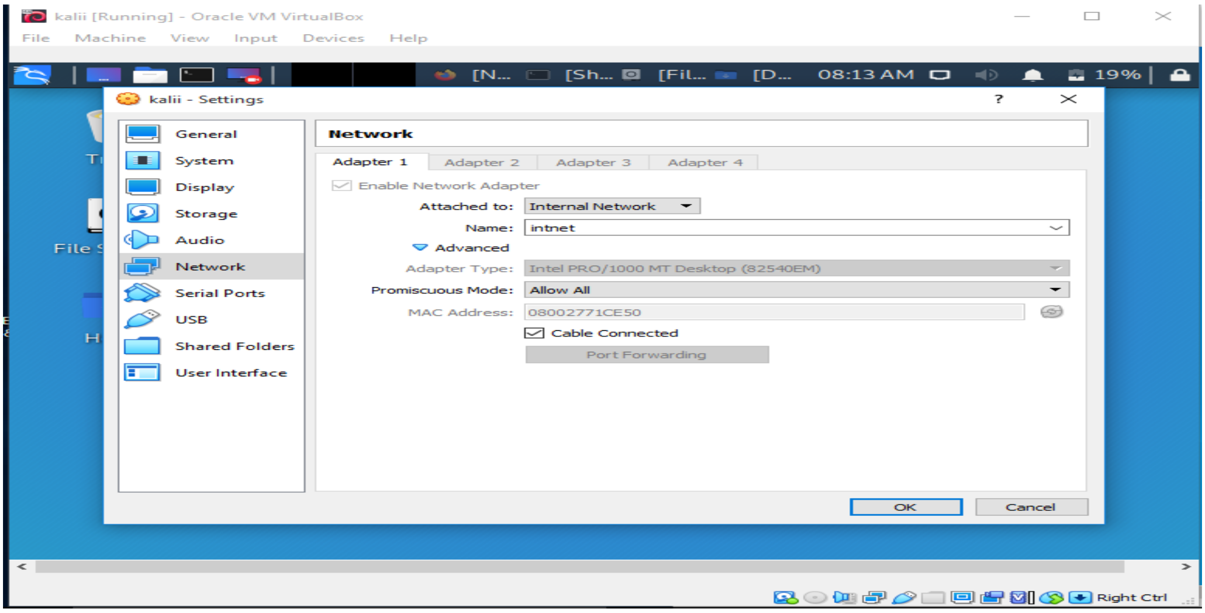


Figure 3.1: Windows 10 & Kali Linux in virtual box environment

2. Next step is to set Virtual networking that required to carry out our vulnerability scan. For that, add an internal network adapter in both virtual machines by choosing intent internal network option [6].



Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet

Advanced

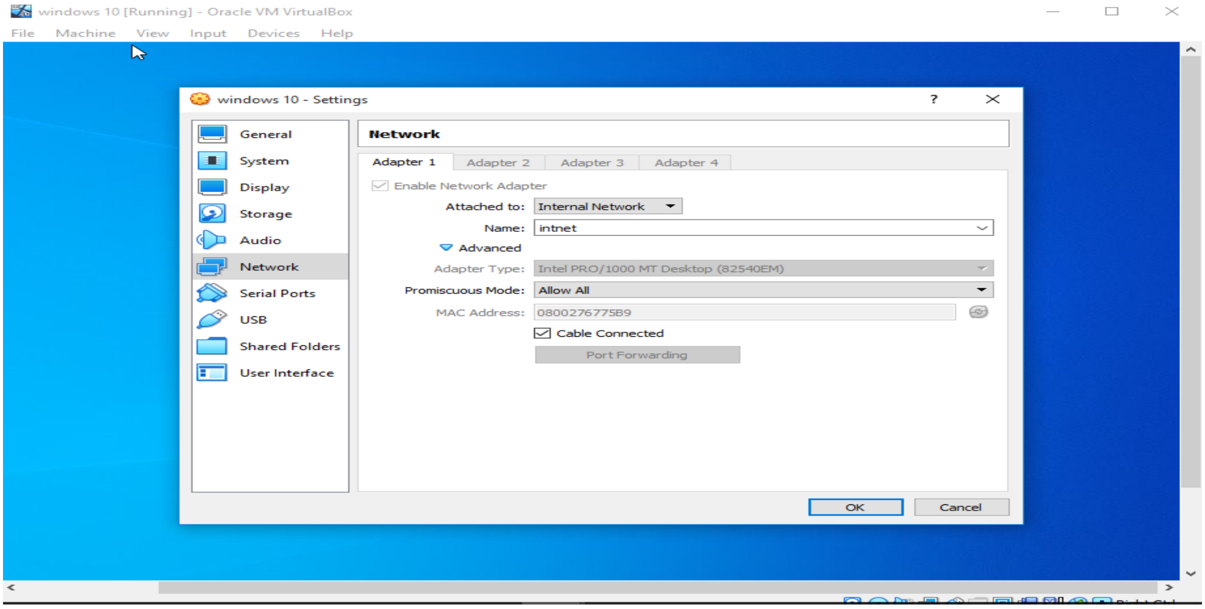
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 08002771CE50

☑ Cable Connected

Figure 3.2: Virtual network Settings in Windows 10



Network

☑ Enable Network Adapter

Attached to: Internal Network

Name: intnet

Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

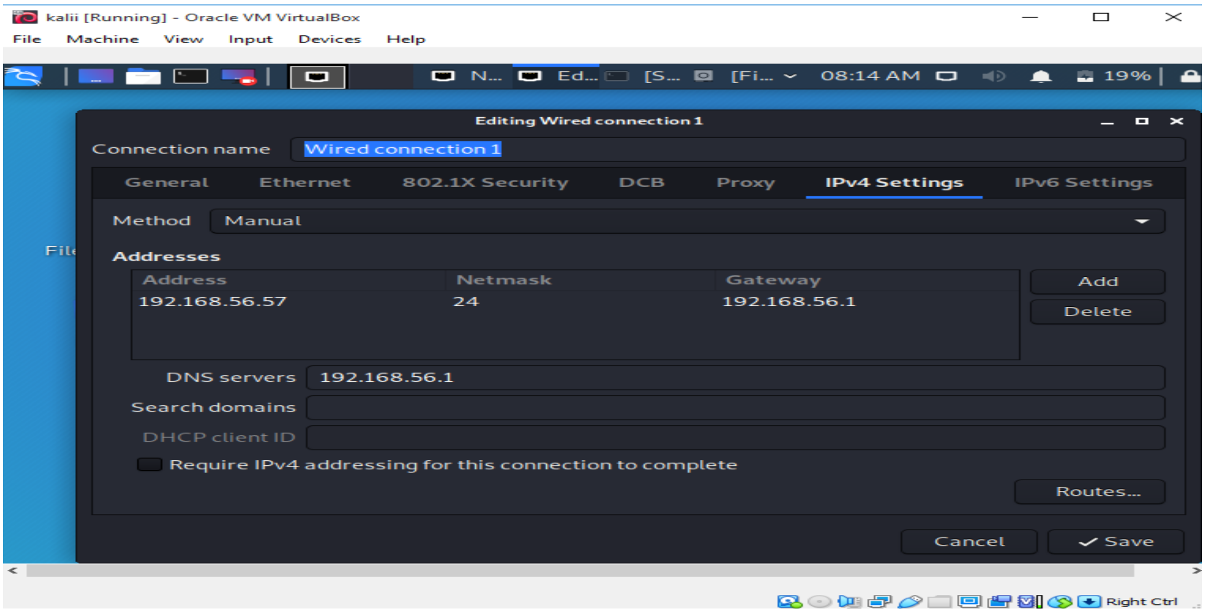
Promiscuous Mode: Allow All

MAC Address: 0800276775B9

☑ Cable Connected

Figure 3.3: Virtual network Settings in Kali Linux

3. We now need to assign a static ip address for the kali Linux instance since it's on a host-only network. As well as kali, configure the networking settings for the Ethernet adapter on windows 10 machine. Both machines ip addresses should in the same subnet range.



kalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
08:14 AM
19%
Editing Wired connection 1
General Ethernet 802.1X Security DCB Proxy IPv4 Settings IPv6 Settings
Add
Delete
Routes...
Cancel
✓ Save
Right Ctrl

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.56.57	24	192.168.56.1

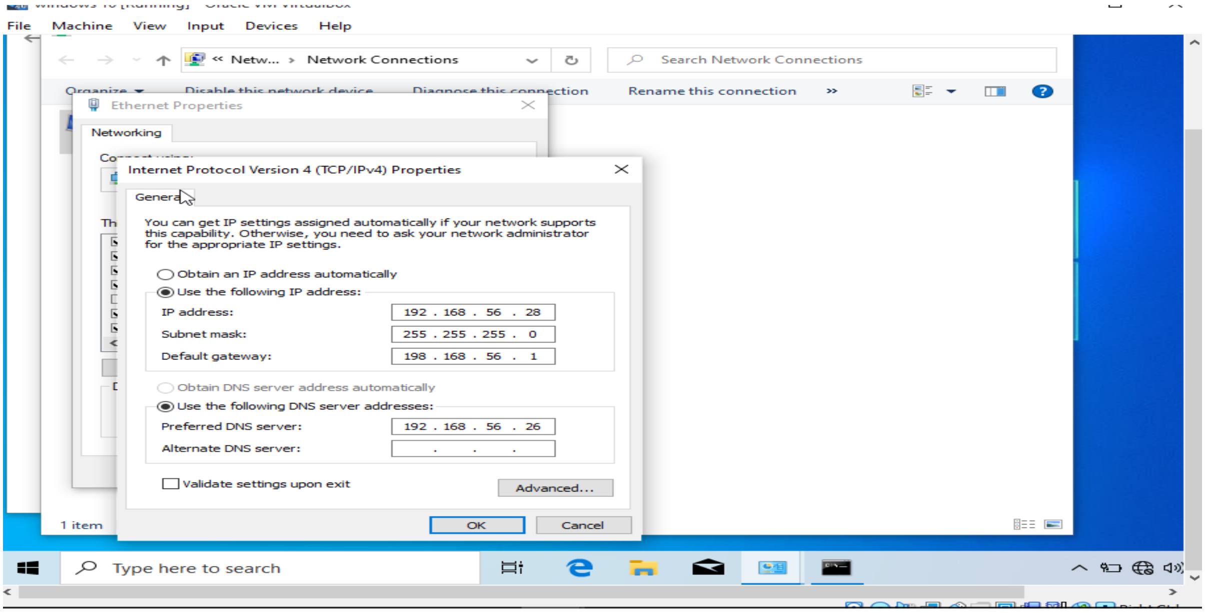
DNS servers: 192.168.56.1

Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

Figure 3.4: Assign static ip address for the kali Linux



File Machine View Input Devices Help
« Netw... › Network Connections
Search Network Connections
Organize ▾ Disable this network device Diagnose this connection Rename this connection »
Ethernet Properties
Networking
1 item
Type here to search
OK
Cancel
Advanced...

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 56 . 28

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 198 . 168 . 56 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

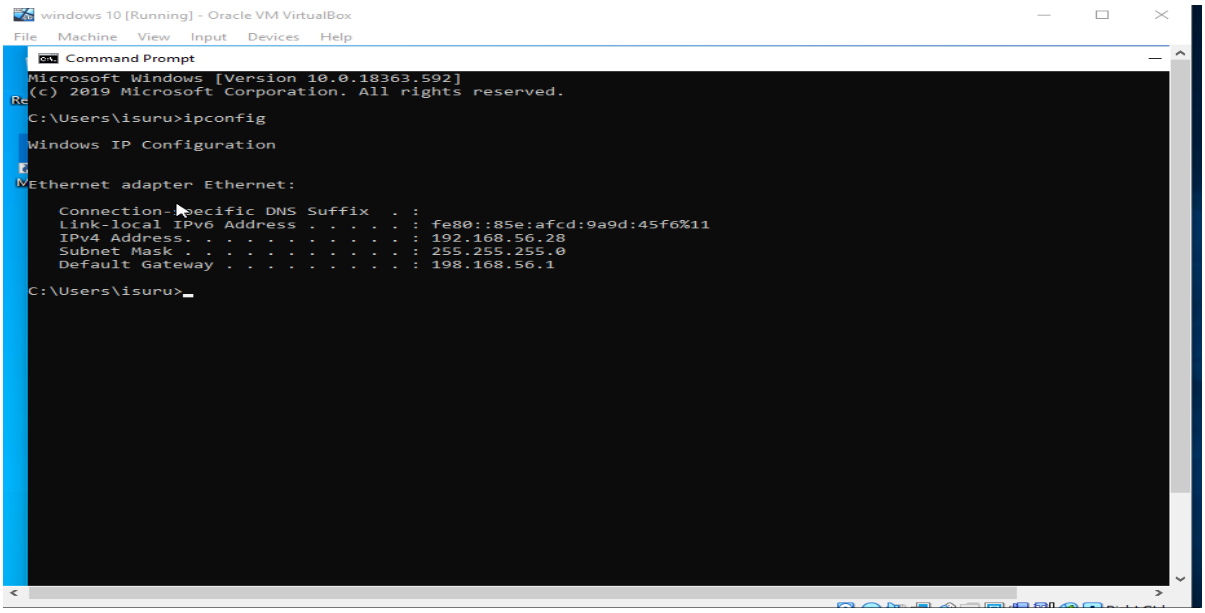
Preferred DNS server: 192 . 168 . 56 . 26

Alternate DNS server: . . .

□ Validate settings upon exit

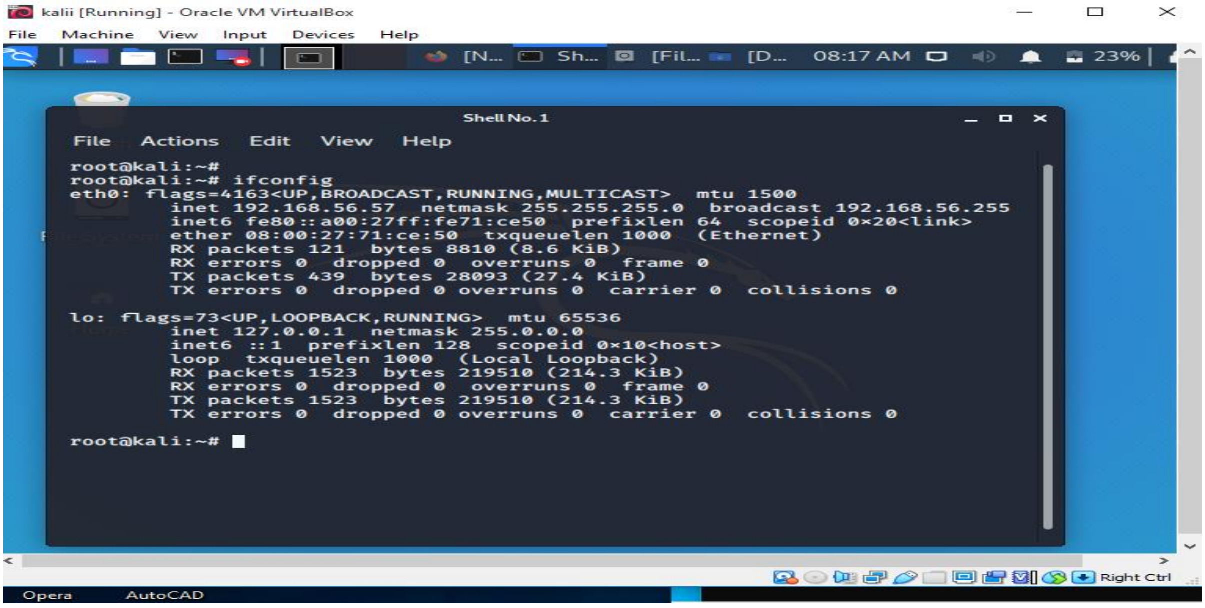
Figure 3.5: Network settings of Ethernet adapter on windows 10

4. After that, check ip addresses of both machines and check the connection between two virtual machines by Pinging from Kali to Windows 10 machine.(Note - disable the firewalls in the windows 10 machine)


windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt

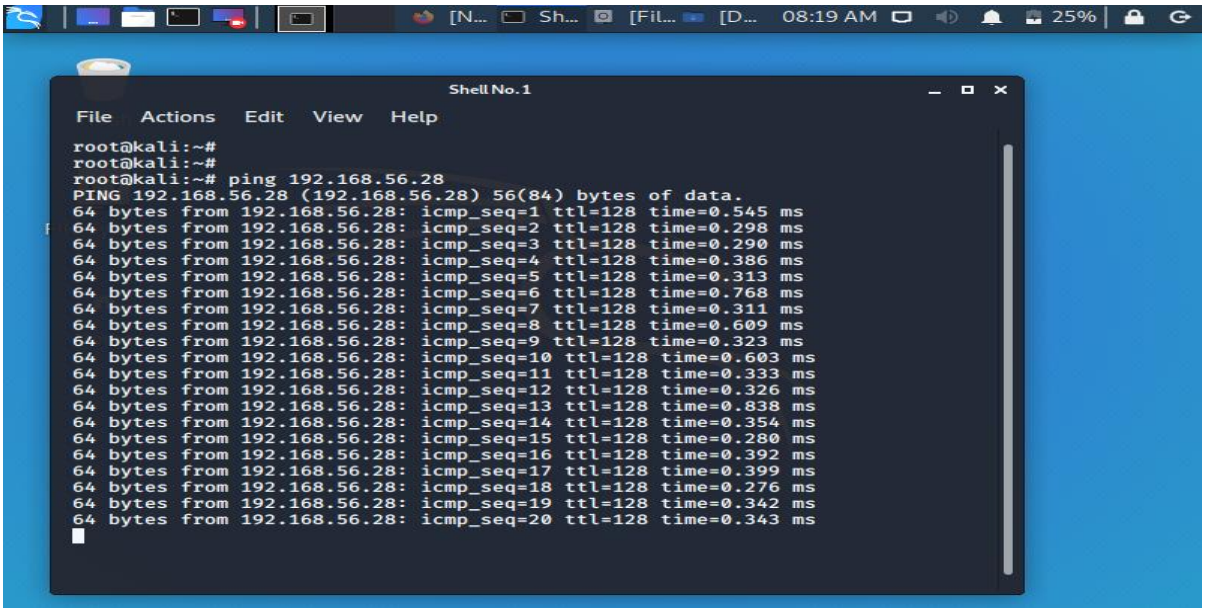
```
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\isuru>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::85e:afcd:9a9d:45f6%11
   IPv4 Address. . . . . . . . . . . : 192.168.56.28
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 198.168.56.1

C:\Users\isuru>_
```

Figure 3.6: Checking ip address of windows 10


kalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[N... Sh... [Fil... [D... 08:17 AM 23%
Shell No. 1
File Actions Edit View Help
Right Ctrl
Opera AutoCAD

```
root@kali:~#
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.57  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::a00:27ff:fe71:ce50  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:71:ce:50  txqueuelen 1000  (Ethernet)
        RX packets 121  bytes 8810 (8.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 439  bytes 28093 (27.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1523  bytes 219510 (214.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1523  bytes 219510 (214.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# █
```

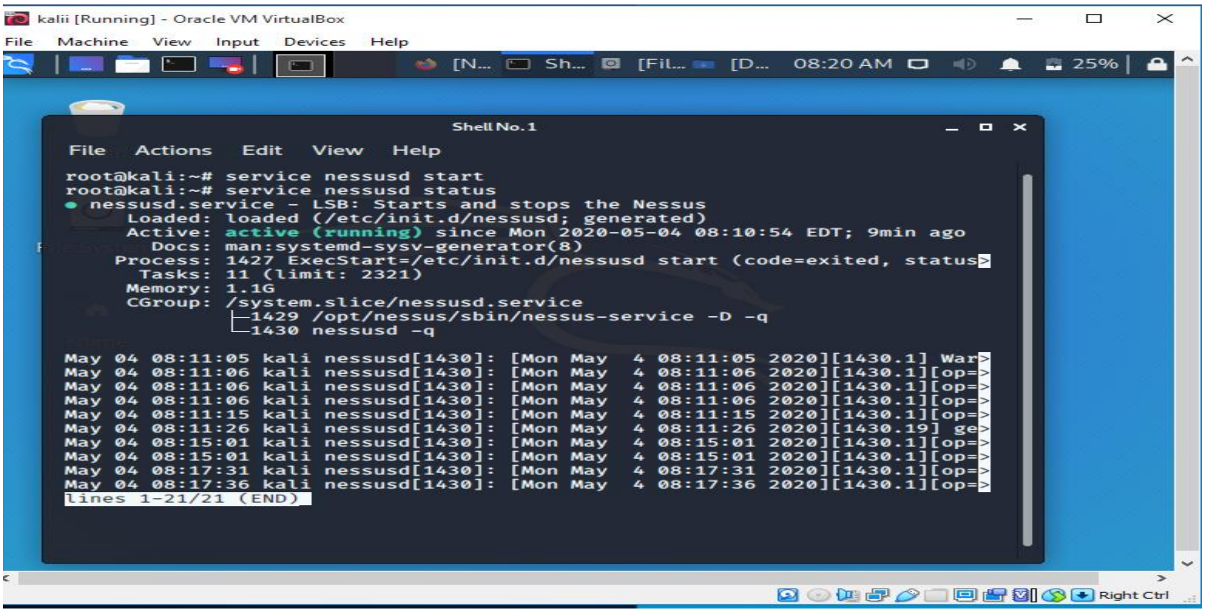
Figure 3.7: Checking ip address of Kali Linux



```
root@kali:~#
root@kali:~#
root@kali:~# ping 192.168.56.28
PING 192.168.56.28 (192.168.56.28) 56(84) bytes of data.
64 bytes from 192.168.56.28: icmp_seq=1 ttl=128 time=0.545 ms
64 bytes from 192.168.56.28: icmp_seq=2 ttl=128 time=0.298 ms
64 bytes from 192.168.56.28: icmp_seq=3 ttl=128 time=0.290 ms
64 bytes from 192.168.56.28: icmp_seq=4 ttl=128 time=0.386 ms
64 bytes from 192.168.56.28: icmp_seq=5 ttl=128 time=0.313 ms
64 bytes from 192.168.56.28: icmp_seq=6 ttl=128 time=0.768 ms
64 bytes from 192.168.56.28: icmp_seq=7 ttl=128 time=0.311 ms
64 bytes from 192.168.56.28: icmp_seq=8 ttl=128 time=0.609 ms
64 bytes from 192.168.56.28: icmp_seq=9 ttl=128 time=0.323 ms
64 bytes from 192.168.56.28: icmp_seq=10 ttl=128 time=0.603 ms
64 bytes from 192.168.56.28: icmp_seq=11 ttl=128 time=0.333 ms
64 bytes from 192.168.56.28: icmp_seq=12 ttl=128 time=0.326 ms
64 bytes from 192.168.56.28: icmp_seq=13 ttl=128 time=0.838 ms
64 bytes from 192.168.56.28: icmp_seq=14 ttl=128 time=0.354 ms
64 bytes from 192.168.56.28: icmp_seq=15 ttl=128 time=0.280 ms
64 bytes from 192.168.56.28: icmp_seq=16 ttl=128 time=0.392 ms
64 bytes from 192.168.56.28: icmp_seq=17 ttl=128 time=0.399 ms
64 bytes from 192.168.56.28: icmp_seq=18 ttl=128 time=0.276 ms
64 bytes from 192.168.56.28: icmp_seq=19 ttl=128 time=0.342 ms
64 bytes from 192.168.56.28: icmp_seq=20 ttl=128 time=0.343 ms
```

Figure 3.8: Checking connection between two virtual machines

5. Start Nessus Scanner by typing > service nessusd start


kalii [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Shell No. 1
File Actions Edit View Help
08:20 AM
Right Ctrl

```
root@kali:~# service nessusd start
root@kali:~# service nessusd status
● nessusd.service - LSB: Starts and stops the Nessus
   Loaded: loaded (/etc/init.d/nessusd; generated)
   Active: active (running) since Mon 2020-05-04 08:10:54 EDT; 9min ago
     Docs: man:systemd-sysv-generator(8)
  Process: 1427 ExecStart=/etc/init.d/nessusd start (code=exited, status>
    Tasks: 11 (limit: 2321)
   Memory: 1.1G
   CGroup: /system.slice/nessusd.service
           ├─1429 /opt/nessus/sbin/nessus-service -D -q
           └─1430 nessusd -q

May 04 08:11:05 kali nessusd[1430]: [Mon May  4 08:11:05 2020][1430.1] War>
May 04 08:11:06 kali nessusd[1430]: [Mon May  4 08:11:06 2020][1430.1][op=>
May 04 08:11:06 kali nessusd[1430]: [Mon May  4 08:11:06 2020][1430.1][op=>
May 04 08:11:06 kali nessusd[1430]: [Mon May  4 08:11:06 2020][1430.1][op=>
May 04 08:11:15 kali nessusd[1430]: [Mon May  4 08:11:15 2020][1430.1][op=>
May 04 08:11:26 kali nessusd[1430]: [Mon May  4 08:11:26 2020][1430.19] ge>
May 04 08:15:01 kali nessusd[1430]: [Mon May  4 08:15:01 2020][1430.1][op=>
May 04 08:15:01 kali nessusd[1430]: [Mon May  4 08:15:01 2020][1430.1][op=>
May 04 08:17:31 kali nessusd[1430]: [Mon May  4 08:17:31 2020][1430.1][op=>
May 04 08:17:36 kali nessusd[1430]: [Mon May  4 08:17:36 2020][1430.1][op=>
lines 1-21/21 (END)
```

Figure 3.9: Start Nessus

6. Then go to https://kali:8834/ and Login to the Nessus by providing username and password.

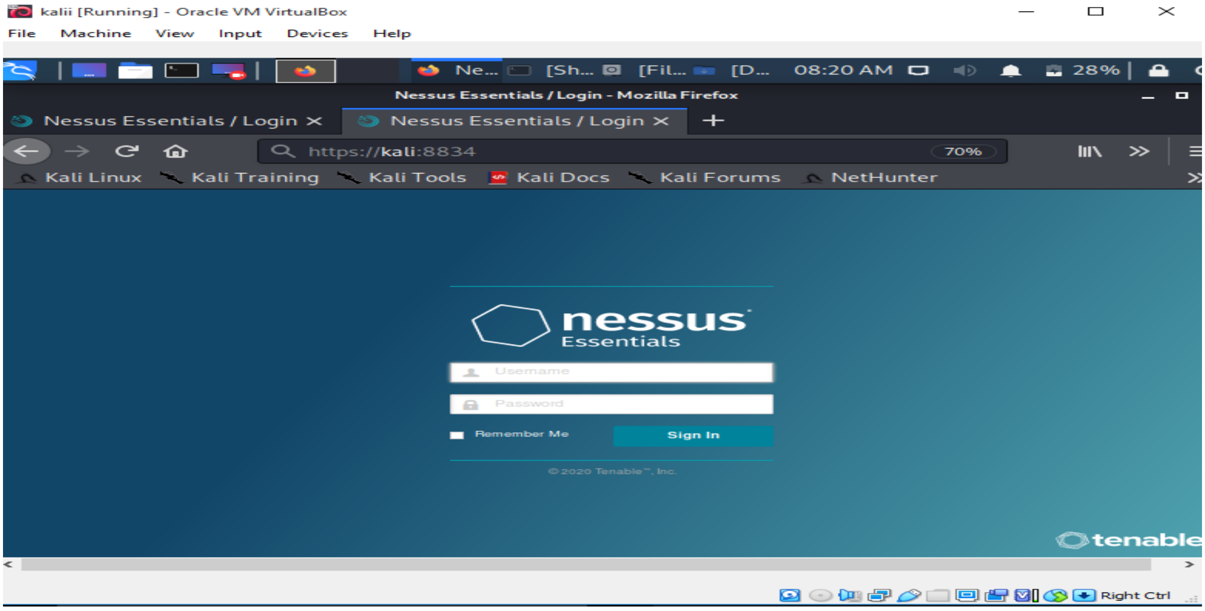
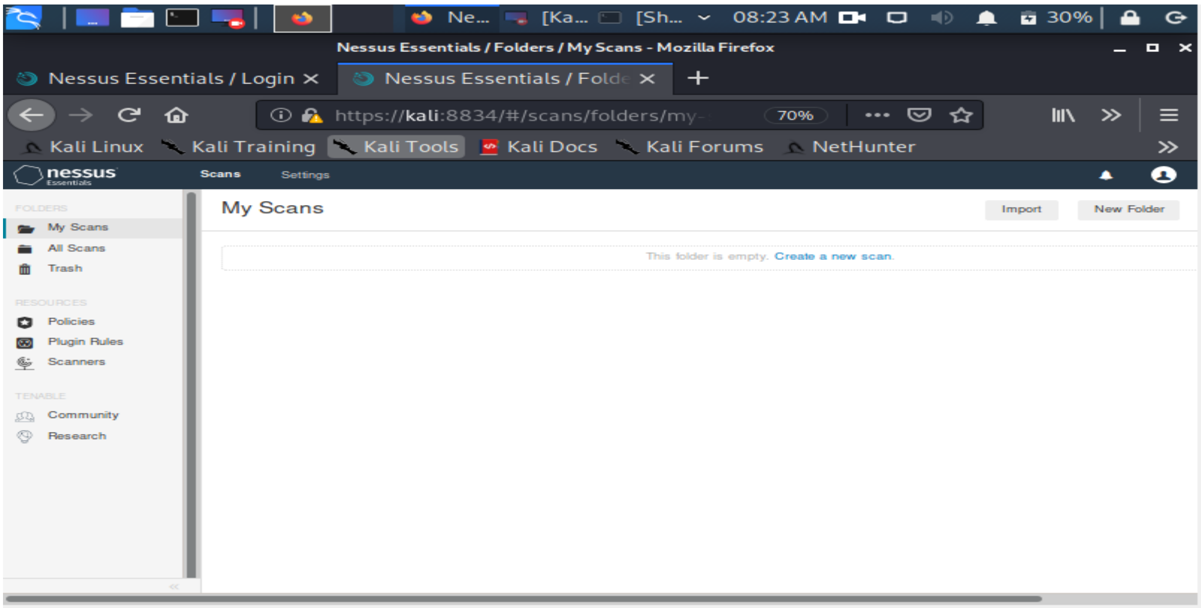


Figure 3.10: Log in to Nessus

7. Click on create new scan and choose the "basic network scan" .Give the scan a name and In the Targets field put the ip address of the Windows 10 host. Then Save the new scan.



This folder is empty. Create a new scan.

Figure 3.11: Create new scan

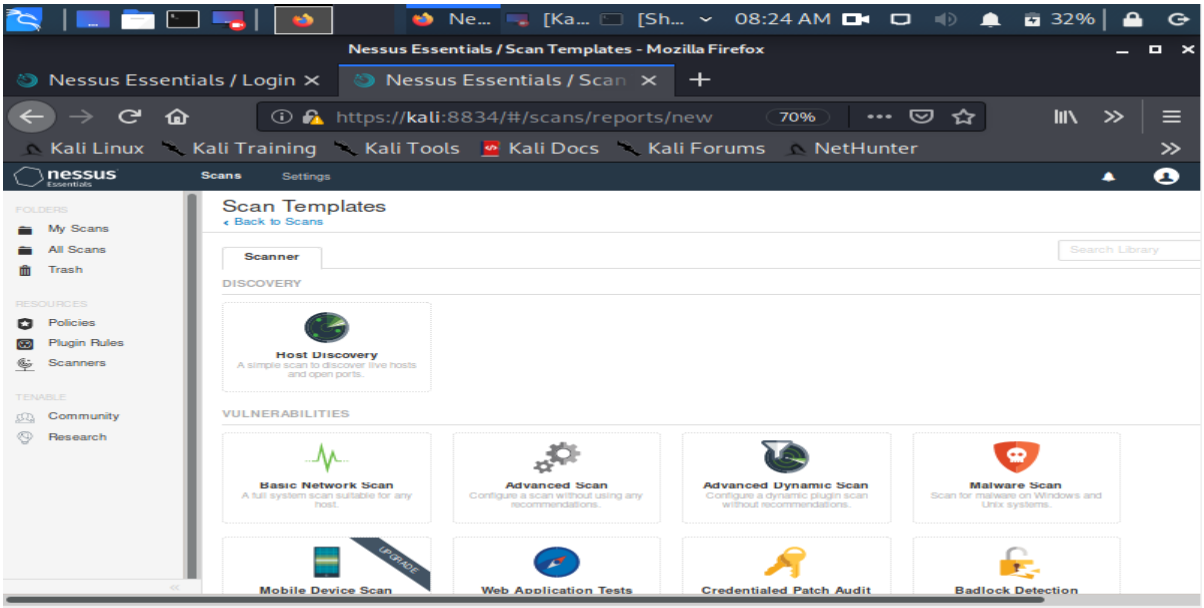
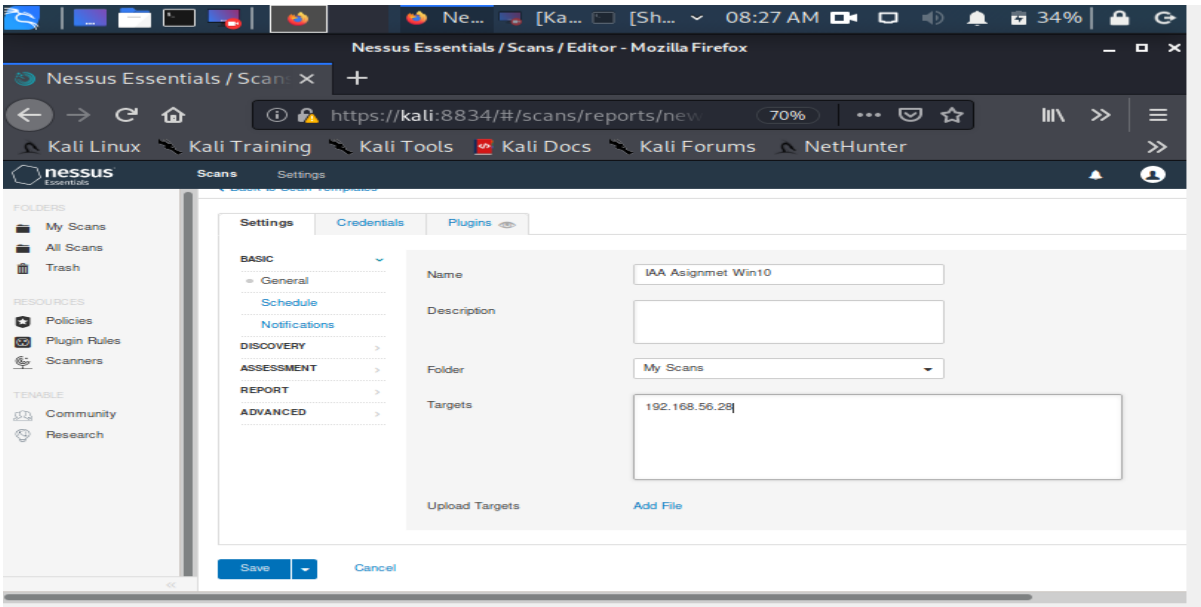


Figure 3.12: Scan template selection



Name: IAA Asignmet Win10

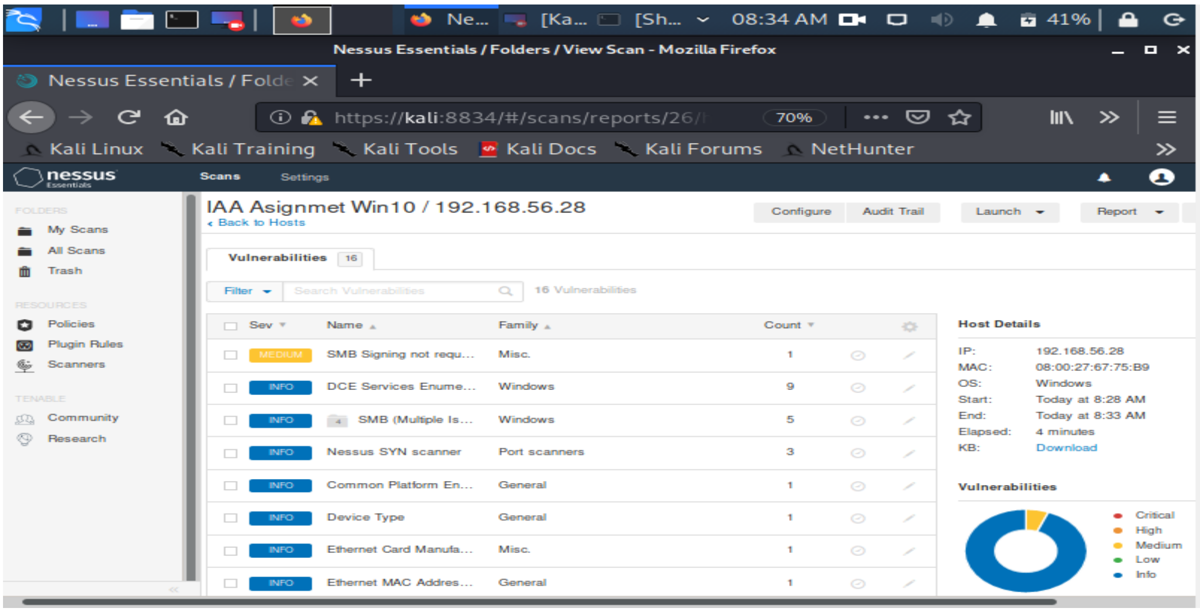
Description:

Folder: My Scans

Targets: 192.168.56.28

Figure 3.13: Enter Scanning details

8. Click on My Scans. Now click Launch on the selected scan that we configured. After completed the scan, results are stored in the My Scans folder on the dashboard. In result, vulnerabilities are categorized as Critical, High, Medium, Low and Informational levels.



IAA Asignmet Win10 / 192.168.56.28

‹ Back to Hosts

Vulnerabilities 16

16 Vulnerabilities

Sev	Name	Family	Count
MEDIUM	SMB Signing not requ...	Misc.	1
INFO	DCE Services Enume...	Windows	9
INFO	4 SMB (Multiple Is...	Windows	5
INFO	Nessus SYN scanner	Port scanners	3
INFO	Common Platform En...	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufa...	Misc.	1
INFO	Ethernet MAC Addres...	General	1

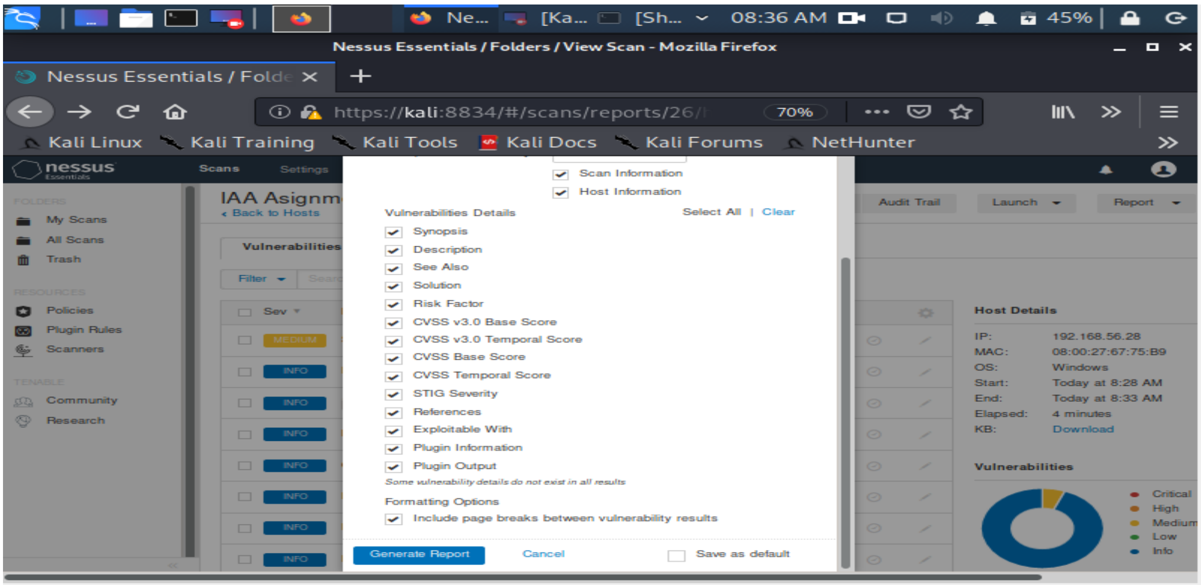
Host Details

IP:	192.168.56.28
MAC:	08:00:27:67:75:B9
OS:	Windows
Start:	Today at 8:28 AM
End:	Today at 8:33 AM
Elapsed:	4 minutes
KB:	Download

Vulnerabilities

Figure 3.14: Scan result

9. Hosts executive summary or Custom Report can be created in HTML, CSV or PDF as we prefer



☑ Scan Information
☑ Host Information

Vulnerabilities Details — Select All | Clear

☑ Synopsis
☑ Description
☑ See Also
☑ Solution
☑ Risk Factor
☑ CVSS v3.0 Base Score
☑ CVSS v3.0 Temporal Score
☑ CVSS Base Score
☑ CVSS Temporal Score
☑ STIG Severity
☑ References
☑ Exploitable With
☑ Plugin Information
☑ Plugin Output

Some vulnerability details do not exist in all results

Formatting Options

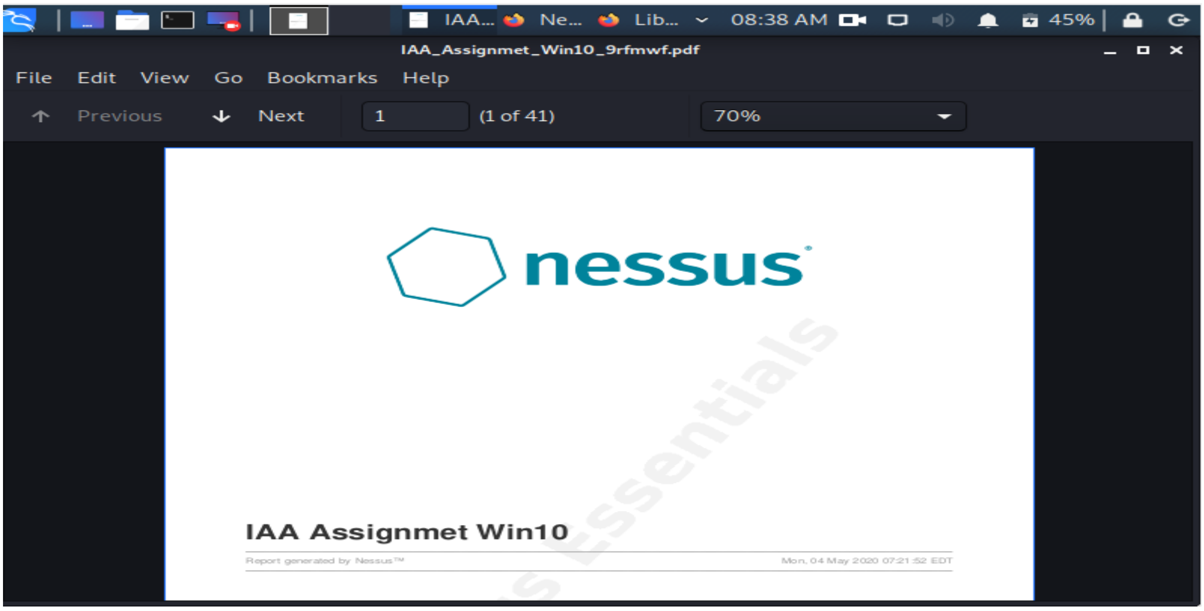
☑ Include page breaks between vulnerability results

Generate Report   Cancel   □ Save as default

Host Details

IP:	192.168.56.28
MAC:	08:00:27:67:75:B9
OS:	Windows
Start:	Today at 8:28 AM
End:	Today at 8:33 AM
Elapsed:	4 minutes
KB:	Download

Figure 3.15: Summary report



IAA Assignmet Win10

Report generated by Nessus™ Mon, 04 May 2020 07:21:52 EDT

Figure 3.16: Summary report

REFERENCES

[1]"Information security audit", *En.wikipedia.org*, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Information_security_audit. [Accessed: 01- May- 2020].

[2]"The Importance of Regular IT Security Audits | Spectrum IT Solutions, LLC", *Spectrum IT Solutions, LLC*, 2020. [Online]. Available: https://www.itbyspectrum.com/the-importance-of-regular-it-security-audits/. [Accessed: 05- May- 2020].

[3]"4 Types Of Security Audits Every Business Should Conduct Regularly | SugarShot", *SugarShot*, 2020. [Online]. Available: https://www.sugarshot.io/types-of-security-audits-every-business-should-conduct-regularly/. [Accessed: 04- May- 2020].

[4]"Nessus Product Family", *Tenable®*, 2020. [Online]. Available: https://www.tenable.com/products/nessus. [Accessed: 07- May- 2020].

[5]"11 Best Network Security Auditing Tools - Full reviews with Free Trial Links", *Comparitech*, 2020. [Online]. Available: https://www.comparitech.com/net-admin/network-security-auditing-tools/. [Accessed: 06- May- 2020].

[6]"Start Using Nessus for Free In 5 Steps - ethicalhackingguru.com", *ethicalhackingguru.com*, 2020. [Online]. Available: https://ethicalhackingguru.com/how-to-use-nessus-at-home-in-5-steps/. [Accessed: 05- May- 2020].