# Capstone Engagement

## Assessment, Analysis, and Hardening of a Vulnerable System

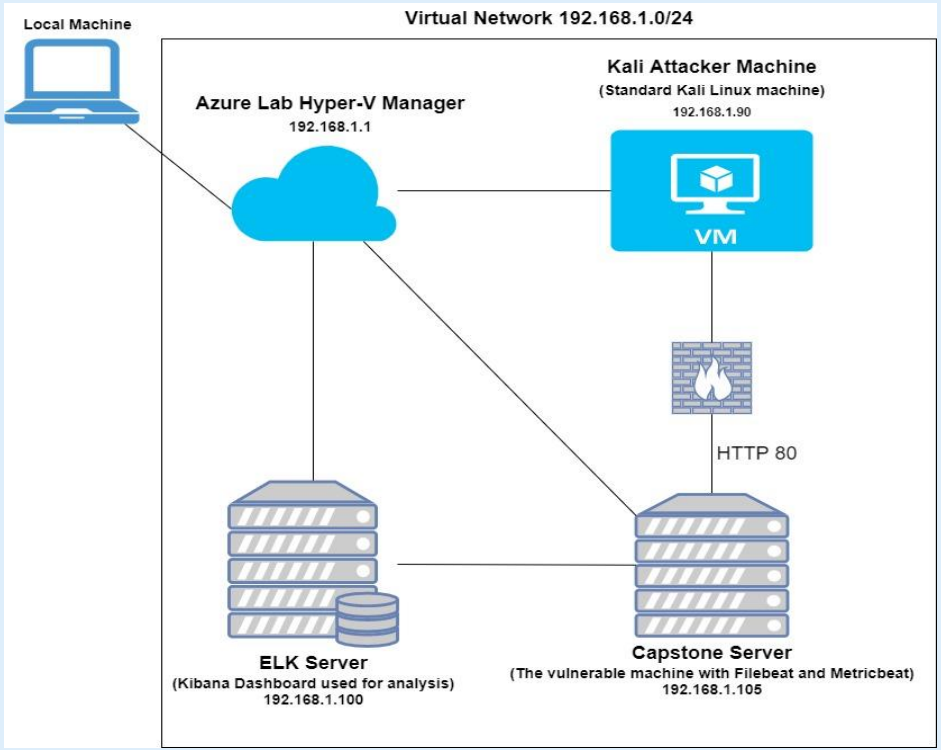
**Nicholas Williams  2/28/22**

# 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
Hostname:
Hyper-V Manager

IPv4: 192.168.1.90
OS: Kali 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 |
|---|---|---|
| Hyper-V Manager | 192.168.1.1 | This is the lab environment virtualizer. |
| Kali | 192.168.1.90 | This Kali Linux machine is the attacking machine. |
| ELK | 192.168.1.100 | This machine hosts the Kibana Dashboard used for Blue Team analysis. |
| Capstone | 192.168.1.105 | This is the vulnerable linux server that will be attacked in this project. This host has Filebeat and Metricbeat installed sending log data to the ELK machine. |

# Vulnerability Assessment

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | The vulnerability means that directories which should be hidden are not. The files can be found by brute forcing file path names until a web page is discovered, using tools like 'dirb'. | This vulnerability gives attackers the ability to find hidden directories that they can then look at and exploit. |
| CWE-307: Improper Restriction of Excessive Authentication Attempts | There is no security implemented to restrict failed authentication attempts meaning that a brute force attack can run unimpeded on the site. | Attackers can brute force the sites username and password authentication page until they crack it. |
| CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') | The PHP program running on the server is allowing remote file inclusion to execute. | It allows attackers to add files (like malware) to the server and run them. |

# Exploitation: CWE-22

01

**Tools & Processes**

Using the “dirb” command we were able to expose two web files that were not meant to be publicly accessible.
The command was:
‘dirb http://192.168.1.105’

02

**Achievements**

The result returned two file paths:
/server-status
And
/webdav

03

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

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

START_TIME: Mon Feb 14 18:31:32 2022
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:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)


-----------------
END_TIME: Mon Feb 14 18:31:38 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~#
```

# Exploitation: CWE-307

01

**Tools & Processes**

We used the command line tool Hydra to brute force the authentication protocols on the website.

The command used:

'hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get HTTP://192.168.1.105/company_folders/secret_folder'

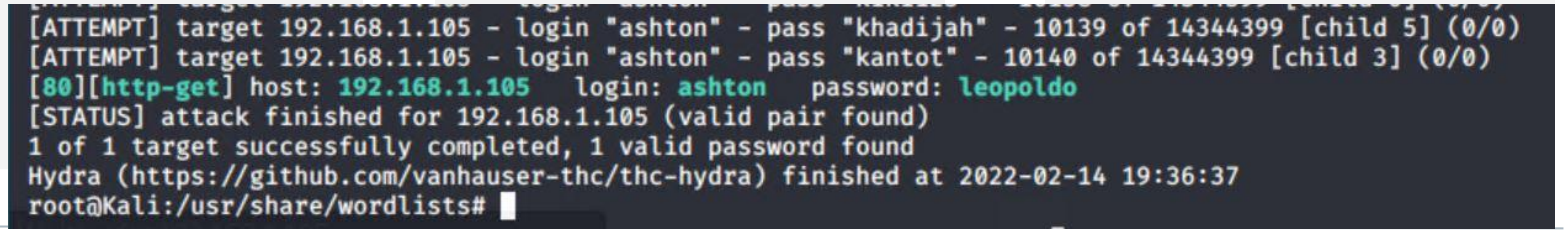
02

**Achievements**

Using this brute force we were able to discover the password for Ashton's account and could now access the restricted file.

03

See Below:



# Exploitation: CWE-98

01

**Tools & Processes**

We were able to use MSFVenom to design and upload a PHP reverse shell into the server.

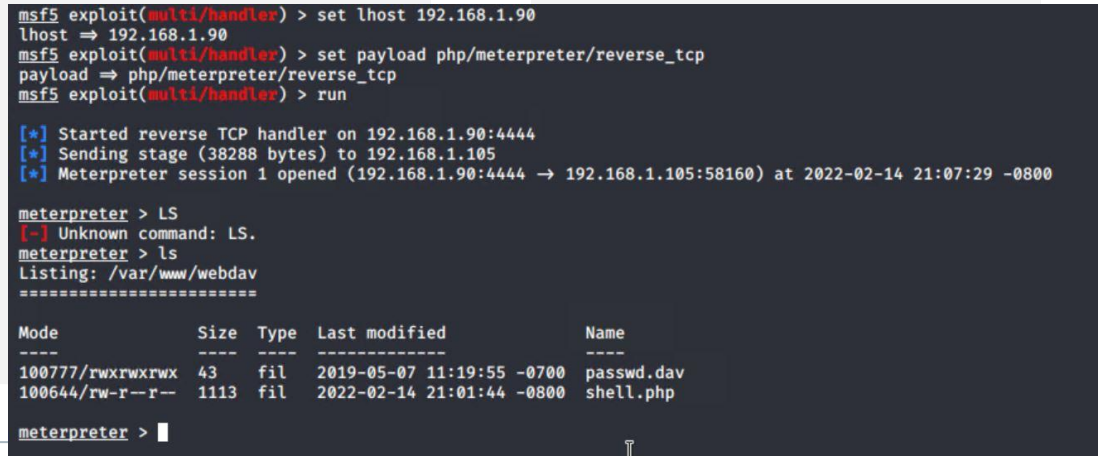
02

**Achievements**

The exploit gave us a backdoor ‘meterpreter’ connection into the server.

03

See Below:



# **Blue Team**
# Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

What time did the port scan occur?

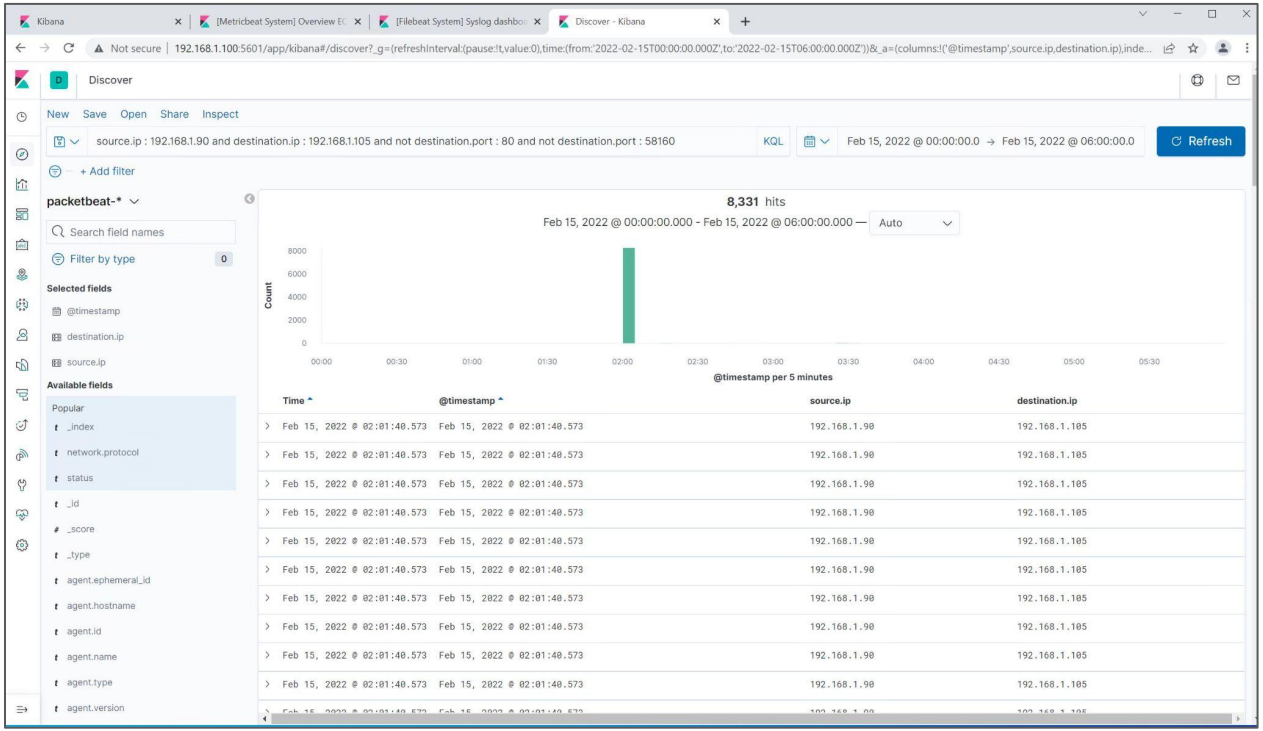
- The port scan began on february 15th, 2022 at 2:01 AM

How many packets were sent, and from which IP?

- There were initially 8,301 hits recorded around the start of the attack.

What indicates that this was a port scan?

- This was a port scan because the destination ports were checked.



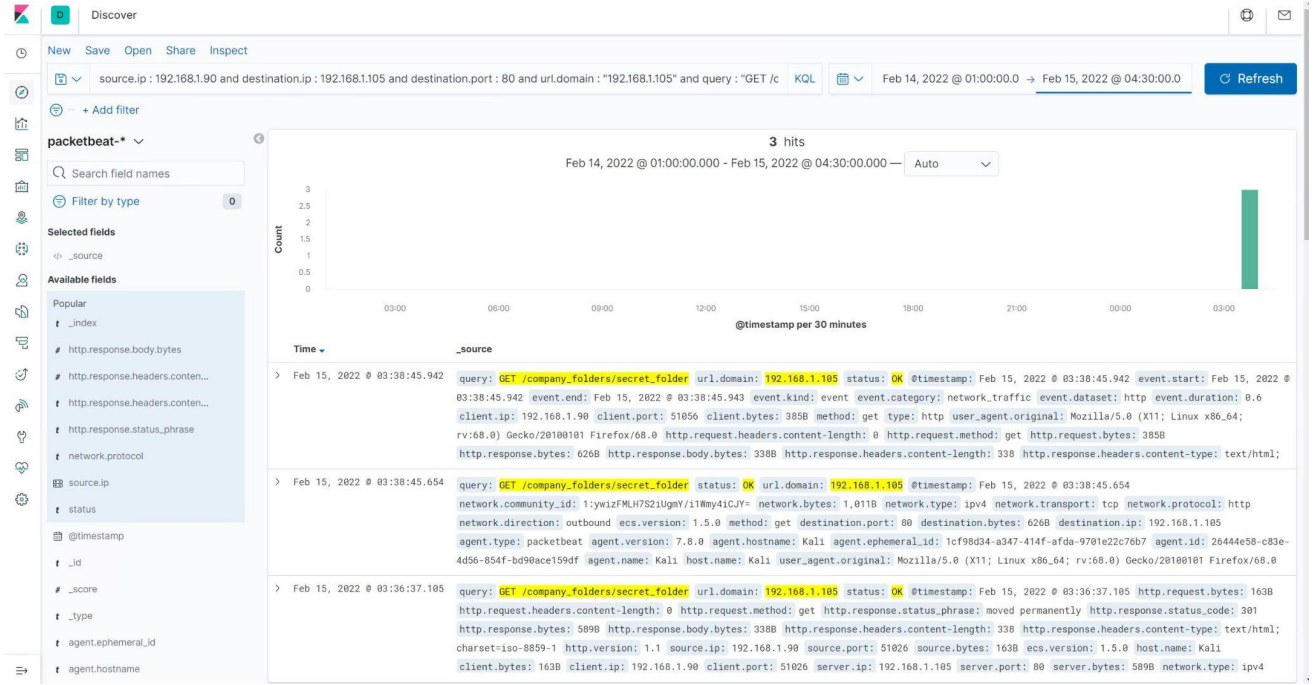
# Analysis: Finding the Request for the Hidden Directory

What time did the request occur? How many requests were made?

- The request for the Hidden Directory began on February 15th, 2022 at 3:38 AM

Which files were requested? What did they contain?

- The requested file was the /secret_folder directory and it contained the information on how to access the secured corporate server.



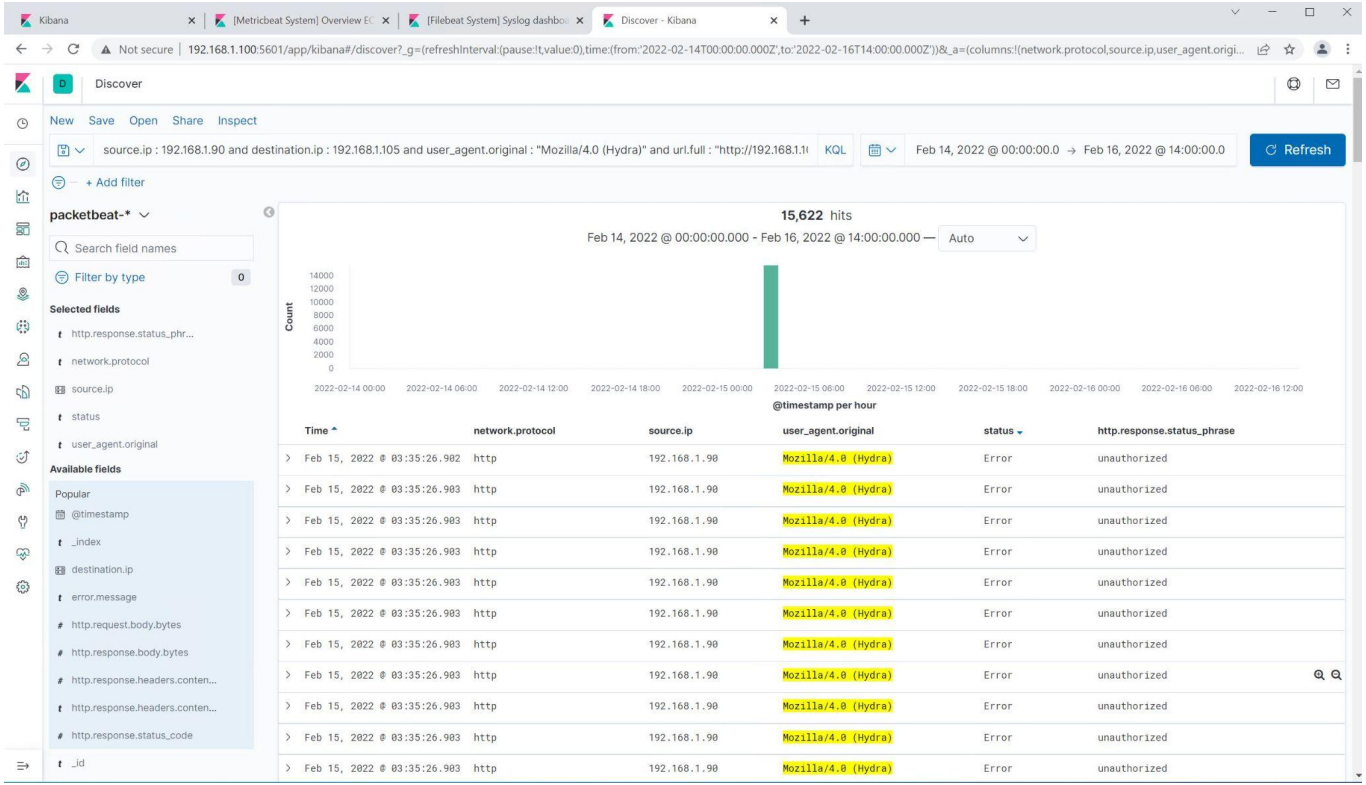
# Analysis: Uncovering the Brute Force Attack

How many requests were made in the attack?

- There were 15,622 attempts by the Hydra program to brute force the authentication.

How many requests had been made before the attacker discovered the password?

- 10,140 attempts.



# Analysis: Finding the WebDAV Connection

How many requests were made to this directory?

- The webdav directory was accessed 62 times.

Which files were requested?

- http://192.168.1.105/webdav

**Top 10 HTTP requests [Packetbeat] ECS**

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/company_folders/secret_folder | 15,652 |
| http://127.0.0.1/server-status?auto= | 1,320 |
| http://192.168.1.105/company_folders/secret_folders | 64 |
| http://192.168.1.105/webdav | 62 |
| http://192.168.1.105/ | 22 |

Export: Raw Formatted

# **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?

- An alert condition can be created in the SIEM that the company uses like Splunk-Enterprise and can be set to notify security personnel when a singular IP address is attempting connection to multiple ports in rapid succession.

What threshold would you set to activate this alarm?

- Alert when an IP address connects to over ten ports within a ten minute period.

## System Hardening

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

- Settings can be put into the firewall to block traffic from an IP address that is connecting to more then one port in a short amount of time.

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

- Using the host based firewall or IPS you could set it to block traffic from IP addresses that repeatedly access different ports.

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

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

- An alert can be designed that will detect when a new IP address not already in the permitted list accesses the protected folder.

What threshold would you set to activate this alarm?

- I would input an alert to the SIEM that alerts when an unrecognized IP accesses the folder.

## System Hardening

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

- If this folder is meant to be secure it should be moved to a different server that is not public facing.

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

- Move the folder to a server that is not public.

# Mitigation: Preventing Brute Force Attacks

## Alarm

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

- An alert should be built to notify when an account username has had multiple incorrect passwords.

What threshold would you set to activate this alarm?

- An alert for any time an account has five or more incorrect password attempts.

## System Hardening

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

- Build in authentication protocols that lock out an account when there is over five incorrect password attempts within a 15 minute period.

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

- Depending on the authentication protocol the system will need to be configured to block excessive failed attempts.

# Mitigation: Detecting the WebDAV Connection

## Alarm

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

- An alert can be designed for any time someone accesses the webdav directory outside of the company area.

What threshold would you set to activate this alarm?

- I would implement an alert for any time an IP address outside of the company state accesses the file.

## System Hardening

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

- Connection to this server should be restricted to only authorized personnel.

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

- This server could only allow access from specific white listed IPs and the authorized users should be forced to use secure authentication methods.

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

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

- An alert can be made that detects when a .php file is added to the webdav server.

What threshold would you set to activate this alarm?

- Any time that a .php file is requested.

## System Hardening

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

- The webdav server must be changed to block uploading files to the server.

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

- Block file creation and upload.


The End