**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 192.168.1.0/24

A screenshot of a computer

Description automatically generated with low confidence

Text

Description automatically generated

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

* Target 1
  + List of open ports
    - 22/tcp
    - 80/tcp
    - 111/tcp
    - 139/tcp
    - 445/tcp
  + Exposed Services
    - ssh OpenSSH 6.7p1
    - http Apache httpd 2.4.10
    - rpcbind
    - netbios-ssn Samba smbd 3.X – 4.X

The following vulnerabilities were identified on each target:

* Target 1
  + WordPress user enumeration

Text

Description automatically generated

Text

Description automatically generated

* + Access to SQL database

Text

Description automatically generated

Text

Description automatically generated

* + Weak password/brute force

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

Text

Description automatically generated

* + Privilege escalation

Text

Description automatically generated

Text

Description automatically generated

**Exploitation**

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

* Target 1
  + flag1.txt

Text

Description automatically generated

* + - **Exploit Used**
      * Used Michaels weak password to ssh into his account and then was able to locate flag1 in /var/www/html
  + flag2.txt

Text

Description automatically generated

* + - **Exploit Used**
      * As stated above, after ssh-ing into Michaels account we actually came across flag2 before flag1 because flag2 was in the directory above flag1 /var/www