# Red Team: Summary of Operations

Report by **Paul Barrett**

**CyberSecurity Analyst**

Version 1 **20th December 2020**

Version 2 **12th January 2020**

## 

## **Table of Contents**

* Exposed Services \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Page 3
* Critical Vulnerabilities \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Page 10
* Exploitation \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Page 12
* Appendix \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Page 22
* References \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Page 23

### 

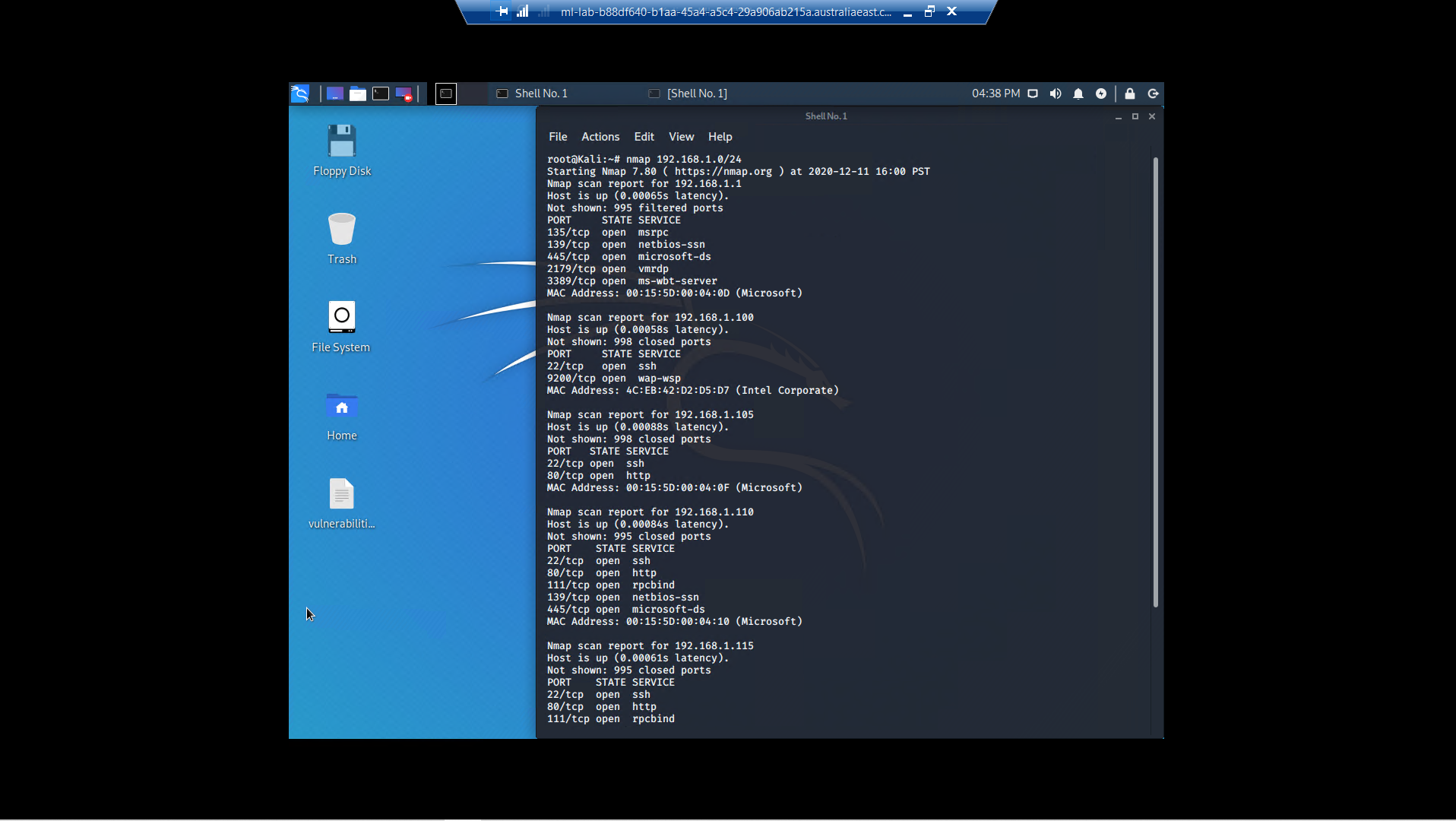
### **Exposed Services**

Note: 3 watchers were set up in Kibana prior to running the following network scans.

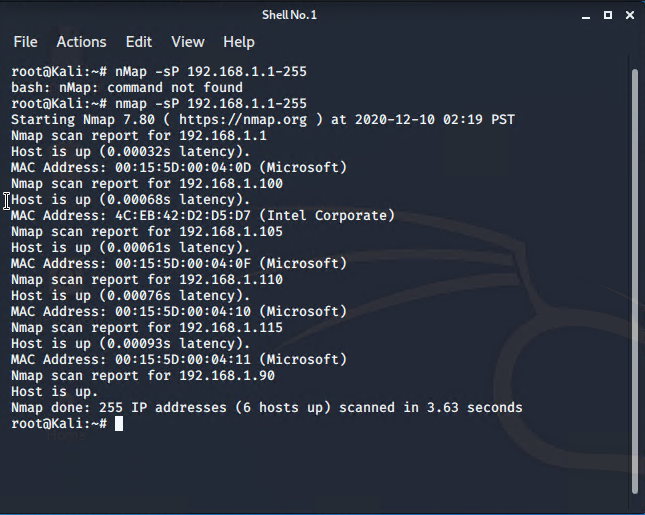
**Nmap scan results for each machine reveal the below services and OS details:**

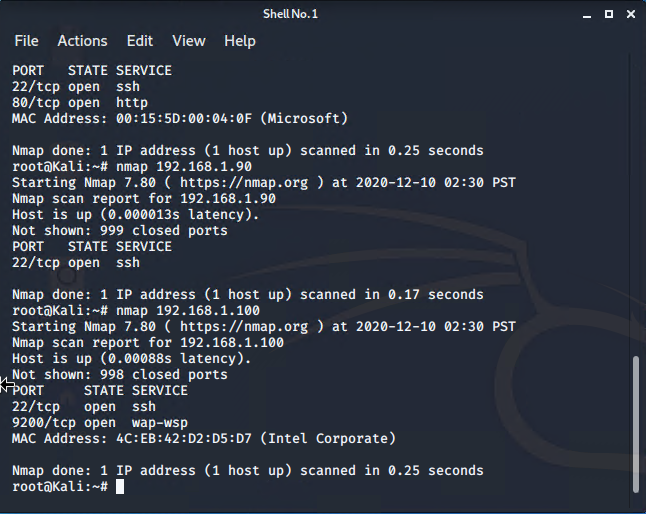
* $ nmap -sV 192.168.1.110

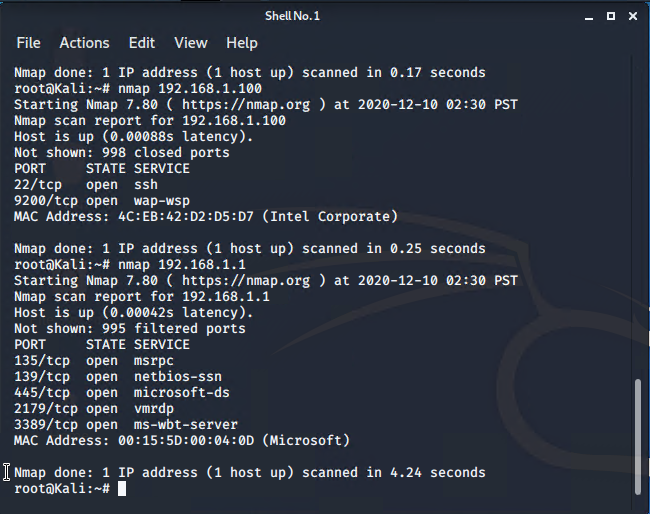
* $ nmap -sV 192.168.1.115





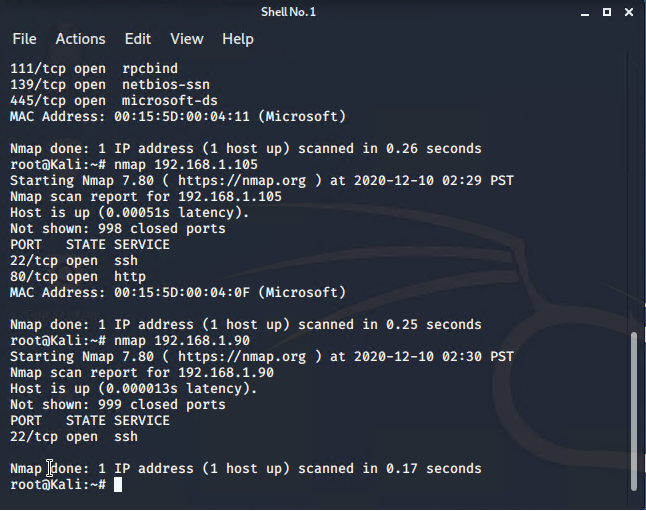




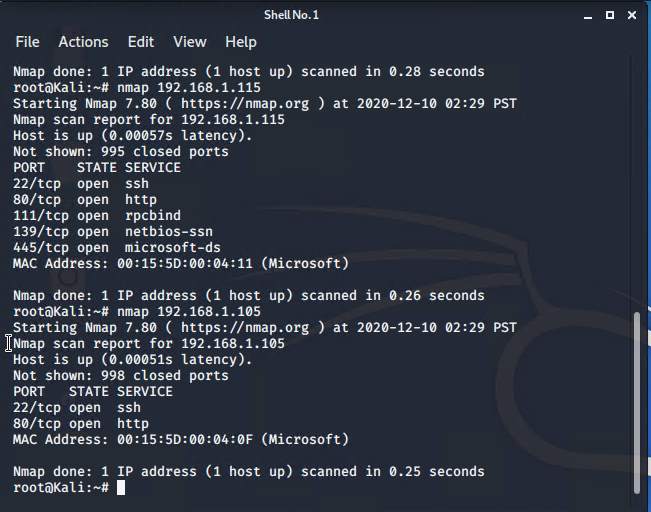
This scan identifies the services below as potential points of entry:

**SSH service running on open port 22**

Port 135 - CVE-2002-1561 if win 2000, NT, XP



**SSH service running on open port 22**



**Target 1 - 192.168.1.110**

1. 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
2. Port 80 open and has HTTP service running - possibly vulnerable to script injection - (CVE-2019-6579) - CVSS Score 7.5
3. Port 111 open and has RPCBIND service running - malicious file uploads may be a possibility - (CVE-2017-8779) - CVSS Score 7.8
4. Port 139 open and has NETBIOS-SSN service running - possible vulnerabile to reverse shell - (CVE-2017-0143) - Nist Score 8.1
5. Port 445 open and has NETBIOS-SSN service running - possible vulnerabile to reverse shell - (CVE-2020-0796) - Nist Score 10.0
6. Simplistic Usernames - extremely high (10/10) Vulnerability
7. Weak Passwords - Top 25 Most Dangerous Software Weaknesses
8. Root Accessibility - extremely high (10/10) Vulnerability
9. Regsvc (CVE-2020-25213) - CVSS Score 9.8
10. SSH Access (CVE-1999-0013) - CVSS Score 7.5
11. Index Access (CWE-548) - Nist Score 4.3
12. Brute Force Capabilities

**Target 2 - 192.168.1.115**

1. The biggest vulnerability for Target 2 was the fact that **Brute Force** access was gained via **username Vagrant**.
2. Port 22 open and has SSH service running - brute force or SSH shell into machine via this port may be a possibility
3. Port 80 open and has HTTP service running - possibly vulnerable to script injection
4. Port 111 open and has RPCBIND service running - malicious file uploads may be a possibility
5. Port 139 open and has NETBIOS-SSN service running - possible vulnerabile to reverse shell
6. Port 445 open and has NETBIOS-SSN service running - possible vulnerabile to reverse shell

### **Critical Vulnerabilities**

The following vulnerabilities were identified on each target:

**Target 1**

1. **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
2. **CVE-1999-0013** - Stolen Credentials from SSH clients via ssh-agent program, allowing other local users to access remote accounts belonging to the ssh-agent user. [APDX0001]
3. **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
4. **CVE-2017-8779 Port 111** - vulnerable to Metasploit exploits
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 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability."
6. [**CVE-2020-0796**](https://packetstormsecurity.com/files/cve/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. **Ability to discover password by John The Ripper or Hydra** (Brute Force attack)
9. **Ability to gain Partial Root Access** giving authorization to execute commands and leverage other vulnerabilities
10. **Simplistic Usernames** (usernames: michael and steven)
11. **Weak Passwords** (passwords: michael and pink84)

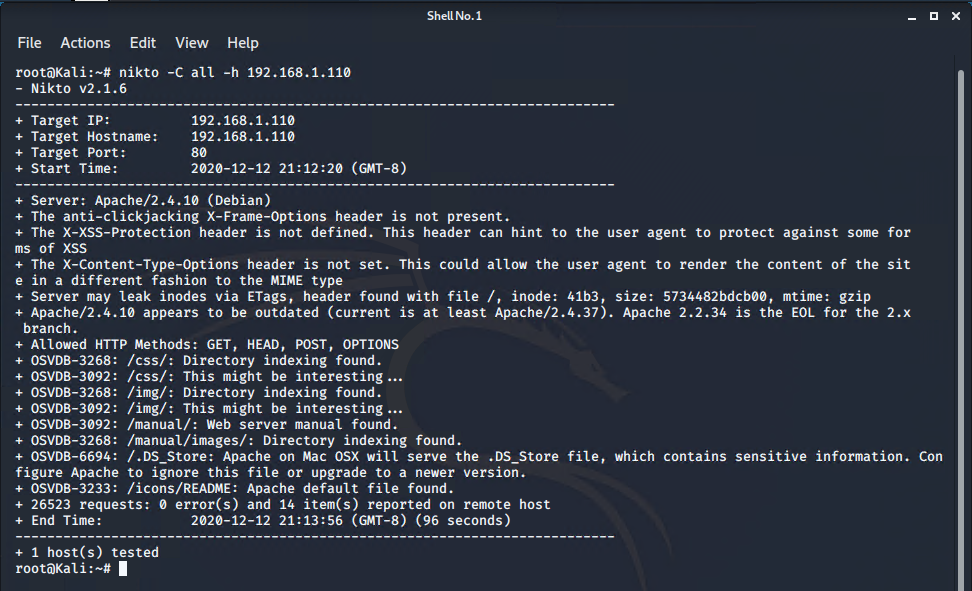
**Target 2**

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
3. **Simplistic Usernames** (username: vagrant)
4. **Weak Passwords** (password: tnargav)

Nikto scan results as proof of the identified vulnerabilities.

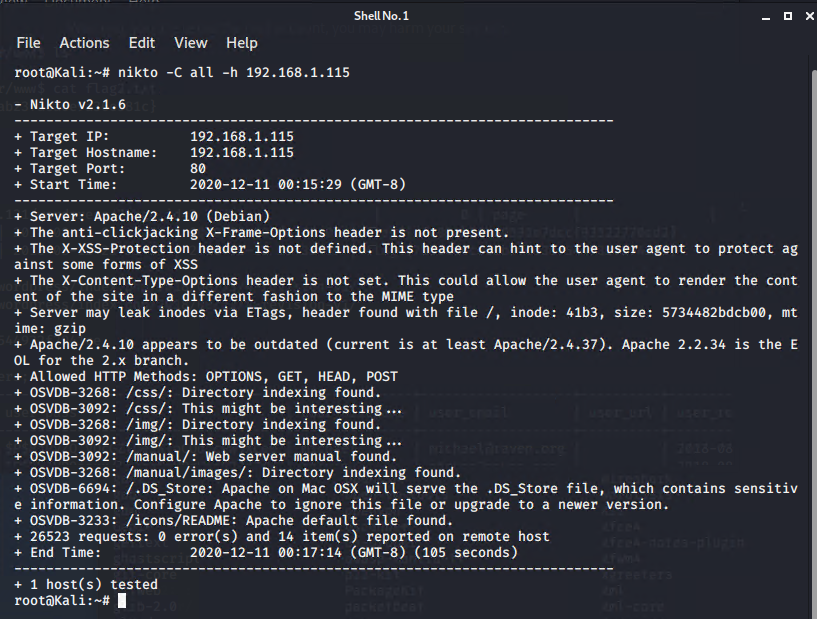
**TARGET 1 NIKTO SCAN:**

Command to run: nikto - all -h 192.168.1.110



**TARGET 1 NIKTO SCAN:**

Command to run: nikto - all -h 192.168.1.115

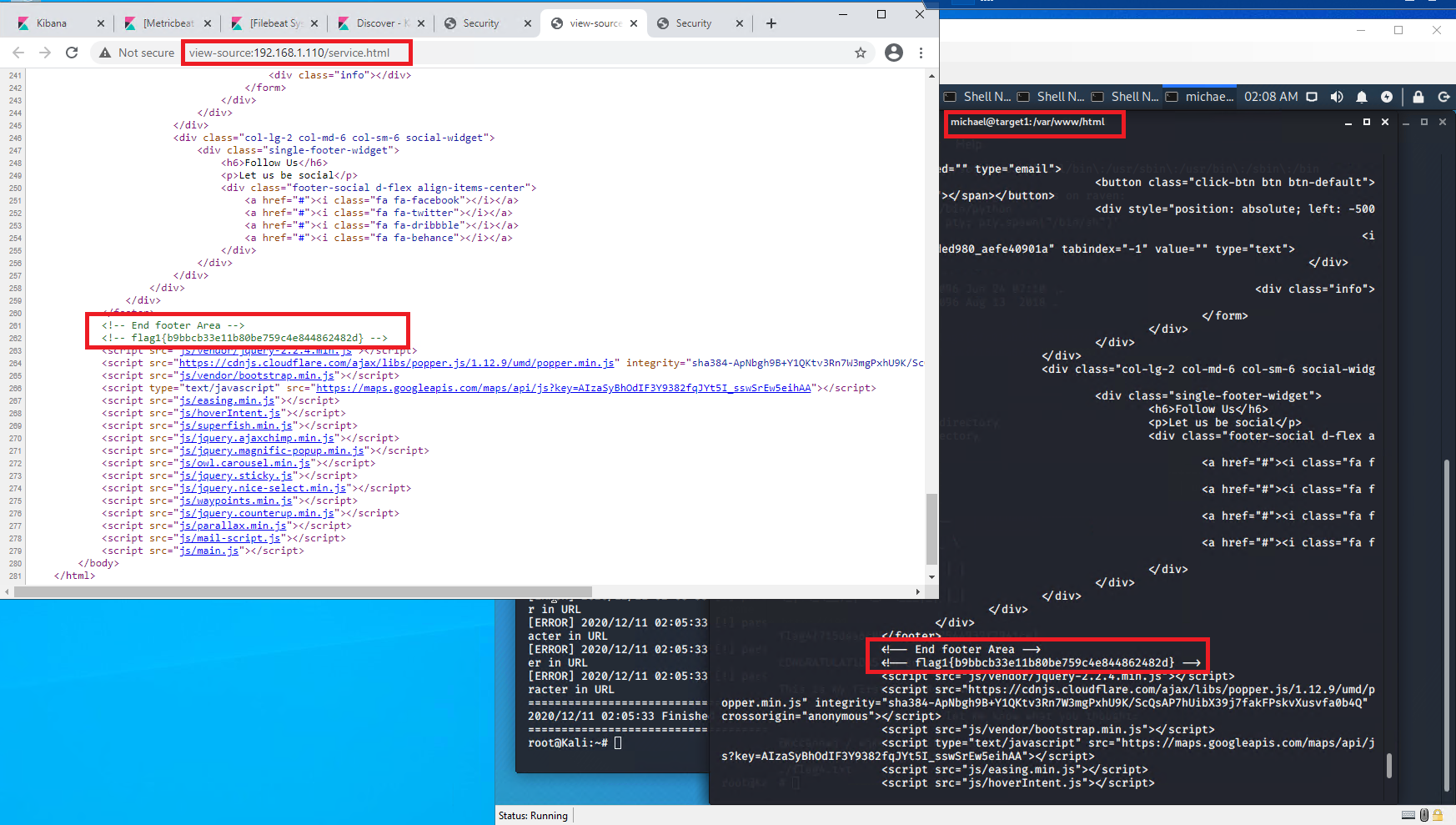


### Exploitation

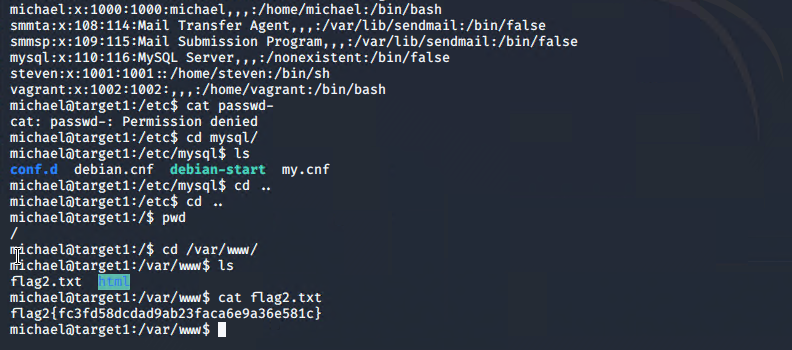
Acting on behalf of the Red Team, I was able to penetrate both Target 1 and Target 2 and retrieve the following confidential data:

**Target 1**

* flag1.txt: **flag1{b9bbcb33e11b80be759c4e844862482d}**
* Exploit Used
  1. TODO: Identify the exploit used.



* flag2.txt: **flag2{fc3fd58dcdad9ab23faca6e9a36e581c}**
* Exploit Used
  1. First I had to SSH using michael as user credentials, and after several failed attempts at guessing his password, his name WAS his password.
  2. I attempted to to cat the passwd and passwd- files, without success
  3. Navigating through folders that michael had access to, I found a file flag2.txt located in /var/www/
  4. When I used the command cat flag2.txt the flag was revealed.

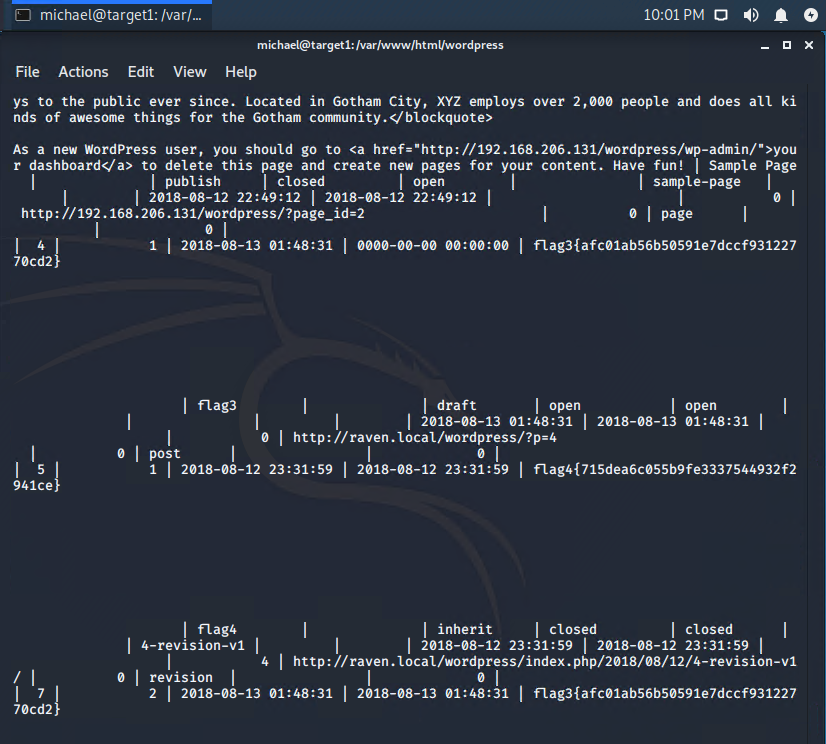


Target 1 limited root access gained

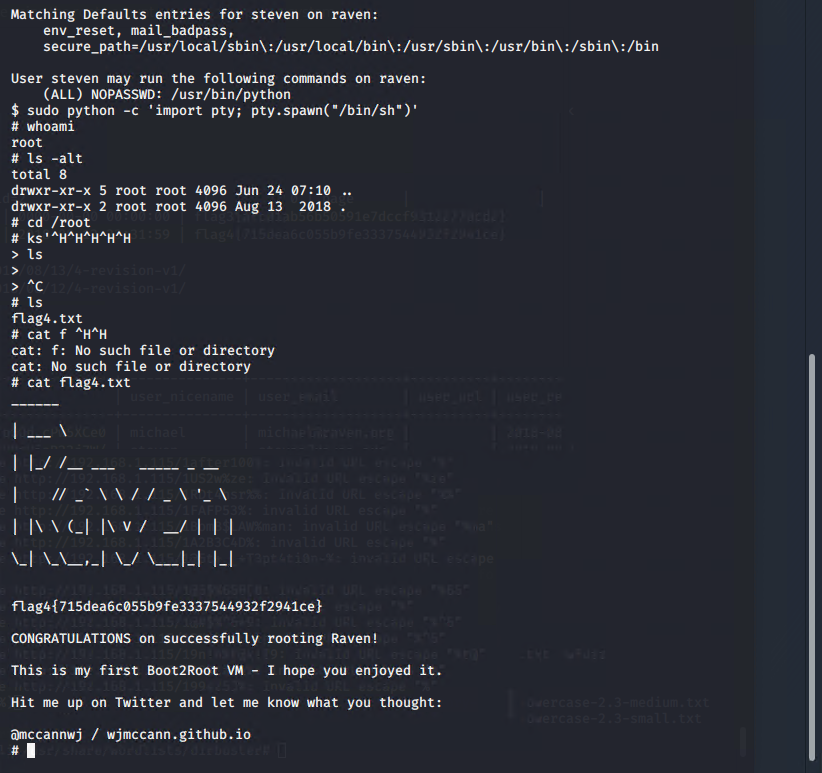
****

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

Flags 3 and 4

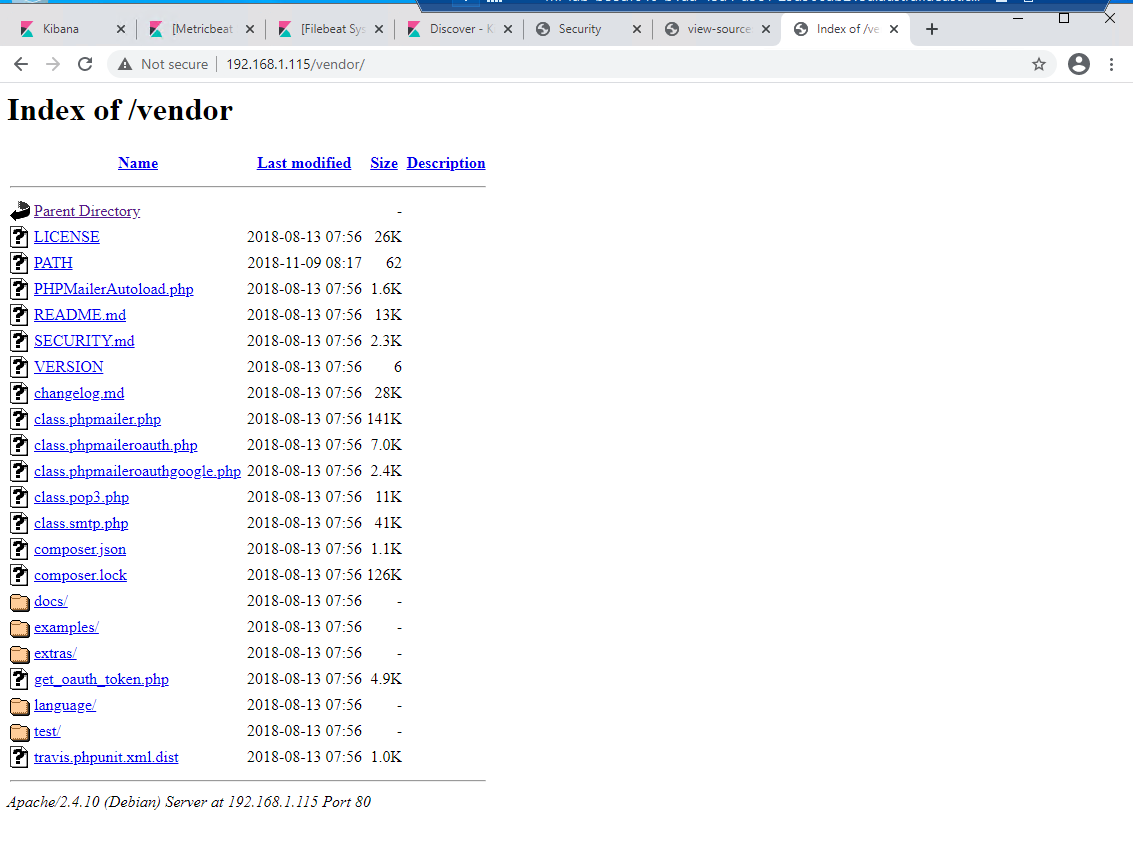
****

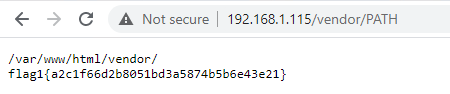
* flag3.txt: **flag3 {afc01ab56b50591e7dccf93122770cd2}**
* flag4.txt: **flag4 {715dea6c055b9fe3337544932f2941ce}**

****

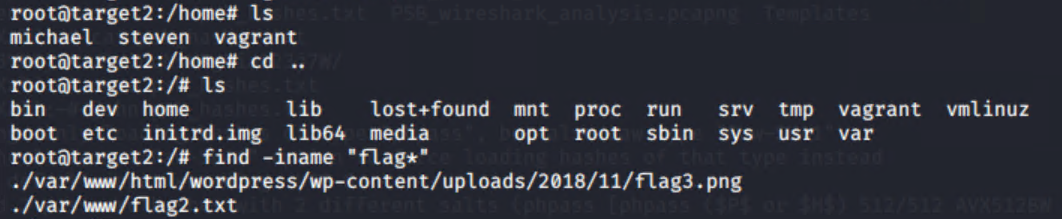
#### **Target 2**

* **flag1.txt:** flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}
* Exploit Used
  1. I used nmap, netdiscover, and wpscan to test what exploits were available.
  2. I navigated my chrome browser to the target2’s IP address, and looked at the subfolder /vendor/ and from there, I snooped around into every link and folder to see what could be found. Within the /PATH/ folder, I found target 2’s flag1.txt





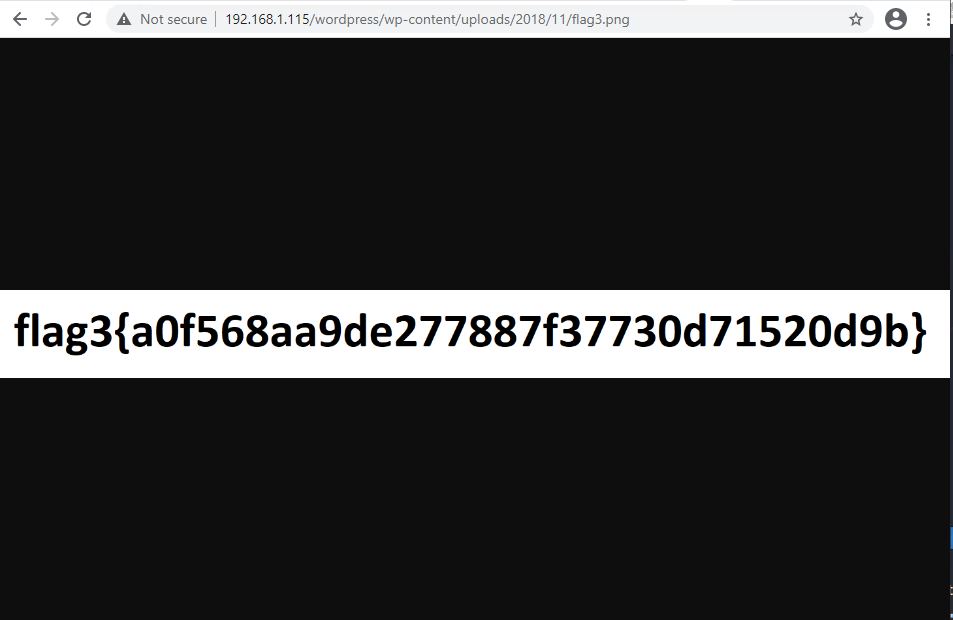
* **flag2.txt:** **flag2{6a8ed560f0b5358ecf844108048eb337}**
* Exploit Used
  1. No exploit was used: a simple file name search was used.
  2. Command: **find -iname “\*flag\*”**
  3. Command: **cat flag2.txt**



Additional Notes:

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

* **flag3.txt:** **flag3{a0f568aa9de277887f37730d71520d9b}**
* Exploit Used
  1. TODO: Identify the exploit used.
  2. TODO: Include the command run.



* flag4.txt: **flag{df2bc5e951d91581467bb9a2a8ff4425}**
* Exploit Used
  1. Exploit used: I conducted a **User name search**, then **brute force password**.
  2. I spent 2 days trying to figure out how to escalate to root without success. While writing up the report, I recalled that I had found 3 user accounts:
     + Michael
     + Steven
     + Vagrant
  3. From there, I sought to explore trying to gain access to the Vagrant account. I believed I had found a salted password for Vagrant, and was not able to crack it. I decided to brute force (guess) in the same way I had accessed Michael’s user account, and found the password to be vagrant backwards: target
  4. I then **ssh vagrant@192.168.1.115** with that password, and i was able to **sudo su** to escalate to full root access
  5. I then ran the Command: **find -iname “\*flag\*”**
  6. And then the Command: **cat flag4.txt**

## 

**Salted passwords found within /etc/shadow**

## 

screenshot above: Flag 4 Screenshot

## 

## Appendix

[APDX0001]



## 

## References

<https://hackt.nl/nmap-cheat-sheet/>

<https://www.cvedetails.com/cve/CVE-2018-6082/>

<https://www.cvedetails.com/cve/CVE-2017-8779/>

<https://www.cvedetails.com/cve/CVE-1999-0013/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>

<https://searchsecurity.techtarget.com/answer/The-dangers-of-open-port-139>

<https://varonis.com/blog.netcat-commands/>

<https://www.thegeekstuff.com/2013/09/mysql-select-command/>

To review

<https://searchsecurity.techtarget.com/answer/Detecting-and-defending-against-TCP-port-445-attacks>

<https://www.guardicore.com/2020/03/how-to-protect-your-systems-against-critical-smb-vulnerabilities-cve-2020-0796/>

<https://medium.com/@simonsulyma/hack-the-box-legacy-penetration-testing-with-metasploit-ad6016757504>

<https://beyondsecurity.com/scan-pentest-network-vulnerabilities-rpc-portmapper.html>

<https://www.rapid7.com/db/vulnerabilities/RPC-PORTMAPPER-0001/>