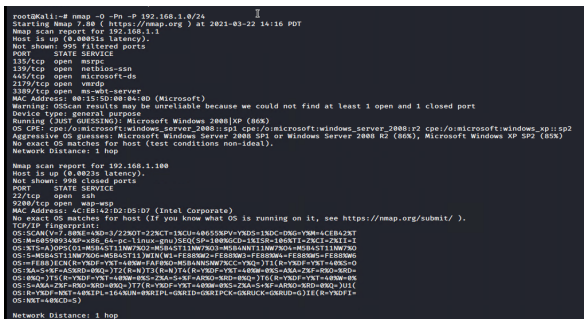
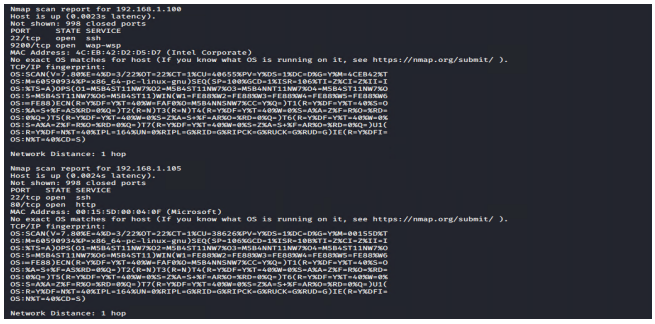
Red Team: Summary of Operations

Table of Contents:

Exposed Services

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





```
Nmap scan report for 192.168.1.110
Host is up (0.00081s 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)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

Nmap scan report for 192.168.1.115
Host is up (0.00074s 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)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

Nmap scan report for 192.168.1.90
Host is up (0.000057s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 21.51 seconds
```

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

Target 1

List of exposed Services :

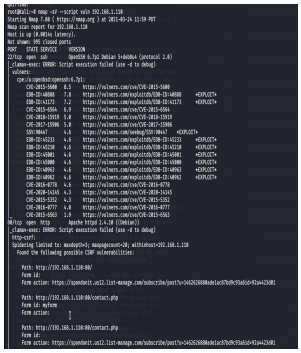
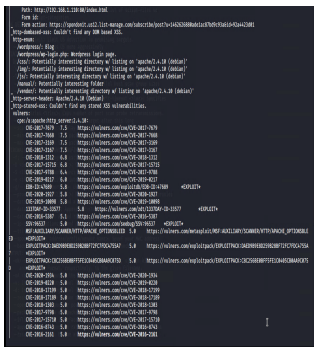
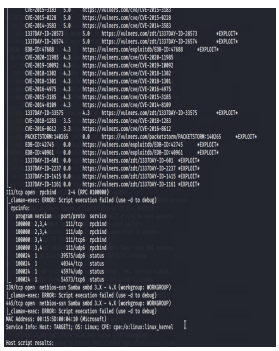
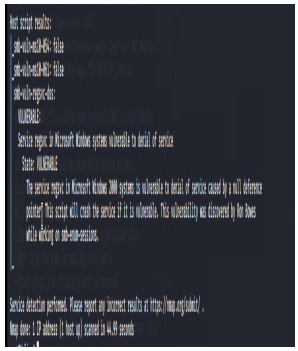
```
root@Kali:~# nmap 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-24 11:57 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00056s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

The following vulnerabilities were identified on each target:

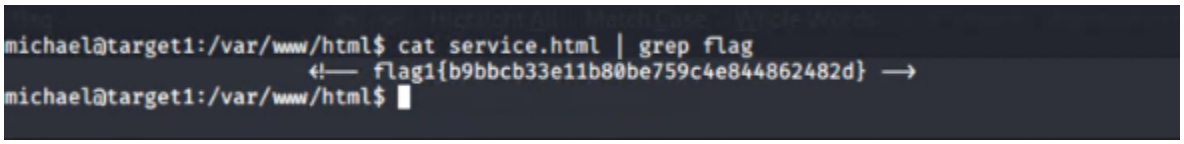
Target 1

List of critical vulnerabilities :

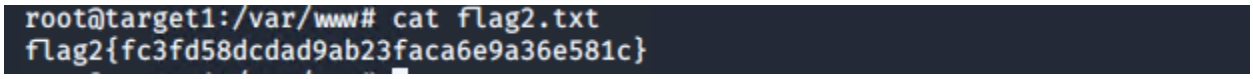





The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

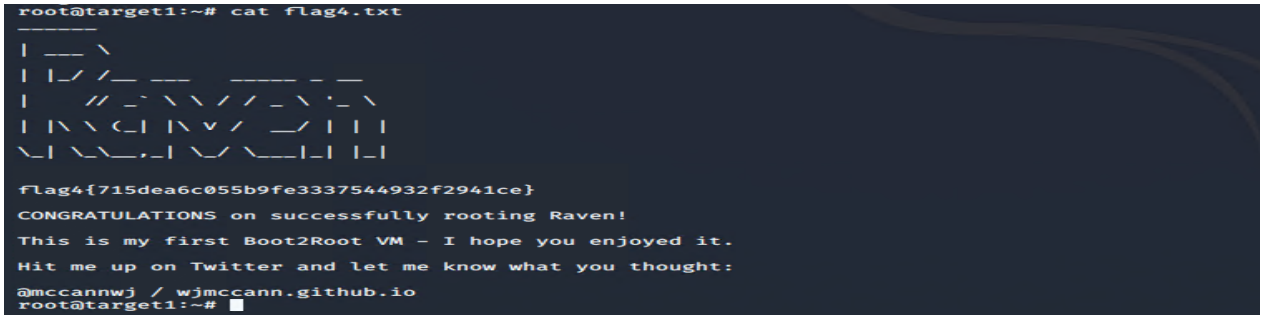
Target 1



We just got into Michael's machine by guessing his password and then we used : cat service.html | grep flag



flag2.txt: TODO: Insert flag2.txt hash value



We escalated to root by SSH-ing to Steven's account by using John to crack his hashed password and then used : cat flag4.txt.
This is the python script we used to escalate to root.