National College of Ireland

Project Submission Sheet

Student Name: Matthew Browne

Student ID: x21174415@student.ncirl.ie

Programme: MSc/PGD in Cybersecurity **Year:** 1

Module: Malware Analysis (H9MWAN)

Lecturer: Michael Pantridge MSc/PGD

Submission Due Date: 26th June 2025

Project Title: Malware Lab & Research-based Malware Analysis

Word Count: Pending 6311

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Matthew Browne

Date: 26th June 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**

5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

[Malware Analysis (H9MWAN)]

Your Name/Student Number	**Course**	**Date**
Name: Matthew Browne Student Number: x21174415	MSc/PGD in Cybersecurity	26/06/2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	**Brief Description**	**Link to tool**

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

Evidence of AI Usage
This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.
Additional Evidence:
[Place evidence here]

Continuous Assessment Name	Malware Lab & Research-based Malware Analysis.
Student Name	Matthew Browne
Student ID	x21174415
Student Email	x21174415@student.ncirl.ie

Malware Lab & Research-based Malware Analysis.

Matthew Browne
Microsoft MVP & CITP
E-mail*x21174415@student.ncirl.ie*

Contents

AI Acknowledgment 2
Description of AI Usage 2
Evidence of AI Usage 3
Additional Evidence: 3
Abstract 4
1. Introduction 5
2. Part A: Analysis of Existing Sandbox 5
3. Part B: Virtual Machine Setup 6
4. Part C: Software Tools 8
5. Part D: Lab Testing 9
Step 1: IP Allocation and Reservation 9
Step 2: Virtual Machine Network Switch 9
Assignment 9
Step 3: Securing the Virtual Machine on the 9
Hypervisor 9
Step 4: Test virtual Machine interconnectivity and 9
test Virtual machine connections to other networks. 9
Step 5: Additional Safety and Precautions 9
6. Section 2: Research-based Malware 10

Analysis (QBOT) 10
Introduction 10
Part A: Identification 10
Part B: Analysis 11
7. Looking at the flow of QBot in more detail 11
Part A, The initialization stage. 11
Part B, The fingerprint stage/ Preparation.......... 11
Part C, The injection Stage 11
Part D, Service Account creation.......... 11
Part E, System Events Control.......... 11
Part F, Domain Lusts and connections.......... 11
8. Part C:.......... 12
C 1 Conclusion/Summary of Findings.......... 12
C 2 Recommendations.......... 12
C 3 Next Steps.......... 12
9. Works Cited 12
10. References.......... 12
11. Appendices 13
Appendix Fig 1.0 Network configuration, ... 14
Appendix Fig 2.0 Host Hyper-V machine lab network configuration.......... 15
Appendix Fig 3.0 Windows virtual machine 16
Appendix Fig 4.0 Kali Linux virtual machine 16
Appendix Fig 5.0 Software install on windows server 2025 virtual machine 17
Appendix Fig 6.0 IP Allocation/reservation 18
Appendix Fig 7.0 Network switch hyperV 18
Appendix Fig 8.0 Virtual machines interconnections and testing 18
FIG 8.1, Kali IP Configuration 21
FIG 8.2, Windows IP Configuration.......... 21
FIG 8.3, Testing of Ping from Kali Linux Machine to windows machine 22
server-test 22
FIG 8.4, Testing of Ping from windows Machine server-test to Kali Linux 22
FIG 8.6, Testing of Ping to other networks.......... 23
FIG 8.7, Testing of Ping to other networks.......... 23
FIG 8.8, Joe Sandbox 24

Section 1: Malware Lab

Abstract

Based on the requirements of our continues assessment we were required to create a malware analysis lab using best practices , alongside this we were also required to research one assigned malware type for my report this was QBot which is also known as a banking malware , for my report I analyzed existing research and incorporated this into my overall structure this included process flow analysis , stages of malware injection , and conclusion into how QBot works in a windows environment and what I would do if I had more time to research further into the malware.

.

1. Introduction

As part of our continuous assessment, we were required to set up and configure a malware analysis lab. The requirement here was to utilize research-based method's in understanding how a malware lab might come to fruition our references could be anything from lab based guides , best practice documentation or perhaps google scholar articles and books. , The key point being to utilize recognized trusted methods of configuring our lab to a best practice or standard.

Another one of the key elements was to understand the process involved in configuring the lab environment, this includes everything from your hardware components such as memory, ram, graphics cards, networking cards, motherboards, backplanes, raid configurations, processors and cpu power, surge protection and so on. As part of this process, we were required to reference best practice in the solution and document these.

The lab was also to provide us with a deeper understanding of how you would ensure isolation from your core network without compromising on security , this can be seen as understanding the isolation process from your virtual machines in your lab network to your core network/home network or enterprise network , part of the process was to understand your starting point with configuring your lab network and then securing this and isolating it from all other networks , understanding your network topology was a key part of this exercise.

Safeguards are a key point to consider as part of any lab and network configuration when introducing malware for testing , virtual machine escape is a key security consideration to understand and undertake when securing your test virtual machines , [1] Safeguard are normally introduced as a way of ensuring abnormal behavior doesn't happen and VM Escape is considered a security risk it effects both the integrity and availability of a virtual machine and can cause issues in enterprise environments a virtual machine should not know its virtualized and should definitely not burst out of its vm if a peace of malware could do this it would then be able to control virtual machines on the host and this would be a security incident. Safeguards are a form of protection against this kind of attack and we incorporate this into our design.

As part of the malware analyses best practice, I utilized a research paper and domains such as google scholar to influence my lab setup. As part of my lab, I was required to complete an analysis into existing sandboxes scenarios , document my virtual machine setup's, and understand what tooling was used to form part of my virtual machines for my test lab and test out some of the features of my lab alongside covering the safe guards and safety procedures i put in place for this.

My Malware lab consisted of many different requirements the first requirement can be described as Hardware requirements , this can include your Firewall appliance , your networking cables , your routers your switches , your internet connection , your hypervisor for storing your virtual machines, your disk storage type and so on.

The next requirement was the balancing act of existing vs new vs used this can be broken down into what you actually have available to you at a present moment which is no cost to implement verses what new equipment you may need to purchase this would be additional to what you already have vs can you purchase equipment at discounted costs or have the ability to purchase re-used equipment. For my lab I based some of the guidance from the book "The Network Security Test Lab: A Step-by-Step Guide by Michael Gregg" [2]

The next requirement was virtual hardware, this could include anything from your Networking setup such as SSID for the wifi , Vlan's , Routers , Virtual network appliances like firewall's and load balancers , access control lists and so on all these take a position in the process for designing your infrastructure with security at the centre often when cybersecurity solution architects are configuring networks they focus on the CIA Triad , confidentiality Integrity Availability [3] also known for being part of the five pillars of information security.

2. Part A: Analysis of Existing Sandbox

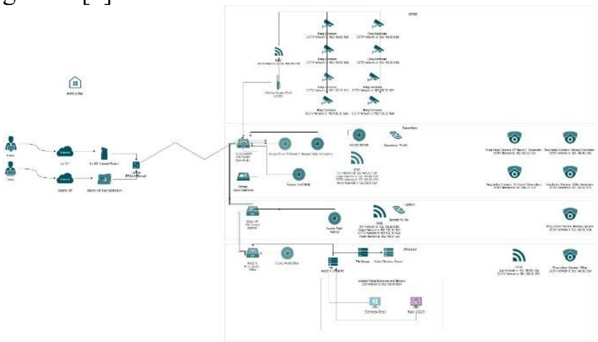
Before we get into our Lab configuration we were asked to do an analysis of an existing sandbox, one of these which could be used is called "JoeSandbox", this allows users to compile an analysis on the behaviour runtime of malware within different environment types e.g. windows, Linux, ubuntu and more , the reports the sandbox creates allows you to develop out a defence in depth approach to indicators of compromise , Mitre attack TTP's and more , it also allows you to essential test out file samples and urls and gives you a comprehensive view into how you could protect your environment. [4]

Additional Screenshots are Available at the end/Appendix of this document for this section see FIG 8.8, Joe Sandbox.

3. Part B: Virtual Machine Setup

Our lab consisted of the following two virtual machines one windows server virtual machine and one Kali Linux virtual machine Hosted on my HP Omen PC with Hyper-V manager enabled. Both virtual machines are configured with the below configurations. Outside of the screenshots below additional screenshots have been added to the Appendix of this document for validation purposes.

Diagram Of Full Network: For this I used Draw.io to create the diagram which is an open-source diagram tool software used by IT Professionals to draw out their diagrams. [4]

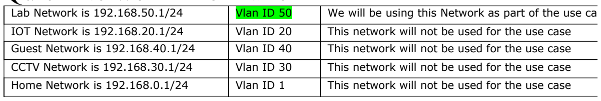


This is the diagram of my network which is separated out into multiple separate networks in my network I have a quantity of 3 switches 1 firewall and multiple Vlan's , for our use case we will be Soley using the Lab network for both virtual machines in which the network adapter will be connected to port number 8 on my upstairs 16 port Omada switch , I have also configured a rule to block all network traffic from the Lab Network to Any other network I did further testing on this for confirmation at a later stage.

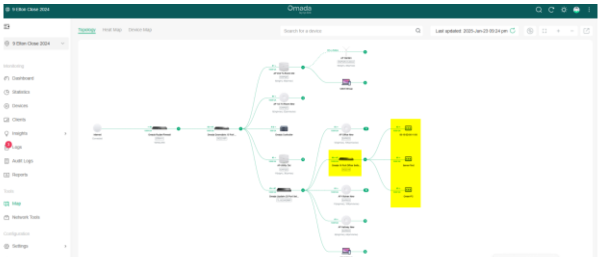
Quick Network Hardware Information Table For Use Case

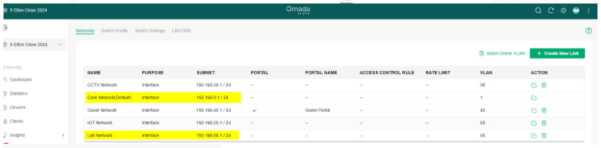
TP-Link Omada ER8411 Router/Firewall	Internet comes in through this router has dual Wan Failover.	
TP-Link Omada SG-2218P Switch	This is the Down Stair Switch Comms A	Switch Connects to ER8411
TP-Link Omada TL-SG 3428 MP Switch	This is the Up Stair Switch Comms B	Switch Connects to SG 3428
TP-Link Omada SG - 2218 Switch	This is the office Switch	Switch Connects to SG-2218P
TP Link Omada EAP653 X 4 Indoor AP	Access Points Indoor	SSID Available for use case
TP Link Omada EAP225 X1 Outdoor AP	Access Points Outdoor	SSID Available for use case
Omen PC	HyperV Host	HP Desktop/Server

Quick Network Information

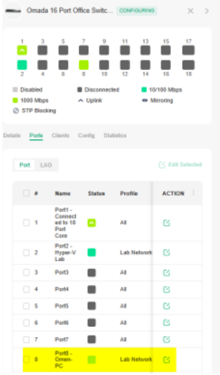


Lab Network is 192.168.50.1/24	Vlan ID 50	We will be using this Network as part of the use ca
IOT Network is 192.168.20.1/24	Vlan ID 20	This network will not be used for the use case
Guest Network is 192.168.40.1/24	Vlan ID 40	This network will not be used for the use case
CCTV Network is 192.168.30.1/24	Vlan ID 30	This network will not be used for the use case
Home Network is 192.168.0.1/24	Vlan ID 1	This network will not be used for the use case



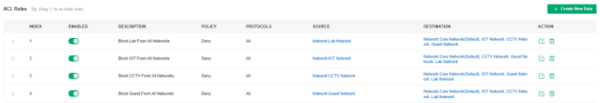


NAME	PURPOSE	SUBNET	PORTAL	PORTAL NAME	ACCESS CONTROL RULE	RATE LIMIT	VLAN
CCTV Network	Interface	192.168.30.1 / 24	--	--	--	--	30
Core Network(Default)	Interface	192.168.0.1 / 24	--	--	--	--	1
Guest Network	Interface	192.168.40.1 / 24	✓	Guest Portal	--	--	40
IOT Network	Interface	192.168.20.1 / 24	--	--	--	--	20
Lab Network	Interface	192.168.50.1 / 24	--	--	--	--	50



#	Name	Status	Profile
1	Port1 - Connected to 18 Port Core		All
2	Port2 - Hyper-V Lab		Lab Network
3	Port3		All
4	Port4		All
5	Port5		All
6	Port6		All
7	Port7		All
8	Port8 - Omen-PC		Lab Network

Additional Screenshots are Available at the end/Appendix of this document for this section see Fig 1.0 Network configuration.

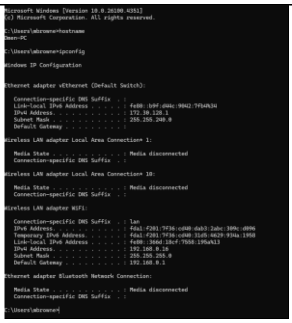
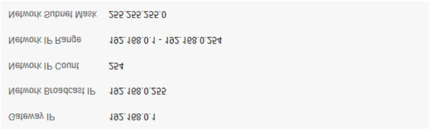


INDEX	ENABLED	DESCRIPTION	POLICY	PROTOCOLS	SOURCE	DESTINATION
1	●	Block Lab From All Networks	Deny	All	Network:Lab Network	Network:Core Network(Default), IOT Network, CCTV Network, Guest Network
2	●	Block IOT From All Networks	Deny	All	Network:IOT Network	Network:Core Network(Default), CCTV Network, Guest Network, Lab Network
3	●	Block CCTV From All Networks	Deny	All	Network:CCTV Network	Network:Core Network(Default), IOT Network, Guest Network, Lab Network
4	●	Block Guest From All Networks	Deny	All	Network:Guest Network	Network:Core Network(Default), IOT Network, CCTV Network, Lab Network

Host Hyper-V Machine

This is my Omen-PC used to host all virtual machines this is on a separate Home Network.

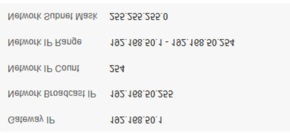
OS Version	Windows 11 Pro
System Name	Omen-PC
Build Version	24H2, 26100, 4351
Ram	48GB

Processor	Core i5-10400f
Cpu	2.90 ghz
Cores	6
C Drive Capacity	930GB
D Drive Capacity	1.81TB
E Drive Capacity	931 GB
VM Virtual Network Configuration	IPv4 Address, 192.168.0.16 Subnet Mask, 255.255.255.0 Default Gateway, 192.168.0.1 DNS, 192.168.0.1
System Type	X64
Image	  Network Subnet Mask 255.255.255.0 Network IP Range 192.168.0.1 - 192.168.0.254 Network IP Count 254 Network Broadcast IP 192.168.0.255 Gateway IP 192.168.0.1

```
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mbrowne>hostname
Omen-PC

C:\Users\mbrowne>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b9f:d44c:9042:7fb4%34
   IPv4 Address. . . . . . . . . . . : 172.30.128.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . : lan
   IPv6 Address. . . . . . . . . . . : fda1:f201:7f36:cd40:dab3:2abc:309c:d096
   Temporary IPv6 Address. . . . . . : fda1:f201:7f36:cd40:31d5:4629:934a:1958
   Link-local IPv6 Address . . . . . : fe80::366d:18cf:7558:195a%13
   IPv4 Address. . . . . . . . . . . : 192.168.0.16
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\mbrowne>
```

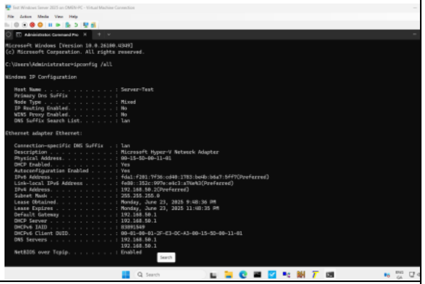
Additional Screenshots are Available at the end/Appendix of this document for this section see Fig 2.0 Host Hyper-V Machine

Lab Network Configuration

Vlan ID	50	
Gateway IP:	192.168.50.1	
Network Broadcast IP	192.168.50.255	
Network IP Count	254 Addresses	
Network IP Range	192.168.50.1 - 192.168.50.254	
Network Subnet Mask	255.255.255.0	
Gateway IP:	192.168.50.1	
Image	 Network Subnet Mask 255.255.255.0 Network IP Range 192.168.50.1 - 192.168.50.254 Network IP Count 254 Network Broadcast IP 192.168.50.255 Gateway IP 192.168.50.1	

Our windows virtual machine had a configuration of:

This is the test windows server virtual machine which is hosted on my Omen-PC but connected to a separate VLAN ID Of 50 for the lab network.

OS Version	Windows Server 2025 Standard
System Name	Server-Test
Build Version	24H2, 26100, 4349
Ram	4GB
Processor	Core i5-10400f
Cpu	2.90 ghz
Cores	3
C Drive Capacity	126GB
VM Virtual Network Configuration	IPv4 Address, 192.168.50.2 Subnet Mask, 255.255.255.0 Default Gateway, 192.168.50.1 DNS 192.168.50.1 
Lab Network Configuration	Gateway IP: 192.168.50.1 Network Broadcast IP 192.168.50.255 Network IP Count 254 Network IP Range 192.168.50.1 - 192.168.50.254 Network Subnet Mask 255.255.255.0

Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File
Action
Media
View
Help
Administrator: Command Pro
Search
Search

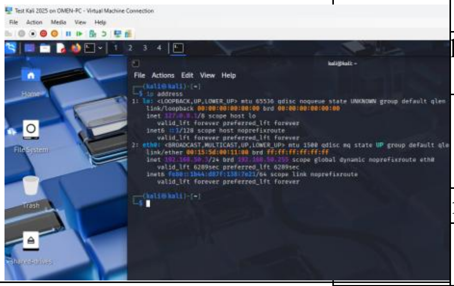
```
Microsoft Windows [Version 10.0.26100.4349]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Server-Test
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : lan

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-15-5D-00-11-01
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fda1:f201:7f36:cd40:1783:be4b:b6a7:5ff7(Preferred)
   Link-local IPv6 Address . . . . . : fe80::352c:997e:e8c3:a7%e%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.50.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, June 23, 2025 9:48:36 PM
   Lease Expires . . . . . . . . . . : Monday, June 23, 2025 11:48:35 PM
   Default Gateway . . . . . . . . . : 192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 83891549
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-E3-0C-A3-00-15-5D-00-11-01
   DNS Servers . . . . . . . . . . . : 192.168.50.1
                                       192.168.50.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Mac Address	00-15-5D-00-11-01
System Type	X64

Additional Screenshots are Available at the end/Appendix of this document for this section see Fig 3.0 windows virtual machine

Our Kali Linux virtual machine had a configuration of

This is the test Kali Linux virtual machine which is hosted on my Omen-PC but connected to a separate VLAN ID Of 50 for the lab network.

OS Version	Kali GNU / Linux Rolling
System Name	Kali
Distributor	Debian
GT Version	3.24.49
Xfce Version	4.20
Kernel Version	6.12.25-amd64
Windowing System	X11
Ram	6GB
Processor	Intel Core i5-10400F
Cpu	2.90 GHz
Cores	2
C Drive Capacity	126GB
VM Virtual Network Configuration	IPv4 Address, 192.168.50.3 Subnet Mask, 255.255.255.0 Default Gateway, 192.168.50.1 DNS 192.168.50.1  Test Kali 2025 on OMEN-PC - Virtual Machine Connection ┌──(kali㉿kali)-[~] └─$ ip address 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host noprefixroute valid_lft forever preferred_lft forever 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qle link/ether 00:15:5d:00:11:00 brd ff:ff:ff:ff:ff:ff inet 192.168.50.3/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0 valid_lft 6289sec preferred_lft 6289sec inet6 fe80::1b44:d87f:138:7e21/64 scope link noprefixroute valid_lft forever preferred_lft forever ┌──(kali㉿kali)-[~] └─$
Lab Network Configuration	Gateway IP: 192.168.50.1 Network Broadcast IP 192.168.50.255 Network IP Count 254 Network IP Range 192.168.50.1 - 192.168.50.254

	Network Subnet Mask 255.255.255.0
Mac Address	00-15-5D-00-11-00
System Type	X86 _64
Upgrades to Application's	Command's Used were sudo apt update and sudo apt upgrade

Additional Screenshots are Available at the end/Appendix of this document for this section see Fig 4.0 Kali Linux virtual machine.

4. Part C: Software Tools

As part of the virtual machine configurations for both Kali and windows we were required to setup and configure both virtual machines accordingly some of the tools I installed as part of the lab configuration for the windows server virtual machine are listed below , because I downloaded the latest edition of Kali allot of the programs that I wanted on it were pre-installed I simply did an update to all the packages to ensure I was using the latest editions where required I installed additional packages as required.

Tool Name	Tool Version Number	My Understanding of each of the Tool Functions	My Reason fo
7-Zip	24.09	Used to unwrap files which can be in compressed formats.	Used by profe
Adobe Reader	25.001	Used to view pdf file formats and other file formats as a reader.	Allows indivi
Advanced IP Scanner	2.5.4594.1	Allows for scans of Ip Address, Network and Subnet ranges.	Used for getti enterprise and
Fiddler Everywhere	6.6.0	Allows for monitoring and analysis of web traffic as its in transit.	Normally use
hrome	137.0.7151	Browers developed by google	Lightweight e
	8.0.4510.10	Used for running Java based applications which run on almost everything.	Required if yo
irefox	139.04	Browser developed by Mozilla	Useful if you
	1.79	Allows for the capture of network traffic and sniffing.	Part of the Wi
Putty	0.83.00	Allows for the connection to telnet sessions.	Allows you to or telnet
Python	3.13	A programming language often used when scripting code	Let's you crea

Resource Hacker	5.2.8	Used when looking to do reverse malware analysis or engineering	Allows you to edit icons and text files alongside executables	Resource Hacker
USBCap	1.5.4	Used to capture traffic from usb devices.	The go to application for capturing data in motion for usb drives	USBCap
Win Rar	7.11.0	Used to compress large file quantities in different file formats	Another form of file compressor	Win Rar
WinSCP	6.5.1	Used for the large quantities of data file shares and transfers.	Allows for ease of data moves between systems	WinSCP
Wireshark	4.4.7	Used to analyse networks , subnets and ranges.	Number one for network packet captures	Wireshark
Autopsy	4.22.1	Used to analyse recover, record and report on disk images for investigation purposes.	Used for evidence collection and harvesting in investigations	Autopsy
BinText	3.0.3	Used for reading code and looking for strings in code	Allows you to do analysis on code and extract characters and texts from it	BinText
Network Miner	3.0	Used for extracting content from network traffic in transit.	Gives you the ability to pull data from packet captures	Network Miner
Tor Browser	14.5.3	A browser which focuses on hidden privacy across the internet utilising vpn technology, this browser has access to the different forms of the web such as surface, deep, dark	Let's you conduct questionable activity via an anonymous network for research purposes as an ethical professional.	Tor Browser

Additional Screenshots are Available at the end/Appendix of this document for this section see Fig 5.0 software install on windows server 2025 virtual machine.

5. Part D: Lab Testing

So, for my lab I was required to do some testing to ensure that both virtual machines were isolated from my network.

Step 1: IP Allocation and Reservation

The first thing I did was configure a Vlan for the Lab Network, this consisted of the following an Ip address range of 192.168.50.1/24 with a VLAN ID of 50 , both virtual machines were allocated to this network one receiving an IP Address of 192.168.50.2 for the windows server and one receiving an IP Address of 192.168.50.3 for the kali Linux machines , next steps were to reserve the Ip addresses for both of these servers in the dhcp pool's.

Additional Screenshots are Available at the end/Appendix of this document for this section see Fig 6.0 IP Allocation/Reservation

Step 2: Virtual Machine Network Switch Assignment

I configured my virtual switch called it MalwareAnalysisLab and assigned it as an external network and attached the Network card too it. I ensure the option for "allow management operating system to share this network adapter" was left unticked as I did not want the host os / Hypervisor my Omen-PC to have any connection with this adapter.

Additional Screenshots are Available at the end/Appendix of this document for this section see Fig 7.0 Network Switch HyperV

Step 3: Securing the Virtual Machine on the Hypervisor

The next step was to secure the virtual machines on the hypervisor, let's start with the Windows Server. My configuration for this was to enable secure boot , this prevents unauthorised code from running when the virtual machine boots up , Enable trusted platform Module alongside enabling Shielding all of these steps ensure a more secure and resilient virtual machine. I also configured the checkpoints for the virtual machine for if and when we need to revert back. One additional option I had was to enable BitLocker should I required it I chose for the lab not to but in a normal product environment you would enable this.

For Linux I didn't have allot of options as it doesn't natively additional configuration for secure boot and other configurations, but I did enable checkpoints for this as well.

Step 4: Test virtual Machine interconnectivity and test Virtual machine connections to other networks.

First step was to confirm the virtual machine IP Address for both systems in cmd or terminal , the next step was to ping both virtual machines from each other and then try to ping outside of the 192.168.50.1/24 network which is the Lab network , confirmed I was unable to do so due to the policies in place which would be correct , tried to complete a scan with Advanced IP scanner of other networks ranges , nothing was discoverable , confirmed isolation via conducting these activities.

Step 5: Additional Safety and Precautions

As part of the lab requirements, we were required to ensure that some security was in place and to call out some additional Steps which could be taken to ensure

Virtual machine security, this is just 3 examples of how I did this.

- Clipboard and network discovery were turned off; this can be a local policy.
- Drag and drop was disabled, this can be a local policy
- Vm snapshots could be taken via checkpoints in Hyper-V manager, this should be enabled as we may inject malware as part of the testing process at some point.

Checkpoints in Hyper-V [5]

Additional Screenshots are Available at the end/Appendix of this document for this section see Fig 8.0 Virtual Machines interconnections and testing.

6. Section 2: Research-based Malware Analysis (QBOT)

Introduction

As part of our continuous assessment, we were required to research a form of Malware in my case the Research was based on a Malware called QBot, on first search this came up with a few names QBot is actually known under many aliases , some include "Qakbot , Quack Bot or Pinkslipbot" [6]3 very quirky names for it , its secotr of speciality is the banking sector and is very well known in this sector. The Malware made its first debut in 2007 its more formally known as a type of Trojan. Since 2007 QBot has been continually developing over the year now going on 18 Years's it started originally as a loader but has sense integrated with other malware types and form one example Conti one similar, we have seen in the HSE attack. QBot since its first up brining original designed to steal banking information has evolved into something much bigger its now able to self-replicates across devices servers and workstations and it learns every time it grows.

To further investigate the QBot Malware family the requirement here was to utilise research-based methods Understand the malware better and how it spreads and traverses across systems , networks , shares and exchange systems from my research I discovered that QBots desired form of delivery was within email attachments and document's often disguising itself as legitimate documents but later becoming evident it had alterior motives , some of QBot main selling points in terms of destruction were

Performing keylogging functions on hosts which were compromised by its malware, meaning it could record user keystrokes and password's. In line with performing keylogging functions it was passing on the stored passwords to third party cnc servers which resulted in the private information being sold to black markets

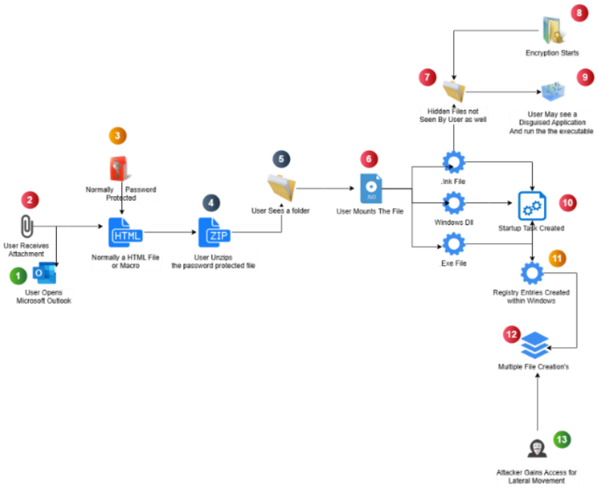
Another speciality it had was to create background tasks and schedules on individuals' systems unknown to the targeted user it was actually creating these without any form of visible changes from there after the persistent methods were created it could traverse across the network at quieter times. As part of the malware analyses research, I looked into this more to understand the rate and infection chain at which the malware performed.

Part A: Identification

So the attack chain from my understanding starts with an unsuspecting user receiving an attachment, this can take the form of an Excel file or a pdf, normally it's a Macro file that must be opened in excel and something that requires a user to specifically be forced to enable the live content deceivingly and unknown to them. This can also come in the form of a zip file as again it would require the user to actually extract it and then run it. When the user extracts the file what the file does it creates three items , one a request that cannot be seen by the user , two a file in a location they cant see and then normally a scheduled task as at this point the file has been deposited into the hidden directory , it will stay here for some time and report back to its cnc server after a period of time , it lays in the system until it has fully unloaded all its dll's and components , part of the malware spends its time evading antivirus and antimalware components often bringing with it obfuscations so that both the users and systems don't know it exists this takes many forms and by the time its found usually its two late.

Based on the research into the file types I was able to see that the malware obfuscated itself as Html files , URL's , fake voicemails /audio attachments for users to open alongside encrypted attachments like Macros and adobe reader files , all of which if they pass the through inspections pose a threat to user's based on my research into the Threllix article [7].

The Attack Chain Diagram
Diagram Of Attack Chain: For this I used Draw.io to create the diagram which is an open-source diagram tool software used by IT Professionals to draw out their diagrams. [4]


8
Encryption Starts
7
Hidden Files not Seen By User as well
9
User May see a Disguised Application And run the the executable
3
Normally Password Protected
5
6
2
User Receives Attachment
1
User Opens Microsoft Outlook
HTML
Normally a HTML File or Macro
4
ZIP
User Unzips the password protected file
User Sees a folder
ISO
User Mounts The File
.lnk File
Windows Dll
.Exe File
10
Startup Task Created
11
Registry Entries Created within Windows
12
Multiple File Creation's
13
Attacker Gains Access for Lateral Movement

Part B: Analysis

In the initialisation phase we see the user getting a malicious email with an attachment the user presumes this is legit as there are no indicator telling them its not.

In the execution phase we see the user opening the malicious html file with the provided password user only sees one file double clicks it mounts , this begins the process of launching malicious and unsuspecting configurations and changes to windows task scheduler , windows registry and creating the exe all in quick succession , the user only see's the exe but there are hidden files already the encryption process has started as the payload has been requested from the cnc server

In the communication the user does not see the attacker already beginning the process of reconnaissance or lateral movement this happens unknowingly to the User the system at this point is compromised and the attacker looks for additional hosts across the network.

if we take all these as one Flow, we can see the process of the attack flow based on my understanding of it very simplified, but it covers the flow.

7. Looking at the flow of QBot in more detail

Part A, The initialization stage.

QBot initiates with a .exe file, in this execution QBot looks to see if it has been launched in a sandbox environment or a real environment, it looks for the file "C:\INTERNAL\__empty" if this file exists it wont run as it understands that's its in a sandbox environment and won't cause any real damage at this point. If it detects its not in a a sandbox environment it will look for a list of known antivirus /antimalware products this is more of an adaptive countermeasure so that QBolt knows how to adjust to the installed AV. [8]

Part B, The fingerprint stage/ Preparation.

QBot initiates the process of fingerprinting the computer before injecting its chosen poison, this will take into effect its previous scan to check which antivirus/antimalware product was installed knowing how to adapt its chosen injection method based on this QBot will try to inject itself into different windows process and antimalware and antivirus processes one could be explorer.exe for example. [8]

Part C, The injection Stage

QBot then continues its process by saving its chosen injection method to disk and continuing to corrupt this, it then goes back to its saved configuration file which was previously stored on the disk and scans the library for needed resources as part of the injection process , it then writes this to the disk and windows registry after this to ensure persistence QBot adds a random folder into the "%APPDATA%\Microsoft" so that the injection can be persistent. QBot repeats the process for all users' login to the effected machine. [8]

Part D, Service Account creation

QBot initiates the process of restoring all its data into the disk and registry, it creates new scheduled tasks which perform the creation of the QBot Service account using "NT AUTHORITY\SYSTEM" , this later helps it to re process parts A, B And C for persistence. At this point QBot has injected the machine corrupted the disk created the tasks and created its service account. [8]

Part E, System Events Control

QBot installs and leaves a copy of its malicious binary files into the CurrentVersion folder for users which allows it to control scheduled tasks processes and reboot and shutdown events. After a reboot of this the evidence of the files is removed from the folders. A monitor like services / events being to occur on the machine allowing QBot to connect with its cnc server, these Ip Addresses are randomized so the individual cannot determine the validity, nor can they trace them.

Part F, Domain Lusts and connections

QBot begins the process of loading communication with domains and installing them into the registry for communication, these are then written to the configuration files which are stored in the registry. From the QBot continues with installing other features like Vnc Servers and more.

8. Part C:

C 1 Conclusion/Summary of Findings

The overall conclusion from my understanding of QBolt is a fast-moving malware, it’s opportunistic with its ability to come in many different formats, XML Html, Excel, Macro and so on. Its ability to be able to self-spread and cohesively deceive system processes and procedures especially for Anti-Virus and Malware programs make it top tier in terms of deception and functionality. Its smart nature to be able to begin the process of execution and lay low allows it to remain hidden on systems for a period of time the deception it perform against users makes it that bit more tricky to spot or isolate , with QBolt being continually developed and popularity for it growing e.g. Conti it means that’s its not going anywhere anytime soon, further research into it should be conducted in how to mitigate the threats it proposes.

C 2 Recommendations

Some of the recommendations you can take from researching into QBolt based on the fact that it has a high probability of attacking Microsoft windows os and server environments is.

- Utilising active directory and group policy management to ensure baselines are created for machine by disabling non required Microsoft office settings such as Macros.

- Utilising active directory and group policy management to ensure scheduled tasks cannot be created by new service accounts and can only be authorised from domain controller group policy management, disabling the ability for QBot to create its own processes.

- Ensure that whatever enterprise level Anti-Virus, Anti-Malware and Anti-Ransomware solutions your using corporate endpoint detection and response behavioural analytics into he solution with the ability to report to a security operation centre and ingest into a siem solution like Microsoft Sentinel.

C 3 Next Steps

If I had more time with the QBot analysis, I would have loved to actually perform the malware analysis myself , utilising some of the tools I previously mentioned getting practical and testing it out would have been beneficial , with the scope of paper to report on and research the malware having been able to analyse the process , dig deeper into the memory dumps and monitor the traffic with Wireshark would have provided for an insightful and eye opener for getting hands on with the malware , I definitely plan to test this out in my last at some point.

9. Works Cited

[1] B. Plankers, “what-is-vm-escape,” 22 09 2007. [Online]. Available: https://lonesysadmin.net/2007/09/22/what-is-vm-escape/. [Accessed 23 June 2025].

[2] M. Gregg, The Network Security Test Lab: A Step-by-Step Guide, New York, United States: Wiley, 14 Aug. 2015.

[3] R. Witcher , “five-pillars-information-security,” 27 April 2025. [Online]. Available: https://destcert.com/resources/five-pillars-information-security/. [Accessed 24 June 2025].

[4] JoeSecurity, “joe-sandbox-cloud,” JoeSecurity, 17 April 2010. [Online]. Available: https://www.joesecurity.org/joe-sandbox-cloud. [Accessed 26th June 2025].

[5] Draw.IO, “https://app.diagrams.net/,” Draw.io, 17 03 2010. [Online]. Available: https://app.diagrams.net/. [Accessed 26 June 2025].

[6] Microsoft, “Using checkpoints to revert virtual machines to a previous state,” Microsoft , 03 Mar 2021. [Online]. Available: https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/checkpoints?tabs=hyper-v-manager. [Accessed 22 June 2025].

[7] O. Yaakobi, “https://www.datto.com/blog/qbot-malware-what-is-it-and-how-does-it-work/,” datto, 29th July 2022. [Online]. Available: https://www.datto.com/blog/qbot-malware-what-is-it-and-how-does-it-work/. [Accessed 24th June 2025].

[8] A. Chandra and S. K. Arya, “demystifying-qbot-malware,” Trellix , 24th August 2022. [Online]. Available: https://www.trellix.com/blogs/research/demystifying-qbot-malware/. [Accessed 24th June 2025].

[9] C. François, “qbot-malware-analysis,” Elastic Security Labs, 14 February 2023. [Online]. Available: https://www.elastic.co/security-labs/qbot-malware-analysis. [Accessed 24th june 2025].

10. References

[1] B. Plankers, “what-is-vm-escape,” 22 09 2007. [Online]. Available: https://lonesysadmin.net/2007/09/22/what-is-vm-escape/. [Accessed 23 June 2025].

[2] M. Gregg, The Network Security Test Lab: A Step-by-Step Guide, New York, United States: Wiley, 14 Aug. 2015.

[3] R. Witcher , “five-pillars-information-security,” 27 April 2025. [Online]. Available: https://destcert.com/resources/five-pillars-information-security/. [Accessed 24 June 2025].

[4] JoeSecurity, “joe-sandbox-cloud,” JoeSecurity, 17 April 2010. [Online]. Available: https://www.joesecurity.org/joe-sandbox-cloud. [Accessed 26th June 2025].

[5] Draw.IO, “https://app.diagrams.net/,” Draw.io, 17 03 2010. [Online]. Available: https://app.diagrams.net/. [Accessed 26 June 2025].

[6] Microsoft, “Using checkpoints to revert virtual machines to a previous state,” Microsoft , 03 Mar 2021. [Online]. Available: https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/checkpoints?tabs=hyper-v-manager. [Accessed 22 June 2025].

[7] O. Yaakobi, “https://www.datto.com/blog/qbot-malware-what-is-it-and-how-does-it-work/,” datto, 29th July 2022. [Online]. Available: https://www.datto.com/blog/qbot-malware-what-is-it-and-how-does-it-work/. [Accessed 24th June 2025].

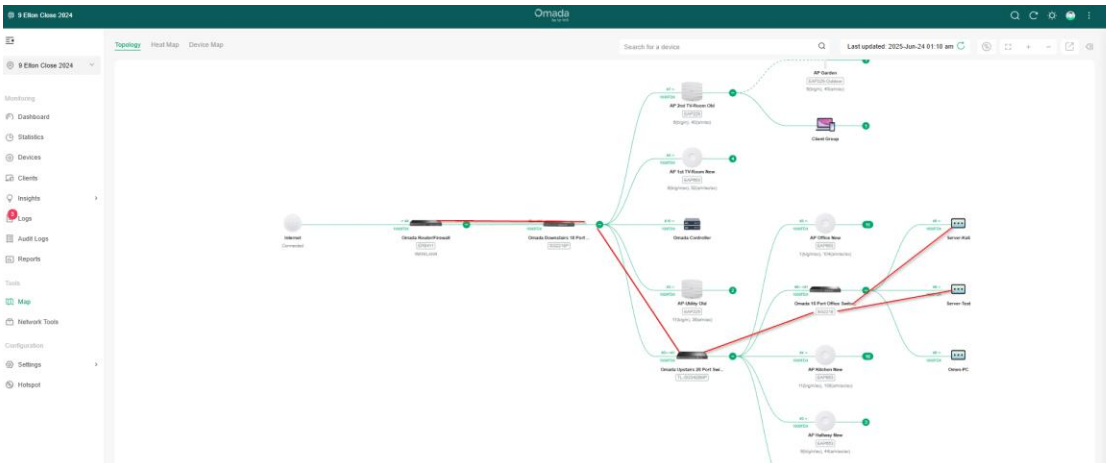
[8] A. Chandra and S. K. Arya, “demystifying-qbot-malware,” Trellix , 24th August 2022. [Online]. Available: https://www.trellix.com/blogs/research/demystifying-qbot-malware/. [Accessed 24th June 2025].

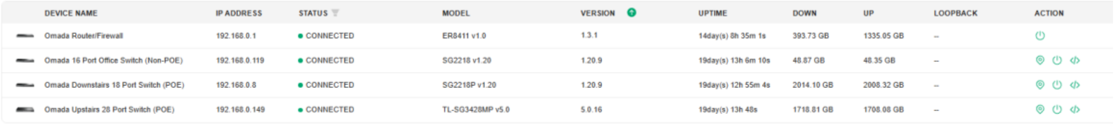
[9] C. François, “qbot-malware-analysis,” Elastic Security Labs, 14 February 2023. [Online]. Available: https://www.elastic.co/security-labs/qbot-malware-analysis. [Accessed 24th june 2025].

11. Appendices

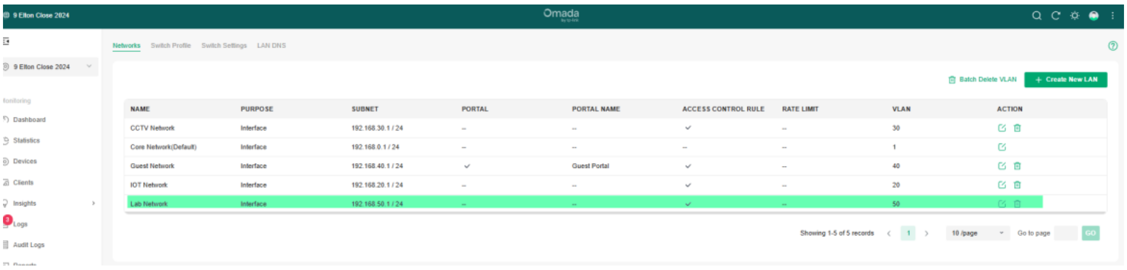
Appendix Fig 1.0 Network configuration,

Includes firewall, switches, ports and Vlan and server paths across network.





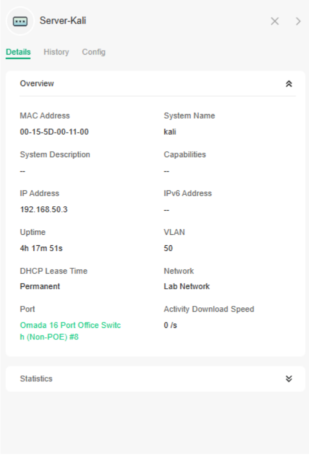
DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION	UPTIME	DOWN	UP	LOOPBACK	ACTION
Omada Router/Firewall	192.168.0.1	● CONNECTED	ER8411 v1.0	1.3.1	14day(s) 8h 35m 1s	393.73 GB	1335.05 GB	--	
Omada 16 Port Office Switch (Non-POE)	192.168.0.119	● CONNECTED	SG2218 v1.20	1.20.9	19day(s) 13h 6m 10s	48.87 GB	48.35 GB	--	
Omada Downstairs 18 Port Switch (POE)	192.168.0.8	● CONNECTED	SG2218P v1.20	1.20.9	19day(s) 12h 55m 4s	2014.10 GB	2008.32 GB	--	
Omada Upstairs 28 Port Switch (POE)	192.168.0.149	● CONNECTED	TL-SG3428MP v5.0	5.0.16	19day(s) 13h 48s	1718.81 GB	1708.08 GB	--	



NAME	PURPOSE	SUBNET	PORTAL	PORTAL NAME	ACCESS CONTROL RULE	RATE LIMIT	VLAN	ACTION
CCTV Network	Interface	192.168.30.1 / 24	--	--	✓	--	30	
Core Network(Default)	Interface	192.168.0.1 / 24	--	--	--	--	1	
Guest Network	Interface	192.168.40.1 / 24	✓	Guest Portal	✓	--	40	
IOT Network	Interface	192.168.20.1 / 24	--	--	✓	--	20	
Lab Network	Interface	192.168.50.1 / 24	--	--	✓	--	50	

Showing 1-5 of 5 records

Both virtual machine IP Information from switch and port highlighted.



MAC Address: 00-15-5D-00-11-00

System Name: kali

System Description: --

Capabilities: --

IP Address: 192.168.50.3

IPv6 Address: --

Uptime: 4h 17m 51s

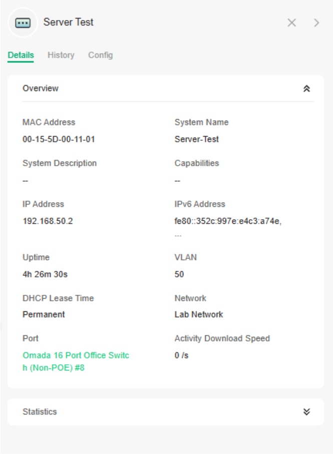
VLAN: 50

DHCP Lease Time: Permanent

Network: Lab Network

Port: Omada 16 Port Office Switch (Non-POE) #8

Activity Download Speed: 0 /s



MAC Address: 00-15-5D-00-11-01

System Name: Server-Test

System Description: --

Capabilities: --

IP Address: 192.168.50.2

IPv6 Address: fe80::352c:997e:e4c3:a74e,

Uptime: 4h 26m 30s

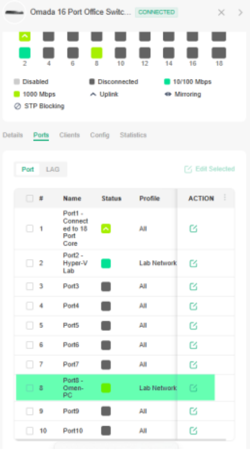
VLAN: 50

DHCP Lease Time: Permanent

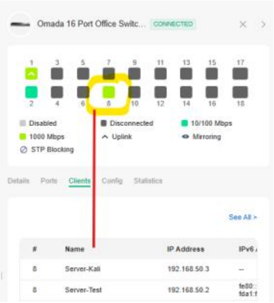
Network: Lab Network

Port: Omada 16 Port Office Switch (Non-POE) #8

Activity Download Speed: 0 /s

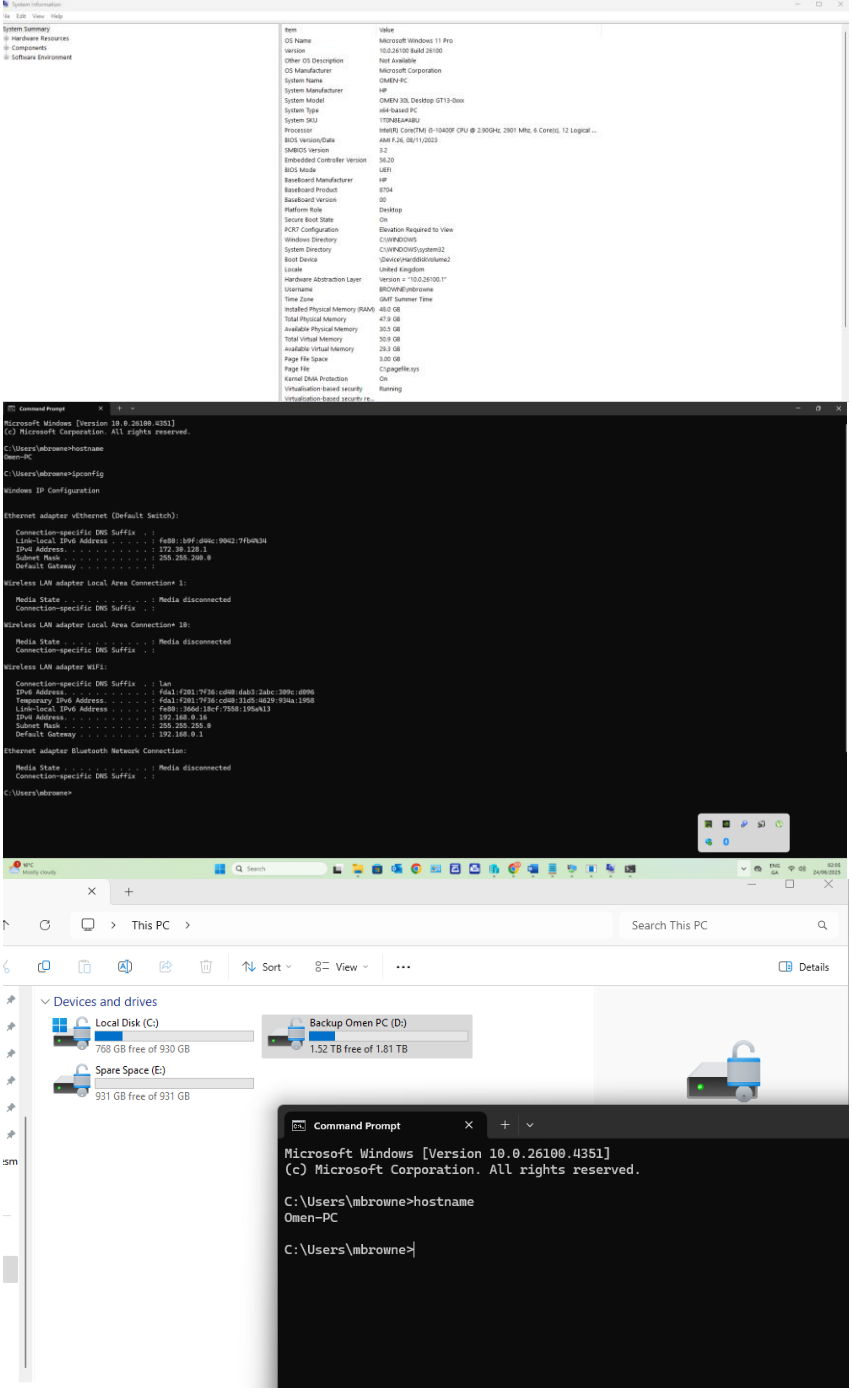


#	Name	Status	Profile	ACTION
1	Port1 - Connected to 18 Port Core		All	
2	Port2 - Hyper-V Lab		Lab Network	
3	Port3		All	
4	Port4		All	
5	Port5		All	
6	Port6		All	
7	Port7		All	
8	Port8 - Omen-PC		Lab Network	
9	Port9		All	
10	Port10		All	



#	Name	IP Address	IPv6 A
8	Server-Kali	192.168.50.3	--
8	Server-Test	192.168.50.2	fe80:: fda1:f

Appendix Fig 2.0 Host Hyper-V machine lab network configuration



Item	Value
OS Name	Microsoft Windows 11 Pro
Version	10.0.26100 Build 26100
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	OMEN-PC
System Manufacturer	HP
System Model	OMEN 30L Desktop GT13-0xxx
System Type	x64-based PC
System SKU	1T0N8EA#ABU
Processor	Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2901 Mhz, 6 Core(s), 12 Logical ...
BIOS Version/Date	AMI F.26, 08/11/2023
SMBIOS Version	3.2
Embedded Controller Version	56.20
BIOS Mode	UEFI
BaseBoard Manufacturer	HP
BaseBoard Product	8704
BaseBoard Version	00
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume2
Locale	United Kingdom
Hardware Abstraction Layer	Version = "10.0.26100.1"
Username	BROWNE\mbrowne
Time Zone	GMT Summer Time
Installed Physical Memory (RAM)	48.0 GB
Total Physical Memory	47.9 GB
Available Physical Memory	30.5 GB
Total Virtual Memory	50.9 GB
Available Virtual Memory	29.3 GB
Page File Space	3.00 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	On
Virtualisation-based security	Running
Virtualisation-based security re...	

```
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mbrowne>hostname
Omen-PC

C:\Users\mbrowne>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b9f:d44c:9042:7fb4%34
   IPv4 Address. . . . . . . . . . . : 172.30.128.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 10:

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

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . : lan
   IPv6 Address. . . . . . . . . . . : fda1:f201:7f36:cd40:dab3:2abc:309c:d096
   Temporary IPv6 Address. . . . . . : fda1:f201:7f36:cd40:31d5:4629:934a:1958
   Link-local IPv6 Address . . . . . : fe80::366d:18cf:7558:195a%13
   IPv4 Address. . . . . . . . . . . : 192.168.0.16
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

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

C:\Users\mbrowne>
```

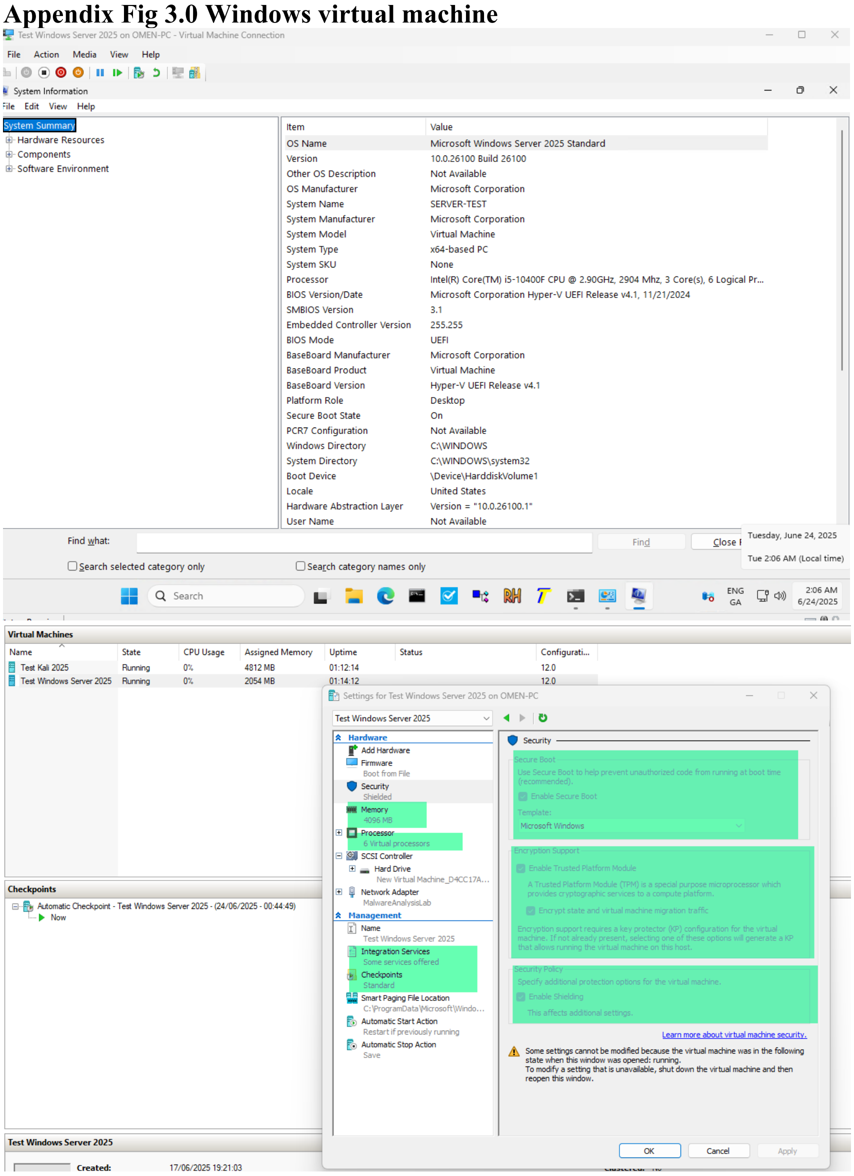
Local Disk (C:)
768 GB free of 930 GB

Backup Omen PC (D:)
1.52 TB free of 1.81 TB

Spare Space (E:)
931 GB free of 931 GB

```
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mbrowne>hostname
Omen-PC

C:\Users\mbrowne>
```

Appendix Fig 3.0 Windows virtual machine



Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection

System Information

System Summary

Item	Value
OS Name	Microsoft Windows Server 2025 Standard
Version	10.0.26100 Build 26100
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	SERVER-TEST
System Manufacturer	Microsoft Corporation
System Model	Virtual Machine
System Type	x64-based PC
System SKU	None
Processor	Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz, 2904 Mhz, 3 Core(s), 6 Logical Pr...
BIOS Version/Date	Microsoft Corporation Hyper-V UEFI Release v4.1, 11/21/2024
SMBIOS Version	3.1
Embedded Controller Version	255.255
BIOS Mode	UEFI
BaseBoard Manufacturer	Microsoft Corporation
BaseBoard Product	Virtual Machine
BaseBoard Version	Hyper-V UEFI Release v4.1
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Not Available
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.26100.1"
User Name	Not Available

Tuesday, June 24, 2025

Tue 2:06 AM (Local time)

2:06 AM 6/24/2025

Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
Test Kali 2025	Running	0%	4812 MB	01:12:14		12.0
Test Windows Server 2025	Running	0%	2054 MB	01:14:12		12.0

Checkpoints

Automatic Checkpoint - Test Windows Server 2025 - (24/06/2025 - 00:44:49)

Now

Settings for Test Windows Server 2025 on OMEN-PC

Test Windows Server 2025

Hardware
- Add Hardware
- Firmware: Boot from File
- Security: Shielded
- Memory: 4096 MB
- Processor: 6 Virtual processors
- SCSI Controller
  - Hard Drive: New Virtual Machine_D4CC17A...
- Network Adapter: MalwareAnalysisLab

Management
- Name: Test Windows Server 2025
- Integration Services: Some services offered
- Checkpoints: Standard
- Smart Paging File Location: C:\ProgramData\Microsoft\Windo...
- Automatic Start Action: Restart if previously running
- Automatic Stop Action: Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

☑ Enable Secure Boot

Template: Microsoft Windows

Encryption Support

☑ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

☑ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

Security Policy

Specify additional protection options for the virtual machine.

☑ Enable Shielding

This affects additional settings.

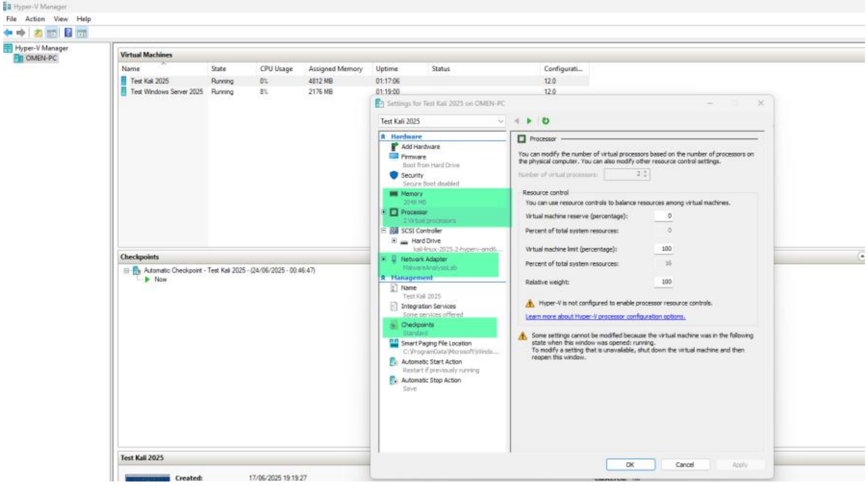
Learn more about virtual machine security.

Some settings cannot be modified because the virtual machine was in the following state when this window was opened: running.
To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.

Test Windows Server 2025

Created: 17/06/2025 19:21:03

Appendix Fig 4.0 Kali Linux virtual machine



Hyper-V Manager

Hyper-V Manager

OMEN-PC

Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
Test Kali 2025	Running	0%	4812 MB	01:17:06		12.0
Test Windows Server 2025	Running	8%	2176 MB	01:19:00		12.0

Checkpoints

Automatic Checkpoint - Test Kali 2025 - (24/06/2025 - 00:46:47)

Now

Settings for Test Kali 2025 on OMEN-PC

Test Kali 2025

Hardware
- Add Hardware
- Firmware: Boot from Hard Drive
- Security: Secure Boot disabled
- Memory: 2048 MB
- Processor: 2 Virtual processors
- SCSI Controller
  - Hard Drive: kali-linux-2025.2-hyperv-amd6...
- Network Adapter: MalwareAnalysisLab

Management
- Name: Test Kali 2025
- Integration Services: Some services offered
- Checkpoints: Standard
- Smart Paging File Location: C:\ProgramData\Microsoft\Windo...
- Automatic Start Action: Restart if previously running
- Automatic Stop Action: Save

Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 2

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage): 0

Percent of total system resources: 0

Virtual machine limit (percentage): 100

Percent of total system resources: 16

Relative weight: 100

Hyper-V is not configured to enable processor resource controls.

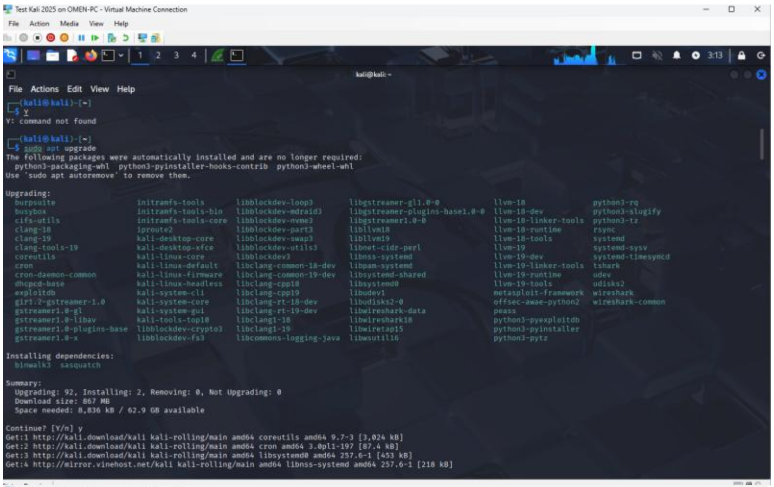
Learn more about Hyper-V processor configuration options.

Some settings cannot be modified because the virtual machine was in the following state when this window was opened: running.
To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.

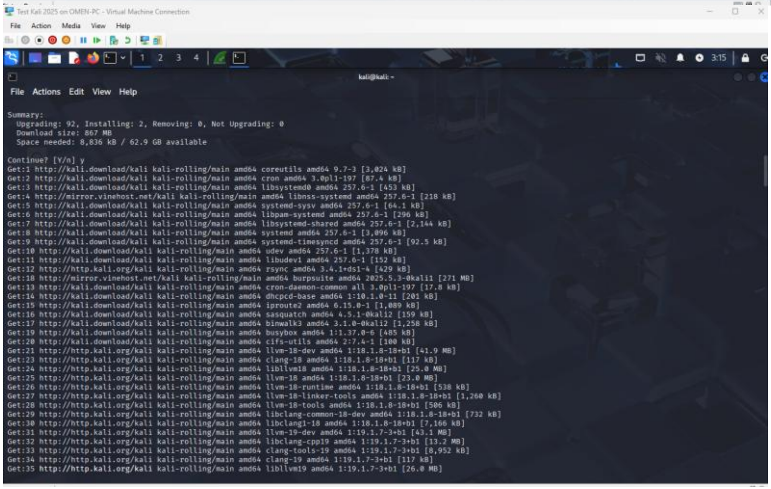
Test Kali 2025

Created: 17/06/2025 19:19:27

Updating Kali Linux

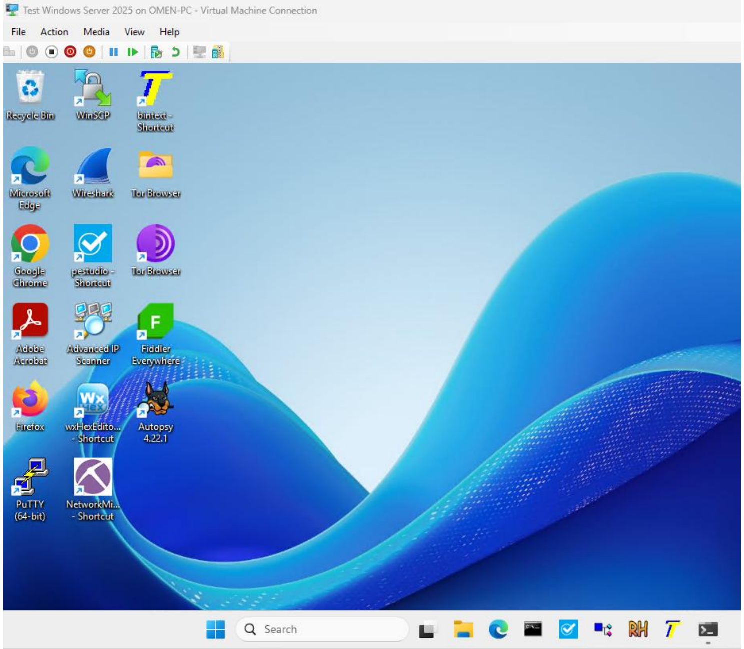

Test Kali 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
1 2 3 4
3:13
kali@kali: ~
File Actions Edit View Help

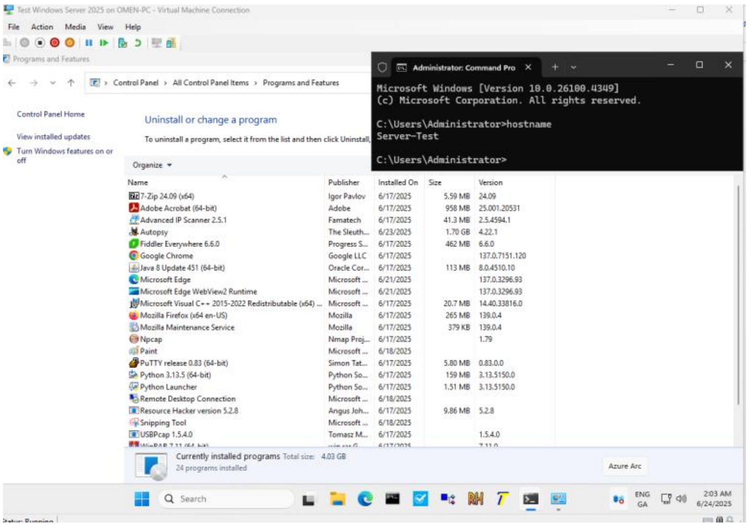
```
┌──(kali㉿kali)-[~]
└─$ Y
Y: command not found

┌──(kali㉿kali)-[~]
└─$ sudo apt upgrade
The following packages were automatically installed and are no longer required:
  python3-packaging-whl  python3-pyinstaller-hooks-contrib  python3-wheel-whl
Use 'sudo apt autoremove' to remove them.

Upgrading:
  burpsuite                 initramfs-tools      libblockdev-loop3       libgstreamer-gl1.0-0           llvm-18              python3-rq
  busybox                   initramfs-tools-bin  libblockdev-mdraid3     libgstreamer-plugins-base1.0-0 llvm-18-dev          python3-slugify
  cifs-utils                initramfs-tools-core libblockdev-nvme3       libgstreamer1.0-0              llvm-18-linker-tools python3-tz
  clang-18                  iproute2             libblockdev-part3       libllvm18                      llvm-18-runtime      rsync
  clang-19                  kali-desktop-core    libblockdev-swap3       libllvm19                      llvm-18-tools        systemd
  clang-tools-19            kali-desktop-xfce    libblockdev-utils3      libnet-cidr-perl               llvm-19              systemd-sysv
  coreutils                 kali-linux-core      libblockdev3            libnss-systemd                 llvm-19-dev          systemd-timesyncd
  cron                      kali-linux-default   libclang-common-18-dev  libpam-systemd                 llvm-19-linker-tools tshark
  cron-daemon-common        kali-linux-firmware  libclang-common-19-dev  libsystemd-shared              llvm-19-runtime      udev
  dhcpcd-base               kali-linux-headless  libclang-cpp18          libsystemd0                    llvm-19-tools        udisks2
  exploitdb                 kali-system-cli      libclang-cpp19          libudev1                       metasploit-framework wireshark
  gir1.2-gstreamer-1.0      kali-system-core     libclang-rt-18-dev      libudisks2-0                   offsec-awae-python2  wireshark-common
  gstreamer1.0-gl           kali-system-gui      libclang-rt-19-dev      libwireshark-data              peass
  gstreamer1.0-libav        kali-tools-top10     libclang1-18            libwireshark18                 python3-pyexploitdb
  gstreamer1.0-plugins-base libblockdev-crypto3  libclang1-19            libwiretap15                   python3-pyinstaller
  gstreamer1.0-x            libblockdev-fs3      libcommons-logging-java libwsutil16                    python3-pytz

Installing dependencies:
  binwalk3  sasquatch

Summary:
  Upgrading: 92, Installing: 2, Removing: 0, Not Upgrading: 0
  Download size: 867 MB
  Space needed: 8,836 kB / 62.9 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 coreutils amd64 9.7-3 [3,024 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 cron amd64 3.0pl1-197 [87.4 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libsystemd0 amd64 257.6-1 [453 kB]
Get:4 http://mirror.vinehost.net/kali kali-rolling/main amd64 libnss-systemd amd64 257.6-1 [218 kB]
```


Test Kali 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
1 2 3 4
3:15
kali@kali: ~
File Actions Edit View Help

```
Summary:
  Upgrading: 92, Installing: 2, Removing: 0, Not Upgrading: 0
  Download size: 867 MB
  Space needed: 8,836 kB / 62.9 GB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 coreutils amd64 9.7-3 [3,024 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 cron amd64 3.0pl1-197 [87.4 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libsystemd0 amd64 257.6-1 [453 kB]
Get:4 http://mirror.vinehost.net/kali kali-rolling/main amd64 libnss-systemd amd64 257.6-1 [218 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 systemd-sysv amd64 257.6-1 [64.1 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libpam-systemd amd64 257.6-1 [296 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libsystemd-shared amd64 257.6-1 [2,144 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 systemd amd64 257.6-1 [3,096 kB]
Get:9 http://kali.download/kali kali-rolling/main amd64 systemd-timesyncd amd64 257.6-1 [92.5 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 udev amd64 257.6-1 [1,378 kB]
Get:11 http://kali.download/kali kali-rolling/main amd64 libudev1 amd64 257.6-1 [152 kB]
Get:12 http://http.kali.org/kali kali-rolling/main amd64 rsync amd64 3.4.1+ds1-4 [429 kB]
Get:18 http://mirror.vinehost.net/kali kali-rolling/main amd64 burpsuite amd64 2025.5.3-0kali1 [271 MB]
Get:13 http://kali.download/kali kali-rolling/main amd64 cron-daemon-common all 3.0pl1-197 [17.8 kB]
Get:14 http://kali.download/kali kali-rolling/main amd64 dhcpcd-base amd64 1:10.1.0-11 [201 kB]
Get:15 http://kali.download/kali kali-rolling/main amd64 iproute2 amd64 6.15.0-1 [1,089 kB]
Get:16 http://kali.download/kali kali-rolling/main amd64 sasquatch amd64 4.5.1-0kali2 [159 kB]
Get:17 http://kali.download/kali kali-rolling/main amd64 binwalk3 amd64 3.1.0-0kali2 [1,258 kB]
Get:19 http://kali.download/kali kali-rolling/main amd64 busybox amd64 1:1.37.0-6 [485 kB]
Get:20 http://kali.download/kali kali-rolling/main amd64 cifs-utils amd64 2:7.4-1 [100 kB]
Get:21 http://http.kali.org/kali kali-rolling/main amd64 llvm-18-dev amd64 1:18.1.8-18+b1 [41.9 MB]
Get:23 http://http.kali.org/kali kali-rolling/main amd64 clang-18 amd64 1:18.1.8-18+b1 [117 kB]
Get:24 http://http.kali.org/kali kali-rolling/main amd64 libllvm18 amd64 1:18.1.8-18+b1 [25.0 MB]
Get:25 http://http.kali.org/kali kali-rolling/main amd64 llvm-18 amd64 1:18.1.8-18+b1 [23.0 MB]
Get:26 http://http.kali.org/kali kali-rolling/main amd64 llvm-18-runtime amd64 1:18.1.8-18+b1 [538 kB]
Get:27 http://http.kali.org/kali kali-rolling/main amd64 llvm-18-linker-tools amd64 1:18.1.8-18+b1 [1,260 kB]
Get:28 http://http.kali.org/kali kali-rolling/main amd64 llvm-18-tools amd64 1:18.1.8-18+b1 [506 kB]
Get:29 http://http.kali.org/kali kali-rolling/main amd64 libclang-common-18-dev amd64 1:18.1.8-18+b1 [732 kB]
Get:30 http://http.kali.org/kali kali-rolling/main amd64 libclang1-18 amd64 1:18.1.8-18+b1 [7,166 kB]
Get:31 http://http.kali.org/kali kali-rolling/main amd64 llvm-19-dev amd64 1:19.1.7-3+b1 [43.1 MB]
Get:32 http://http.kali.org/kali kali-rolling/main amd64 libclang-cpp19 amd64 1:19.1.7-3+b1 [13.2 MB]
Get:33 http://http.kali.org/kali kali-rolling/main amd64 clang-tools-19 amd64 1:19.1.7-3+b1 [8,952 kB]
Get:34 http://http.kali.org/kali kali-rolling/main amd64 clang-19 amd64 1:19.1.7-3+b1 [117 kB]
Get:35 http://http.kali.org/kali kali-rolling/main amd64 libllvm19 amd64 1:19.1.7-3+b1 [26.0 MB]
```

Appendix Fig 5.0 Software install on windows server 2025 virtual machine




Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
Programs and Features
Control Panel › All Control Panel Items › Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize
Administrator: Command Pro
Azure Arc
Search
ENG GA
2:03 AM 6/24/2025
Status: Running

Uninstall or change a program

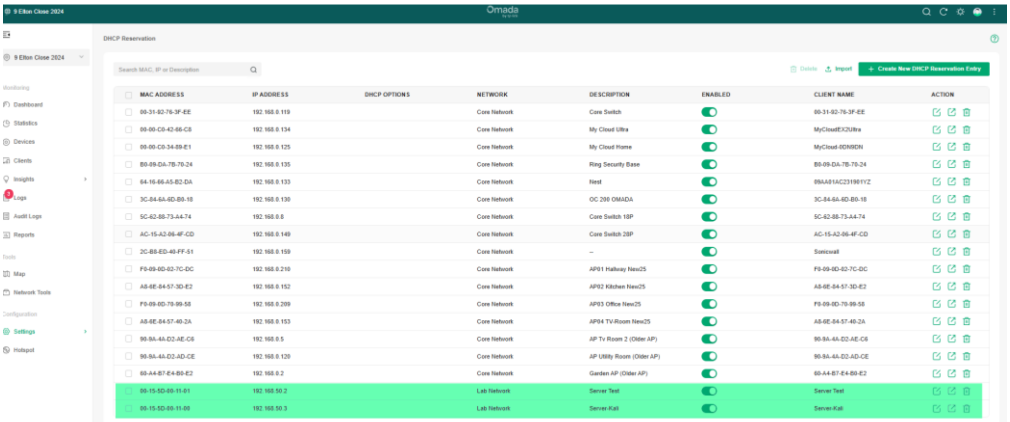
To uninstall a program, select it from the list and then click Uninstall,

Name	Publisher	Installed On	Size	Version
7-Zip 24.09 (x64)	Igor Pavlov	6/17/2025	5.59 MB	24.09
Adobe Acrobat (64-bit)	Adobe	6/17/2025	958 MB	25.001.20531
Advanced IP Scanner 2.5.1	Famatech	6/17/2025	41.3 MB	2.5.4594.1
Autopsy	The Sleuth...	6/23/2025	1.70 GB	4.22.1
Fiddler Everywhere 6.6.0	Progress S...	6/17/2025	462 MB	6.6.0
Google Chrome	Google LLC	6/17/2025		137.0.7151.120
Java 8 Update 451 (64-bit)	Oracle Cor...	6/17/2025	113 MB	8.0.4510.10
Microsoft Edge	Microsoft ...	6/21/2025		137.0.3296.93
Microsoft Edge WebView2 Runtime	Microsoft ...	6/21/2025		137.0.3296.93
Microsoft Visual C++ 2015-2022 Redistributable (x64) ...	Microsoft ...	6/17/2025	20.7 MB	14.40.33816.0
Mozilla Firefox (x64 en-US)	Mozilla	6/17/2025	265 MB	139.0.4
Mozilla Maintenance Service	Mozilla	6/17/2025	379 KB	139.0.4
Npcap	Nmap Proj...	6/17/2025		1.79
Paint	Microsoft ...	6/18/2025		
PuTTY release 0.83 (64-bit)	Simon Tat...	6/17/2025	5.80 MB	0.83.0.0
Python 3.13.5 (64-bit)	Python So...	6/17/2025	159 MB	3.13.5150.0
Python Launcher	Python So...	6/17/2025	1.51 MB	3.13.5150.0
Remote Desktop Connection	Microsoft ...	6/18/2025		
Resource Hacker version 5.2.8	Angus Joh...	6/17/2025	9.86 MB	5.2.8
Snipping Tool	Microsoft ...	6/18/2025		
USBPcap 1.5.4.0	Tomasz M...	6/17/2025		1.5.4.0
WinRAR 7.11 (64-bit)	win.rar G...	6/17/2025		7.11.0

Currently installed programs Total size: 4.03 GB
24 programs installed

```
Microsoft Windows [Version 10.0.26100.4349]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>hostname
Server-Test

C:\Users\Administrator>
```

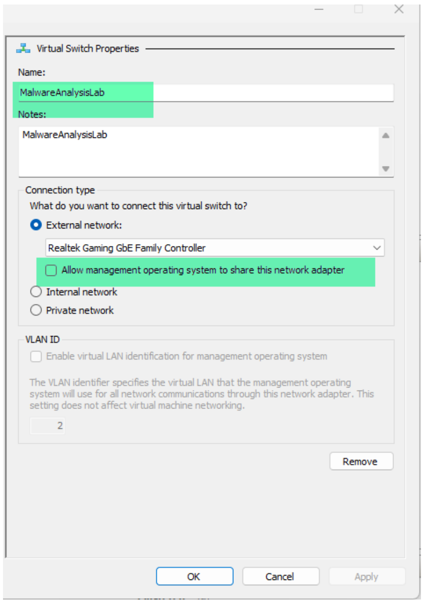
Appendix Fig 6.0 IP Allocation/reservation



DHCP Reservation

MAC ADDRESS	IP ADDRESS	DHCP OPTIONS	NETWORK	DESCRIPTION	ENABLED	CLIENT NAME
00-31-92-76-3F-EE	192.168.0.119		Core Network	Core Switch	●	00-31-92-76-3F-EE
00-00-C0-42-66-C8	192.168.0.134		Core Network	My Cloud Ultra	●	MyCloudEX2Ultra
00-00-C0-34-89-E1	192.168.0.125		Core Network	My Cloud Home	●	MyCloud-0DN9DN
B0-09-DA-7B-70-24	192.168.0.135		Core Network	Ring Security Base	●	B0-09-DA-7B-70-24
64-16-66-A5-B2-DA	192.168.0.133		Core Network	Nest	●	09AA01AC231901YZ
3C-84-6A-6D-B0-18	192.168.0.130		Core Network	OC 200 OMADA	●	3C-84-6A-6D-B0-18
5C-62-88-73-A4-74	192.168.0.8		Core Network	Core Switch 18P	●	5C-62-88-73-A4-74
AC-15-A2-06-4F-CD	192.168.0.149		Core Network	Core Switch 28P	●	AC-15-A2-06-4F-CD
2C-B8-ED-40-FF-51	192.168.0.159		Core Network	--	●	Sonicwall
F0-09-0D-02-7C-DC	192.168.0.210		Core Network	AP01 Hallway New25	●	F0-09-0D-02-7C-DC
A8-6E-84-57-3D-E2	192.168.0.152		Core Network	AP02 Kitchen New25	●	A8-6E-84-57-3D-E2
F0-09-0D-70-99-58	192.168.0.209		Core Network	AP03 Office New25	●	F0-09-0D-70-99-58
A8-6E-84-57-40-2A	192.168.0.153		Core Network	AP04 TV-Room New25	●	A8-6E-84-57-40-2A
90-9A-4A-D2-AE-C6	192.168.0.5		Core Network	AP Tv Room 2 (Older AP)	●	90-9A-4A-D2-AE-C6
90-9A-4A-D2-AD-CE	192.168.0.120		Core Network	AP Utility Room (Older AP)	●	90-9A-4A-D2-AD-CE
60-A4-B7-E4-B0-E2	192.168.0.2		Core Network	Garden AP (Older AP)	●	60-A4-B7-E4-B0-E2
00-15-5D-00-11-01	192.168.50.2		Lab Network	Server Test	●	Server Test
00-15-5D-00-11-00	192.168.50.3		Lab Network	Server-Kali	●	Server-Kali

Appendix Fig 7.0 Network switch hyperV



Name: MalwareAnalysisLab

Notes: MalwareAnalysisLab

Connection type
What do you want to connect this virtual switch to?
● External network:
Realtek Gaming GbE Family Controller
□ Allow management operating system to share this network adapter
○ Internal network
○ Private network

VLAN ID
□ Enable virtual LAN identification for management operating system
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2

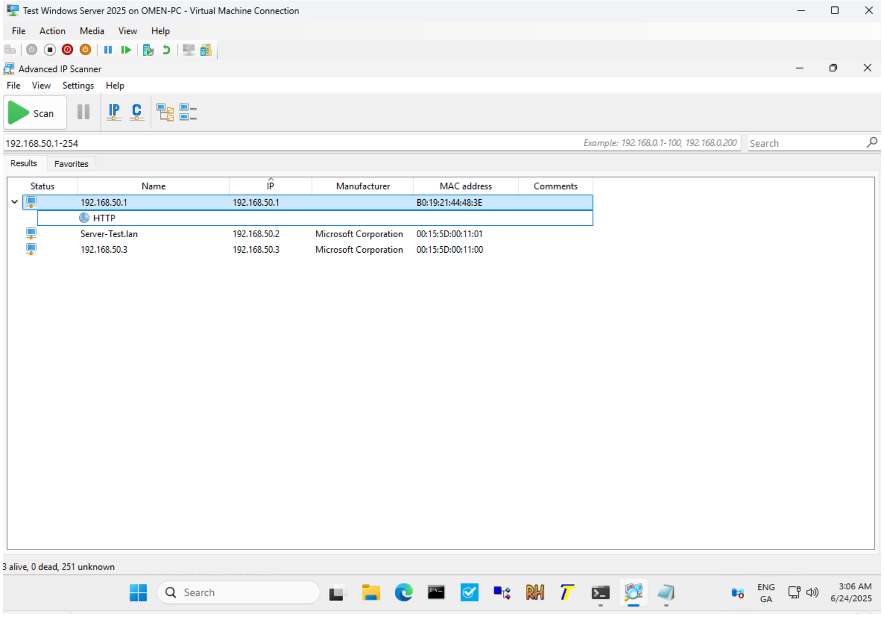
Appendix Fig 8.0 Virtual machines interconnections and testing

Advanced IP Scanner Tests to below VLAN’s

1. Lab Network is 192.168.50.1/24

We can see here advanced IP Scanner can see 3 devices

- Server-Test, Windows Test Server
- Kali Linux, Kali Linux Server
- Omada Gateway, Firewall/Router


Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
Advanced IP Scanner
File View Settings Help
Scan
IP C
Example: 192.168.0.1-100, 192.168.0.200
Search
Results Favorites
Search
ENG GA
3:06 AM
6/24/2025

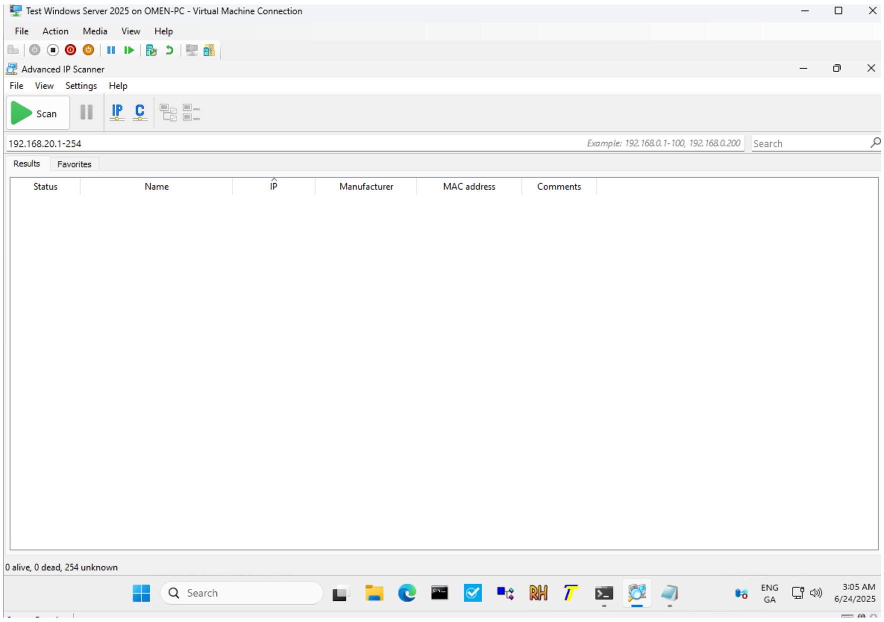
192.168.50.1-254

Status	Name	IP	Manufacturer	MAC address	Comments
	192.168.50.1	192.168.50.1		B0:19:21:44:48:3E	
	HTTP				
	Server-Test.lan	192.168.50.2	Microsoft Corporation	00:15:5D:00:11:01	
	192.168.50.3	192.168.50.3	Microsoft Corporation	00:15:5D:00:11:00	

3 alive, 0 dead, 251 unknown

2. IOT Network is 192.168.20.1/24

We can see here advanced IP Scanner can see nothing on this VLAN , Thanks to the rules on the IOT VLAN Which I created earlier.


Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
Advanced IP Scanner
File View Settings Help
Scan
IP C
Example: 192.168.0.1-100, 192.168.0.200
Search
Results Favorites
Search
ENG GA
3:05 AM
6/24/2025

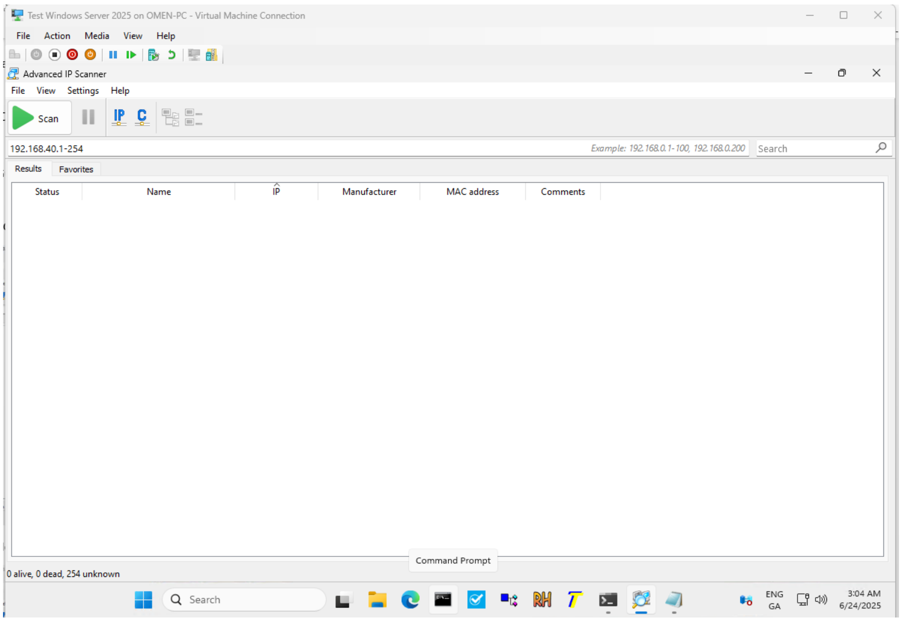
192.168.20.1-254

Status	Name	IP	Manufacturer	MAC address	Comments

0 alive, 0 dead, 254 unknown

3. Guest Network is 192.168.40.1/24

We can see here advanced IP Scanner can see nothing on this VLAN, Thanks to the rules on the Guest VLAN Which I created earlier.

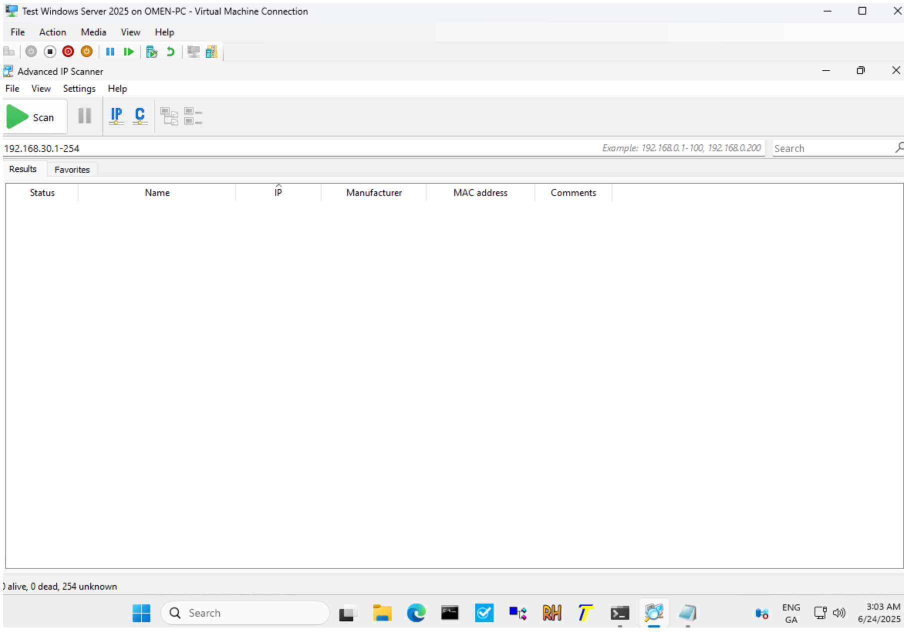

Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
Advanced IP Scanner
File View Settings Help
Scan
Example: 192.168.0.1-100, 192.168.0.200
Search
Results Favorites
Status Name IP Manufacturer MAC address Comments
Command Prompt
Search
ENG GA
3:04 AM 6/24/2025

192.168.40.1-254

0 alive, 0 dead, 254 unknown

4. CCTV Network is 192.168.30.1/24

We can see here advanced IP Scanner can see nothing on this VLAN , Thanks to the rules on the CCTV VLAN Which I created earlier.

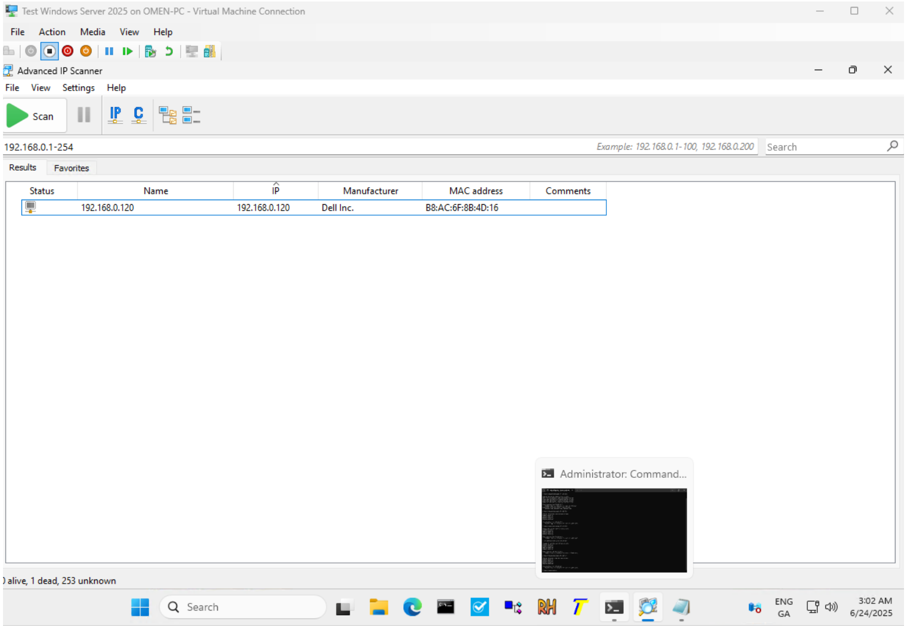

Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
Advanced IP Scanner
File View Settings Help
Scan
Example: 192.168.0.1-100, 192.168.0.200
Search
Results Favorites
Status Name IP Manufacturer MAC address Comments
Search
ENG GA
3:03 AM 6/24/2025

192.168.30.1-254

) alive, 0 dead, 254 unknown

5. Home Network is 192.168.0.1/24

We can see here advanced IP Scanner can see nothing on this VLAN , Thanks to the rules on the Home VLAN Which I created earlier.

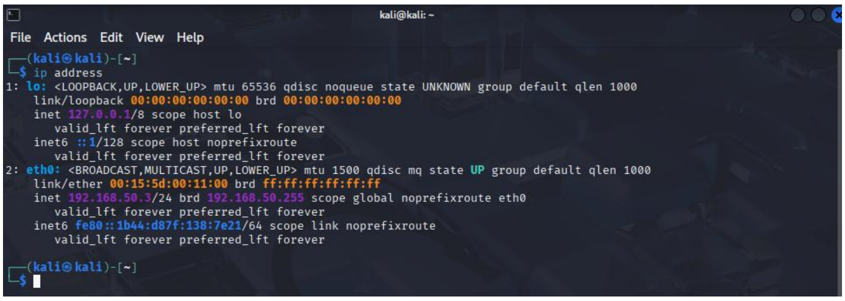

Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
Advanced IP Scanner
File View Settings Help
Scan
Example: 192.168.0.1-100, 192.168.0.200
Search
Results
Favorites
Administrator: Command...
Search
ENG
GA
3:02 AM
6/24/2025

192.168.0.1-254

Status	Name	IP	Manufacturer	MAC address	Comments
	192.168.0.120	192.168.0.120	Dell Inc.	B8:AC:6F:8B:4D:16	

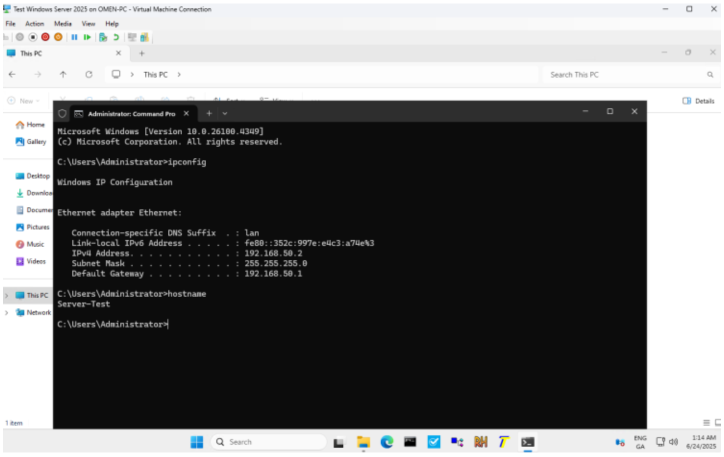
) alive, 1 dead, 253 unknown

FIG 8.1, Kali IP Configuration



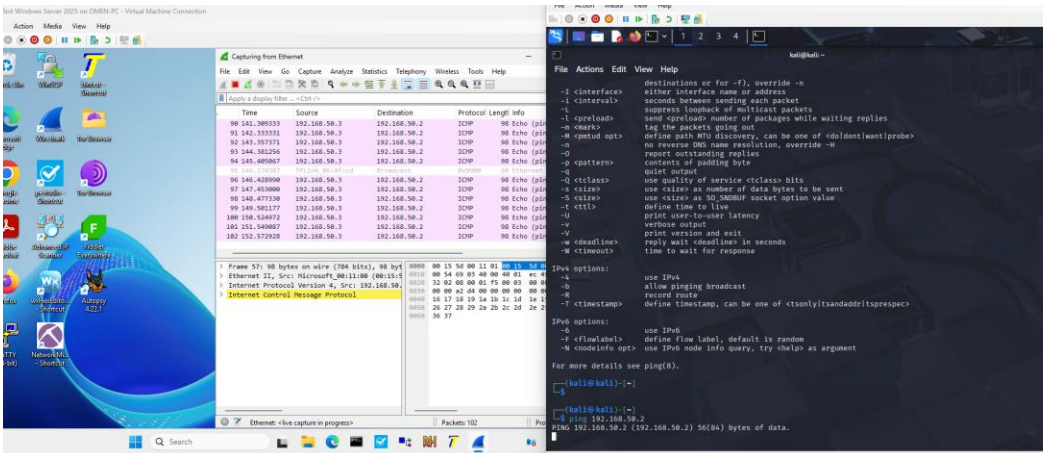
```
┌──(kali㉿kali)-[~]
└─$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:11:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.3/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::1b44:d87f:138:7e21/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

FIG 8.2, Windows IP Configuration



```
Microsoft Windows [Version 10.0.26100.4349]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::352c:997e:e4c3:a74e%3
   IPv4 Address. . . . . . . . . . . : 192.168.50.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1

C:\Users\Administrator>hostname
Server-Test

C:\Users\Administrator>
```

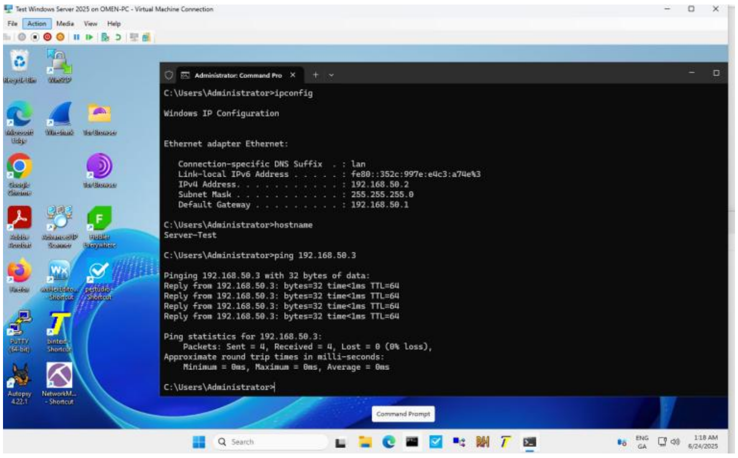
FIG 8.3, Testing of Ping from Kali Linux Machine to windows machine server-test



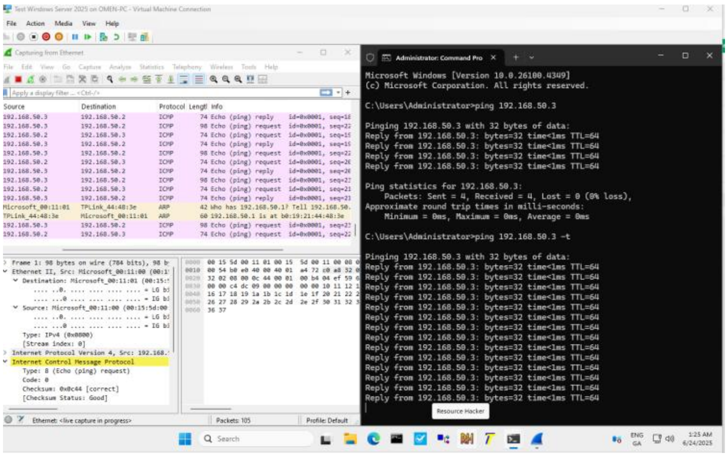
```
    Time        Source            Destination       Protocol Lengtl Info
 90 141.309333  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
 91 142.333331  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
 92 143.357371  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
 93 144.381256  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
 94 145.405067  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
 95 146.274387  TPLink_06:4f:cd   Broadcast         0x9000      60 Ethernet
 96 146.428990  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
 97 147.453000  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
 98 148.477330  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
 99 149.501177  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
100 150.524972  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
101 151.549087  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin
102 152.572928  192.168.50.3      192.168.50.2      ICMP        98 Echo (pin

> Frame 57: 98 bytes on wire (784 bits), 98 byt
> Ethernet II, Src: Microsoft_00:11:00 (00:15:5
> Internet Protocol Version 4, Src: 192.168.50.
> Internet Control Message Protocol

0000  00 15 5d 00 11 01 00 15  5d 0
0010  00 54 69 03 40 00 40 01  ec 4
0020  32 02 08 00 01 f5 00 03  00 0
0030  00 00 a2 d4 00 00 00 00  00 0
0040  16 17 18 19 1a 1b 1c 1d  1e 1
0050  26 27 28 29 2a 2b 2c 2d  2e 2
0060  36 37
```

```
                        destinations or for -f), override -n
  -I <interface>        either interface name or address
  -i <interval>         seconds between sending each packet
  -L                    suppress loopback of multicast packets
  -l <preload>          send <preload> number of packages while waiting replies
  -m <mark>             tag the packets going out
  -M <pmtud opt>        define path MTU discovery, can be one of <do|dont|want|probe>
  -n                    no reverse DNS name resolution, override -H
  -O                    report outstanding replies
  -p <pattern>          contents of padding byte
  -q                    quiet output
  -Q <tclass>           use quality of service <tclass> bits
  -s <size>             use <size> as number of data bytes to be sent
  -S <size>             use <size> as SO_SNDBUF socket option value
  -t <ttl>              define time to live
  -U                    print user-to-user latency
  -v                    verbose output
  -V                    print version and exit
  -w <deadline>         reply wait <deadline> in seconds
  -W <timeout>          time to wait for response

IPv4 options:
  -4                    use IPv4
  -b                    allow pinging broadcast
  -R                    record route
  -T <timestamp>        define timestamp, can be one of <tsonly|tsandaddr|tsprespec>

IPv6 options:
  -6                    use IPv6
  -F <flowlabel>        define flow label, default is random
  -N <nodeinfo opt>     use IPv6 node info query, try <help> as argument

For more details see ping(8).

┌──(kali㉿kali)-[~]
└─$ 

┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.2
PING 192.168.50.2 (192.168.50.2) 56(84) bytes of data.
```

FIG 8.4, Testing of Ping from windows Machine server-test to Kali Linux


Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File
Action
Media
View
Help
Administrator: Command Pro
Command Prompt
Search
ENG
GA
1:18 AM
6/24/2025

```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::352c:997e:e4c3:a74e%3
   IPv4 Address. . . . . . . . . . . : 192.168.50.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1

C:\Users\Administrator>hostname
Server-Test

C:\Users\Administrator>ping 192.168.50.3

Pinging 192.168.50.3 with 32 bytes of data:
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

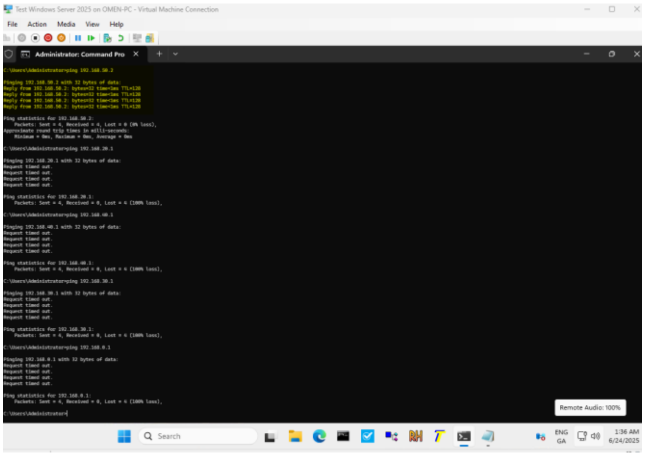

Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File
Action
Media
View
Help
Capturing from Ethernet
Apply a display filter ... <Ctrl-/>
Ethernet: <live capture in progress>
Packets: 105
Profile: Default
Administrator: Command Pro
Resource Hacker
Search
ENG
GA
1:25 AM
6/24/2025

```
Source              Destination         Protocol Lengtl Info
192.168.50.3        192.168.50.2        ICMP        74 Echo (ping) reply    id=0x0001, seq=18
192.168.50.3        192.168.50.2        ICMP        98 Echo (ping) request  id=0x0001, seq=22
192.168.50.2        192.168.50.3        ICMP        74 Echo (ping) request  id=0x0001, seq=15
192.168.50.3        192.168.50.2        ICMP        74 Echo (ping) reply    id=0x0001, seq=15
192.168.50.3        192.168.50.2        ICMP        98 Echo (ping) request  id=0x0001, seq=22
192.168.50.2        192.168.50.3        ICMP        74 Echo (ping) request  id=0x0001, seq=26
192.168.50.3        192.168.50.2        ICMP        74 Echo (ping) reply    id=0x0001, seq=26
192.168.50.3        192.168.50.2        ICMP        98 Echo (ping) request  id=0x0001, seq=22
192.168.50.2        192.168.50.3        ICMP        74 Echo (ping) request  id=0x0001, seq=21
192.168.50.3        192.168.50.2        ICMP        74 Echo (ping) reply    id=0x0001, seq=21
Microsoft_00:11:01  TPLink_44:48:3e     ARP         42 Who has 192.168.50.1? Tell 192.168.50.
TPLink_44:48:3e     Microsoft_00:11:01  ARP         60 192.168.50.1 is at b0:19:21:44:48:3e
192.168.50.3        192.168.50.2        ICMP        98 Echo (ping) request  id=0x0001, seq=22
192.168.50.2        192.168.50.3        ICMP        74 Echo (ping) request  id=0x0001, seq=22

> Frame 1: 98 bytes on wire (784 bits), 98 b
v Ethernet II, Src: Microsoft_00:11:00 (00:1
  v Destination: Microsoft_00:11:01 (00:15:5
      .... ..0. .... .... .... .... = LG bi
      .... ...0 .... .... .... .... = IG bi
  v Source: Microsoft_00:11:00 (00:15:5d:00
      .... ..0. .... .... .... .... = LG bi
      .... ...0 .... .... .... .... = IG bi
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x0c44 [correct]
    [Checksum Status: Good]

0000  00 15 5d 00 11 01 00 15  5d 00 11 00 08 0
0010  00 54 b0 e0 40 00 40 01  a4 72 c0 a8 32 0
0020  32 02 08 00 0c 44 00 01  00 b4 04 ef 59 6
0030  00 00 c4 dc 09 00 00 00  00 00 10 11 12 1
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 2
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 3
0060  36 37
```

```
Microsoft Windows [Version 10.0.26100.4349]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.50.3

Pinging 192.168.50.3 with 32 bytes of data:
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.50.3 -t

Pinging 192.168.50.3 with 32 bytes of data:
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
Reply from 192.168.50.3: bytes=32 time<1ms TTL=64
```

FIG 8.6, Testing of Ping to other networks

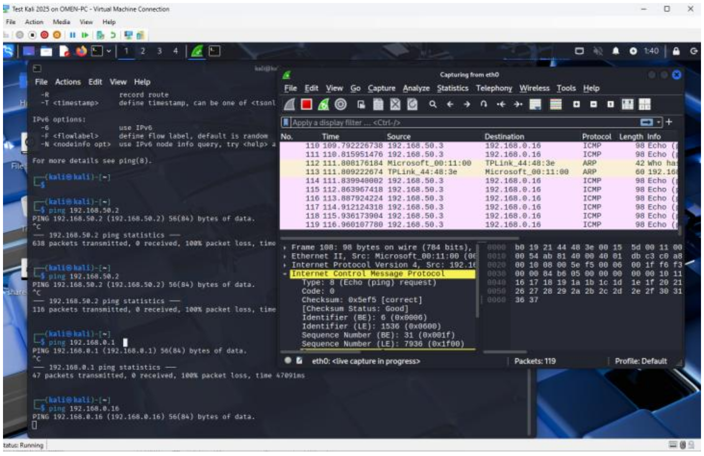
This comes from windows (Nothing should work beyond lab)


Test Windows Server 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
Administrator: Command Pro
Remote Audio: 100%
Search
ENG
GA
1:36 AM
6/24/2025

```
C:\Users\Administrator>ping 192.168.50.2

Pinging 192.168.50.2 with 32 bytes of data:
Reply from 192.168.50.2: bytes=32 time=1ms TTL=128
Reply from 192.168.50.2: bytes=32 time<1ms TTL=128
Reply from 192.168.50.2: bytes=32 time<1ms TTL=128
Reply from 192.168.50.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.50.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 192.168.40.1

Pinging 192.168.40.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.40.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>
```

FIG 8.7, Testing of Ping to other networks

e.g. hypervisor on 192.168.0.16 From Kali (Nothing should work beyond lab)


Test Kali 2025 on OMEN-PC - Virtual Machine Connection
File Action Media View Help
1 2 3 4
1:40
File Actions Edit View Help
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Status: Running

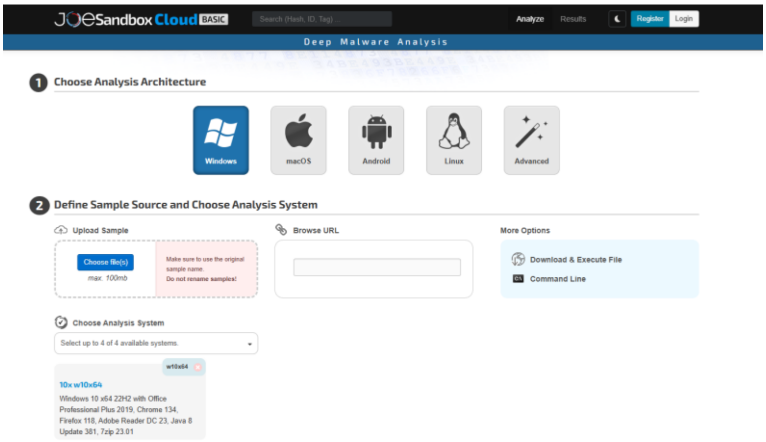
```
  -R                    record route
  -T <timestamp>        define timestamp, can be one of <tsonl

IPv6 options:
  -6                    use IPv6
  -F <flowlabel>        define flow label, default is random
  -N <nodeinfo opt>     use IPv6 node info query, try <help> a

For more details see ping(8).

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.2
PING 192.168.50.2 (192.168.50.2) 56(84) bytes of data.
^C
── 192.168.50.2 ping statistics ──
638 packets transmitted, 0 received, 100% packet loss, time

┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.2
PING 192.168.50.2 (192.168.50.2) 56(84) bytes of data.
^C
── 192.168.50.2 ping statistics ──
116 packets transmitted, 0 received, 100% packet loss, time

┌──(kali㉿kali)-[~]
└─$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
^C
── 192.168.0.1 ping statistics ──
47 packets transmitted, 0 received, 100% packet loss, time 47091ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.0.16
PING 192.168.0.16 (192.168.0.16) 56(84) bytes of data.
```

```
No.    Time          Source                Destination           Protocol Length Info
   110 109.792226738 192.168.50.3          192.168.0.16          ICMP       98 Echo (
   111 110.815951476 192.168.50.3          192.168.0.16          ICMP       98 Echo (
   112 111.808176184 Microsoft_00:11:00    TPLink_44:48:3e       ARP        42 Who has
   113 111.809222674 TPLink_44:48:3e       Microsoft_00:11:00    ARP        60 192.168
   114 111.839940002 192.168.50.3          192.168.0.16          ICMP       98 Echo (
   115 112.863967418 192.168.50.3          192.168.0.16          ICMP       98 Echo (
   116 113.887924224 192.168.50.3          192.168.0.16          ICMP       98 Echo (
   117 114.912124318 192.168.50.3          192.168.0.16          ICMP       98 Echo (
   118 115.936173904 192.168.50.3          192.168.0.16          ICMP       98 Echo (
   119 116.960107780 192.168.50.3          192.168.0.16          ICMP       98 Echo (
```

```
› Frame 108: 98 bytes on wire (784 bits),      0000  b0 19 21 44 48 3e 00 15  5d 00 11 00
› Ethernet II, Src: Microsoft_00:11:00 (00     0010  00 54 ab 81 40 00 40 01  db c3 c0 a8
› Internet Protocol Version 4, Src: 192.16     0020  00 10 08 00 5e f5 00 06  00 1f f6 f3
⌄ Internet Control Message Protocol            0030  00 00 84 b6 05 00 00 00  00 00 10 11
    Type: 8 (Echo (ping) request)              0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21
    Code: 0                                    0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31
    Checksum: 0x5ef5 [correct]                 0060  36 37
    [Checksum Status: Good]
    Identifier (BE): 6 (0x0006)
    Identifier (LE): 1536 (0x0600)
    Sequence Number (BE): 31 (0x001f)
    Sequence Number (LE): 7936 (0x1f00)
```

eth0: <live capture in progress>   Packets: 119   Profile: Default

FIG 8.8, Joe Sandbox



1 Choose Analysis Architecture

2 Define Sample Source and Choose Analysis System

Make sure to use the original sample name.
Do not rename samples!

Choose Analysis System

Select up to 4 of 4 available systems.

10x w10x64

Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 134, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01