Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Presented by Phi-Huynh Nguyen

Table of Contents

This document contains the following sections:

01 **Network Topology**

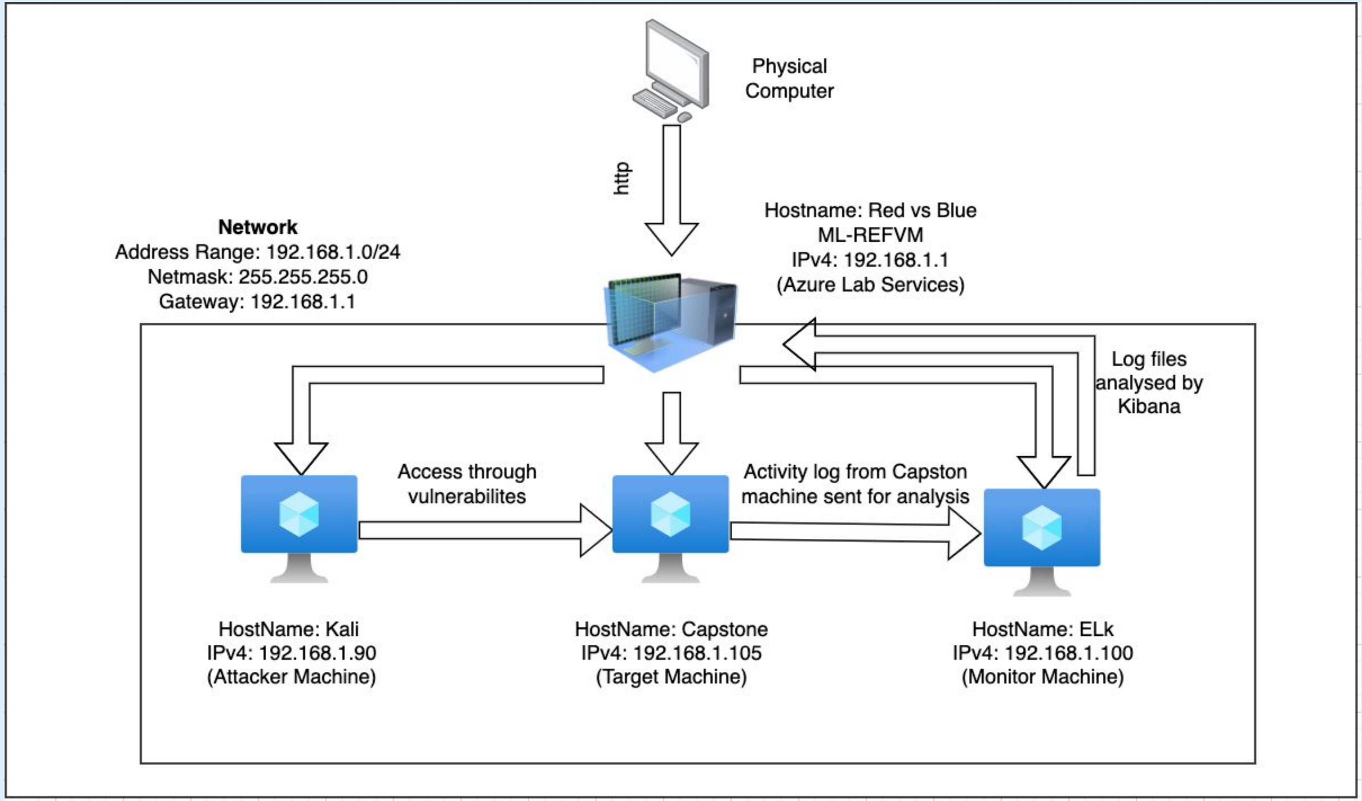
02 **Red Team**: Security Assessment

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
Hostname: Kali
(Attacker)

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone
(Victim)

IPv4: 192.168.1.1
OS: Windows
Hostname: Red vs Blue - ML-REFVM

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red vs Blue ML-REFVM-684427 OS Window	192.168.1.1	Host Machine that will displaced log datas
Kali (Attack VM) OS Kali Linux	192.168.1.90	Attack Virtual Machine
ELK (Monitor) OS Linux	192.168.1.100	Monitor Machine that capture logs activity data from Capstone machine
Capstone (Target VM) OS Linux	192.168.1.105	Target machine with vulnerabilities

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80	Open ports allowed hackers an exploitable access to private information and increase risk of data breach.	Allowed hackers (Red Team) to be able to access private informations.
Accessible Files	Web servers, FTP servers, and other similar accessible servers store a set of files in a “root” directory that is accessible to server’s users.	Allowed hacker to view files after gaining access to the IP on port 80 from a web browser.
Brute Force Password	Common used password that can be find in a brute force wordlist.	Allowed hacker to brute force Ashton’s password, and access to the secret files in the system.
Hashed Password	Hashed password can be cracked through different software(John the Ripper, hashcat, also online tools).	Using hashcat to identify password for Ryan.
WebDav Vulnerability	Exploit WebDav on a server and gain access to drop shell command.	Allowed Redteam to remotely modify website content.

Exploitation: Open Port 80

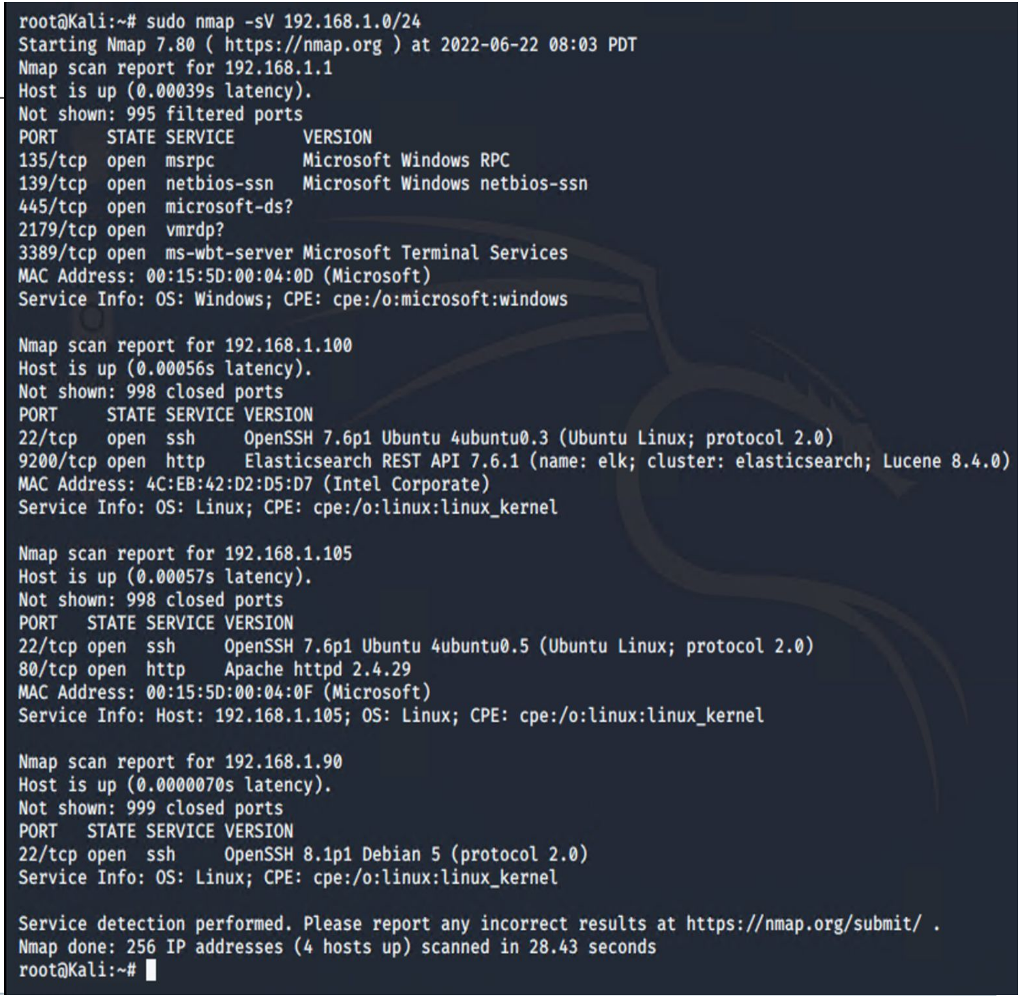
01

Tools & Processes
Used **nmap** to scan for any open ports and services in 192.168.1.0/24

sudo nmap -sV 192.168.1.0/24

02

Achievements
Found that IP address 192.168.1.105 has an open port 80, gaining access to a directory with information on privates files.



```
root@Kali:~# sudo nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-22 08:03 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00039s 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  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00056s 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 (0.00057s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (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 (0.0000070s 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 28.43 seconds
root@Kali:~# 
```

Exploitation: Accessible Files

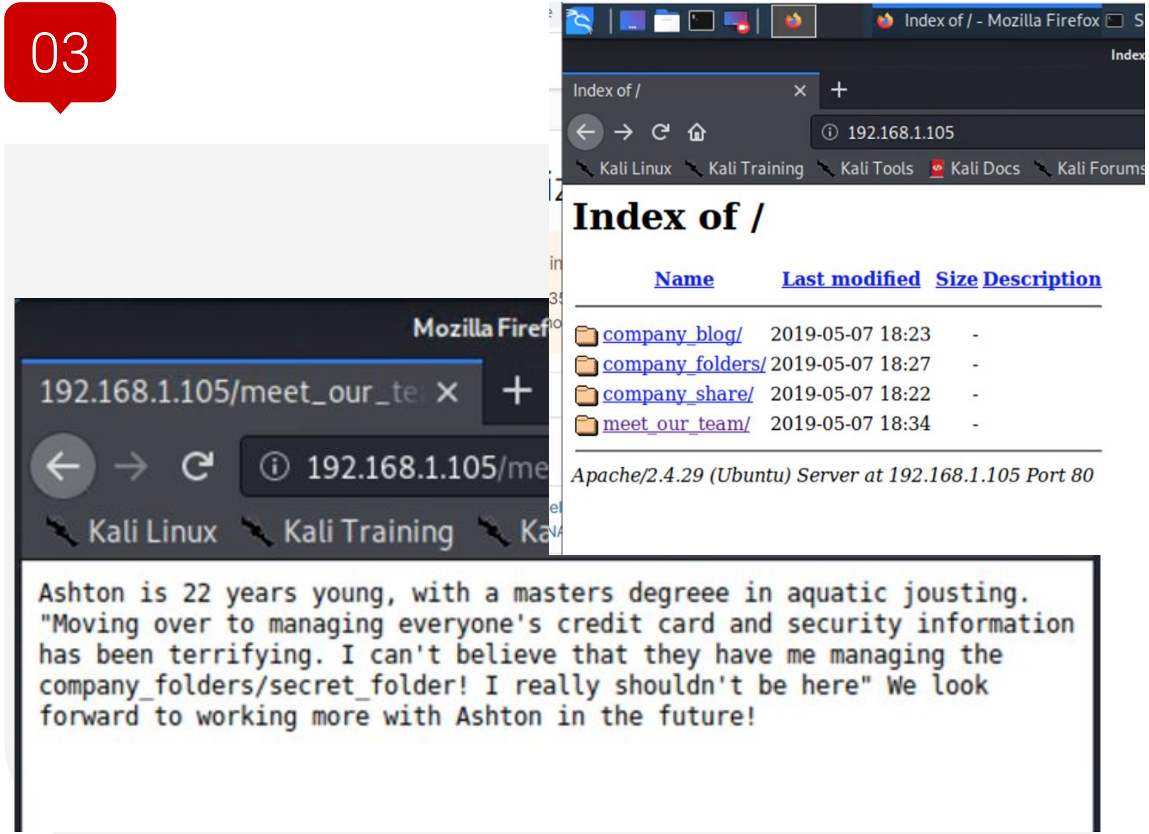
01

Tools & Processes
Using open port 80, Red Team opened a web browser with the root index for 192.168.1.105

02

Achievements
Navigating the files led the Red team to uncover which users had access to secured files and where the company secret files is located.

03



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

```
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: Brute Force Password

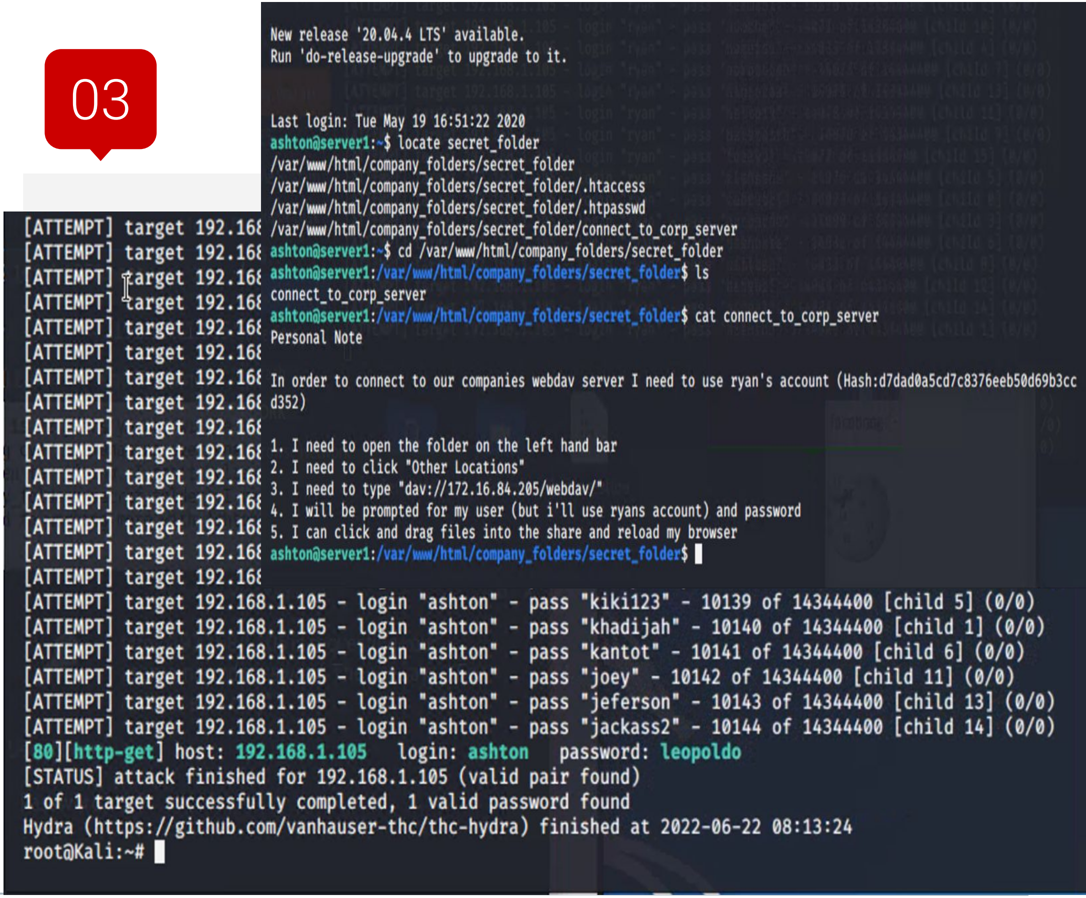
01

Tools & Processes
Using **Hydra**, the Red Team was able to brute force Ashton's password using rockyou.txt (common used password lists)

02

Achievements
Able to uncover Ashton password thus granting user shell access into the company servers.

03



```
New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Tue May 19 16:51:22 2020
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:/var/www/html/company_folders/secret_folder$ ls
connect_to_corp_server
ashton@server1:/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:d7dad0a5cd7c8376eeb50d69b3cc
d352)

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
ashton@server1:/var/www/html/company_folders/secret_folder$ 
```

```
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10139 of 14344400 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10140 of 14344400 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10141 of 14344400 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10142 of 14344400 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10143 of 14344400 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10144 of 14344400 [child 14] (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 (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-22 08:13:24
root@Kali:~# 
```

Exploitation: Hashed Password

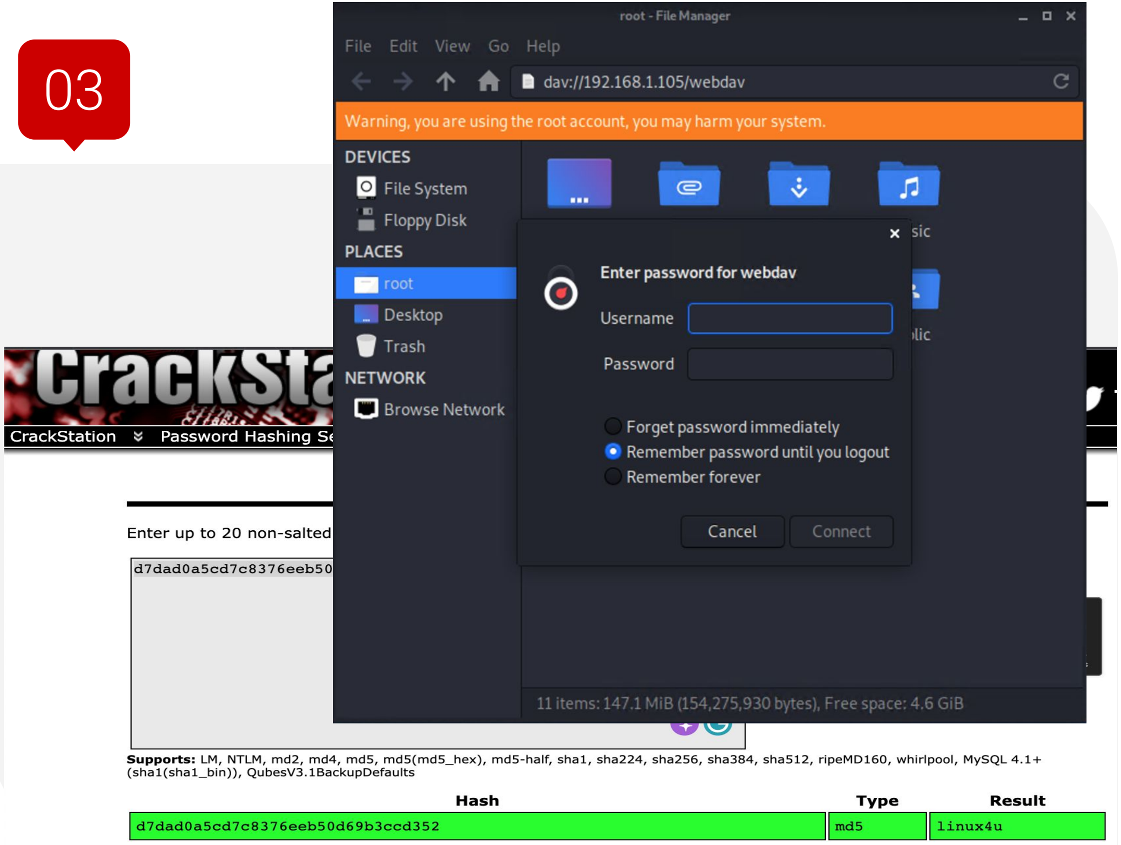
01

Tools & Processes
Using www.crackstation.net, the Red Team was able to find the plain text for the hashed password of Ryan

02

Achievements
Ryan account granted the Red Team access to the system through the WebDav connection.

03



dav://192.168.1.105/webdav

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

Enter password for webdav

Username

Password

○ Forget password immediately
● Remember password until you logout
○ Remember forever

11 items: 147.1 MiB (154,275,930 bytes), Free space: 4.6 GiB

Enter up to 20 non-salted

```
d7dad0a5cd7c8376eeb50
```

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: WebDav Vulnerability

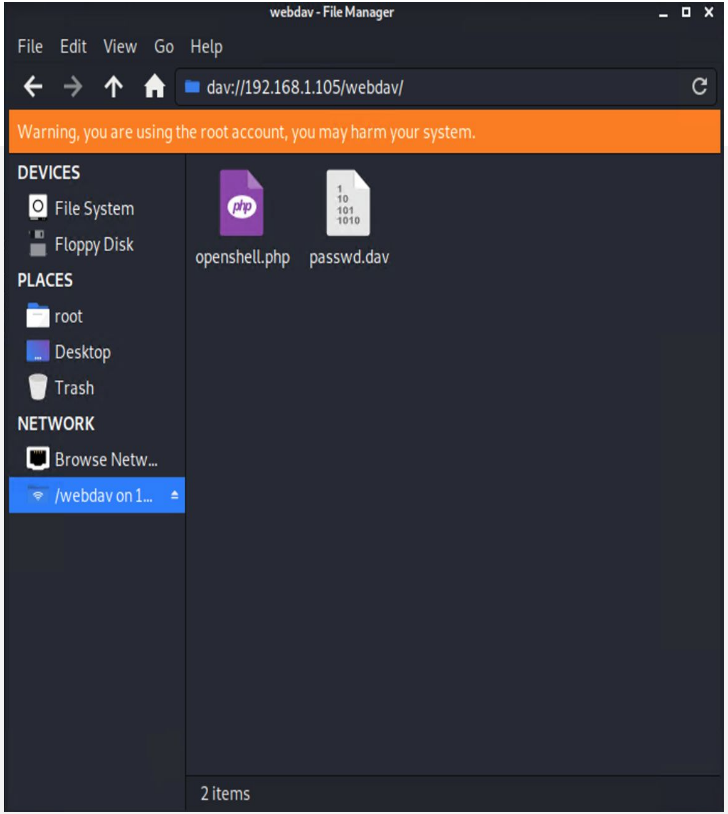
01

Tools & Processes
Once the passwords was cracked, it was easy to log into the company server remotely due to WebDav.

02

Achievements
This then allowed a quicker way of injecting malware unto the company server.

03



webdav - File Manager

dav://192.168.1.105/webdav/

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

openshell.php

passwd.dav

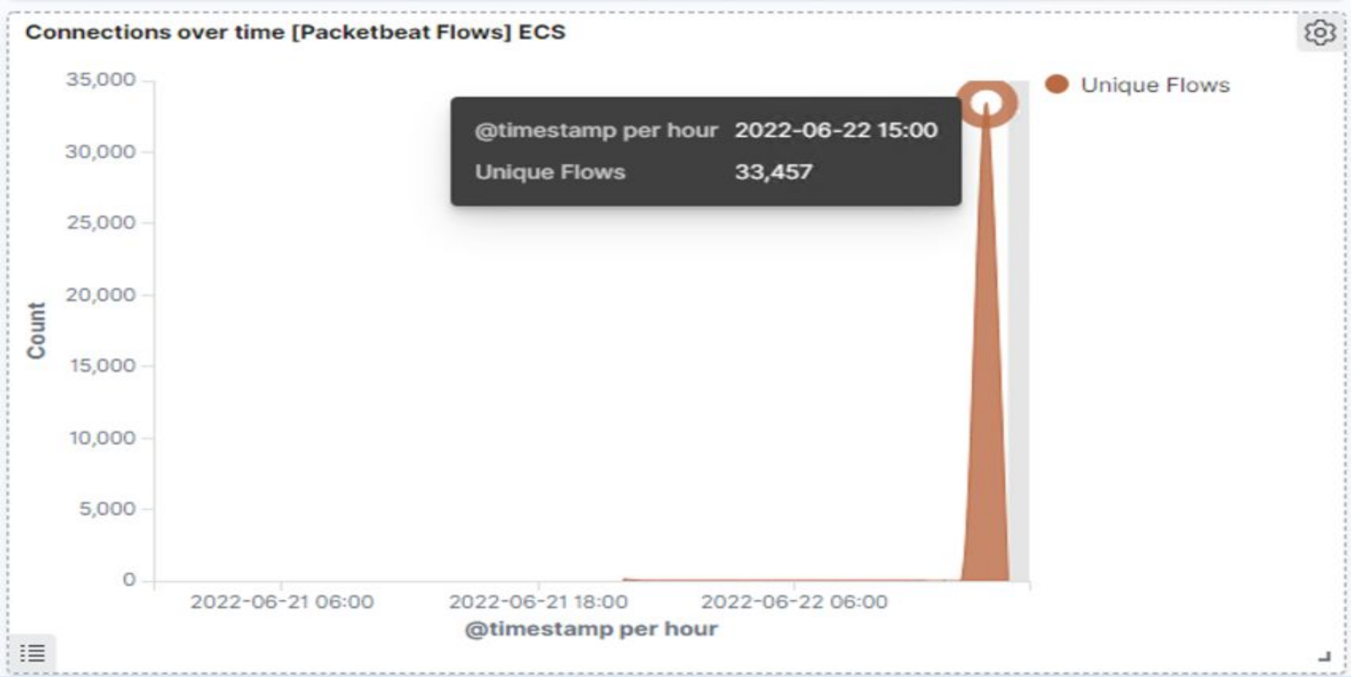
2 items

Blue Team

Log Analysis and Attack Characterization

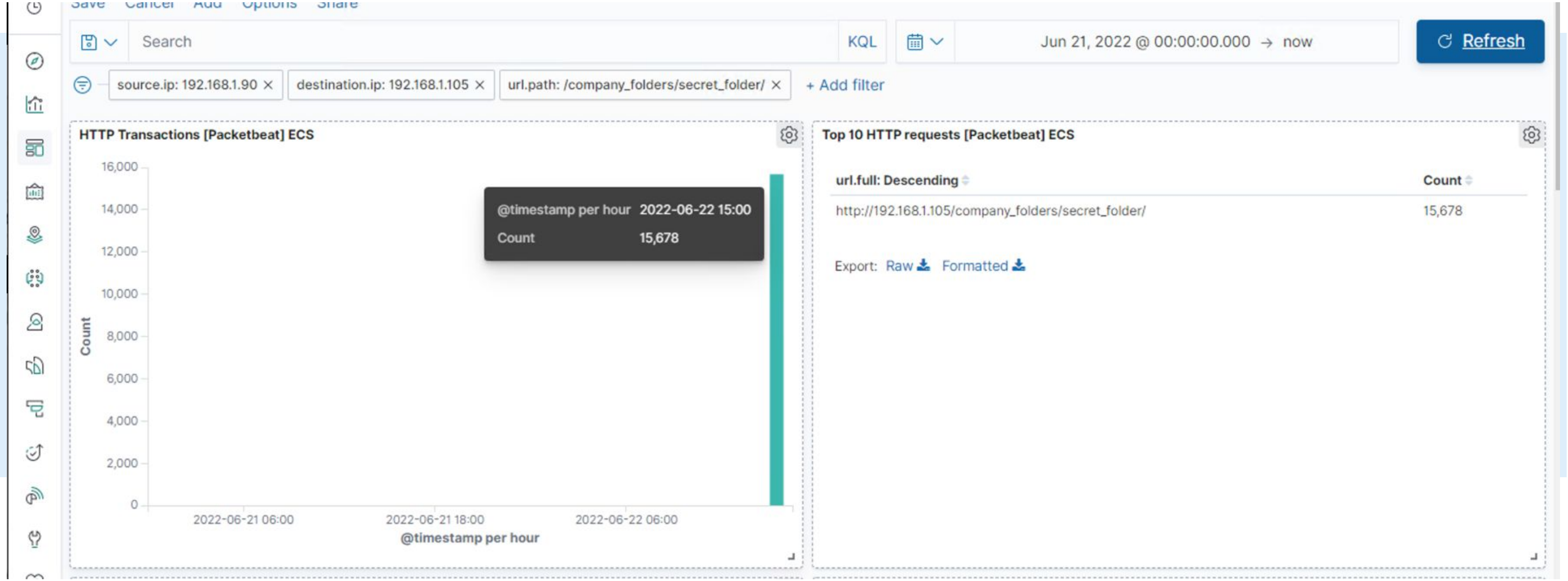
Analysis: Identifying the Port Scan

- The port scan began on June 22, 2022 around 3pm.
- 33,457 connections occurred at the peak with the source IP 192.168.1.90
- A high peaks in network traffic indicate that this was a port scan.



Analysis: Finding the Request for the Hidden Directory

- The request was done close to the time of the port scan on June 22, 2022 around 3pm. With 15,678 requested being made for access to http://192.168.1.105/company_folders/secret_folder
- This folder contained a hash password and clue on how to access the system using another employee's credentials(Ryan)



Jun 21, 2022 @ 00:00:00.000 → now

source.ip: 192.168.1.90 ×

destination.ip: 192.168.1.105 ×

url.path: /company_folders/secret_folder/ ×

HTTP Transactions [Packetbeat] ECS

@timestamp per hour	2022-06-22 15:00
Count	15,678

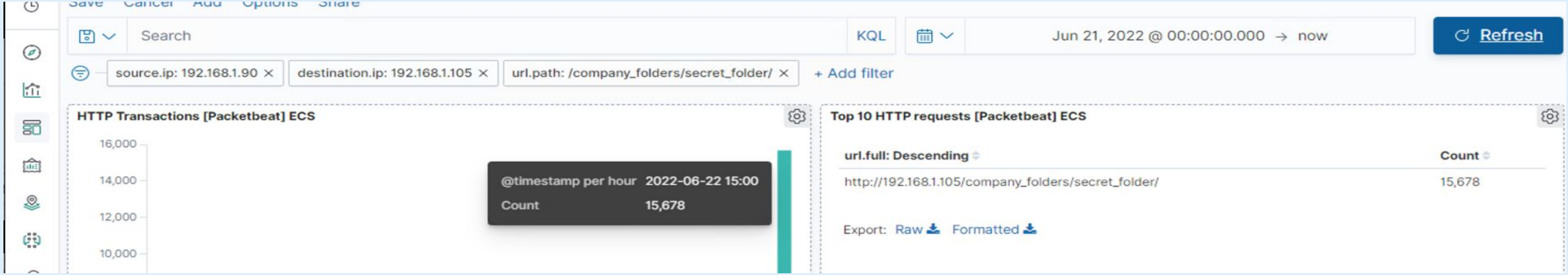
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	15,678

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

- There was a total of 15,678 count to access the secret_folder, with 3 count of the http:response status as “authorized”



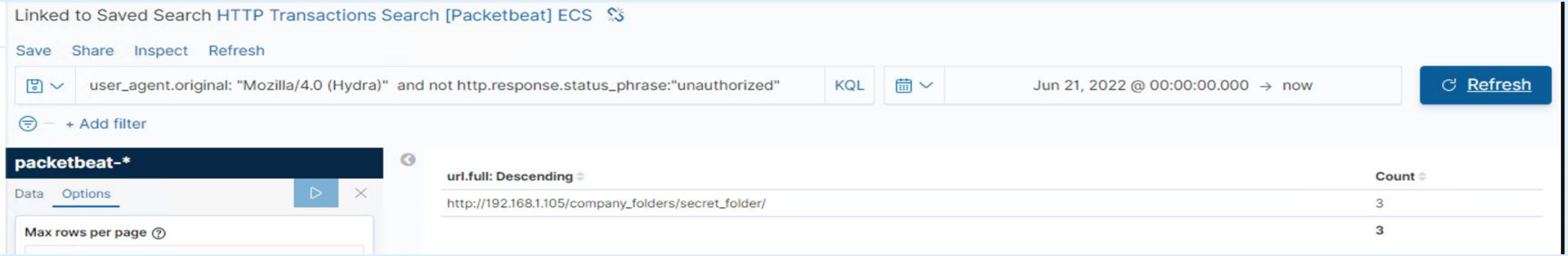
source.ip: 192.168.1.90 × destination.ip: 192.168.1.105 × url.path: /company_folders/secret_folder/ ×

HTTP Transactions [Packetbeat] ECS

@timestamp per hour	2022-06-22 15:00
Count	15,678

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	15,678



Linked to Saved Search HTTP Transactions Search [Packetbeat] ECS

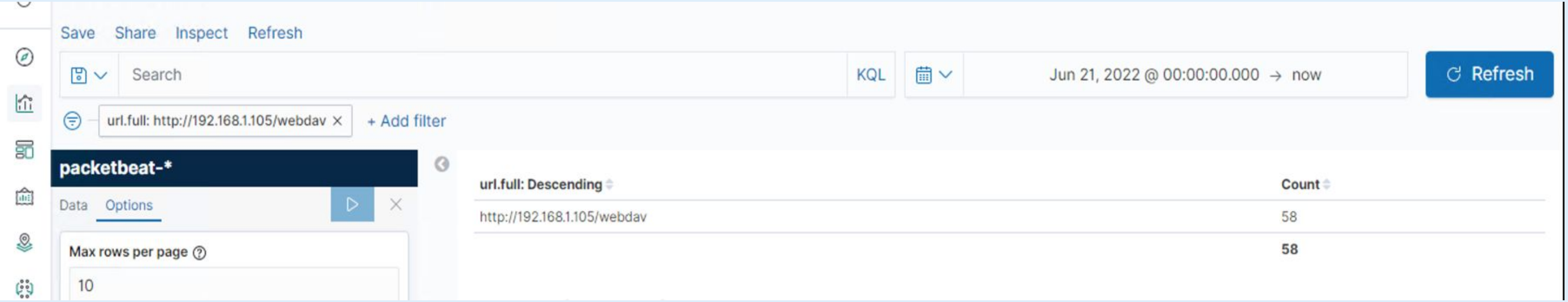
```
user_agent.original: "Mozilla/4.0 (Hydra)"  and not http.response.status_phrase:"unauthorized"
```

Max rows per page

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	3
	3

Analysis: Finding the WebDAV Connection

- http://192.168.1.105/webdav has 58 count of requests.
- With the open-shell.php being the primary requests.



Jun 21, 2022 @ 00:00:00.000 → now

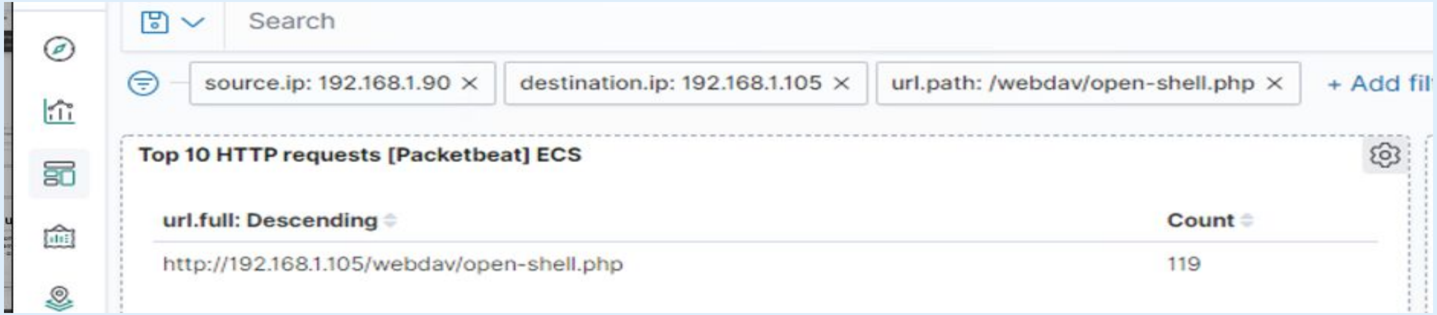
url.full: http://192.168.1.105/webdav

packetbeat-*

Max rows per page

10

url.full: Descending	Count
http://192.168.1.105/webdav	58
	58



source.ip: 192.168.1.90

destination.ip: 192.168.1.105

url.path: /webdav/open-shell.php

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/open-shell.php	119

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Having a threshold of 10 ports scans for low-level alert, and anything more than 100 will come with a severe alerts that need the IT department to look into.

System Hardening

- Enable only traffic from certain IP addresses that can access internal hosts.
- Password policy of 5 allowed failed login, otherwise redirected to IT department.
- Educated employees on the risk of cyber hackers and make sure that all employee understand the correct process of login.
- All employee will have their own login informations, and can not shared with others.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Low-level alert for 3 login failures.
- Critical alert for more than 3 fail attempts.
- Alert from non-authorized IPs.

System Hardening

- Complex username and password.
- Force password reset every 3 months.
- Limit user access to directory
- Removed all reference to the directory in the web server.
- Able multi-factor authentication.
- Blacklist IP after 3 failed login and can only be removed by IT department.

Mitigation: Preventing Brute Force Attacks

Alarm

- Alert for any value of ‘Hydra’
- Low-level alert for 3 failed login
- Critical alerts for 5 failed login
- Alert from unfamiliar IP addresses

System Hardening

- Account lockout after 5 failed login
- Complex username and password
- Password Expiry every 3 months.
- Multi-factor authentication

Mitigation: Detecting the WebDAV Connection

Alarm

- Alert if from unfamiliar IP address
- High Alert after 1 failed attempted

System Hardening

- Limited user access to WebDAV
- Complex username and password
- Update to more secure application
- Allowed only internal access from approved external connections.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- High Alert for any ‘.php’ files.
- Alert for all uploads that triggered anti-virus/anti-malware.

All alert has a threshold of 1.

System Hardening

- Limited file types being uploaded.
- Uploaded files is ‘Read-Only’ unless uploaded from company computer.

The End