# **Red Team: Summary of Operations**

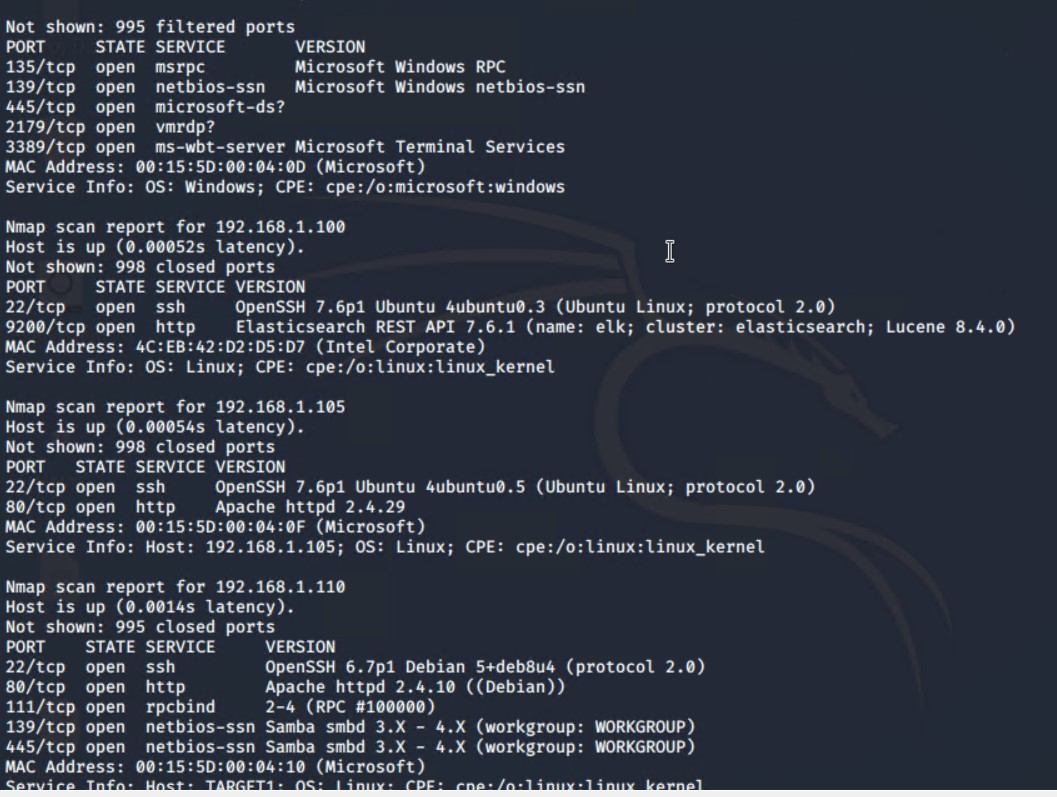
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

$ nmap -sV 192.168.1.1-255



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

* Target 1
  + Port 22 - ssh
  + Port 80 - http
  + Port 111 - rpcbind
  + Port 139 - netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
  + Port 445 - netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

The following vulnerabilities were identified on each target:

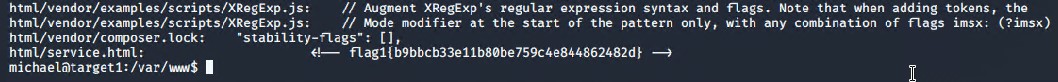
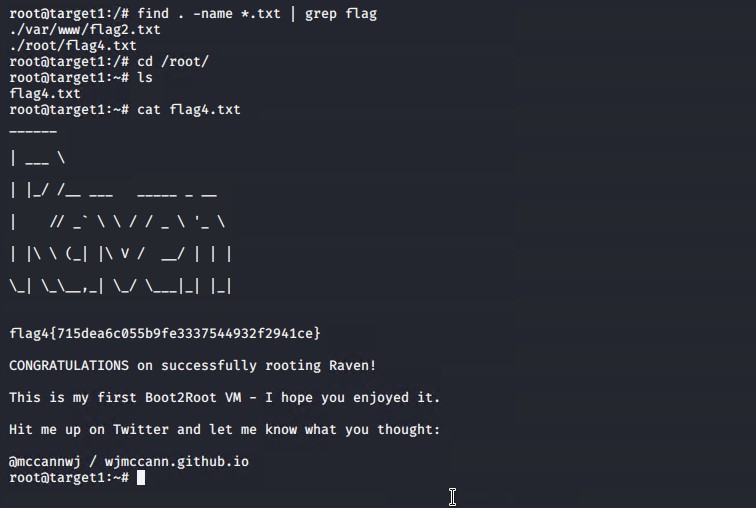
* Target 1
  + Credential Based Attack - Severe

## Remote User Enumeration - CVE-2012-5615 - Severe

* + Privilege Escalation

### **Exploitation**

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

* Target 1
  + flag1.txt: **
    - **Exploit Used**
      * wpscan
      * wpscan –url <http://192.168.1.110/wordpress> -eu
  + flag2.txt: **
    - **Exploit Used**
      * Directory traversal
      * cd /var/www/
  + flag4.txt: 
    - **Exploit Used**
      * Privilege escalation
      * 