Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Brandon Webb

Table of Contents

This document contains the following sections:

01 **Network Topology**

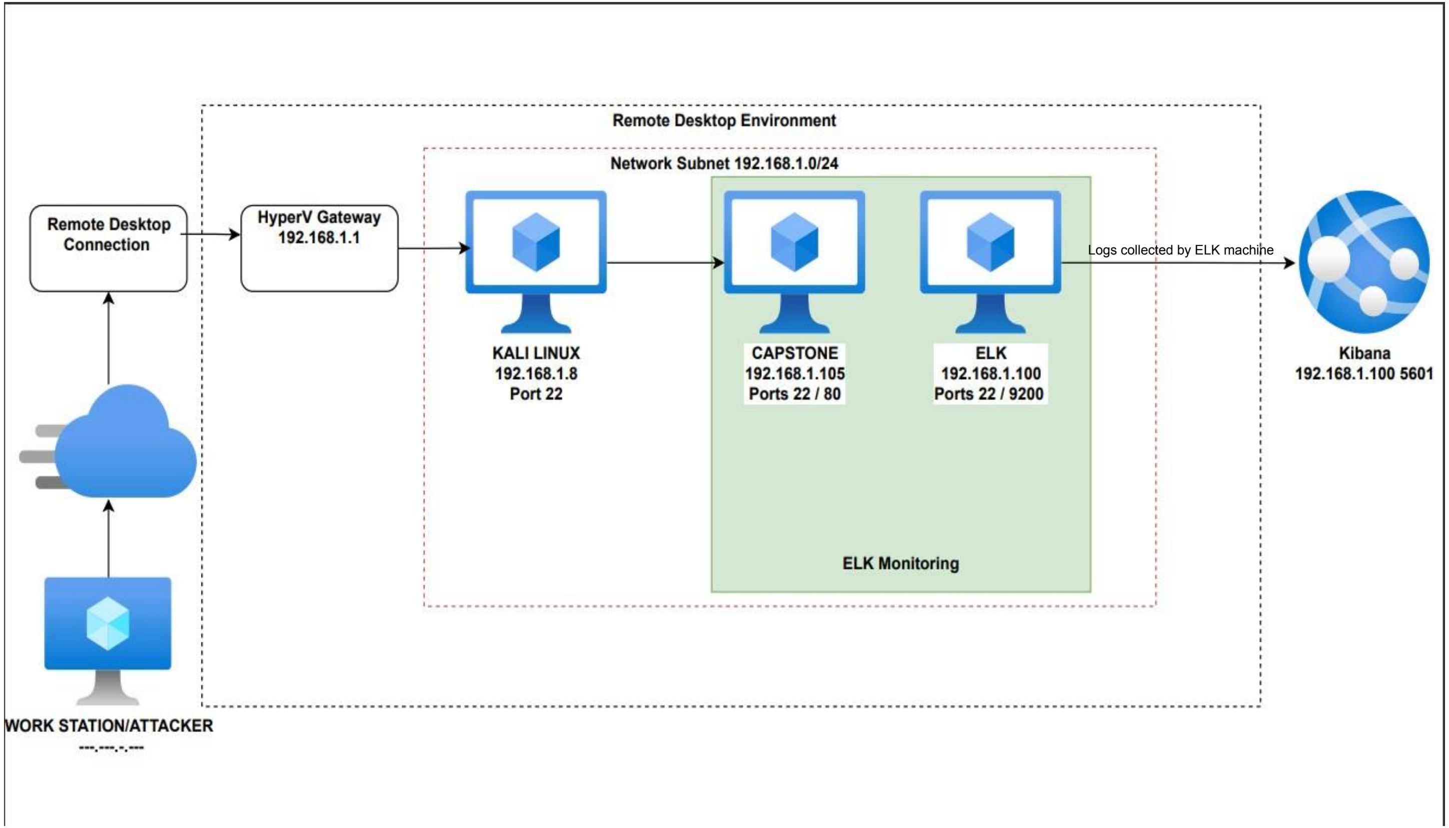
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology


Remote Desktop Environment
Network Subnet 192.168.1.0/24
Remote Desktop Connection
HyperV Gateway 192.168.1.1
KALI LINUX 192.168.1.8 Port 22
CAPSTONE 192.168.1.105 Ports 22 / 80
ELK 192.168.1.100 Ports 22 / 9200
Logs collected by ELK machine
Kibana 192.168.1.100 5601
ELK Monitoring
WORK STATION/ATTACKER
---.---.-.---

Network
Address Range: 192.1.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows 10
Hostname: HyperV Gateway

IPv4: 192.168.1.8
OS: Linux
Hostname: Kali Linux

IPv4: 192.168.1.105
OS: Linux Ubuntu
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux Ubuntu
Hostname: ELK

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper V (Azure) ML-REFVM-684427	192.168.1.1	NATSwitch (Host Machine Cloud based, hosting the 3 VM's.
Kali	192.168.1.8	Attack Machine
ELK	192.168.1.100	Monitoring Machine w/Kibana, logs (data) from Capstone Machine 192.168.1.05
Capstone	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 open with public access.	Open and unsecured access to pretty much anyone on port 80.	Allows anyone on the internet using a web browser (HTTP), access Capstones web server where they can find hidden directories, hidden files, usernames and sensitive data.
Week passwords	Lack of strong passwords like the inclusion of symboles.	Passwords could be discover by social engineering (password checker Leopoldo 21 seconds.
Usernames	To simple can be easily guessed.	Hannah, Ryan, Ashton are predictable names that can be guessed, easily.
Weak Hashed Passwords	Hashed passwords can be easily cracked with websites like crackstation.net	Attackers just need the username and password to corrupt a account.

Exploitation: Open TCP Port 80

01

Tools & Processes

Open and unsecured access to anyone attempting entry using Port 80. Used common command nmap to scan the environment for open TCP ports.

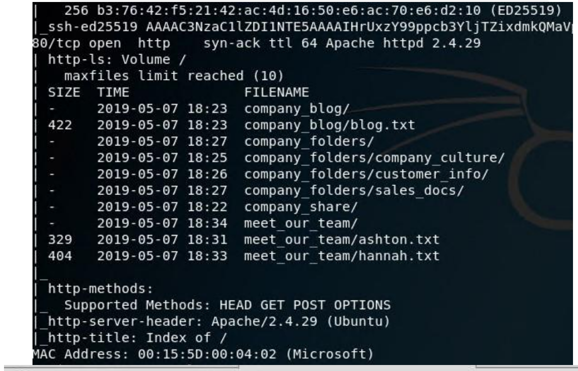
Found the web server port 80 on 192.168.1.105

02

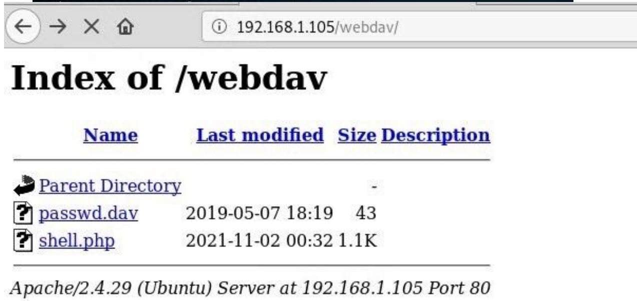
Achievements

This is not a exploit but rather a known method, used by anyone to determine system information like what TCP ports are open, running operating systems. The discovered files on meet_our_team/ashton.txt The ashton.txt allowed the discovery of the secret folder at /company_folders/secret_folder

03



```
|   256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHrUxzY99ppcb3YljTZixdmkQMaV
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
|_
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:02 (Microsoft)
```



192.168.1.105/webdav/

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-11-02 00:32	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Week Password

01

Tools & Processes

Hydra was used to bruteforce ashton's username against the webserver's password protected area.

hydra -l ashton -P /opt/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get "/company_folders/secret_folder"

02

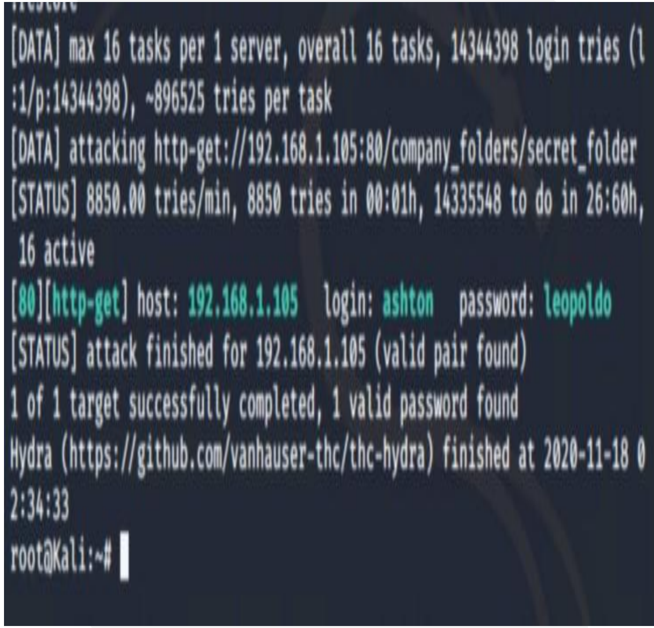
Achievements

This attack provided ashton's password, which was a simple name – **leopoldo**. This provided access to the hidden directory in the webserver.

This revealed a document that contained instructions to connect to webdav with the CEO's username and password hash.

SSH entry into system. This provided access to Ashton's files and the first flag.txt

03



```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l
:1/p:14344398), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder
[STATUS] 8850.00 tries/min, 8850 tries in 00:01h, 14335548 to do in 26:60h,
 16 active
[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 2020-11-18 0
2:34:33
root@Kali:~#
```

Exploitation: Weak Hash Passwords

01

Tools & Processes

Using Crackstation, the hash was simply entered into the online tool and cracked in seconds.

02

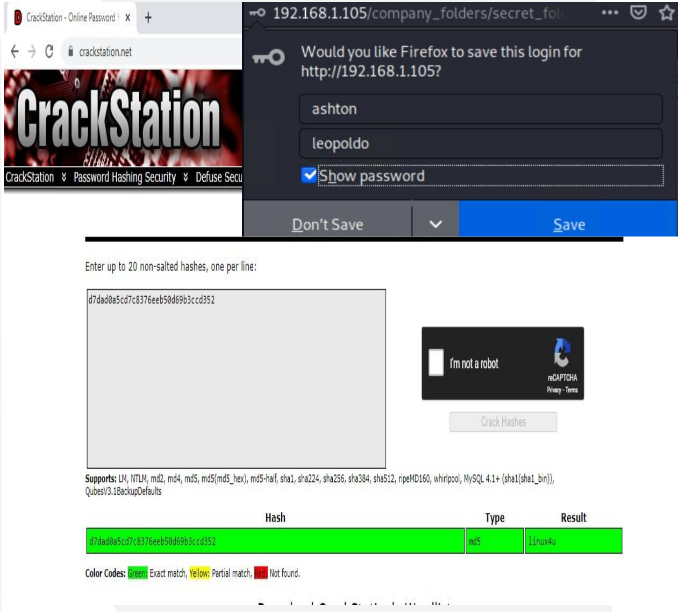
Achievements

This provided the password for the CEO – **linux4u**

This attack yielded access to webdav and the ability to upload a malicious script.

Once the password is cracked, and if a username is already known, a hacker can access system files.

03



Would you like Firefox to save this login for http://192.168.1.105?

ashton

leopoldo

☑ Show password

Enter up to 20 non-salted hashes, one per line:

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

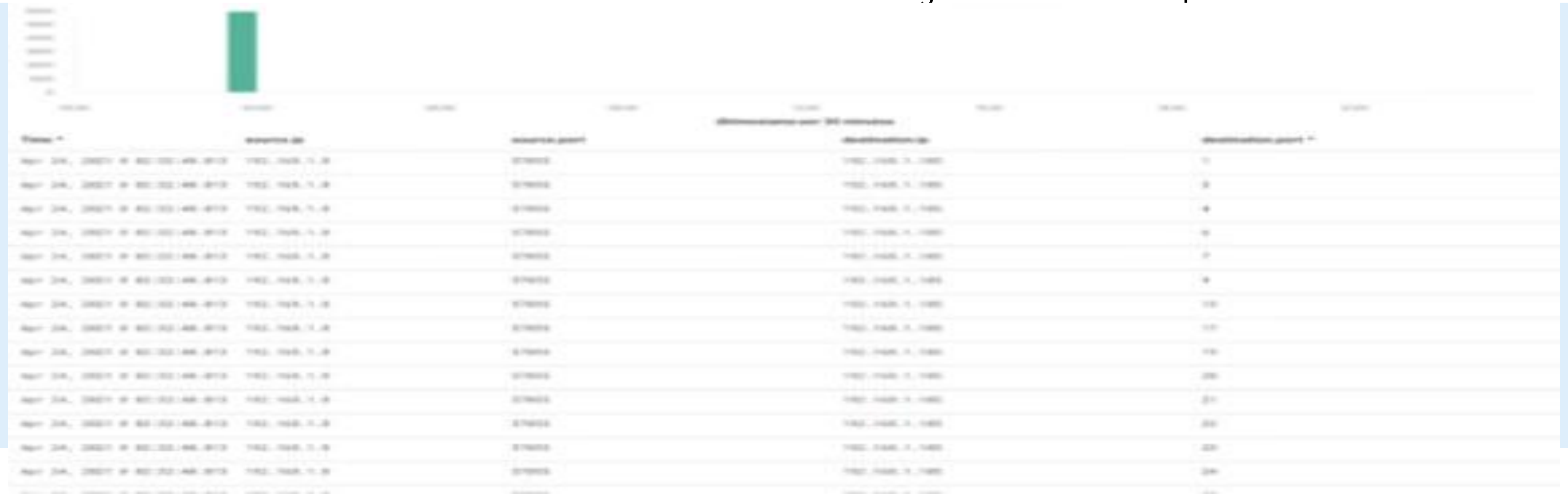
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

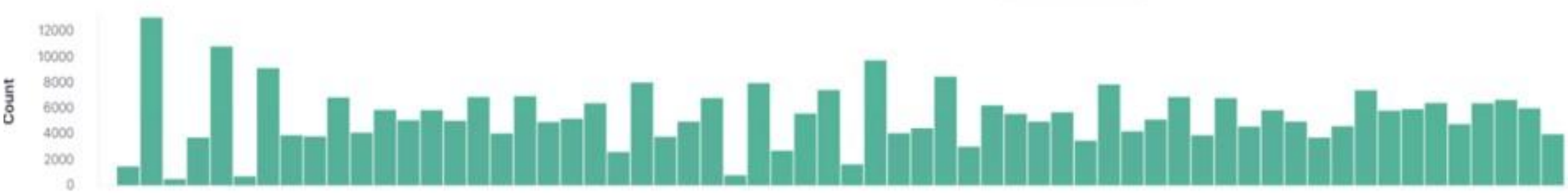
- October 27 2021@ 08:21pm.
- 6000 packets were sent from IP address 192.168.1.8 on TCP port 57055 to 192.167.1.105 with Nmap
- Search string used “ destination.ip : 192.168.1.105



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.

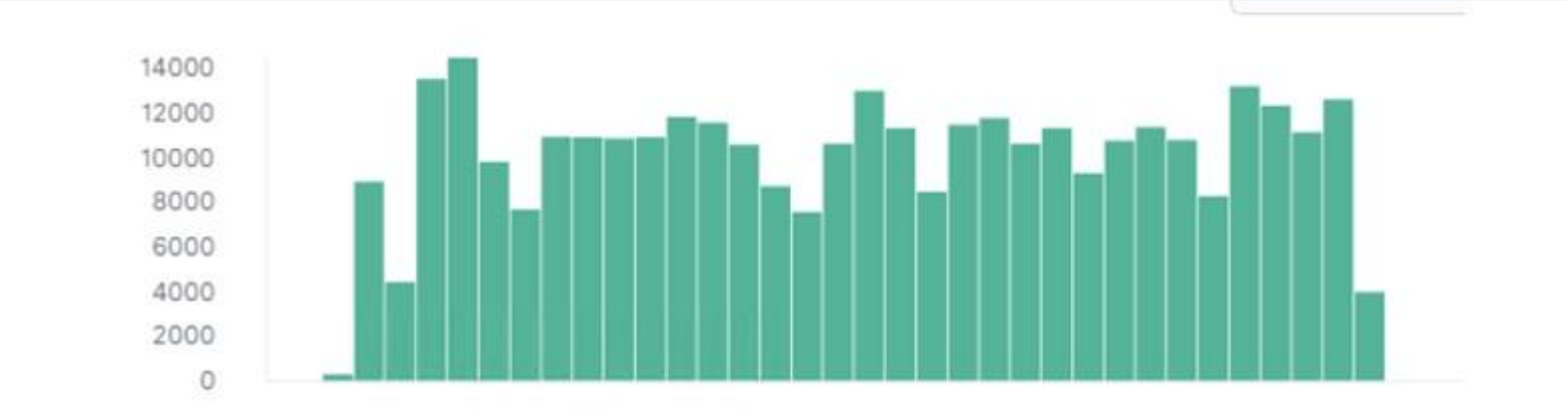
- 334,325 requests were made to the hidden directory between 09:03 and 09:35 on 10/27.
- “connect_to_the_corp_server” which contained details on how connect to the server, including using webdav.



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.

- 346,594 request made before password was cracked.



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.

- 25
- File requested was the reverse.php file used in attack.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Setup a low-level alert for any port scanning, with a threshold of 10, and a severe alert for anything above 100.
Have alerts for any use of Nmap.
Setup a critical alert for aggressive scans.

System Hardening

Enable only the traffic needed to access internal hosts, deny everything else. Including the standard ports, such as TCP 80 for HTTP and ICMP for ping requests.

Create and setup IPtables for the firewall port blocking and scanning. An IDS like Kibana, or SPLUNK allows for an immediate alerting of port scan activity, thereby facilitating rapid response to the potential threats.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Alarm should be configured to trigger if any request is made for the hidden directories from outside the company's internal network. The hidden directories are for company use only and should not be accessible from outside the premises.

Threshold for collected requests from a single IP address should be set for greater than 0 requests made. Send an email to the SOC Analyst when it's triggered by unknown IP.

System Hardening

Stronger usernames and password requirements for users that have access to the hidden directories. Disable directories listing in the Apache. Encrypt the contents of the hidden directories, and its contents.

Create a whitelist for authorized IP addresses. Make the folder private by changing permissions. Encrypt data contained within confidential folders

Mitigation: Preventing Brute Force Attacks

Alarm

An alarm should be set to trigger if a predefined number of requests are issued to the server from a single IP address, especially if those requests result in HTTP 401 (Unauthorized) responses. Since the brute force attack requires a high number of requests to complete, this traffic could potentially be blocked before the password is guessed. Threshold should be set for greater than 10 requests from an IP address in the span of 30 minutes

System Hardening

Increase password strength requirements and expiry every 3 months. Setup account timeout and lockout rules for failed password attempts to block brute forcing. After 3 failures a 30min timer is triggered and increases with every successive password failure, up to 10, upon which the user account is locked, a password expiry is triggered and a critical alert is sent to the security team.

Mitigation: Detecting the WebDAV Connection

Alarm

An alarm should be set to trigger if any access to the WebDAV directory is made from outside the company's internal network.

A single instance would trigger an alarm, if the WebDAV directory is accessed, or possible of uploading of any files to the directory.

System Hardening

The host should be configured to deny WebDAV uploads by default, and only allow uploads from a specific IP address. This can be accomplished using Apache's configuration files. Make sure software patches are up to date. Disable WebDAV or make sure it's configured correctly.

Install Filebeat on host machine. for monitoring.

```
iptables -A INPUT -s [IP address] –p tcp –m multiport! --dports 80,443 -j ACCEPT
```

Mitigation: Identifying Reverse Shell Uploads

Alarm

Monitor all incoming uploads and setup an alert for anything triggered by anti-virus/anti-malware.

Create an alert for files that contain suspicious code/scripts/file extensions.

An alert can be set for any traffic attempting to access port 4444. The threshold for the alert to be sent is when one or more attempt is made. Setting up an alert for any files being uploaded into the /webDAV folder. The threshold for the alert to be sent is when one or more attempt is made.

System Hardening

Setup a secure anti-virus/anti-malware application that screens all incoming files and automatically updates daily.

Update firewall rules.

Limit file types that can be uploaded, including restricting php.

Ensure only necessary ports are open. Set access to the /webDAV folder to read only to prevent payloads from being uploaded.

The End