# Red Team: Summary of Operations

## 

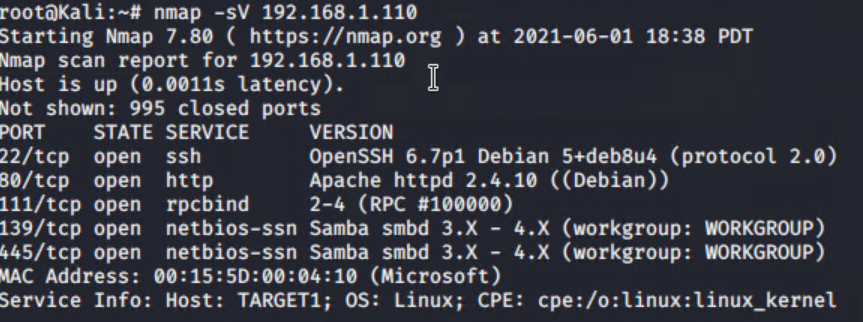
## Table of Contents

* 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:

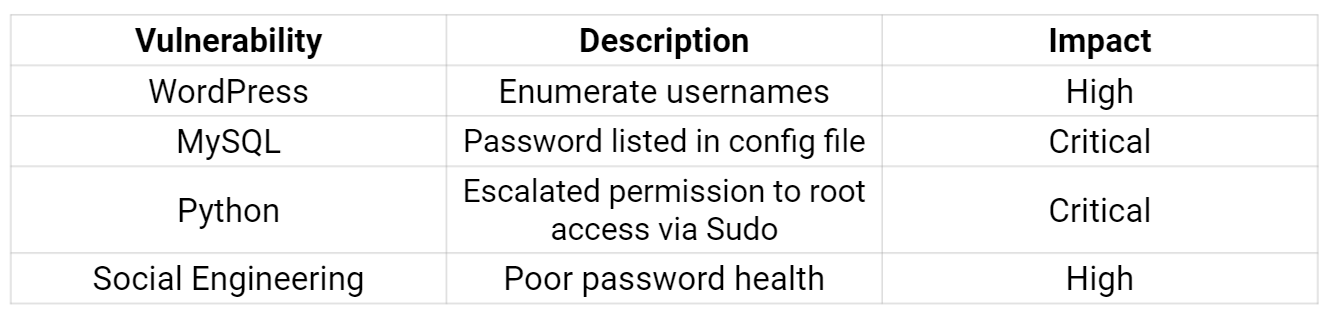
**Target 1**

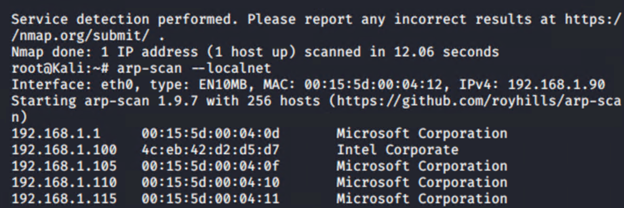
1. List of exposed services: Port 22 ssh
2. List of exposed services: Port 80 http
3. List of exposed services: Port 111 rpcbind

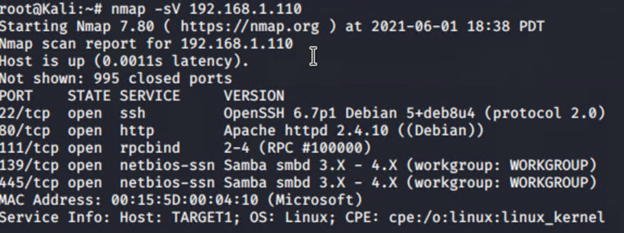
### Critical Vulnerabilities

The following vulnerabilities were identified on each target:

**Target 1**









Exploitation

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

**Target 1**

Flag 1:

/var/www/html$ grep -ir flag1



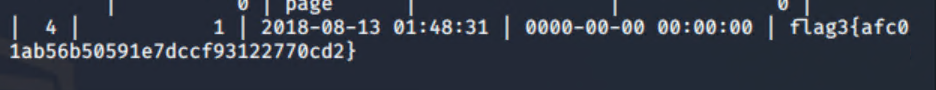
Flag 2:

cat ./var/www/flag2.txt



Flag 3:

Select \* from wp\_posts;



Flag 4:

