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

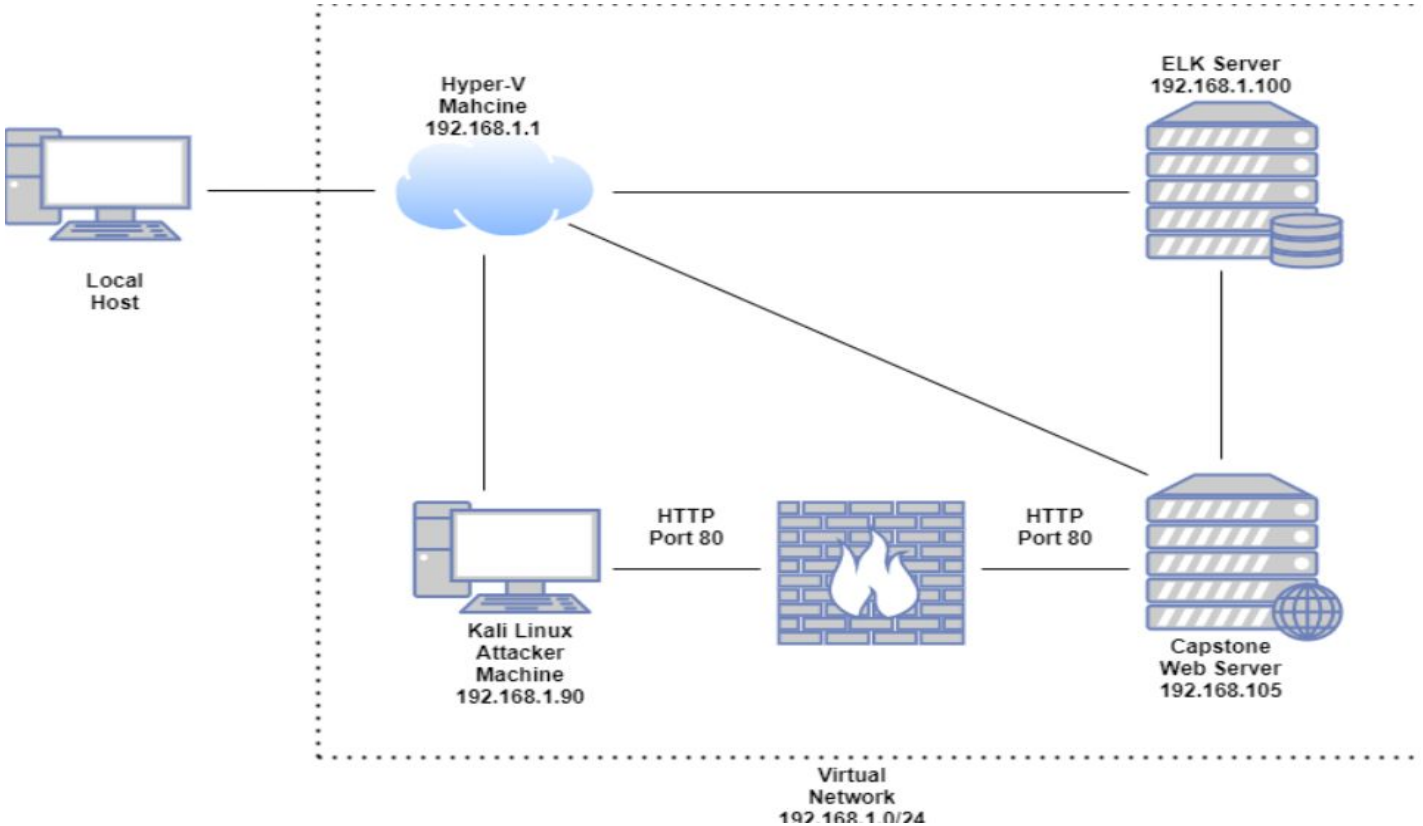
03 **Blue Team**: Log Analysis and Attack Characterization

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

Network Topology

Red Team
Security Assessment

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux 2020.1
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04.1
Hostname: ELK

IPv4:192.168.1.105
OS: 18.04.1
Hostname:
Capstone/server1

IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper-V
Manager

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kai Machine	192.169.1.90	Attacker Machine
Capstone	192.168.1.105	Vulnerable Machine
ELK	192.168.1.100	Monitoring Machine
Hyper V Manger	192.168.1.1	Software that virtualizes hardware into virtual machines/servers

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80	Any open ports can be used as an attack by a hacker to get into the system. Port 80 is a common open port on servers.	It allowed the red team to find private directory with accessible files.
Accessible Files	Servers may store a set of files underneath a “root” directory that is accessible to the server’s users.	It allowed the red team to find and exploit the user files after accessing the IP on port 80.
Brute Force Password	In a BFA the password is easy to obtain found in a wordlist to be hacked.	The red team used BFA to find Ashtons password which was Leopoldo.
Hashed Password	Hashed password can be cracked through diffent types of tools such as hashcat, John the Ripper, etc.	This allowed the red team to use md5cracker to identify the password for John. which was linux4u.

Exploitation: Open Port 80

01

Tools & Processes

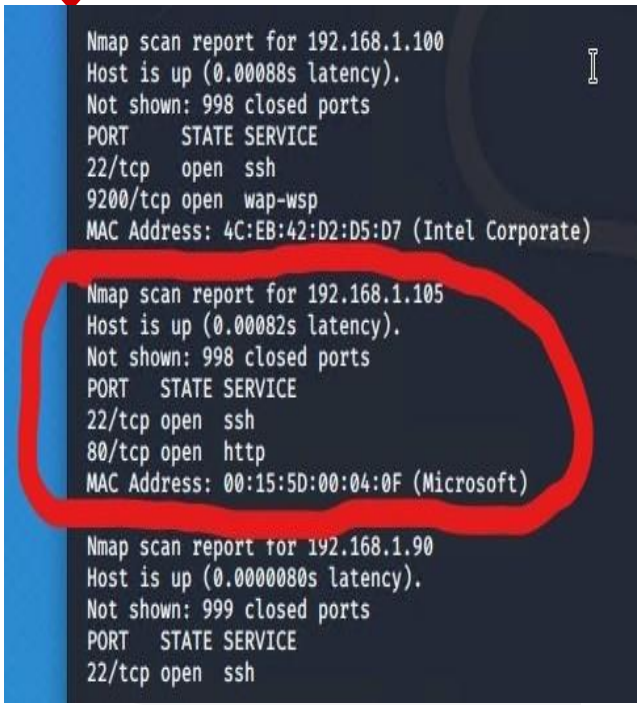
I used nmap to scan for any open ports and services in our network.

02

Achievements

We found that IP address 192.168.1.105 had an open port 80, through which we were able to access a directory with important files.

03



Exploitation: Accessible Files

01

Tools & Processes

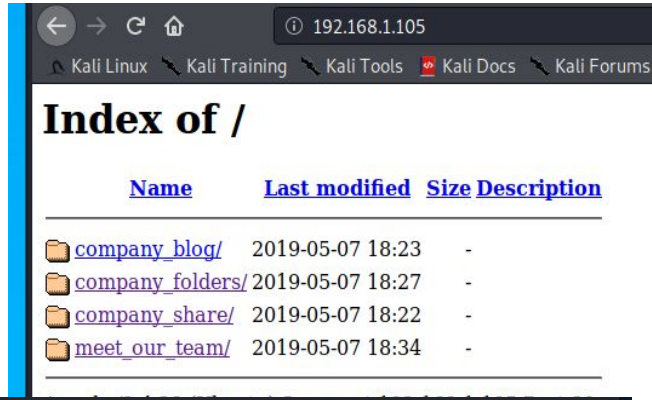
Using the open port 80, we opened a web browser and navigate to 192.168.1.105 to see and view anything important.

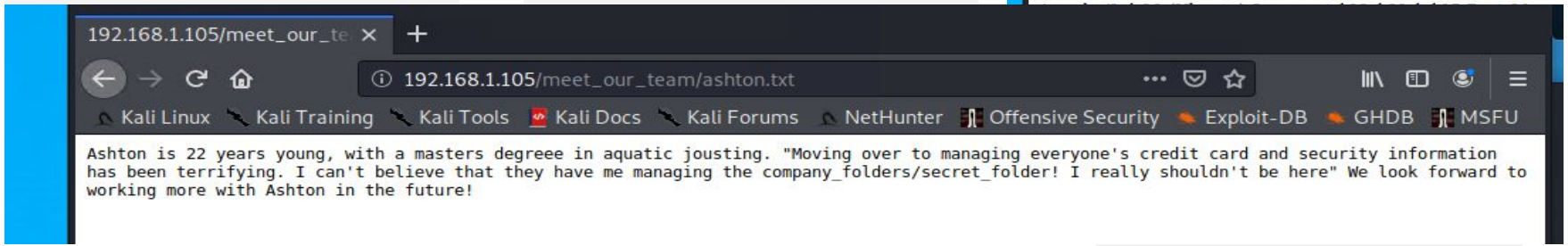
02

Achievements

Accessing the files gave us information on which users had access to what and that where their secret files were located

03





Exploitation: Brute Force Attack

01

Tools & Processes

Use the tool Hydra to brute force Ashtons password using his username.

02

Achievements

The exploit granted us user shell access into the victim's machine so we could navigate to the secret files.

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 o
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 o
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 o
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 101
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 o
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143
[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 2021-10-21
root@Kali:/usr/share/wordlists#
```

Exploitation: Webdav Connection

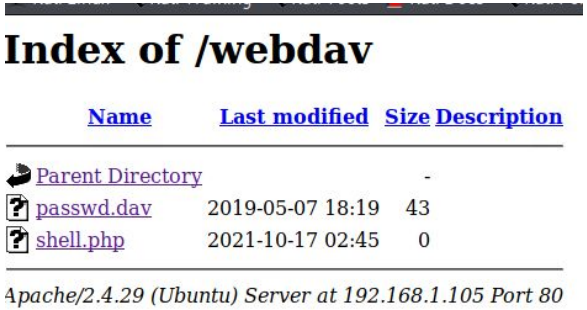
01

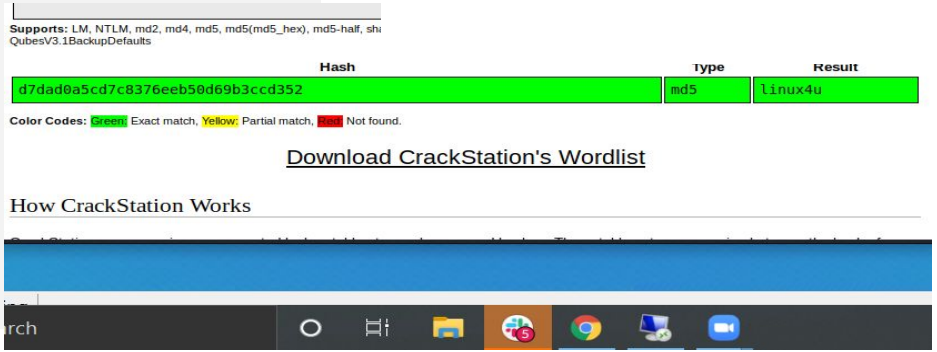
Tools & Processes
I used the website CrackStation to find the decipher the hashed password for John.

02

Achievements
The password found granted us access to system through th WebDav connection, which later allowed us to upload a shell script to attack.

03





Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Evidence Explantation

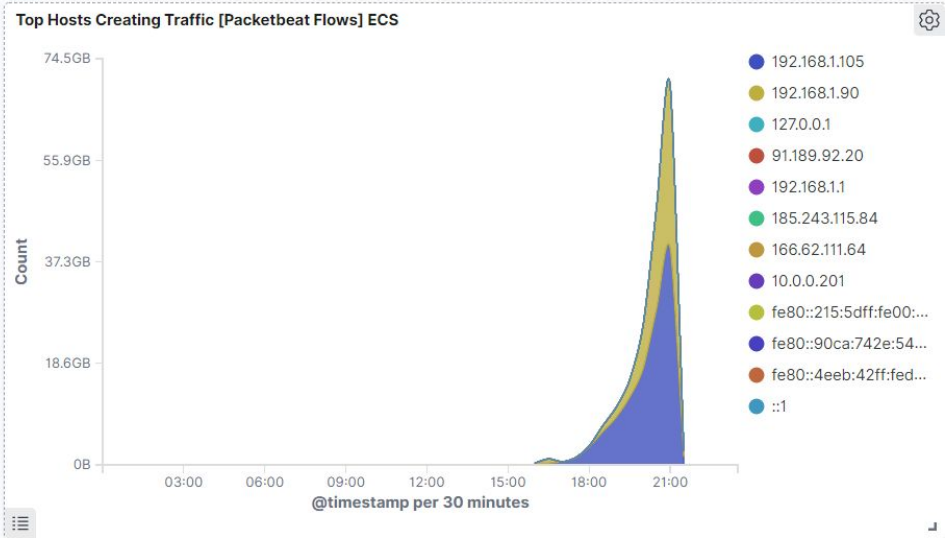
- Port scan started at 4:00pm.
- 130.5MB packets were sent from 192.168.1.90.
- The high point of the traffic shows that this is a port scan.

Dashboard

Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.105	192.168.1.100	120.3GB	6.5GB
192.168.1.105	185.125.190.28	457.4KB	205.4MB
192.168.1.105	91.189.88.142	120.2KB	25.1MB
192.168.1.105	169.254.169.254	108KB	266.2KB
192.168.1.105	91.189.92.38	71.8KB	5.1MB
192.168.1.90	192.168.1.100	64.9GB	1.7GB
192.168.1.90	192.168.1.105	130.5MB	242.2MB
192.168.1.90	192.168.1.1	1.9MB	142.6KB
192.168.1.90	192.168.1.90	756KB	704KB
192.168.1.90	142.250.65.68	251KB	4MB

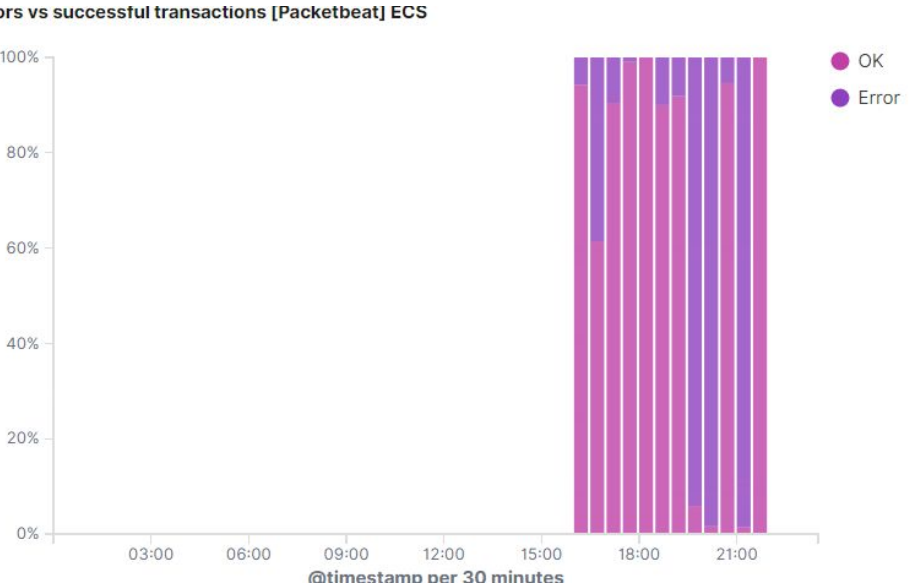
Export: Raw Formatted

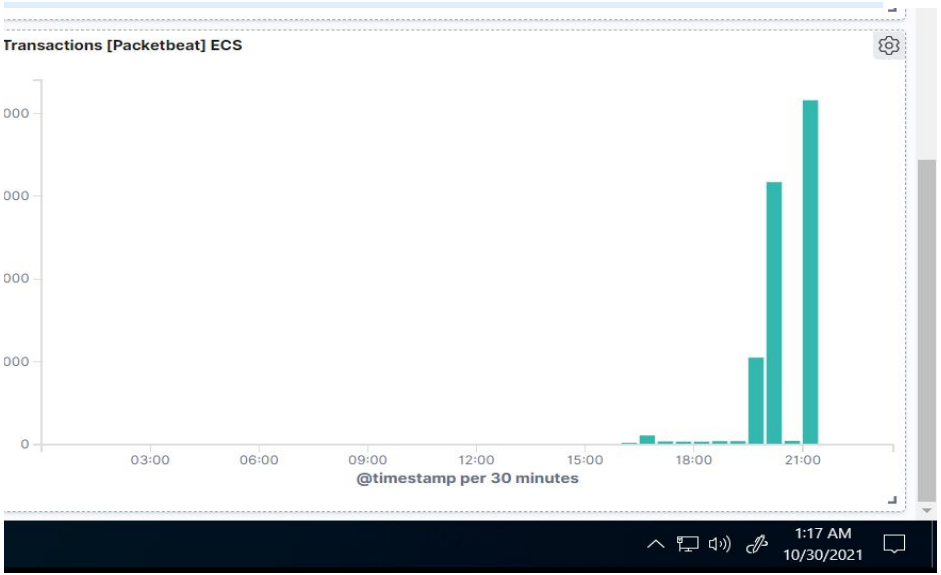


Analysis: Finding the Request for the Hidden Directory

Evidence Explained

- The requests started at 4pm with 30,847 requested
- The Secret Folder was requested which contained instructions on how to access the webdav server, along with a hashed password.





Analysis: Finding the WebDAV Connection

Evidence Explained

- 26 requests were in this webdav directory.
- The php- reverse shell php file was requested a number of times.

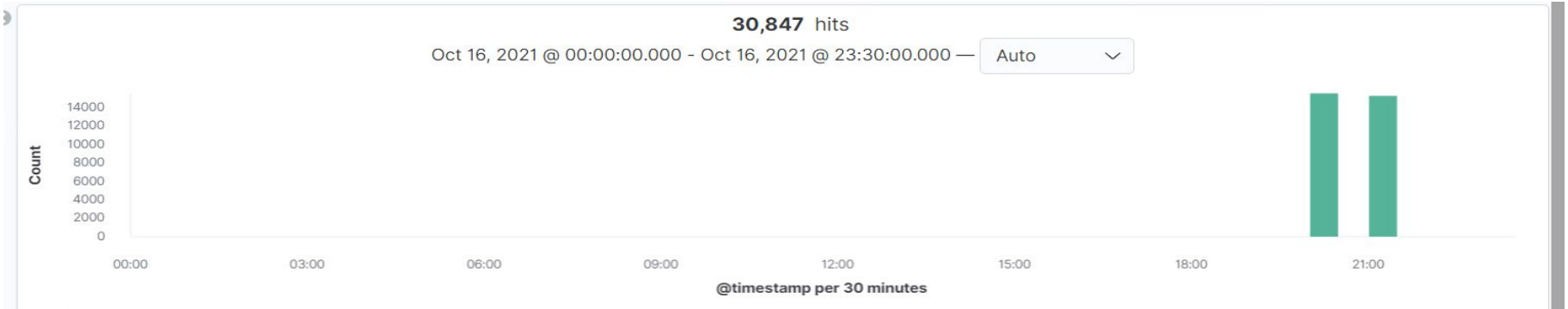
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	30,847
http://127.0.0.1/server-status?auto=	1,783
http://192.168.1.105/	26
http://192.168.1.105/webdav	26
http://192.168.1.105/company_folders/secret_folder/	18

Analysis: Uncovering the Brute Force Attack

Evidence Explained

- 30,847 requests were made in the attack.
- Out of 30,847 18 were successful.



Time	_source
Oct 16, 2021 @ 21:06:01.337	url.path: /company_folders/secret_folder @timestamp: Oct 16, 2021 @ 21:06:01.337 source.ip: 192.168.1.90 source.port: 51094 source.bytes: 163B client.ip: 192.168.1.90 client.port: 51094 client.bytes: 163B server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized http.version: 1.1
Oct 16, 2021 @ 21:06:01.337	url.path: /company_folders/secret_folder @timestamp: Oct 16, 2021 @ 21:06:01.337 type: http http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.headers.content-length: 460 http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.version: 1.1 http.request.bytes: 163B http.request.headers.content-length: 0 http.request.method: get destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http

Mitigation: Blocking the Port Scan

Alarm

A filter can be activated if detected traffic from a single source IP address is connecting to different ports.

Any IP attempting at access closed ports should have the filter activate.

System Hardening

Install a firewall, an IPS can detect ports scans and shut them down.

Filtering traffic from an IP triggered by the IPS can effectively mitigate port scans.

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alarm could be set to go off for any IP address not on the whitelist that attempts to access.

The threshold for this alarm would be 1, any machine accessing it.

System Hardening

This directory should not allowed to exist on the server.

Rmdir -r this can be used to the remove all files and the directory itself from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

An alert can be made if 401 Unauthorized is returned from the server over a threshold.

Begin with 5 over a 30 minute span to allow forgotten or mistyped passwords and refine.

System Hardening

Limit failed login attempts as well as logins to a whitelist of IP address.

Configure account policies on your server to limit failed login attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

Set an alert for any blacklisted IP attempting to access this directory and all IPs outside the server range should be blacklisted.

The threshold for this alarm should be 1 any attempt should trigger the alarm.

System Hardening

Connections to this shared folder should not be accessible from the web and restricted by the machine using a blacklisted firewall rule.

Blocking ports 80 and 443 and blacklisting all external IPs.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Set an alarm for any .php file that is uploaded. Set firewall to block traffic to the shared folder on ports 80, 443 and 4444.

Any traffic on these ports would warrant a alarm trigger.

System Hardening

Remove the ability to upload files from over the web, all file uploads should be from a local source.

Block port 80, 443, and 4444.


The End