# **Red Team: Summary of Operations**

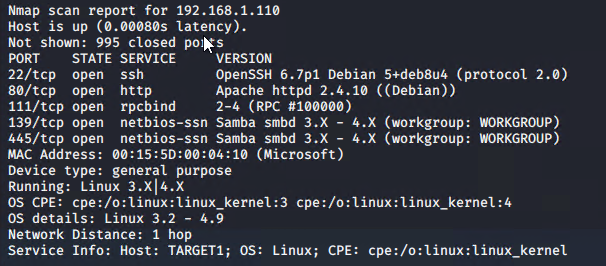
## **Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

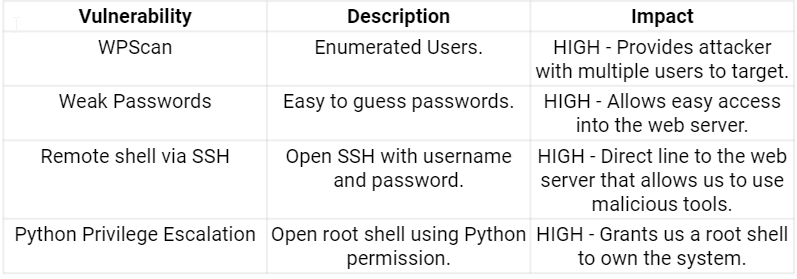
### **Exposed Services***.*

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

nmap -sV -O 192.168.1.110/24 

scan output

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

* Target 1
  + Ssh 22
  + Http 80
  + In addition to the obvious open ports, and after some digging, other vulnerabilities were discovered. The following vulnerabilities were identified on each target:

| 1. |
| --- |
| 2. |
| 3. |
| 4. |

### 

### 

### 

### 

### 

### 

### 

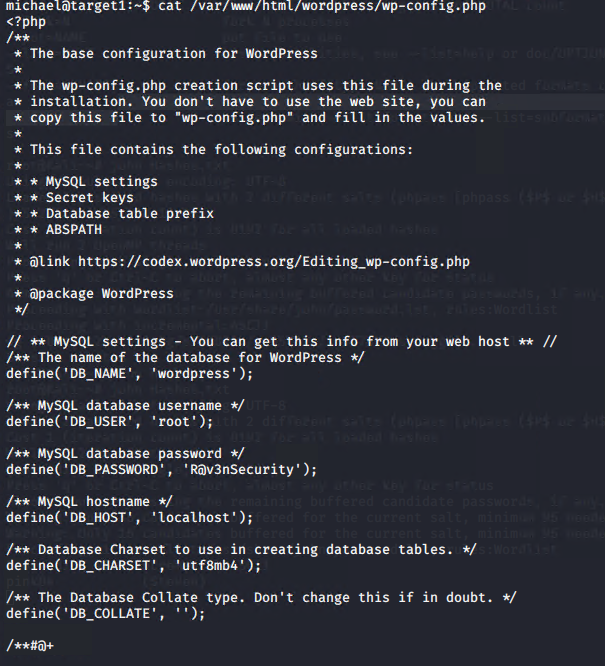
### 

### 

### 

### 

### 



### 

### 

### 

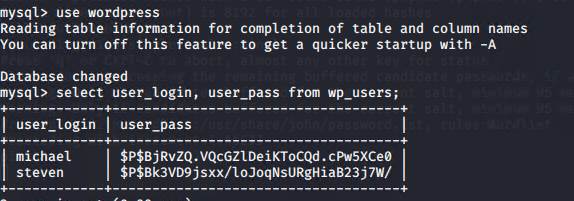
### 

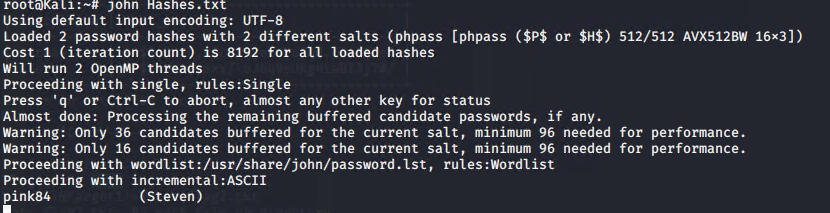
### 

### 

### 

### 

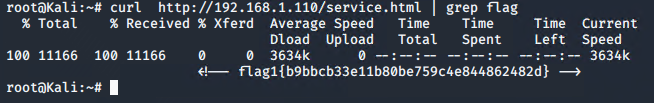


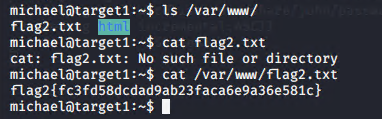


### **Exploitation**

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

* Target 1
  + flag1.txt: *TODO: Insert flag1.txt hash value*
    - **Exploit Used**
      * A simple curl request to test the ports of the network revealed the first flag



* + flag2.txt: *TODO: Insert flag2.txt hash value*
    - **Exploit Used**
      * *After gaining access to michials account i found flag2 in the /var/www directory *
  + flag4.txt: *TODO: Insert flag2.txt hash value*
    - **Exploit Used**
      * *After gaining root access into Target1 i found Flag4 in the /root directory*

