Capstone Engagement

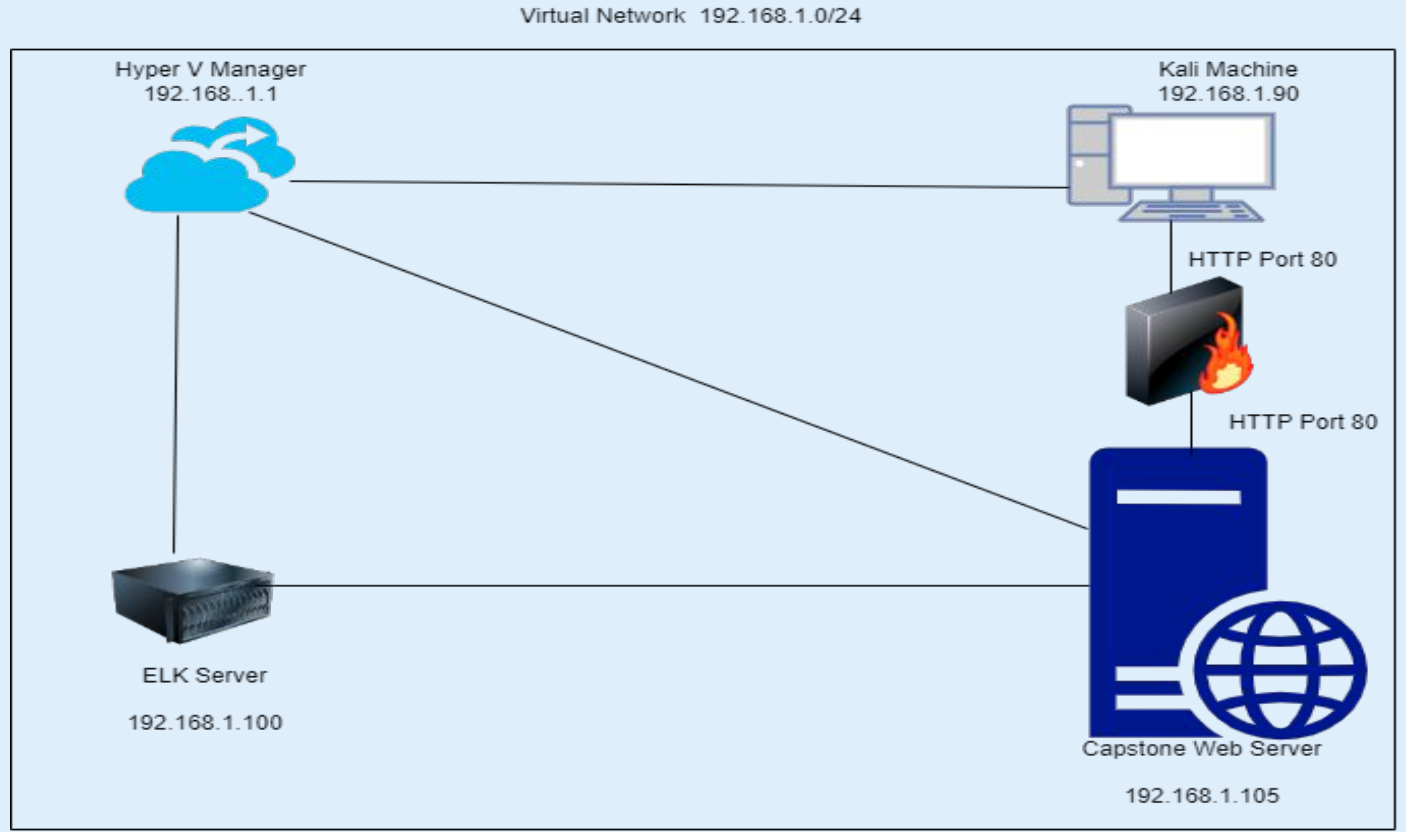
Assessment, Analysis, and Hardening of a Vulnerable System

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
Hostname: Red vs Blue

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.105
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
Capstone	192.168.105	This is a target machine using the apache web server
Kali	192.168.1.90	This is the attacking machine
ELK	192.168.1.100	It basically acts as a Logged Server.
Red vs Blue	192.168.1.1	Virtual Host Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port Scan /Brute Force Attack	Open port allow backdoor access and conduct brute force attack on victim's machine.	This allows the Red Team to gain access to machine using cracked users credentials.
Hash Password/Webdav	A Hashes password can be cracked through different tools. Web Server may store set of files in a root directories that can be accessible to the server's user	This allows an Red Team to identify the password.
Script Injection/ Payload	User account has compromised and a malicious script has been uploaded	Vulnerable to any malicious activity

Exploitation: Port Scan/Brute- Force Attack

01

Tools & Processes

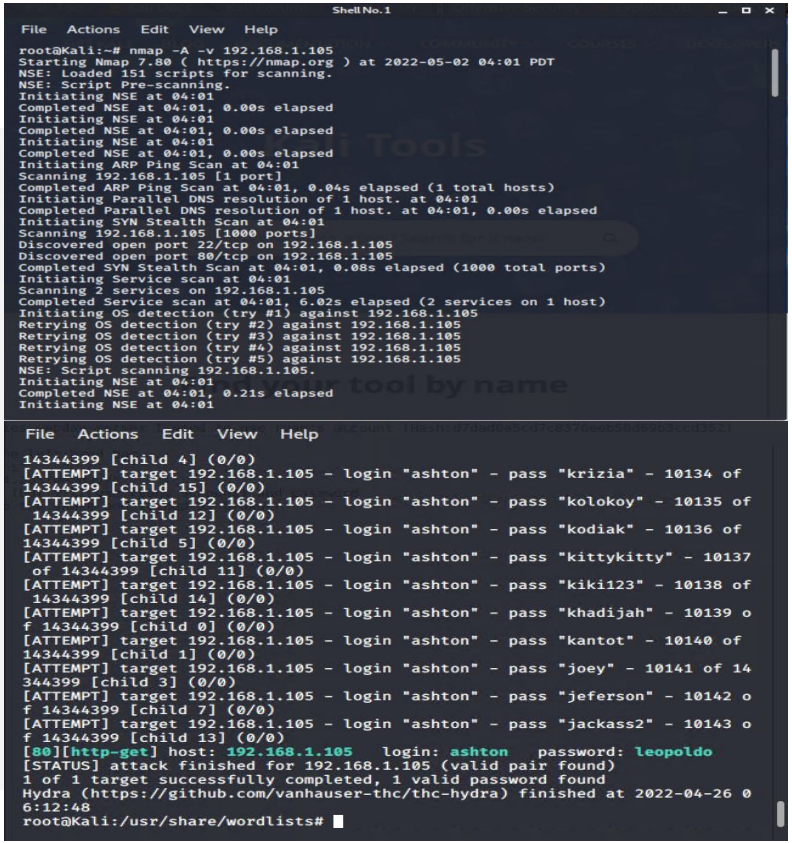
Nmap to scan for any open port.

Hydra is used to crack user's Credential.

02

Achievements

Credential access



Exploitation: Hash password/webdav

01

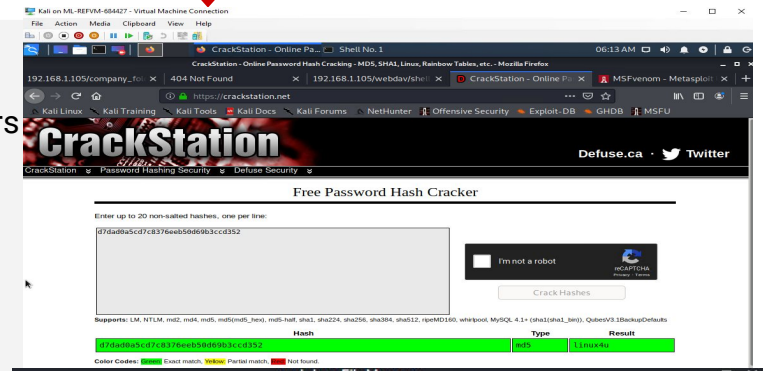
Tools & Processes
Crackstation.com site was used to crack Ryan password.

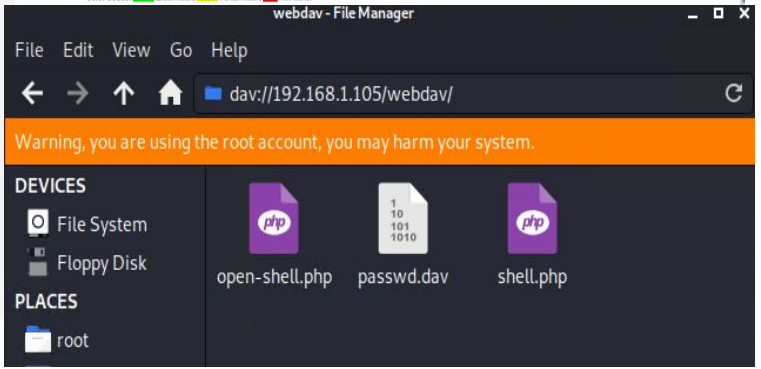
A PHP reverse shell payload Has been added in the directory.

02

Achievements
Gained access to the users secrete folder and the file Has been added.

03





Exploitation: Script Injection and Payload

01

Tools & Processes

Metasploit

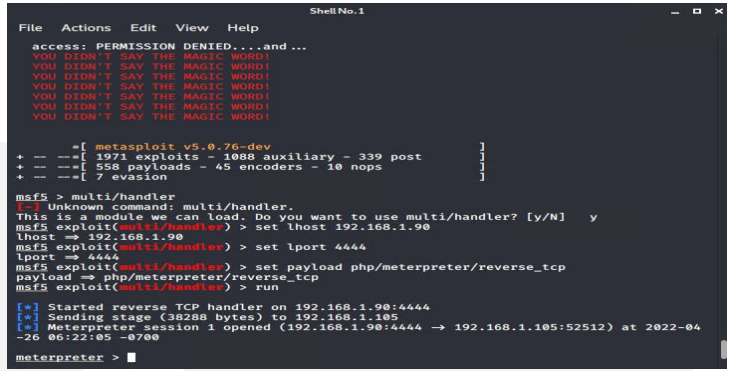
- MSF-Venom
- Meterpreter

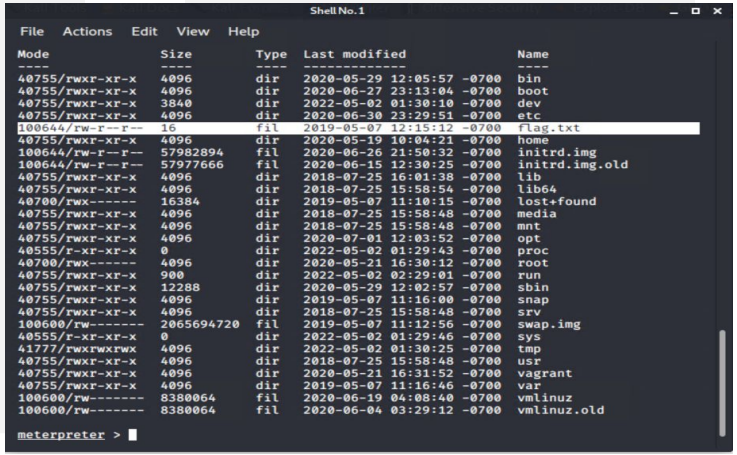
This perform reverse shell payload in victims machine

02

Achievements

Payload has been executed

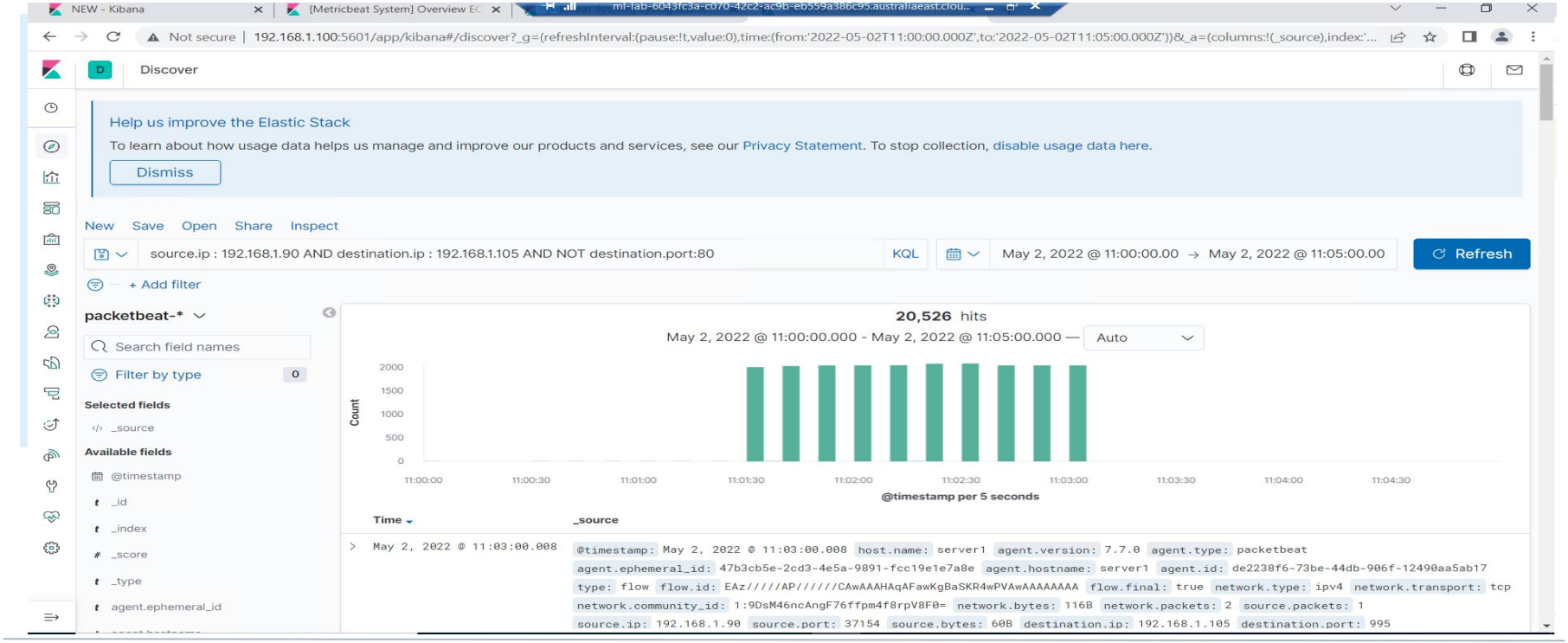




Blue Team
Log Analysis and Attack Characterization

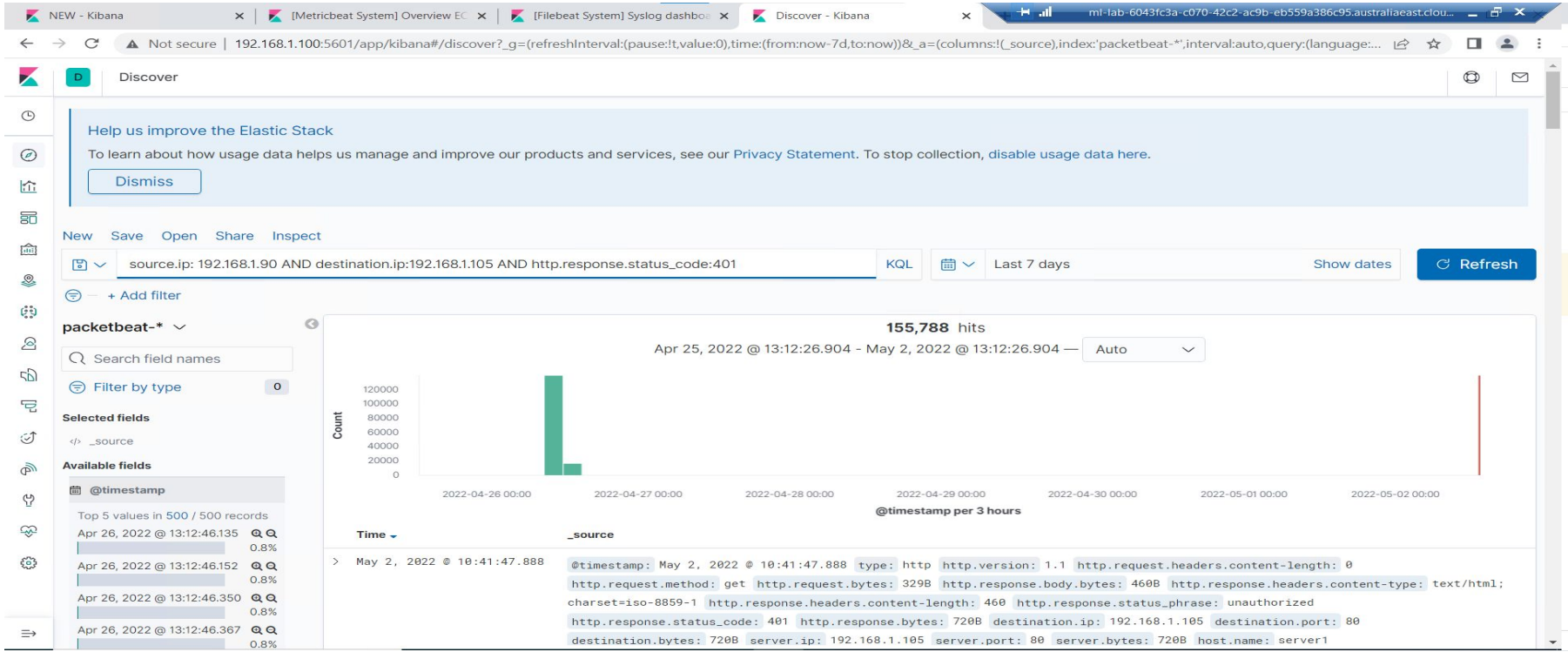
Analysis: Identifying the Port Scan

- The Port Scan occurred at 11:00pm
- 20,526 packets were sent from 192.168.1.90
- Request for port numbers



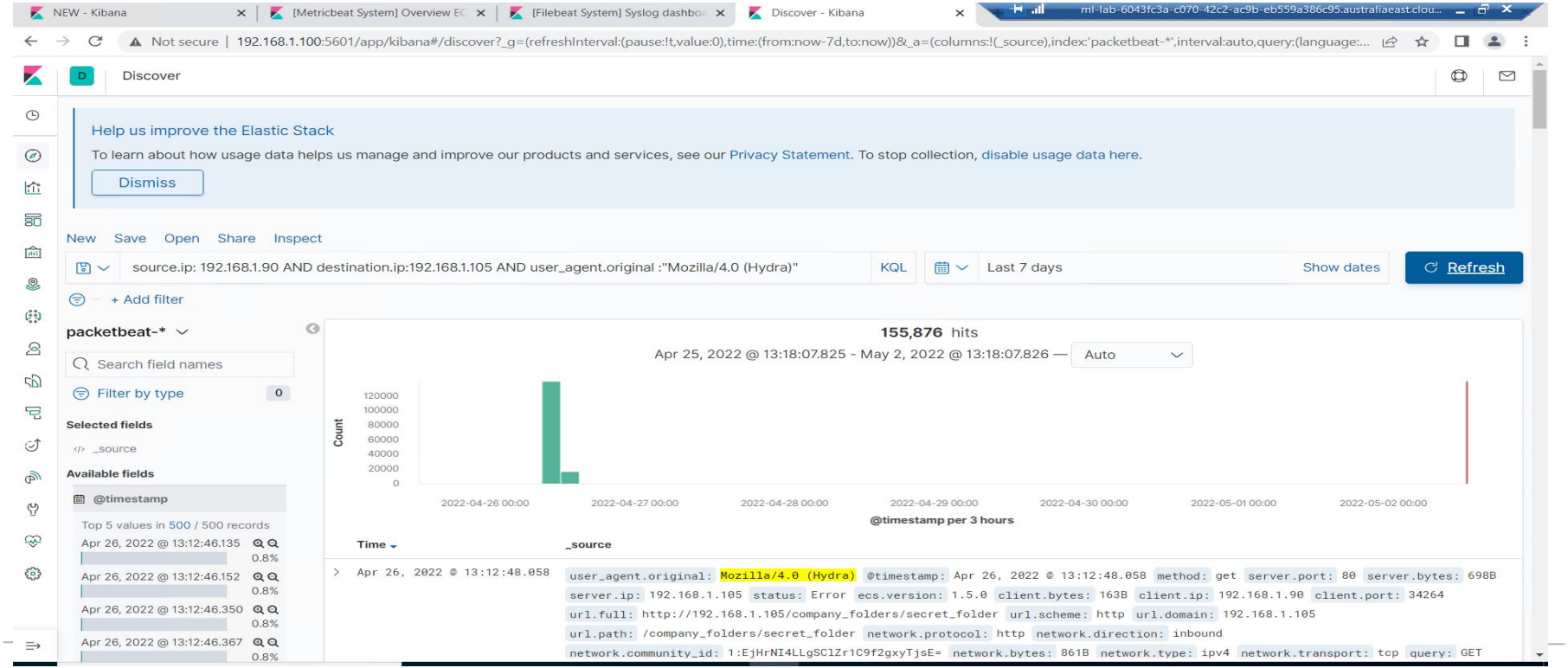
Analysis: Finding the Request for the Hidden Directory

- Around 9:00 pm 155,788 request were made.
- The file requested was a secret folder hidden within company folders.



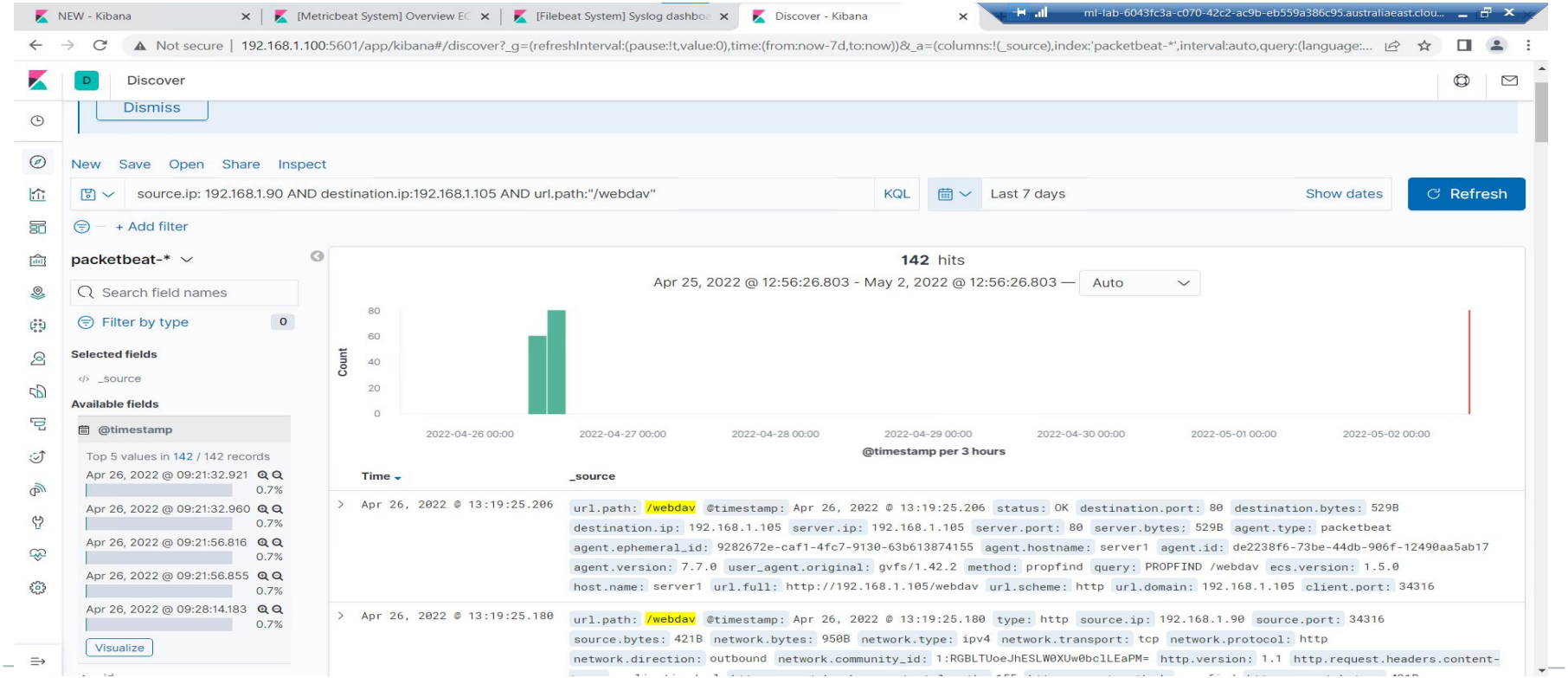
Analysis: Uncovering the Brute Force Attack

- 155,879 hits were made during the attack.
- Once the password was cracked the hydra stopped sending further request.



Analysis: Finding the WebDAV Connection

- 142 request were made to the webdav directory.
- The shell.php file was requested several times.



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?

- ★ A Filter can be applied to detect if source IP address is trying to connect to any ports.

What threshold would you set to activate this alarm?

- ★ If multiple attempts to connect to different ports occur an alarm can be configured to let know a port scan is happening and blocking the attacker before any further step can be taken

System Hardening

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

- ★ Firewall configuration
- ★ Alerts on unusual port scan
- ★ Block port scan

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

- ★ Filtering traffic from an IP triggered by IPS can effectively mitigate port scan

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- ★ Set Alarm if any connection made to 192.168.1.105/company_folders/secret_folder

What threshold would you set to activate this alarm?

- ★ The threshold for alarm would be 1, if any IP is trying to connect.

System Hardening

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

- ★ Removing sensitive directories and file from the web server.
- ★ OR only allowing know IP to connect to these directories in the web server.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- ★ Set an alarm for detecting status code for 401 if more than three attempts are made.

System Hardening

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

- ★ Multi-factor authentication
- ★ Lock any account after three failed attempts
- ★ Configure Account policies in server to limit failed attempts

Mitigation: Detecting the WebDAV Connection

Alarm

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

- ★ Set an alert for any IP trying to access the File System.
- ★ Threshold for the alarm should be 1.

System Hardening

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

- ★ Implementing policy that restricts credential storage on server.
- ★ Two-Factor Authentication.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- ★ Set an alarm if any .php file is uploaded
- ★ Set firewall to block traffic to shared folder

System Hardening

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

- ★ Restrict any file upload to File system other than from known IP.

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

- ★ Block ports 280,443,4444.


The End