

# Digital SkillUp Africa Final Capstone Project in Cybersecurity

Project Title: Building a Virtual  
Cybersecurity Laboratory and Conducting  
Android Forensics Investigations

Part Number: ONE

Part Title: Virtual Cybersecurity Lab Step

Student Name: ONAEKO, Emmanuel  
Oladipupo

Email: eonaeko778@gmail.com

## Activites

- Install a Type 2 hypervisor
- Create and configure two virtual Machines
- Establish internal virtual networking between VMs
- Verify connectivity via ping tests, shared directories and service enumeration.

## Tools used for this cybersecurity lab setup

Operations	Tools
Hypervisor	Virtual Box
Operating Systems	Kali Linux, Windows
Service Enumeration	Nmap

## Installation of Type 2 hypervisor

This virtual cybersecurity lab was set up through the use of a Type 2 hypervisor “**Virtual Box**” which was the platform to visualize two different operating systems used in the lab which are **Kali Linux** and **Windows 10**, the OS were allocated the memory and processor needed to perform effectively and efficiently and were configured with password and user profile as required and they were tested for some functionality that is also present in the host device like internet connectivity.

## Internal Virtual networking between VMs

The VMs, although under the same hypervisor, are separate devices and would not normally communicate, so to enable them to communicate or perform internal networking, they must be under the network, and to do this, I perform the following:

### 1. Change of network adapter settings

The network adapter configuration was configured on the hypervisor “Virtual Box” to change from NAT to internal network, and this was done for both Kali Linux and Windows VMs, which meant that they were now on the same logical network.

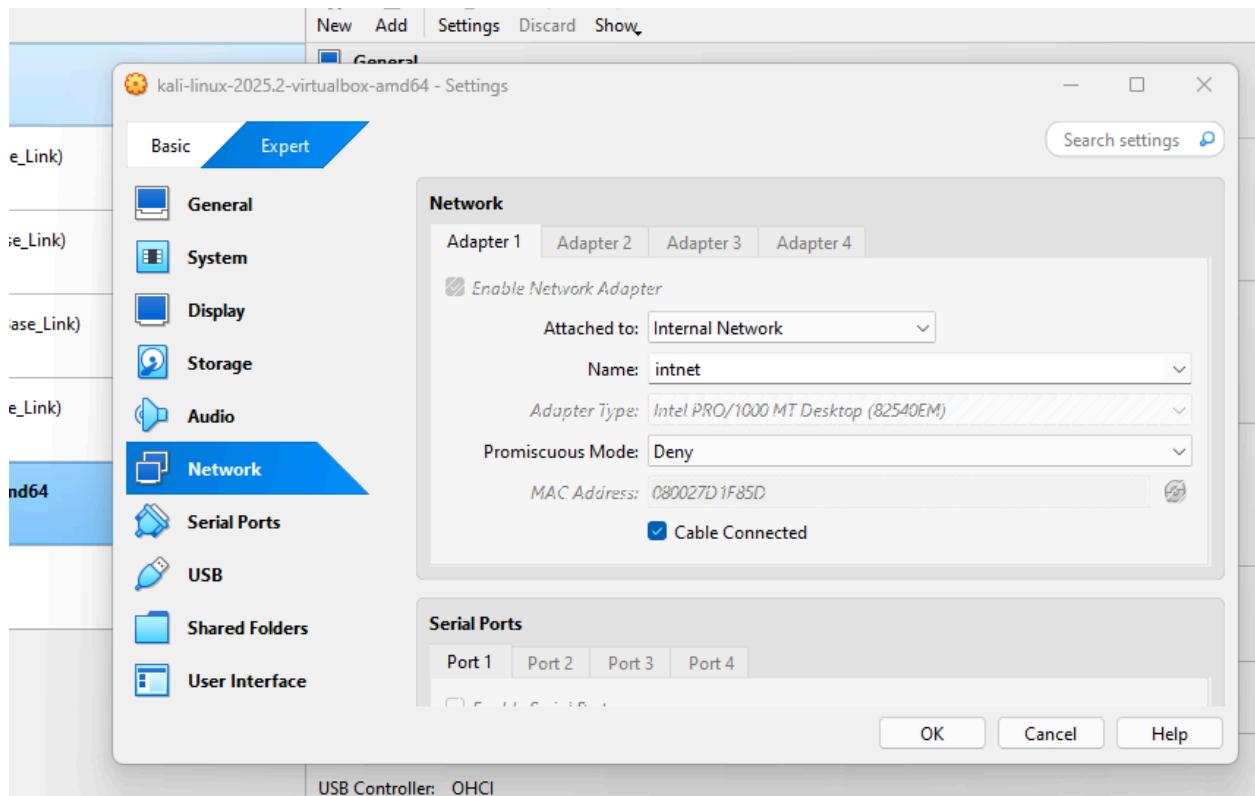


Fig. 1 shows the configuration of the network adapter on Kali Linux.

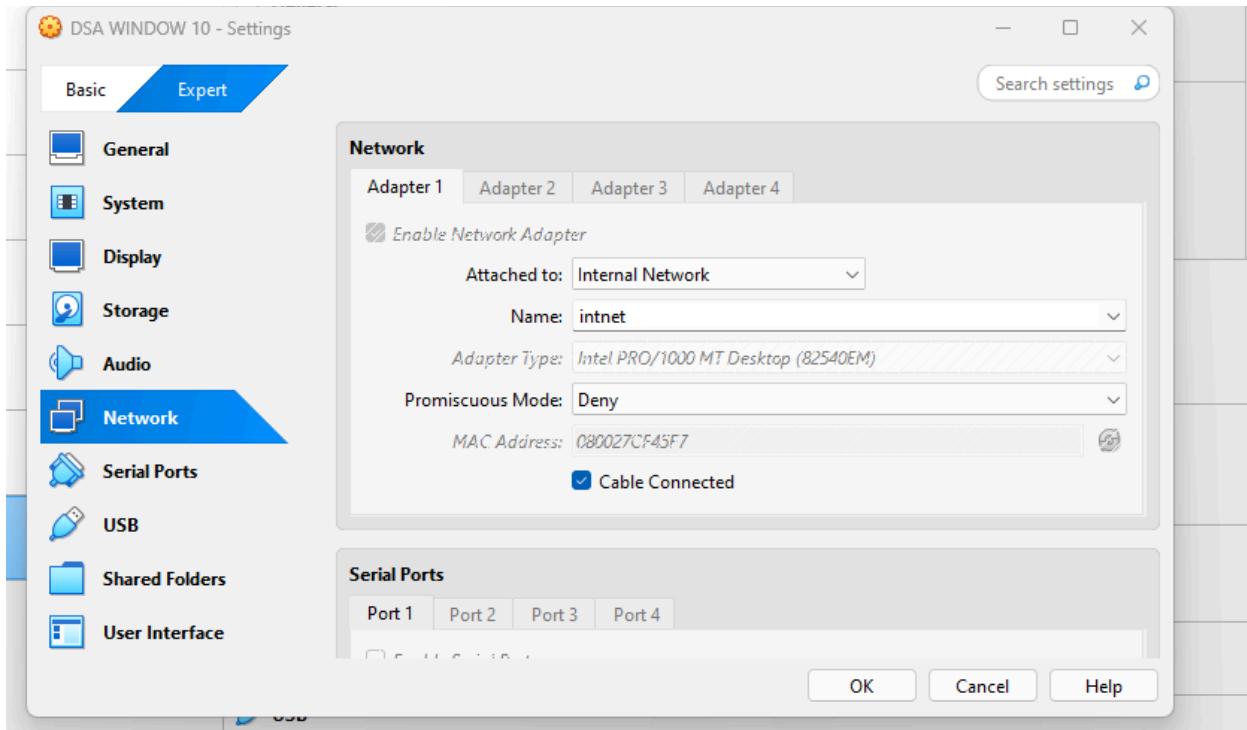
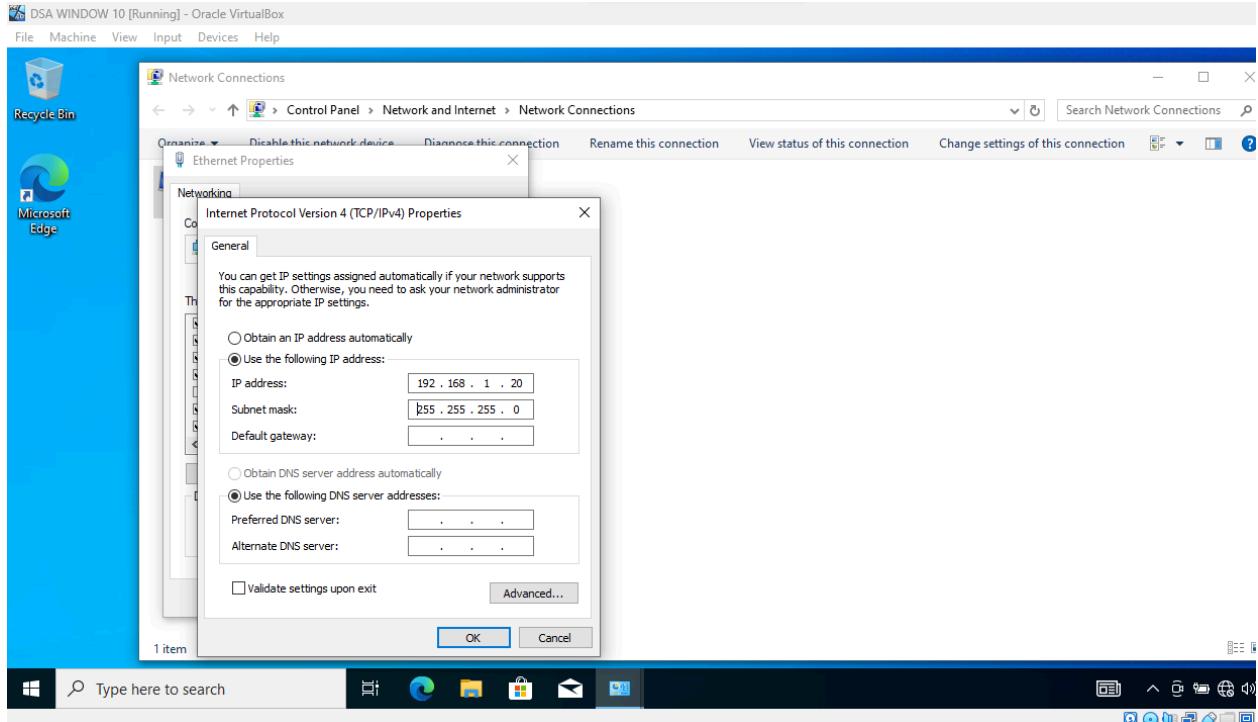


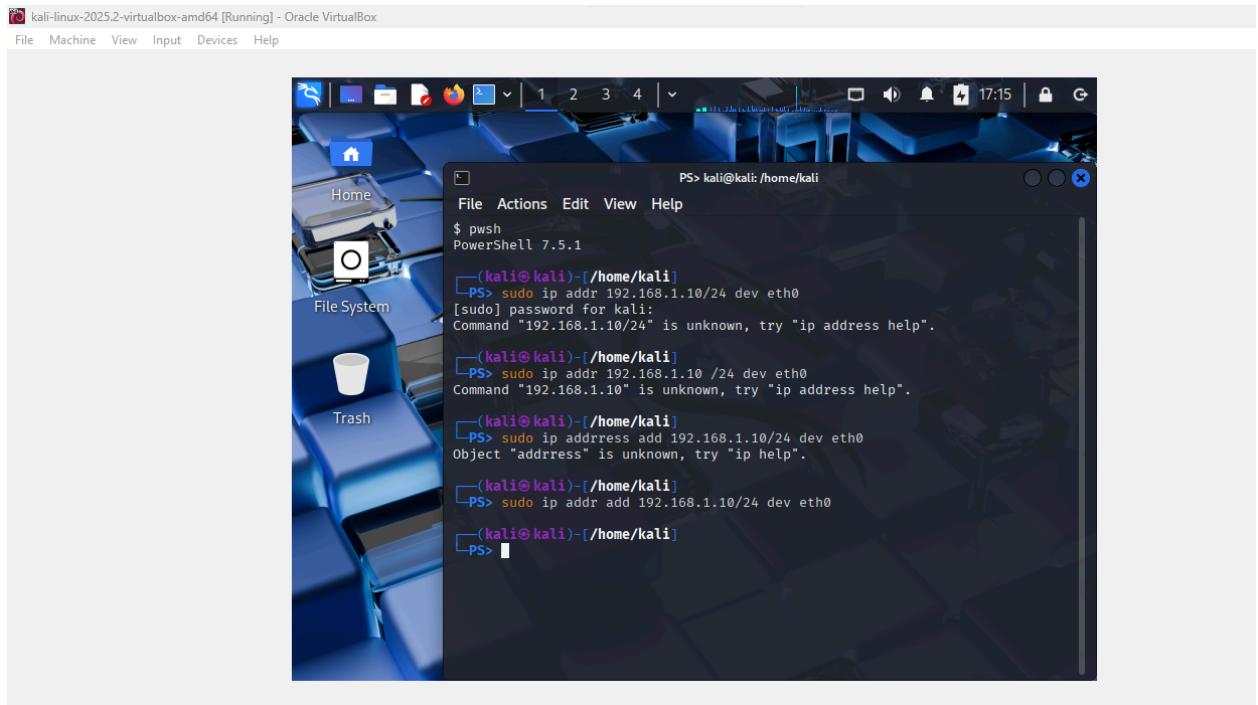
Fig. 2 shows the configuration of the network adapter on Windows 10

## 2. Configure private IP addresses from the same subnet to both VMs

For internal networking and communications to occur, both Kali Linux were configured with IP addresses from the same subnets. I configured Kali with IP address **192.168.1.10** with subnet mask: **255.255.255.0** and Windows VMs with IP address **192.168.1.20** with subnet mask: **255.255.255.0**. Kali Linux was configured from the terminal with the command: “`sudo ip addr add 192.168.1.10`” while Windows was configured through the GUI



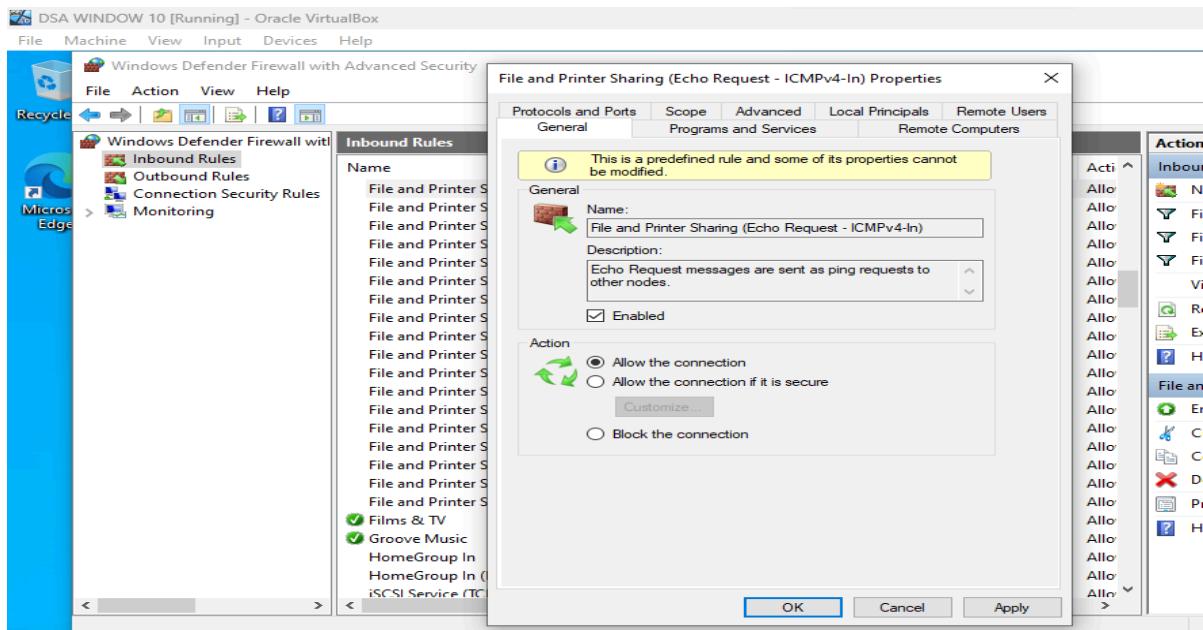
*Fig. 3 shows the IP configuration on the Windows VM*



*Fig. 4 shows the IP configuration on Kali Linux.*

### 3. Verification of Internal networking via ping tests

I verify their internal networking and communications by carrying out ping tests on the terminal of both virtual machines. The ping fails at first, but after setting up the inbound rules on Windows Firewall to allow ICMP ECHO messages, I ping again, and the result was successful.



*Fig. .5 shows a capture of the Windows Defender firewall being configured to allow transport.*

The screenshot shows a Kali Linux terminal window titled 'Server Not Found'. The terminal output is as follows:

```

PS> kali@kali: /home/kali
File Actions Edit View Help
From 192.168.1.10 icmp_seq=3 Destination Host Unreachable
From 192.168.1.10 icmp_seq=4 Destination Host Unreachable
From 192.168.1.10 icmp_seq=5 Destination Host Unreachable
From 192.168.1.10 icmp_seq=6 Destination Host Unreachable
^C
— 192.168.1.20 ping statistics —
9 packets transmitted, 0 received, +6 errors, 100% packet loss, time 8176ms
pipe 3

└─(kali㉿kali)-[~/home/kali]
└─PS> ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=128 time=2.01 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=128 time=1.39 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=128 time=0.710 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=128 time=0.625 ms
64 bytes from 192.168.1.20: icmp_seq=5 ttl=128 time=0.758 ms
64 bytes from 192.168.1.20: icmp_seq=6 ttl=128 time=0.819 ms
64 bytes from 192.168.1.20: icmp_seq=7 ttl=128 time=0.816 ms
64 bytes from 192.168.1.20: icmp_seq=8 ttl=128 time=0.766 ms
64 bytes from 192.168.1.20: icmp_seq=9 ttl=128 time=0.783 ms
64 bytes from 192.168.1.20: icmp_seq=10 ttl=128 time=0.745 ms
^C
— 192.168.1.20 ping statistics —
10 packets transmitted, 10 received, 0% packet loss, time 9173ms
rtt min/avg/max/mdev = 0.625/0.941/2.008/0.406 ms
└─(kali㉿kali)-[~/home/kali]

```

Fig. .6 shows a capture of the successful ping tests to 192.168.1.20 from Kali Linux.

## 4. Shared Files

After Connectivity was established between the two VMs, I created a folder on the Windows VM, named WannaShare, and configured it to be a shared folder accessible to computers on the network. I accessed the file through the Kali Linux VMs after proper research on how to access the files through the terminal. I use the command: “`sudo smbclient //192.168.1.20/WannaShare -u 'emmanuel' -dfr dsa`” to access the content of the folder, which was successful.

```

kali@kali:~$ tree connect failed: NT_STATUS_BAD_NETWORK_NAME youtube.com
└── (kali㉿kali)-[~]
    └── $ sudo smbclient //192.168.1.20/Sharedfiles -U "emmanuel dfir dsa"
        Password for [WORKGROUP]emmanuel dfir dsa:
        tree connect failed: NT_STATUS_BAD_NETWORK_NAME

        (kali㉿kali)-[~]
        └── $ sudo smbclient //192.168.1.20/WannaShare -U "emmanuel dfir dsa"
            Password for [WORKGROUP]emmanuel dfir dsa:
            tree connect failed: NT_STATUS_BAD_NETWORK_NAME

            Hmm. We're having trouble finding that site.

            (kali㉿kali)-[~]
            └── $ sudo smbclient //192.168.1.20/WannaShare -U "emmanuel dfir dsa"
                Password for [WORKGROUP]emmanuel dfir dsa:
                Try "help" to get a list of possible commands.
                smb: > ls
                    .                               we can't connect to the server at www.youtube.com.
                    D          0 Sat Jul  5 18:37:43 2025
                    ..                         D If you 0 Sat Jul  5 18:37:43 2025
                    Abstact for journal of sociology (1).docx   A  16376 Sat Jul  5 18:37:43 2025
                    :38 2025                         * To again later
                    ABSTRACT FOR NIGERIAN LABOUR LAWS AND EMPLOYMENT PRACTICES.docx   A
                    13976 Sat Jul  5 18:37:38 2025                         * Check your network connection
                    AFRICA EXECUTIVE TRAINING AND CAREER LIMITED.docx   A  13143 Sat Jul
                    5 18:37:37 2025                         * Check that Firefox has permission to access the web (you might be connected but behind a firewall)

                12953651 blocks of size 4096. 7389829 blocks available
                smb: > [REDACTED] Try Again

```

Fig. .7 shows a capture of the shared folders being accessed, with some previous errors on Kali Linux.

```

kali@kali:~$ tree connect failed: NT_STATUS_BAD_NETWORK_NAME youtube.com
└── (kali㉿kali)-[~]
    └── $ sudo smbclient //192.168.1.20/Sharedfiles -U "emmanuel dfir dsa"
        Password for [WORKGROUP]emmanuel dfir dsa:
        tree connect failed: NT_STATUS_BAD_NETWORK_NAME

        (kali㉿kali)-[~]
        └── $ sudo smbclient //192.168.1.20/WannaShare -U "emmanuel dfir dsa"
            Password for [WORKGROUP]emmanuel dfir dsa:
            tree connect failed: NT_STATUS_BAD_NETWORK_NAME

            Hmm. We're having trouble finding that site.

            (kali㉿kali)-[~]
            └── $ sudo smbclient //192.168.1.20/WannaShare -U "emmanuel dfir dsa"
                Password for [WORKGROUP]emmanuel dfir dsa:
                Try "help" to get a list of possible commands.
                smb: > ls
                    .                               we can't connect to the server at www.youtube.com.
                    D          0 Sat Jul  5 18:37:43 2025
                    ..                         D If you 0 Sat Jul  5 18:37:43 2025
                    Abstact for journal of sociology (1).docx   A  16376 Sat Jul  5 18:37:43 2025
                    :38 2025                         * To again later
                    ABSTRACT FOR NIGERIAN LABOUR LAWS AND EMPLOYMENT PRACTICES.docx   A
                    13976 Sat Jul  5 18:37:38 2025                         * Check your network connection
                    AFRICA EXECUTIVE TRAINING AND CAREER LIMITED.docx   A  13143 Sat Jul
                    5 18:37:37 2025                         * Check that Firefox has permission to access the web (you might be connected but behind a firewall)

                12953651 blocks of size 4096. 7389829 blocks available
                smb: > [REDACTED] Try Again

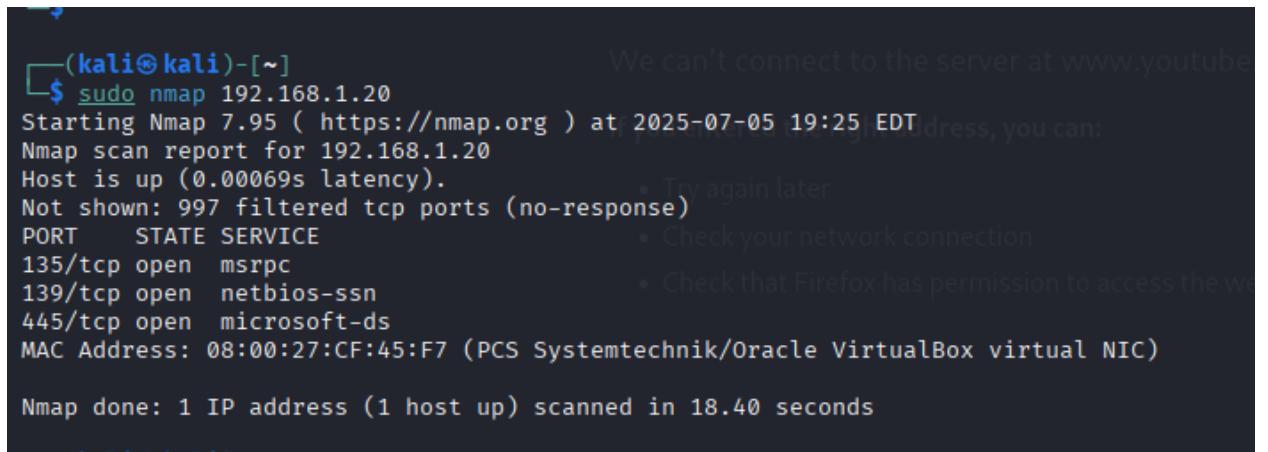
```

Fig. .8 shows a capture of the files being accessed through the terminal.

## 5. Service Enumeration

To perform service enumeration, I used the nmap function to do a number of vulnerability assessments on the Windows OS.

### **nmap 192.168.1.20 to scan for the IP address 192.168.1.20**

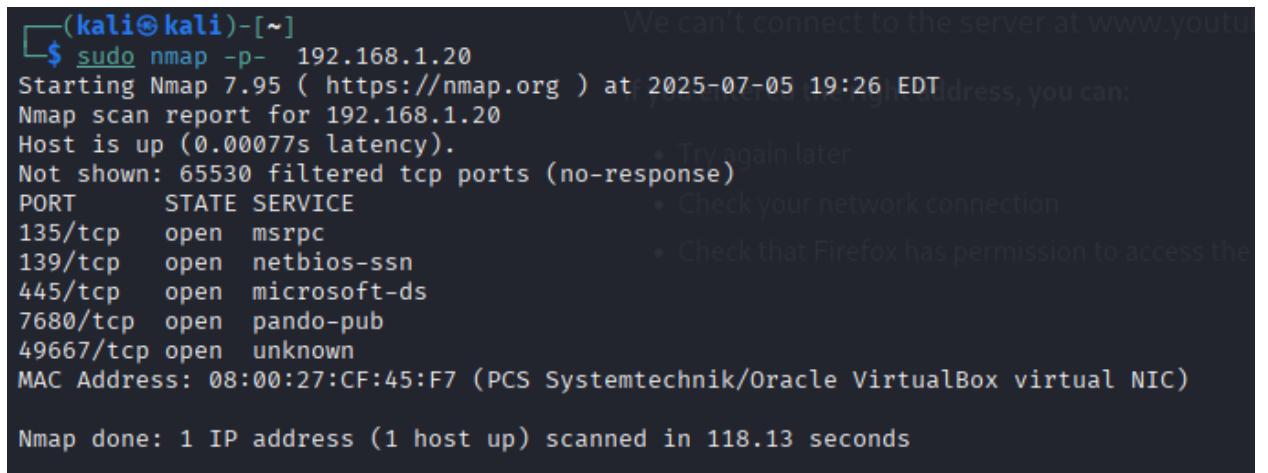


```
(kali㉿kali)-[~]
$ sudo nmap 192.168.1.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 19:25 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00069s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:CF:45:F7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.40 seconds
```

Fig. .9 shows a capture of nmap scanning the IP address of 192.168.1.20

### **nmap -p- 192.168.1.20 scans all 65535 ports on the target IP address: 192.168.1.20**



```
(kali㉿kali)-[~]
$ sudo nmap -p- 192.168.1.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 19:26 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00077s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
7680/tcp   open  pando-pub
49667/tcp  open  unknown
MAC Address: 08:00:27:CF:45:F7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 118.13 seconds
```

Fig. .10 shows a capture of nmap scanning the IP address of 192.168.1.20 for open ports

### **Nmap-sS -sV 192.168.1.20 scans for all services running on open ports.**

```
(kali㉿kali)-[~] $ sudo nmap -sS -sV 192.168.1.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 19:30 EDT
Nmap scan report for 192.168.1.20
Host is up (0.00063s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
MAC Address: 08:00:27:CF:45:F7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.24 seconds
(kali㉿kali)-[~]
```

Fig. .11 shows a capture of nmap scanning the IP address of 192.168.1.20 for all services on open ports