

# **Capstone Engagement**

## **Assessment, Analysis, and Hardening of a Vulnerable System**

# 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

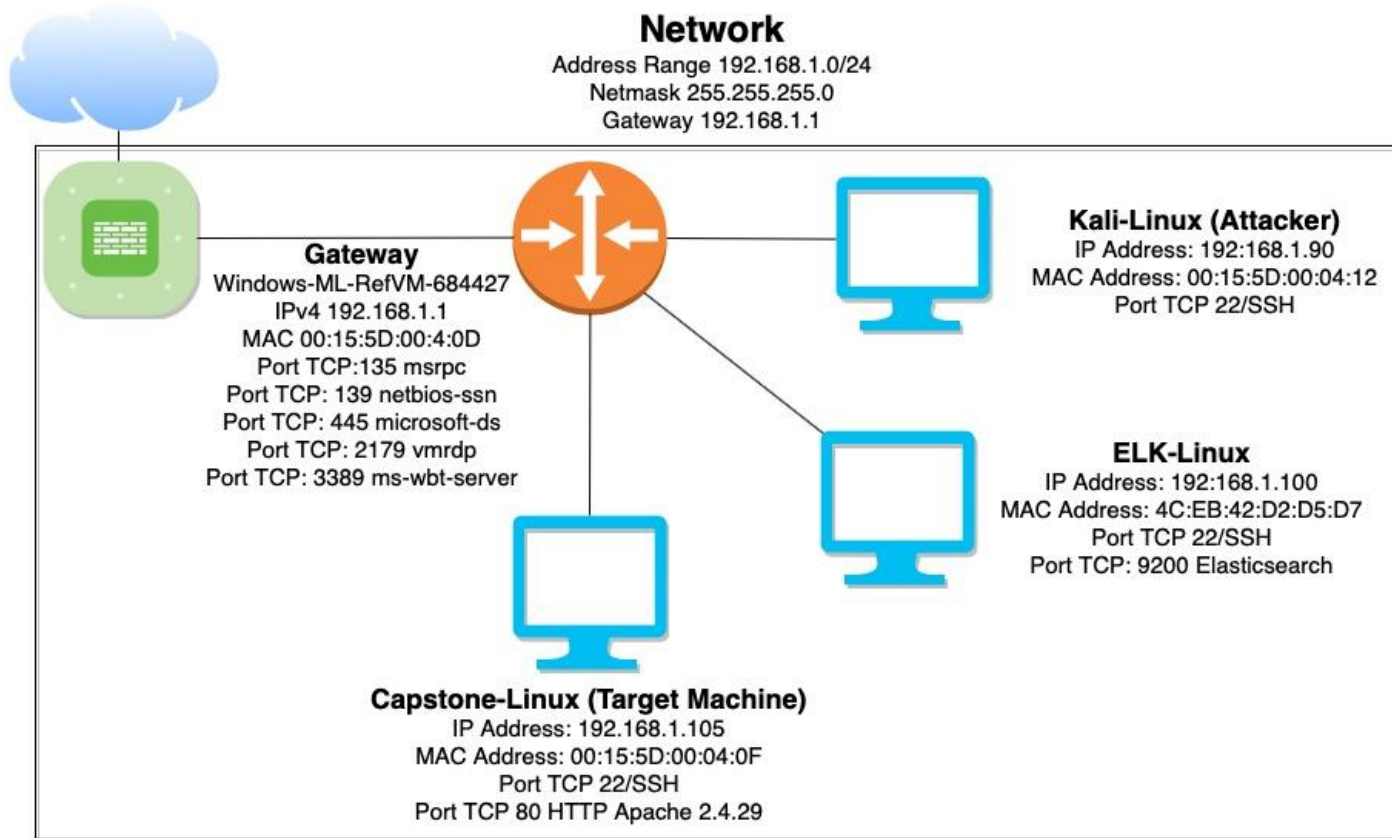
04

**Hardening:** Proposed Alarms and Mitigation Strategies

---

# Network Topology

# Network Topology



## Network

**IP Range:** 192.168.1.0/24  
**Netmask:** 255.255.255.0  
**Gateway:** 192.168.1.1

## Machines

**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, almost black, geometric pattern composed of numerous triangles and polygons of varying shades, 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
<b>Sensitive Data Exposure</b>	Red Team used a web browser and were able access sensitive data to read the full contents of /company_folders/secret_folder on the Capstone server	The contents of this directory revealed that Ashton is the administrator for /company_folders/secret_folder
<b>Security Misconfiguration</b>	The system settings in place allowed for a brute force attack due to no lockout policy for failed attempts	This allowed red team to crack Ashton's password using hydra. Therefore allow further access to Ryan's information contained in this secret folder /webdav using crackstation.net
<b>Unrestricted File Upload</b>	A .php file was uploaded to Ryan's /webdav folder	The successful implant of this file allowed for Red Team to access the Capstone via a backdoor

# Exploitation: Sensitive Data Exposure

01

## Tools & Processes

NMap was used to scan the following IP address range 192.168.1.0/24

The scan revealed that Port 80/HTTP was open. This allowed Red Team to access sensitive data via Mozilla Firefox

```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-06 00:04 PST
Nmap scan report for 192.168.1.1
Host is up (0.00065s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vmrpd
3389/tcp   open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00063s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00068s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.27 seconds
root@Kali:~#
```







# Exploitation: Sensitive Data Exposure

03

## Achievements

The NMnap scan allowed allowed Red Team to gain additional information. It revealed that Ashton is the admin and overseer of /company\_folder/secret\_folder. This folder proved vulnerable to brute force attacks

## Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <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*



http://192.168.1.105 is requesting your username and password. The site says: "For ashtons eyes only"

# Exploitation: Security Misconfiguration

01

## Tools & Processes

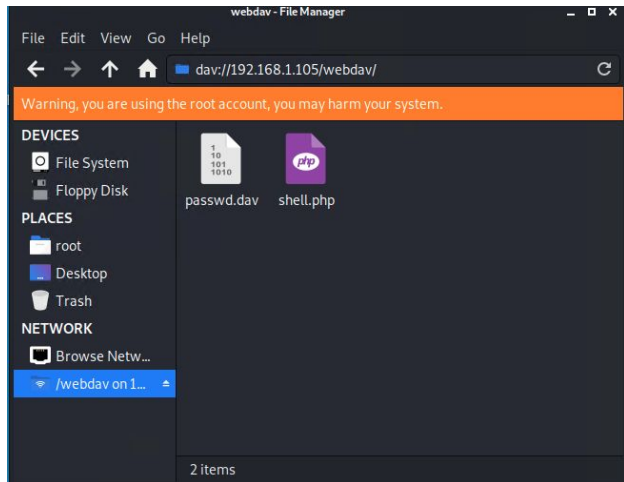
Hydra a Kali Linux tool was used to crack Ashton's password on /company\_folders/secret\_folder

02

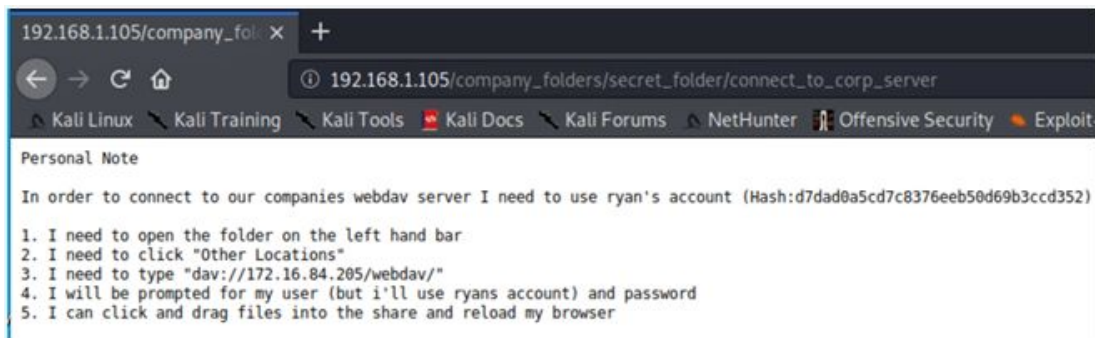
## Achievements

Upon access to the secret folder, the password hash for Ryan was found.

Used crackstation to crack his password hash and gave further access to dav://192.168.1.105/webdav/



```
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 2020-12-06 00:14:25
root@Kali:~#
```



# Exploitation: Unrestricted File Upload

01

## Tools & Processes

Used msfvenom to create and upload a script:  
php/meterpreter/reverse\_tcp

Used shell to explore and compromise target.  
This payload was uploaded to /webdav

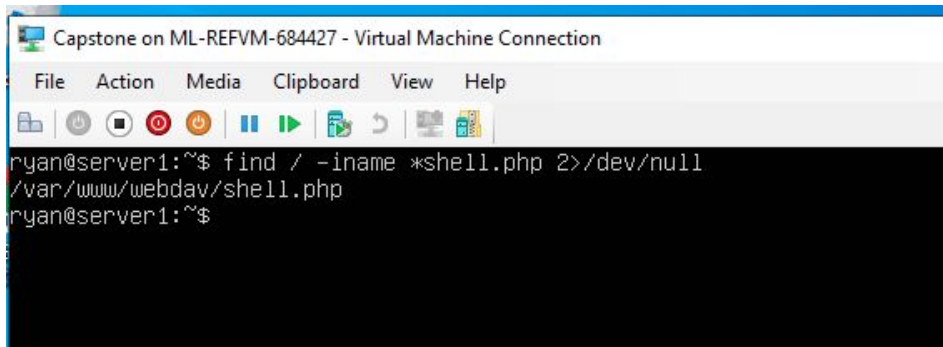
```
meterpreter > shell
Process 2009 created.
Channel 0 created.
```

```
vmlinux.old
cat flag.txt
b1ng0w@5h1sn@m0
```


02

## Achievements

Due to webdav not being secure it allowed Red Team to plant the .php file and give them back door access via a reverse shell on the Capstone web server



```
Capstone on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
ryan@server1:~$ find / -iname *shell.php 2>/dev/null
/var/www/webdav/shell.php
ryan@server1:~$
```



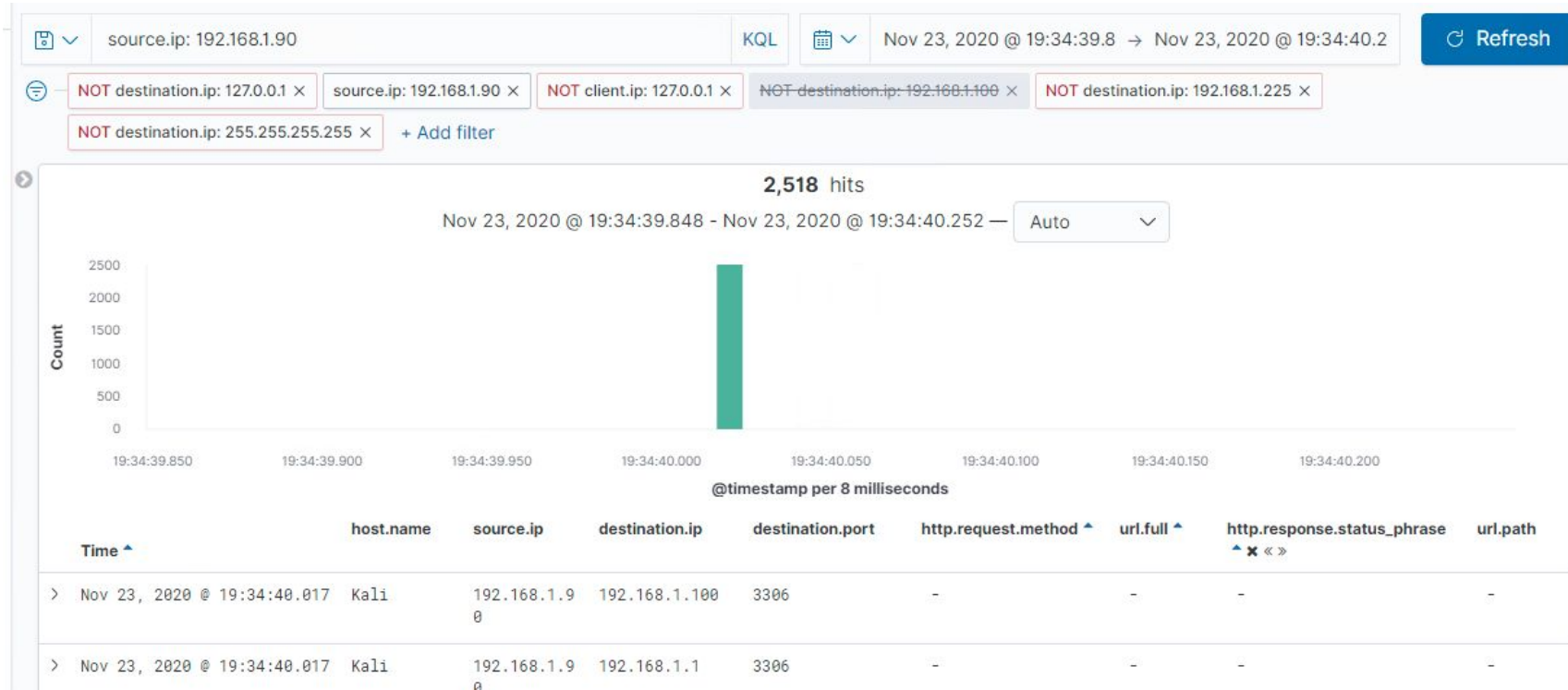
# **Blue Team**

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

The Port Scan took place November 23, at 7:34 pm / 19:34:39

2,518 packets were sent from 192.168.1.90



# Analysis: Finding the Request for the Hidden Directory

We can see that the attack started at **8:02/20:02** with **16,164** requests.

The top three hits for directories and files that were requested were:

## Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,164
http://192.168.1.105/webdav	186
http://192.168.1.105/webdav/shell.php	40
http://192.168.1.105/webdav/passwd.dav	30
http://192.168.1.105/webdav/	28

Export: Raw  Formatted 

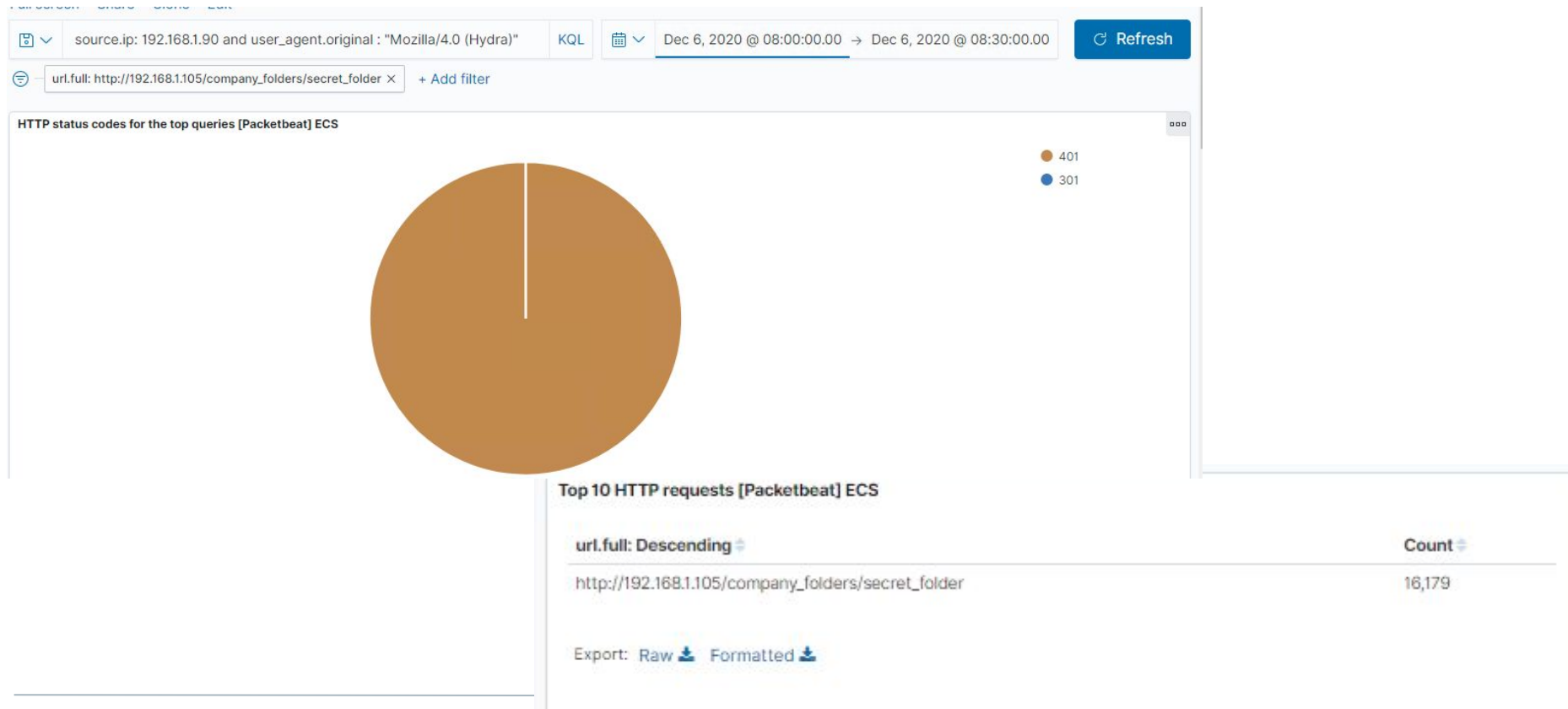
http://192.168.1.105/company\_folder/secret\_folder  
http://192.168.1.105/company\_folder/webdav  
http://192.168.1.105/webdav/shell.php

Nov 23, 2020 @ 20:02:03.544

```
url.path: /company_folders/secret_folder @timestamp: Nov 23, 2020 @ 20:02:03.544
url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http
url.domain: 192.168.1.105 client.ip: 192.168.1.90 client.port: 44858 client.bytes: 167B
server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B network.transport: tcp
network.protocol: http network.direction: outbound
```

# Analysis: Uncovering the Brute Force Attack

16,179 attempts were made with Hydra



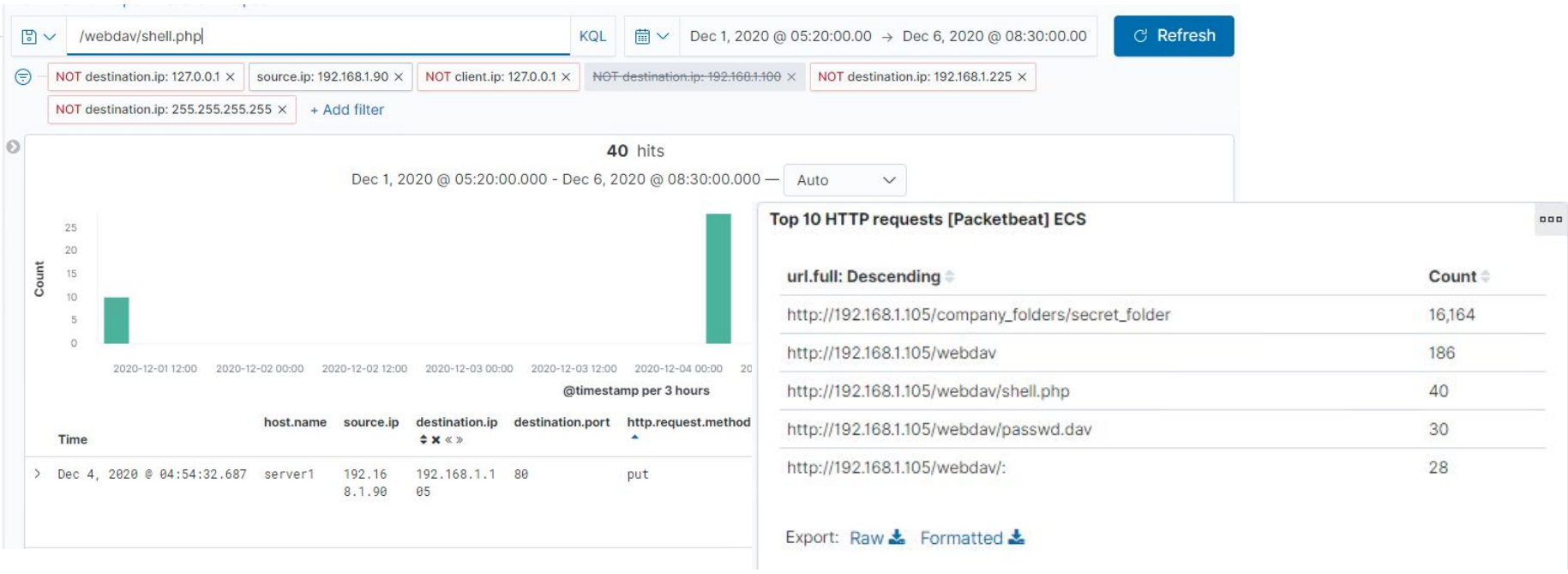
# Analysis: Finding the WebDAV Connection

/webdav was requested 186 times

/webdav/shell.php was requested 40 times

/webdav/passwd.dav was requested 30 times

webdav/ was requested 28 times







# **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?**

- An alarm can be set If an IP address is scanning the network, and is not a trusted IP address.

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

- Alarms should fire if a given IP address not apart of the network sends more than **10 requests per second** for **more than 5 seconds**

## System Hardening

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

- Conduct a thorough scan of the ports on the network. If there are ports open that are not suppose to be than it is good to close them. Create a firewall to block incoming and outgoing traffic to unused ports.
- A web application firewall should also be configured to help mitigate malicious requests before they reach applications

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

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

- A trip alarm: If data is being accessed by a non whitelist IP address from the network

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

- If the incoming IP is not whitelisted, and they are trying to access sensitive data

## System Hardening

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

- Access to the sensitive file can be locally restricted to a specific user.
- Sensitive data should be taken off public facing web servers, other either encrypted with a two-factor login
- Using the command `/etc/httpd/conf/httpd.conf` allows for IP addresses to be allowed access or denied access

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

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

- Multiple failed login attempts
  - 401 error requests in short period of time
  - 200 OK requests in a short period of time from IP addresses outside the whitelist

What threshold would you set to activate this alarm?

- More than 100 requests per second for 5 seconds should trigger the alarm

## System Hardening

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

- Configuring and setting up strong passwords will mitigate brute force attacks.
- Account lockout policy if login attempts surpasses 2-3 tries
- Two factor login

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

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

- Monitor access to webdav with Filebeat
- An alarm should be triggered on any read performed on files within webdav outside of whitelist

What threshold would you set to activate this alarm?

- An alarm should go off anytime an IP address outside the whitelist tries to access /webdav

## System Hardening

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

- Administrators must install and configure Filebeat on the host
- Control access can also be configured in `/etc/httpd/conf/httpd.conf`

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

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

- Alarms should fire upon receipt of any POST request containing form or file data of a disallowed file type not familiar with the network like .php

What threshold would you set to activate this alarm?

- The alarm should fire whenever users upload a forbidden file.

## System Hardening

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

- Filebeat should be enabled and configured.
- Additional configuration can be done in `/etc/httpd/conf/httpd.conf`

*The  
End*