# **Red Team: Summary of Operations**

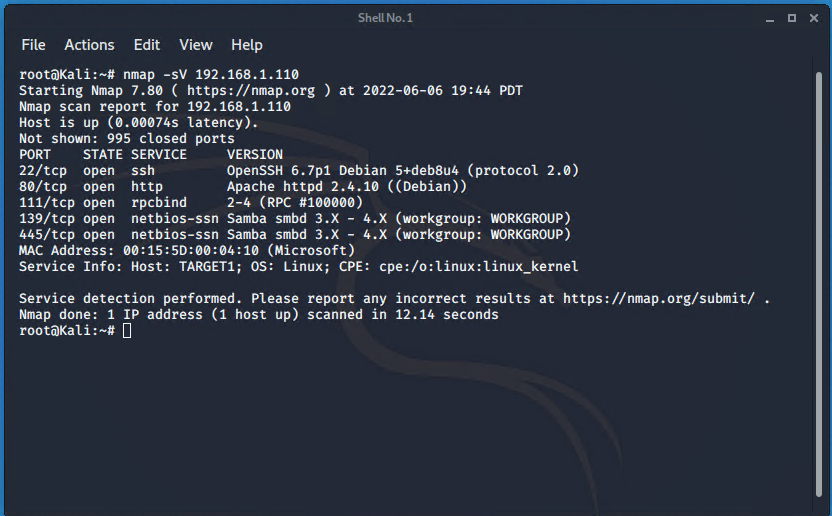
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

$ nmap -sV 192.168.1.110



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

* Target 1
  + Port 22/tcp open ssh
  + Port 80/tcp open http
  + Port 111/tcp open rpcbind
  + Port 139/tcp open netbios-ssn
  + Port 445/tcp open netbios-ssn

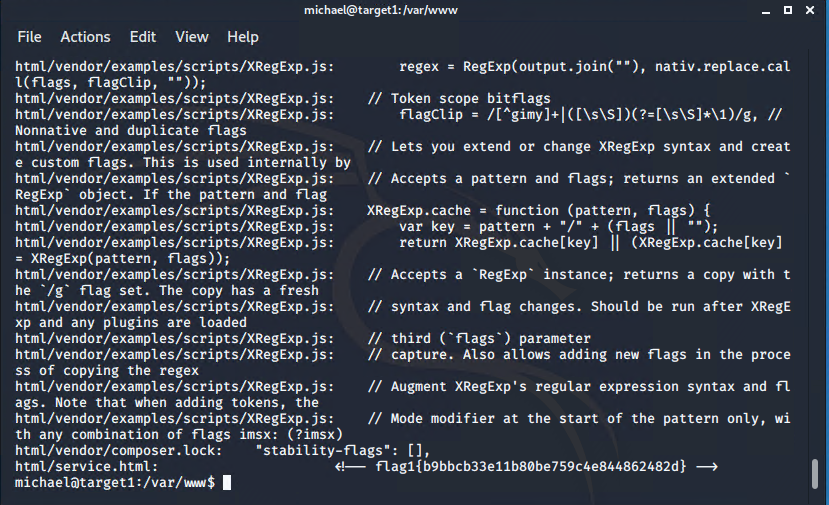
The following vulnerabilities were identified on Target 1:

* + Open SSH CVE-2021-28041
  + Open rpcbind can provide attackers with the ability to launch a remote DoS attack CVE-2017-8779
  + Open NetBIOS server CVE-2017-7494
  + CVE-2019-6579 open Port 80 allows the opportunity to execute system commands with administrative privileges

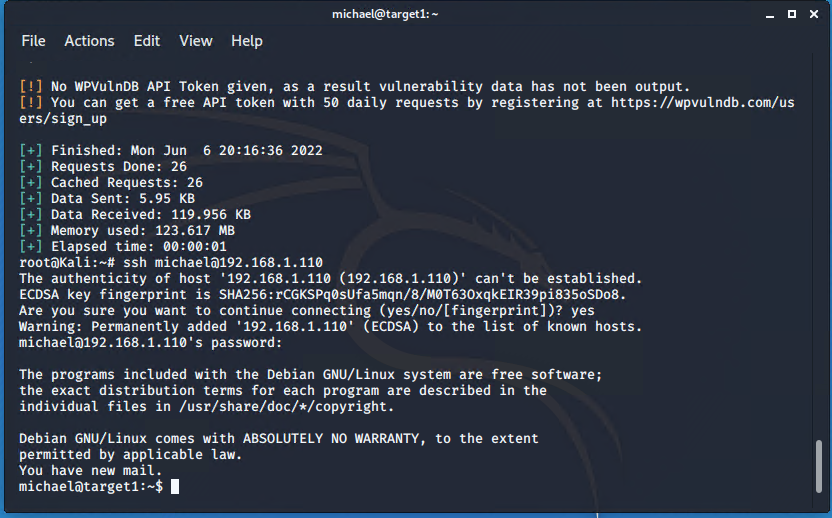
### **Exploitation**

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

* Target 1
  + flag1.txt: *flag1{b9bbcb33e11b80be759c4e844862482d}*
    - **Exploit Used**
      * ssh into Michael’s account michael@192.168.1.110
      * cd /var/www
      * grep -RE flag html



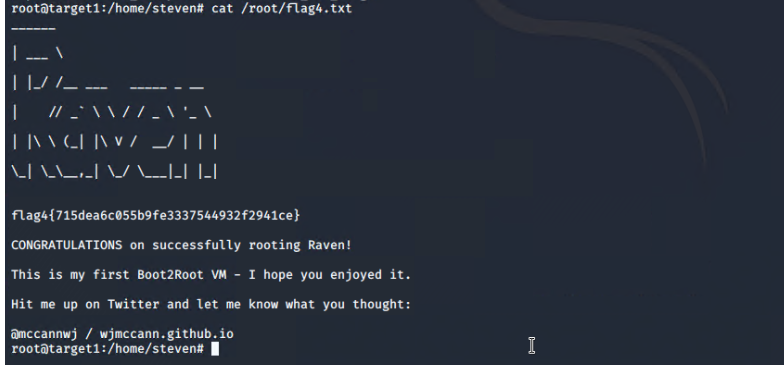
* + flag2.txt: *flag2{fc3fd58dcdad9ab23faca6e9a36e581c}*
    - **Exploit Used**
      * ssh michael@192.168.1.110
      * Password: michael



* + flag3.txt: *flag3{afc01ab56b5059e7dccf9122770cd2}*

**

* + flag4.txt: *flag4{715dea6c055b9fe3337544932f2941ce}*



RESOURCES:

“CVE-2017-7494.” *NVD*, https://nvd.nist.gov/vuln/detail/CVE-2017-7494.

“CVE-2017-8779.” *NVD*, https://nvd.nist.gov/vuln/detail/CVE-2017-8779.

“CVE-2019-6579 Detail.” *NVD*, https://nvd.nist.gov/vuln/detail/cve-2019-6579.

“CVE-2021-28041 Detail.” *NVD*, https://nvd.nist.gov/vuln/detail/CVE-2021-28041.