# **Red Team: Summary of Operations**

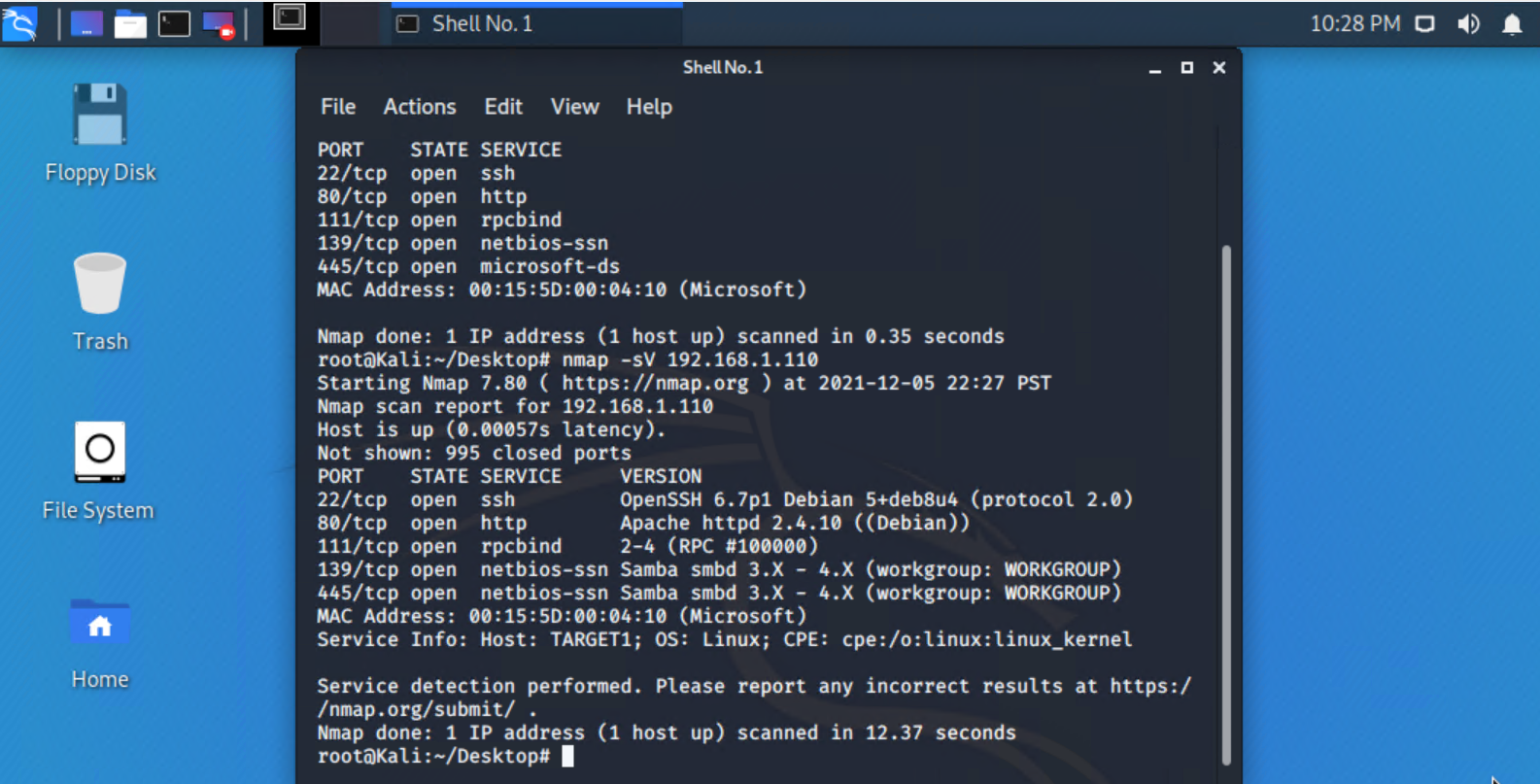
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

### **Exposed Services**

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

$ nmap 192.168.1.110

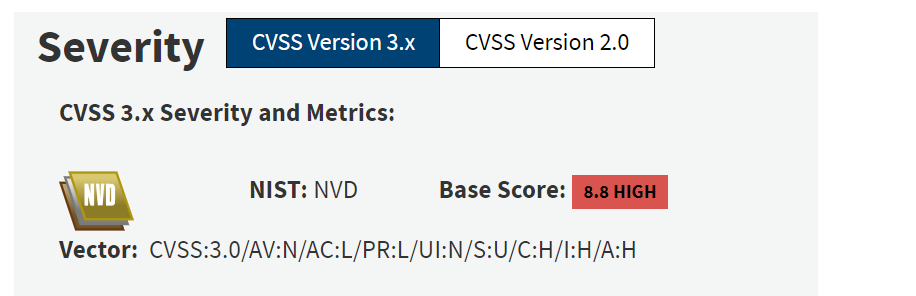


This scan identifies the services below as potential points of entry:

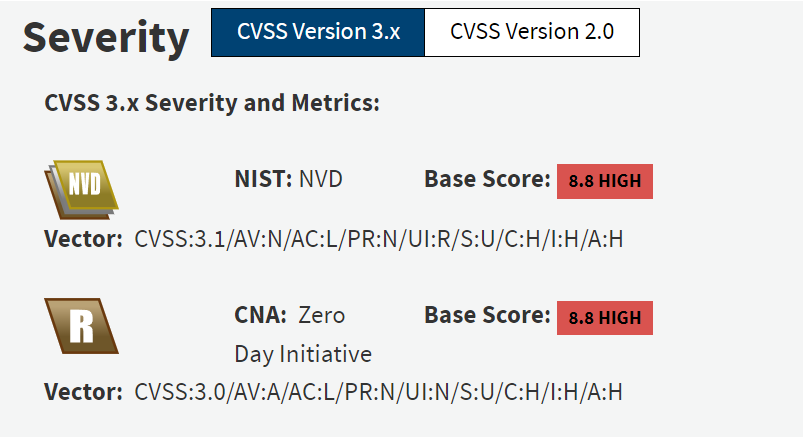
* Target 1
  + 22/tcp open ssh
  + 80/tcp open http
  + 111/tcp open rpcbind
  + 139/tcp open netbios-ssn
  + 445/tcp open microsoft-ds

The following vulnerabilities were identified on each target:

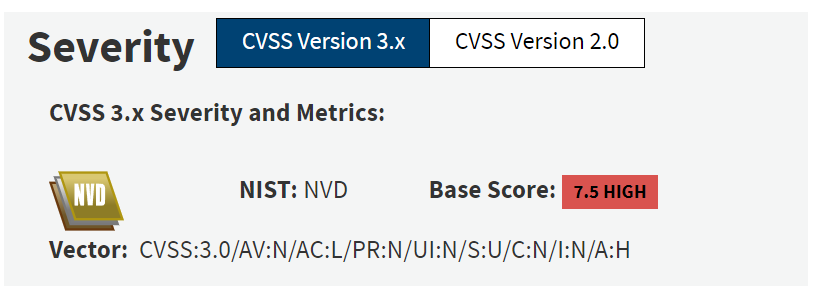
* Target 1
  + Port 22/tcp: SSH service open
    - Severity: 8.8 HIGH
    - CVE-2017-3818: privilege escalation



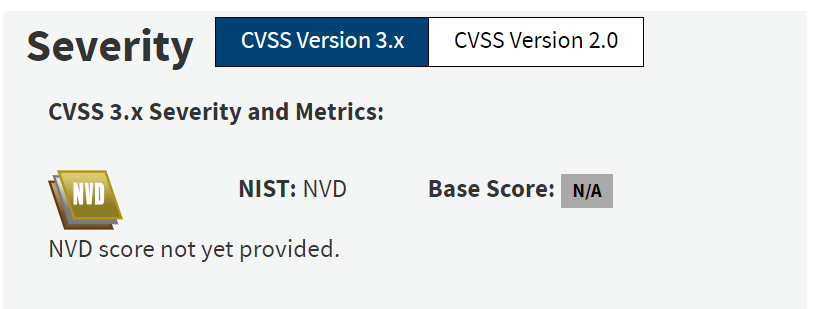
* + Port 80/tcp: HTTP service open
    - Severity: 8.8 HIGH
    - CVE-2019-17147: vulnerability attacker can execute code as user admin



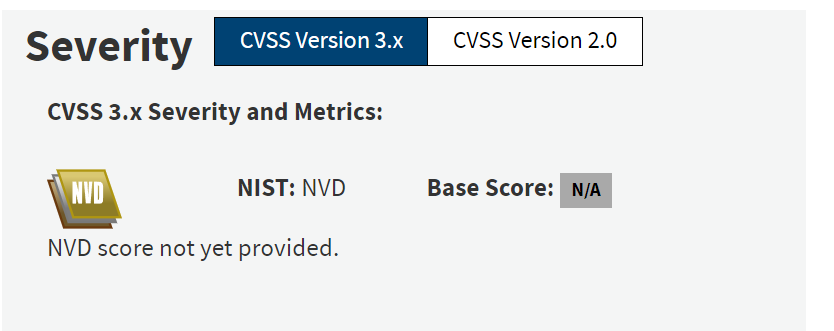
* + Port 111/tcp: rpcbind service open
    - Severity: 7.5 HIGH
    - CVE-2017-8779: DDOS vulnerability during memory allocation for XDR strings



* + Port 139/tcp: netbios-ssn service open
    - Severity: N/A based on NIST
    - CVE-2007-3923: DDOS vulnerability when flooded with TCP SYN packets to either port 139/tcp or port 445/tcp



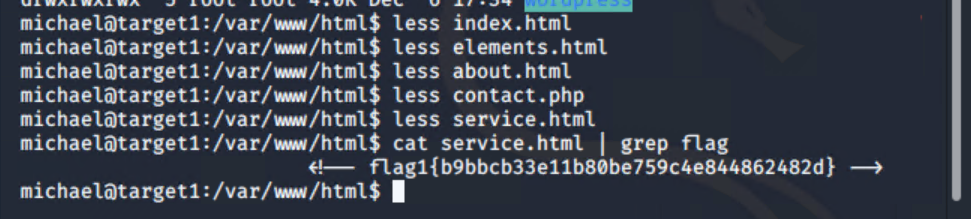
* + Port 445/tcp: microsoft-ds service open
    - Severity: N/A According to NIST
    - CVE-2007-0597: FID=XD query reveals full file path in error message



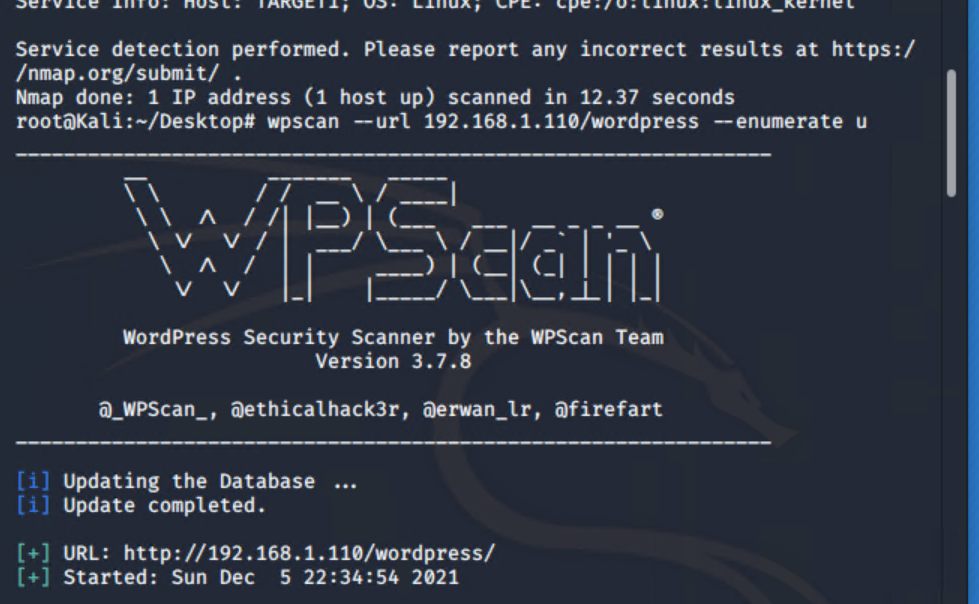
### **Exploitation**

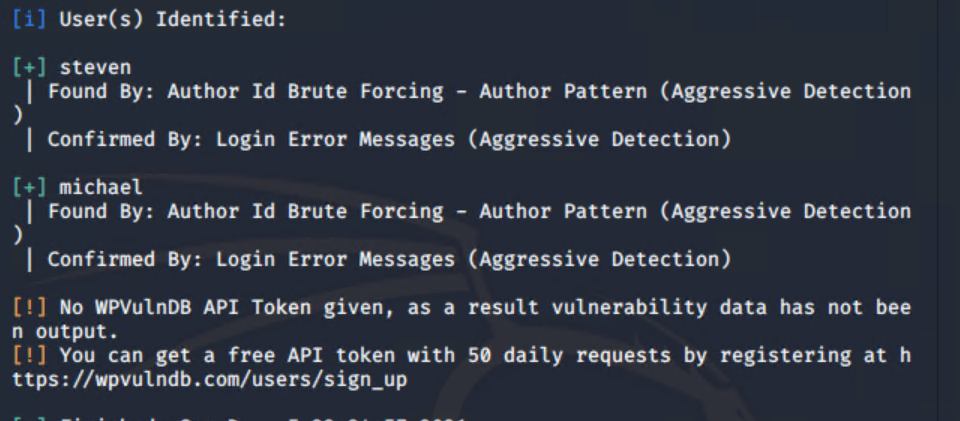
The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

* Target 1
  + flag1.txt: *flag1{b9bbcb33e11b80be759c4e844862482d}*

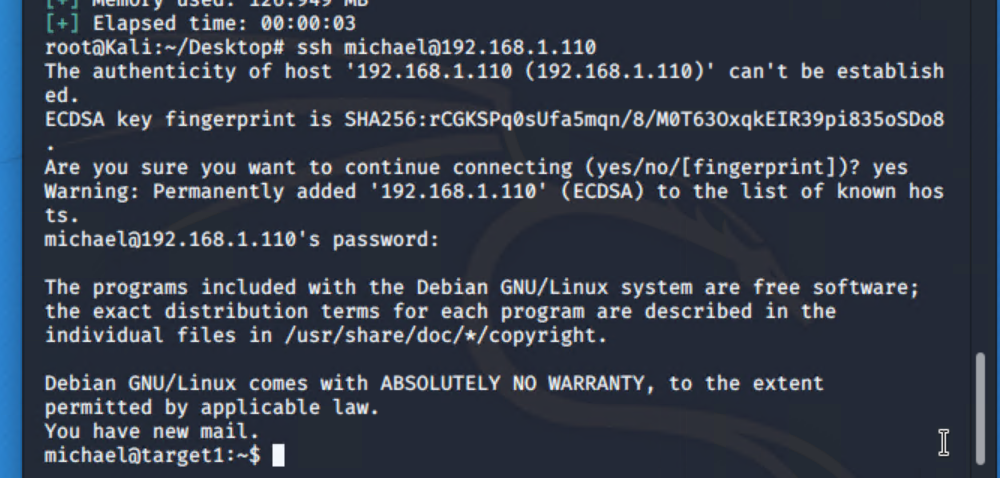
**

* + - **Exploit Used: wpscan/ssh**
      * Wpscan --url 192.168.1.110/wordpress --enumerate u

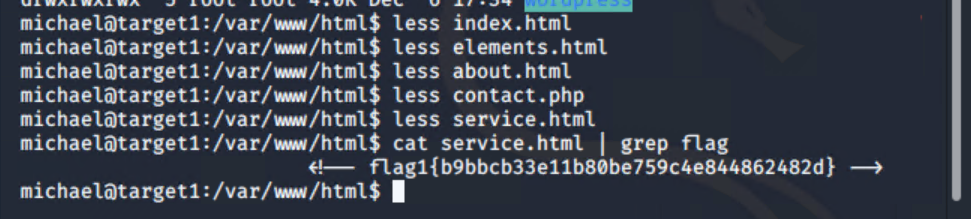




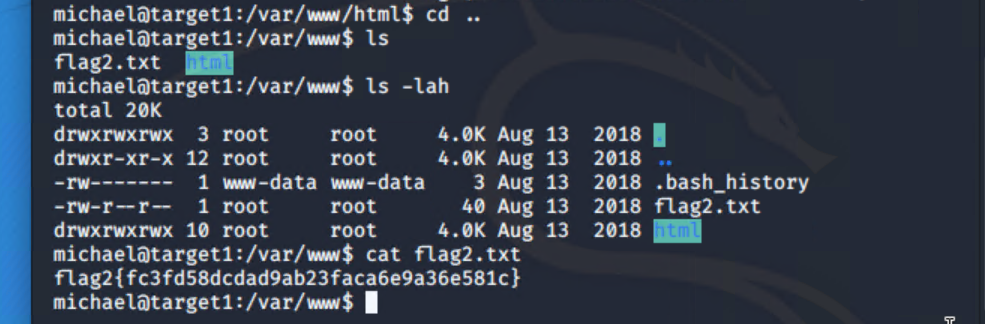
* + - * Ssh michael@192.168.1.110 with password: michael



* + - * Cd /var/www
      * Ls -lah
      * cd html
      * Less all html/php files to read through contents
      * Once flag1 is seen then cat service.html | grep flag1



* + flag2.txt: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
    - **Exploit Used: wpscan/ssh**
      * *ssh michael@192.168.1.110*
      * *cd /var/www*
      * *Ls -lah*

**

* + - * *cat flag2.txt*