Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Prepared By: Stephen Corey Jacobs, November 12, 2020

Table of Contents

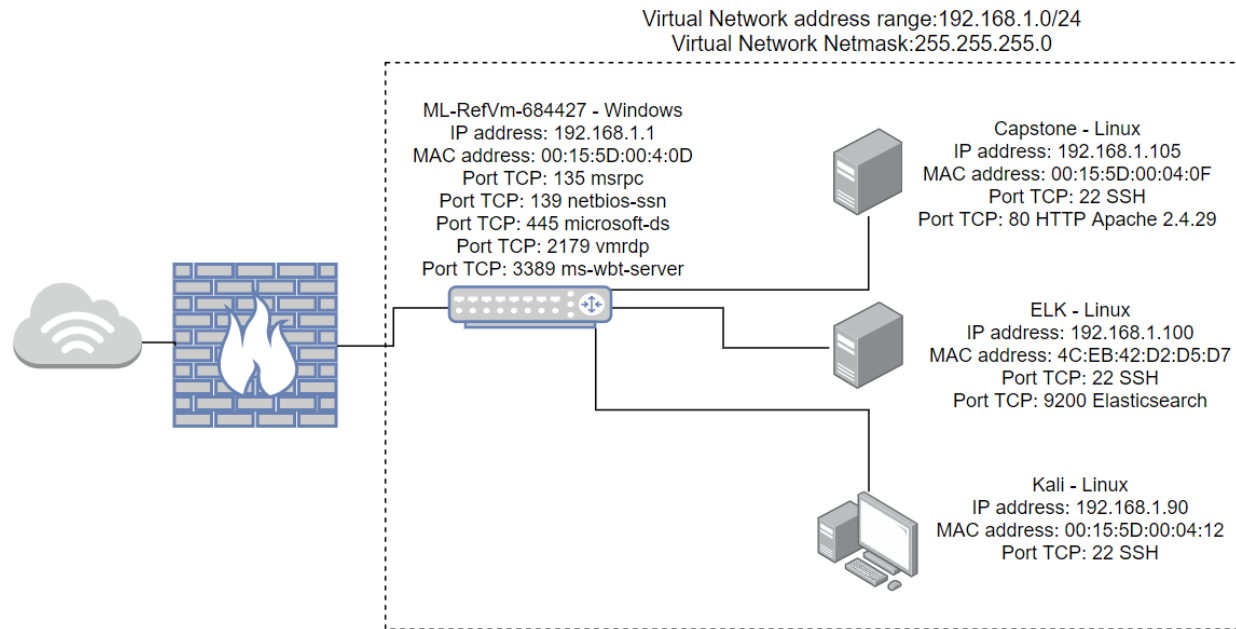This document contains the following sections:

Network Topology

Network Topology

Virtual Network address range:192.168.1.0/24
Virtual Network Netmask:255.255.255.0

ML-RefVm-684427 - Windows
IP address: 192.168.1.1
MAC address: 00:15:5D:00:4:0D
Port TCP: 135 msrpc
Port TCP: 139 netbios-ssn
Port TCP: 445 microsoft-ds
Port TCP: 2179 vmrdp
Port TCP: 3389 ms-wbt-server

Capstone - Linux
IP address: 192.168.1.105
MAC address: 00:15:5D:00:04:0F
Port TCP: 22 SSH
Port TCP: 80 HTTP Apache 2.4.29

ELK - Linux
IP address: 192.168.1.100
MAC address: 4C:EB:42:D2:D5:D7
Port TCP: 22 SSH
Port TCP: 9200 Elasticsearch

Kali - Linux
IP address: 192.168.1.90
MAC address: 00:15:5D:00:04:12
Port TCP: 22 SSH

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
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 an 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.
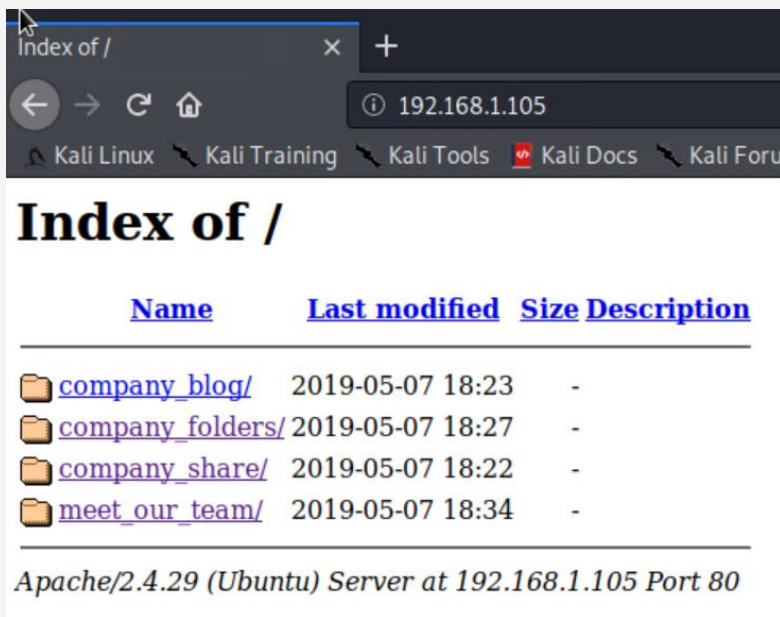
02

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

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

03


```
[ATTEMPT] target 192.168.1.105  login  ashton  pass  jackass2  10149 of 14344399
[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#
```

192.168.1.105/company_fol ×   +

← → C ⌂   ⓘ 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-

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

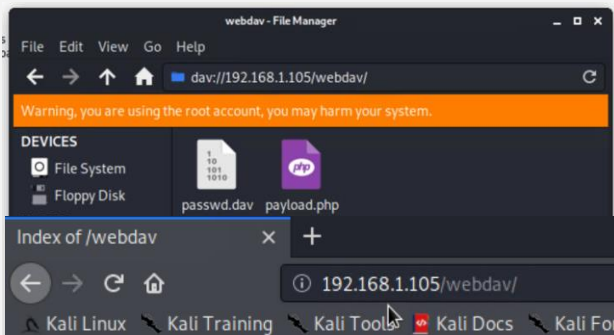Created payload file was uploaded to the target server /webdav folder and executed.

02

Achievements
Backdoor was created and accessed with metasploit meterpreter.

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

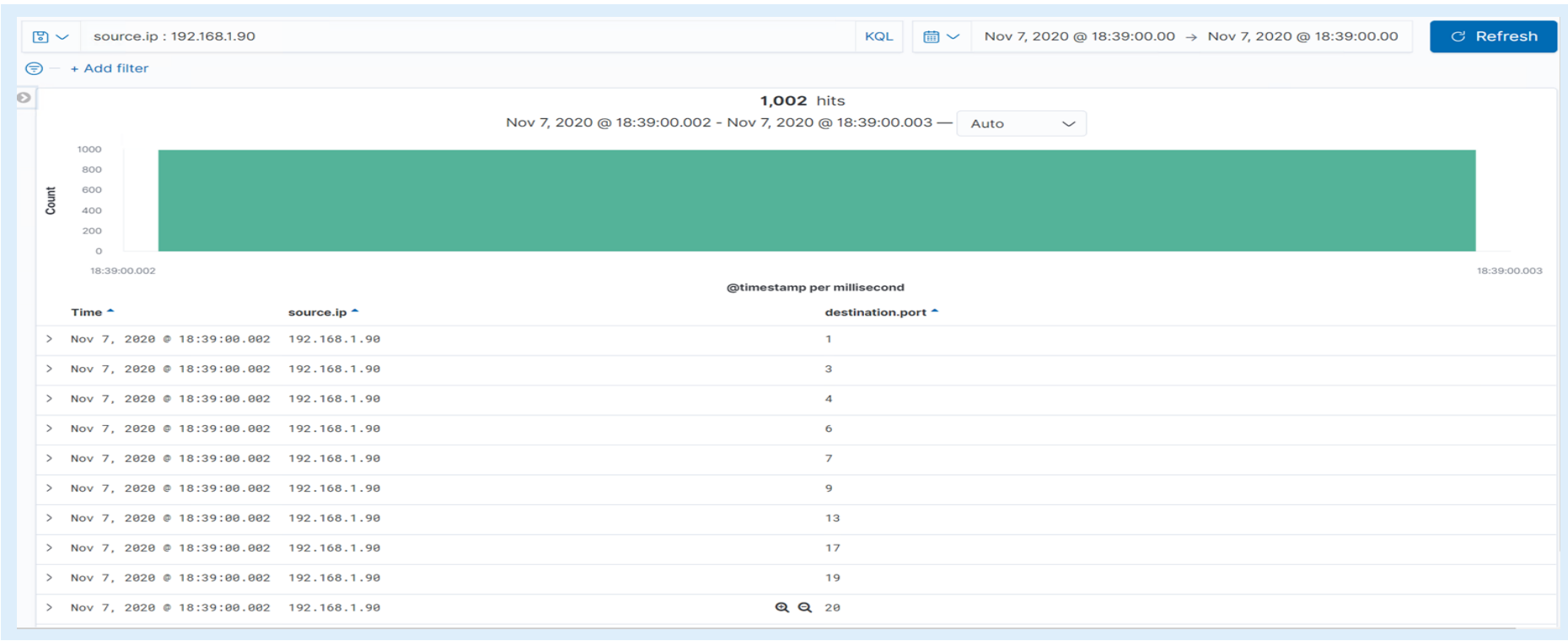# Exploitation: Unrestricted File Upload

03

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 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
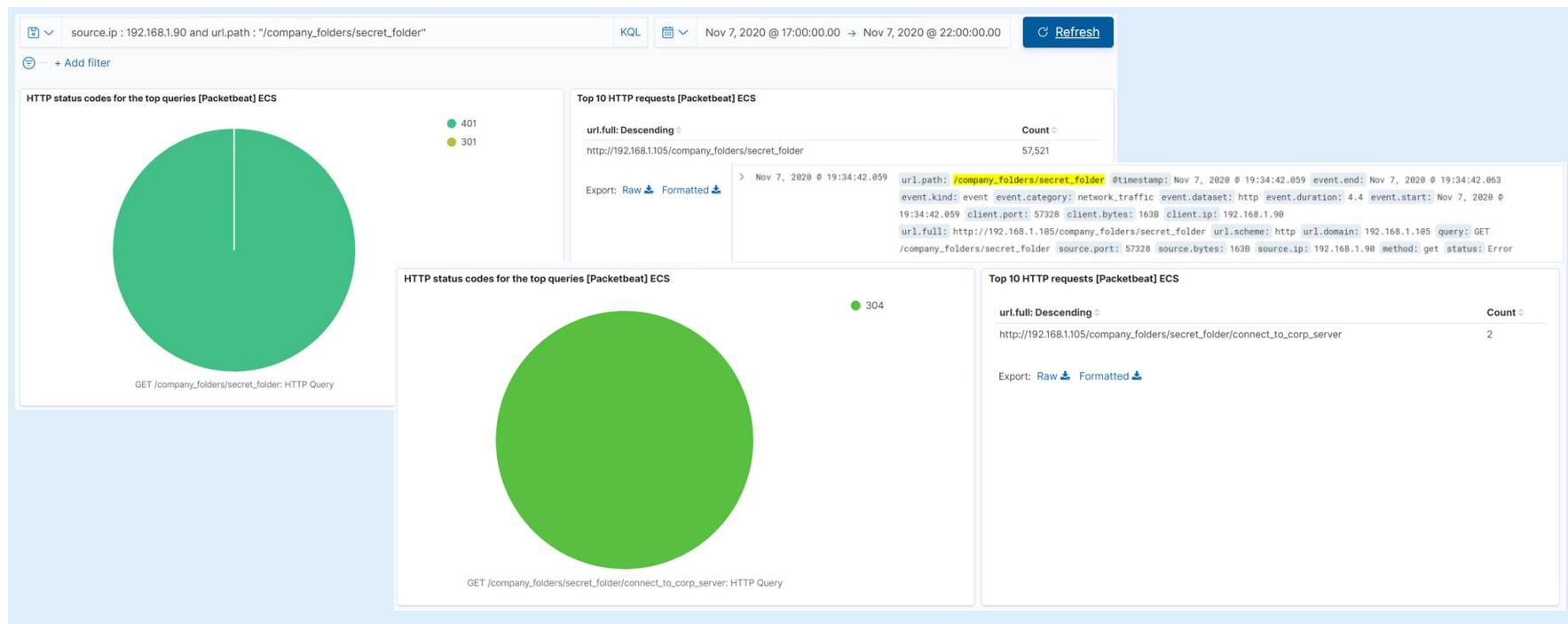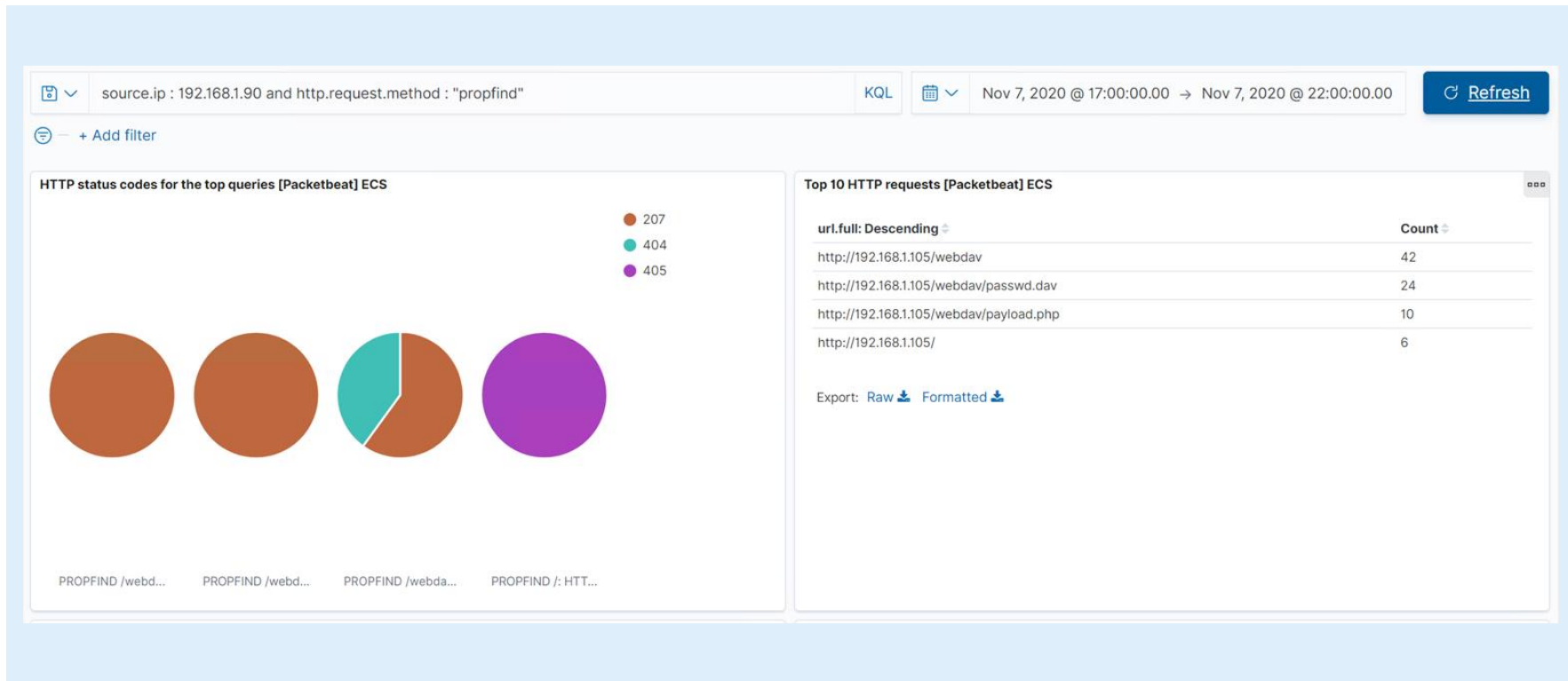
Analysis: Uncovering the Brute Force Attack

● 57,516 login attempts were made with Hydra before the password was cracked.
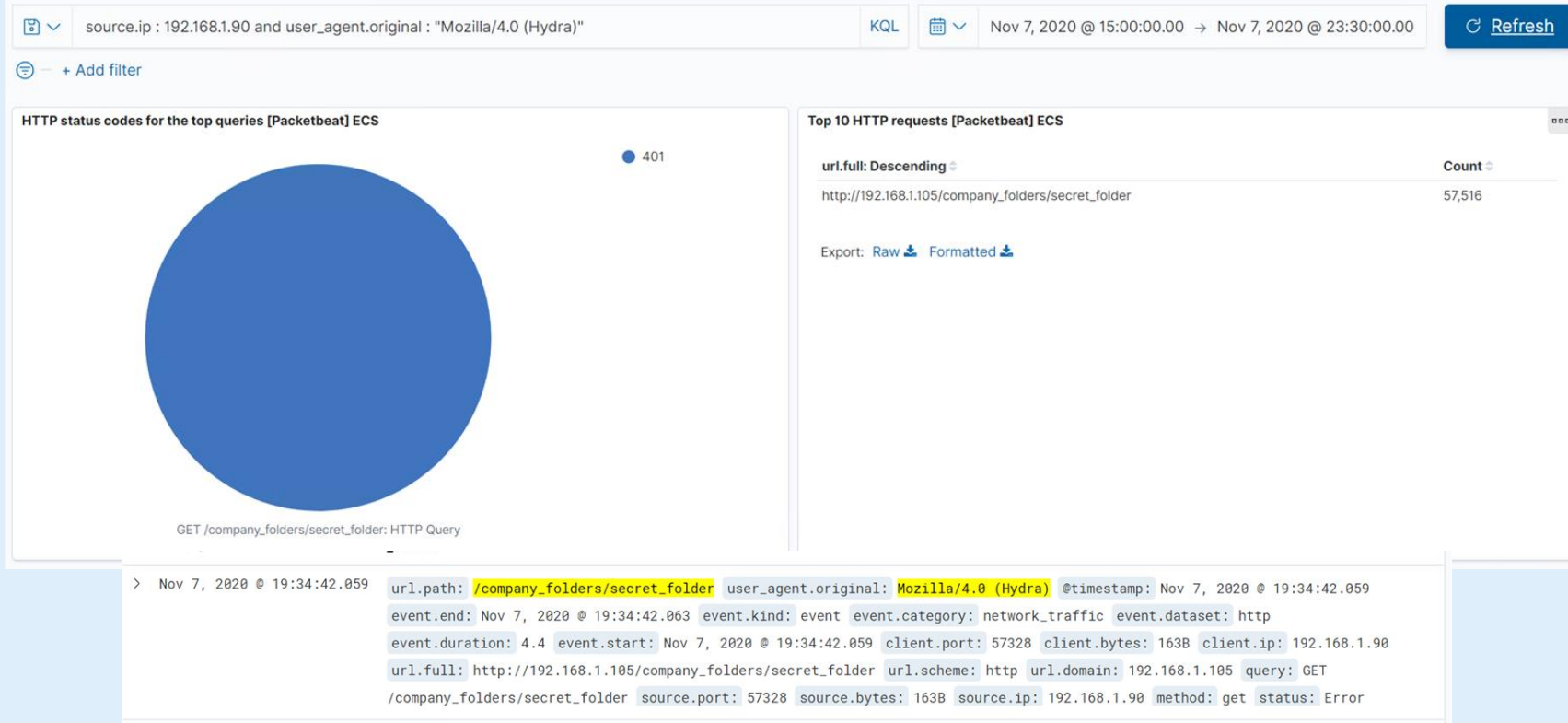
Analysis: Finding the WebDAV Connection

- **/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 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 attacked 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 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.