

# Capstone Engagement Assessment, Analysis, and Hardening of a Vulnerable System

Prepared By: Stephen Corey Jacobs, November 12, 2020

# Table of Contents

---

This document contains the following sections:

01

**Network Topology**

02

**Red Team:** Security Assessment

03

**Blue Team:** Log Analysis and Attack Characterization

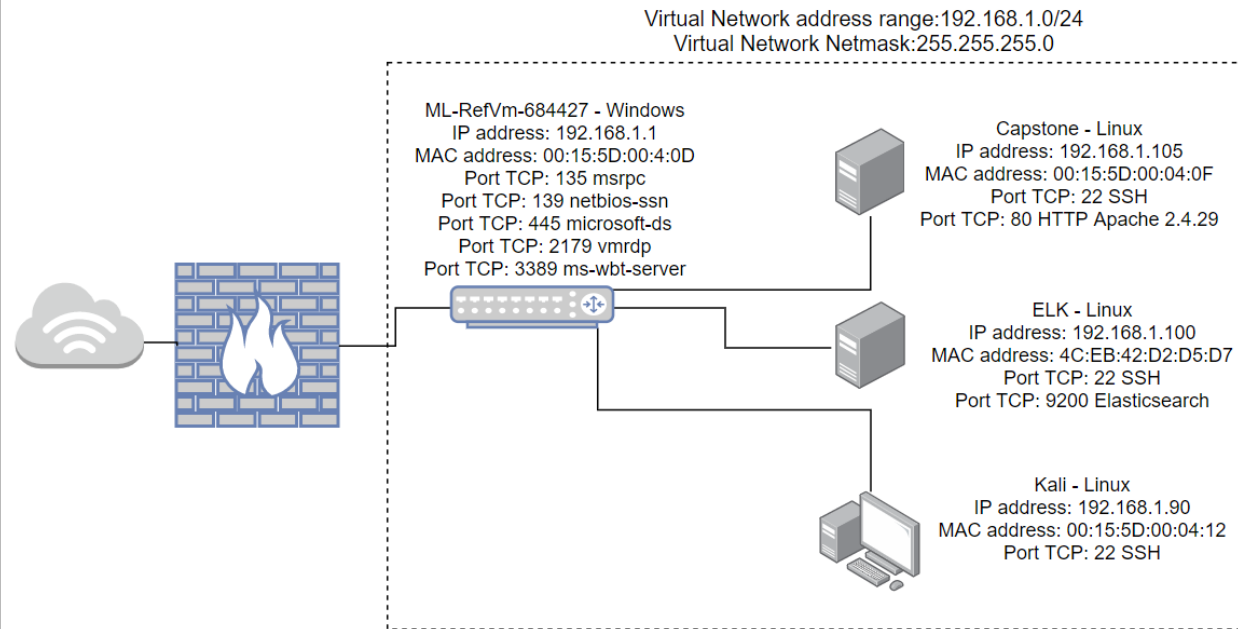
04

**Hardening:** Proposed Alarms and Mitigation Strategies

---

# 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

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

# Red Team Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVm-684427	192.168.1.1	NAT Switch / Gateway
Kali	192.168.1.90	Network Attacking System
ELK	192.168.1.100	Network Security Monitor
Capstone	192.168.1.105	Apache Web Server ( Target Machine )

---

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure	Sensitive data namely /company_folders/secret_folder and /webdav were public facing and accessible via web browser	Accessed data revealed user 'Ashton' as the administrator for '/company_folders/secret_folder'
Security Misconfiguration	Server security settings had no limit for failed attempted logins, leaving it vulnerable to Brute-force attack.	User Ashton's login credentials were found via Brute-force attack. Access was granted to /secret_folder. User 'Ryan' was found with a password hash, as well as instructions for upload to /webdav folder
Unrestricted File Upload	Server allowed upload of .php script file to /webdav folder	Upload of reverse_tcp .php script allowed backdoor access and complete C2 of the Capstone web server

# Exploitation: Sensitive Data Exposure

---

01

## **Tools & Processes**

NMap scan revealed Apache Server at IP address 192.168.1.105 and open HTTP port 80.

Access to company folders was accomplished via Web Browser. Mozilla FireFox in this case.

02

## **Achievements**

Company file structure was determined. Namely the  
/company\_folders/secret\_folders and  
/meet\_our\_team folders

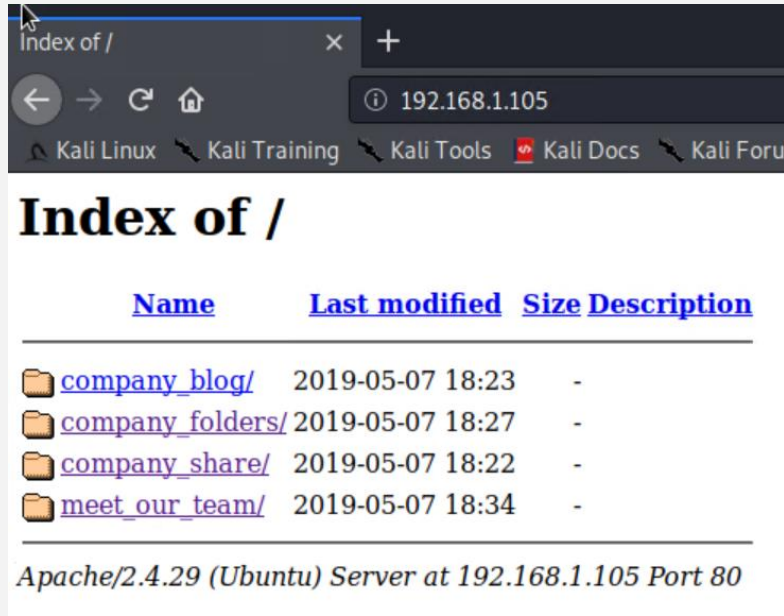
It was determined that Ashton was the administrator for  
/company\_folders/secret\_folders



# Exploitation: Sensitive Data Exposure

03

```
Nmap scan report for 192.168.1.105
Host is up (0.0013s 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)
ssh-hostkey:
  2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
  256  c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
_ 256  b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29
http-ls: Volume /
maxfiles limit reached (10)
SIZE      TIME      FILENAME
-         2019-05-07 18:23 company_blog/
422       2019-05-07 18:23 company_blog/blog.txt
-         2019-05-07 18:27 company_folders/
-         2019-05-07 18:25 company_folders/company_culture/
-         2019-05-07 18:26 company_folders/customer_info/
-         2019-05-07 18:27 company_folders/sales_docs/
-         2019-05-07 18:22 company_share/
-         2019-05-07 18:34 meet_our_team/
329       2019-05-07 18:31 meet_our_team/ashton.txt
404       2019-05-07 18:33 meet_our_team/hannah.txt
_
http-server-header: Apache/2.4.29 (Ubuntu)
_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
```



Index of /

Name	Last modified	Size	Description
<a href="#">company_blog/</a>	2019-05-07 18:23	-	
<a href="#">company_folders/</a>	2019-05-07 18:27	-	
<a href="#">company_share/</a>	2019-05-07 18:22	-	
<a href="#">meet_our_team/</a>	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

# Exploitation: Security Misconfiguration

---

01

## **Tools & Processes**

Kali Linux tool, Hydra, was used to Brute-force access to the /company\_folders/secret\_folder with Ashton's login credentials.

02

## **Achievements**

Ashton's password was found via Brute-force attack.

Access to /secret\_folder granted.

/webdav location and access instructions found

User Ryan password hash found.

# Exploitation: Security Misconfiguration

```
[ATTACK] target 192.168.1.105 login ashton pass jackass2 10145 01 143445
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 192.168.1.105 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-13 16:35:09
root@Kali:/usr/share/wordlists#
```

+

① 192.168.1.105/company\_folders/secret\_folder/connect\_to\_corp\_server

[Kali Linux](#) [Kali Training](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [NetHunter](#) [Offensive Security](#) [Exploit-DB](#)

### 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

# Exploitation: Unrestricted File Upload

---

01

## Tools & Processes

Created and uploaded a .php reverse\_tcp script with msfvenom.

php/meterpreter/reverse\_tcp

Created payload file was uploaded to the target server /webdav folder and executed.

02

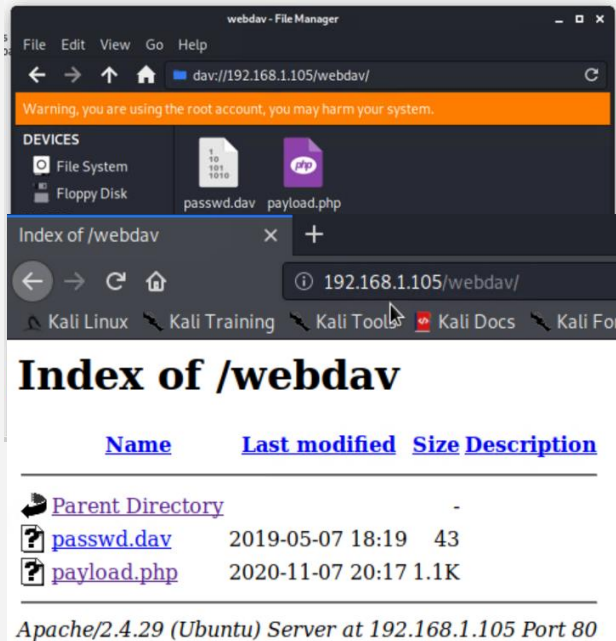
## Achievements

Backdoor was created and accessed with metasploit meterpreter.


C2 of target system was achieved and flag.txt file was “captured”

# Exploitation: Unrestricted File Upload

03



```
meterpreter > shell
Process 3613 created.
Channel 2 created.
pwd
/var/www/webdav
cd /
find / -iname *flag* 2>/dev/null
/flag.txt
cat flag.txt
b1ng0w@5h1sn@m0
```

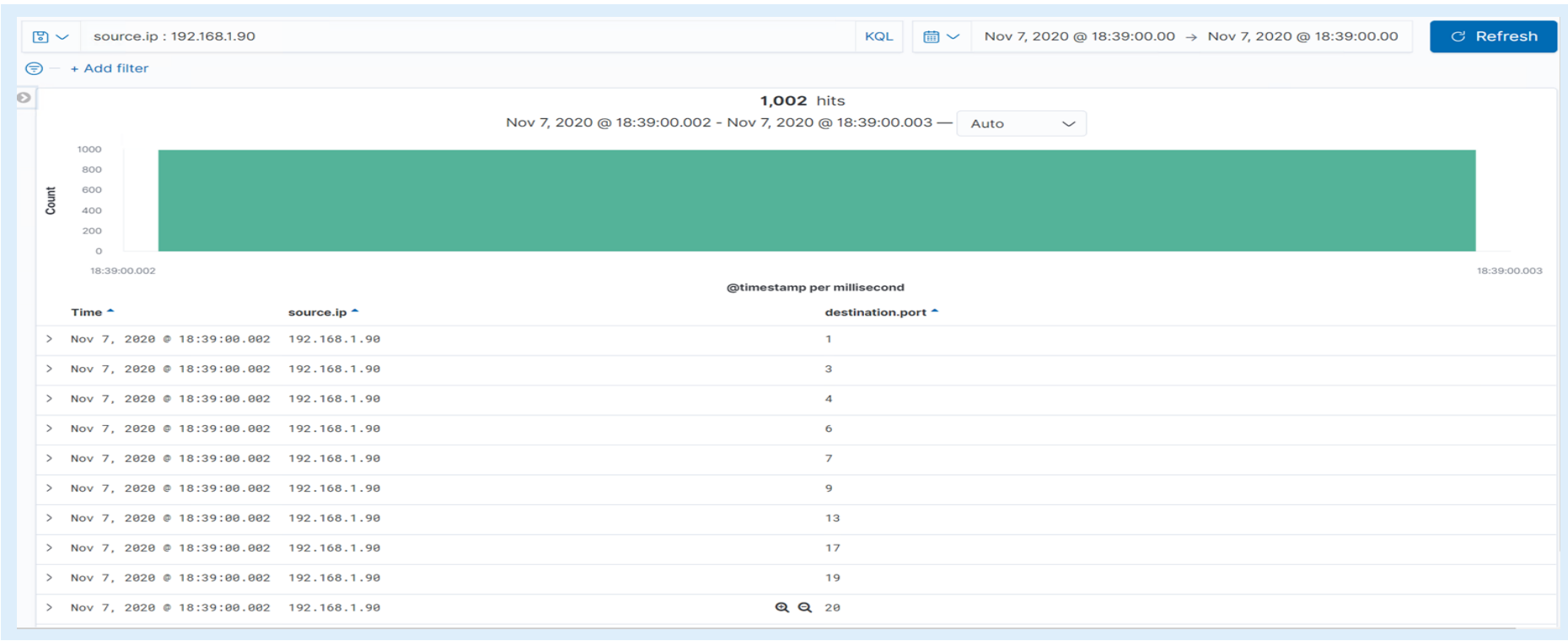


# **Blue Team**

## Log Analysis and Attack Characterization

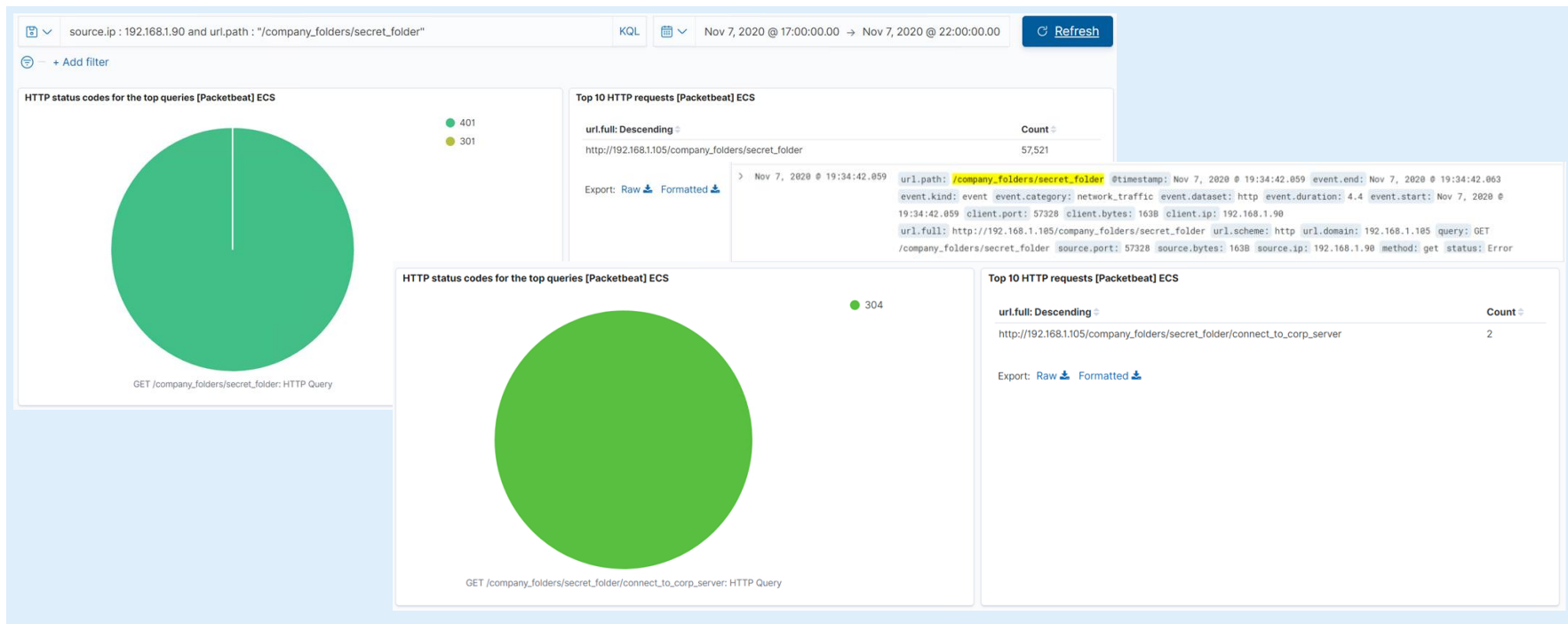
# Analysis: Identifying the Port Scan

- Port Scan occurred 11/7/2020 @ 18:39:00:002.
- 1002 packets were sent from the attacking 192.168.1.90 ip address.
- All ports were scanned in sequential order in one millisecond.



# Analysis: Finding the Request for the Hidden Directory

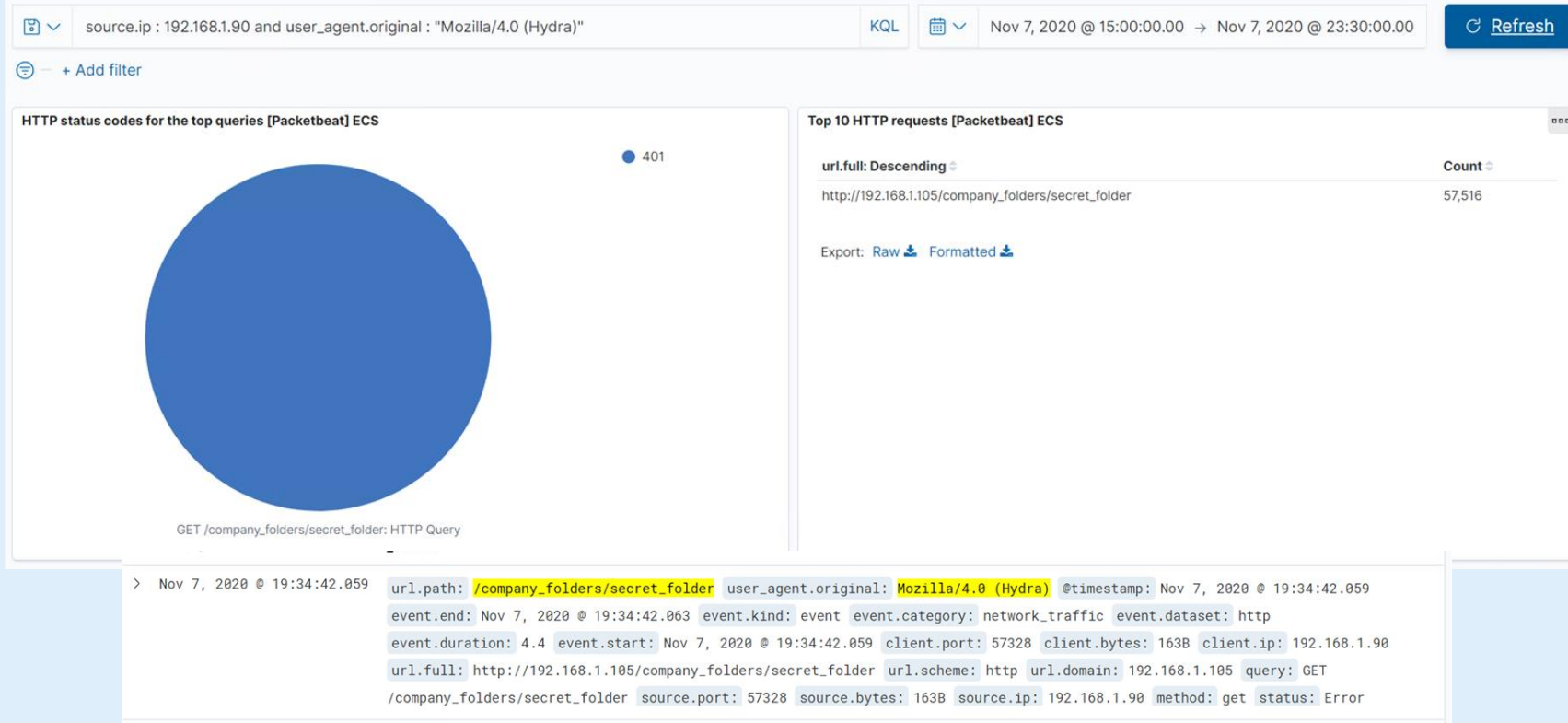
- The first request happened on 11/7/2020 at 19:34. 57521 requests were made to the /secret\_folder.
- Connect\_to\_corp\_server files was accessed. This file had instructions to access /webdav as well as user Ryan's password hash





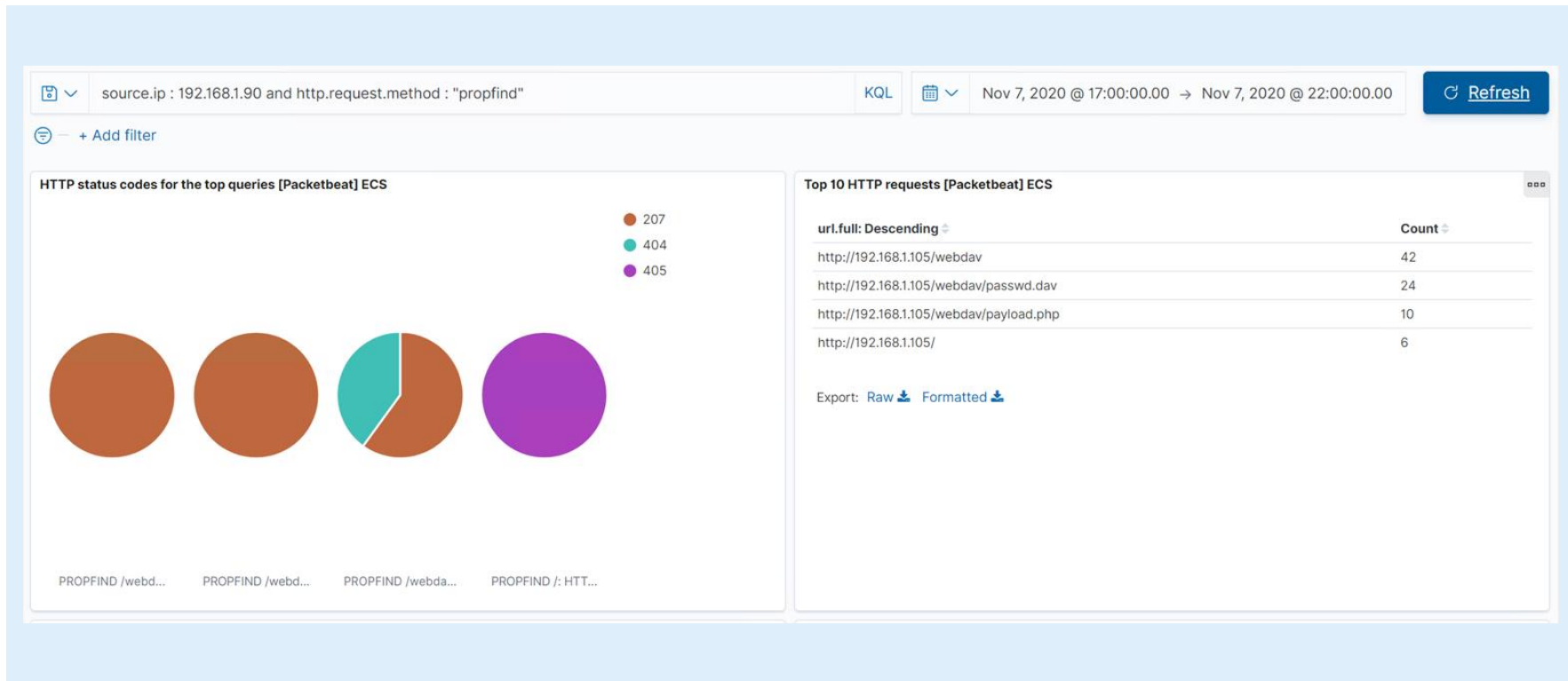
# Analysis: Uncovering the Brute Force Attack


- 57,516 login attempts were made with Hydra before the password was cracked.



# Analysis: Finding the WebDAV Connection

- /webdav was requested a total of 42 times.
- Passwd.dav as requested as well as payload.php





# **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?**

Alarm can be set if any ip address is scanned that is NOT our web server (192.168.1.105) and destination ports that are not HTTP related (80, 443)

**What threshold would you set to activate this alarm?**

Email and Log when non-HTTP ports are requested > 5 times for a given time-stamp.

## System Hardening

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

Network Firewalls should be configured to block all incoming and outgoing traffic except for ports 80 and 443.

An additional network-based Web Application Firewall (WAF) would enhance server security by protecting HTTP(S) protocols at the application level.

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

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

Alarm can be set to alert if sensitive files and directories are accessed by non whitelisted ip address.

**What threshold would you set to activate this alarm?**

Email and log anytime a directory or file deemed sensitive has been accessed by an ip address outside of the white list.

## System Hardening

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

Ip addresses can be white or black listed in `/etc/httpd/conf/httpd.conf`

In this case internal ip addresses would be allowed while our attackers ip address would be denied.

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

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

Alarm would be set for anytime multiple failed logins happen in a short time period. Also, alarm would be set anytime the Mozilla/4.0 (Hydra) user agent attempts a login.

**What threshold would you set to activate this alarm?**

Email and log > 5 failed login attempts in 1 minute.

Email and log any login attempts by Hydra user agent.

## System Hardening

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

Strong password policy with required password lengths and special characters will deter brute force attacks and make password hashes harder to crack.

Multi-factor authentication would require users to provide an additional credential in addition to their password.

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

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

Alarm can be set to alert if sensitive files and directories are accessed by non whitelisted ip address.

**What threshold would you set to activate this alarm?**

Email and log anytime a directory or file deemed sensitive has been accessed by an ip address outside of the white list.

## System Hardening

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

Much like with our secret\_folder directory these settings will be configured in the /etc/httpd/conf/httpd.conf file.

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

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

Alarm will be set to alert anytime web server files are altered by non whitelisted ip addresses. In addition alarms will be made anytime the server receives a “put” HTTP request for a non whitelisted ip.

**What threshold would you set to activate this alarm?**

Email and log anytime put HTTP request is received from non whitelisted ip address.

## System Hardening

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

Blocking HTTP request types will again be done in the `/etc/httpd/conf/httpd.conf` file.



*The  
End*