# **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 -sP 192.168.1.1-255**

**Text

Description automatically generated**

**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 rcpbind
  + Port 139/TCP Open netbios-ssn
  + Port 445/TCP Open netbios-ssn

# **The following vulnerabilities were identified on each target:**

# **Target 1**

# **Weak User Password (Brute Force)**

# **Misconfiguration of User Privileges/Privilege Escalation**

# **User Enumeration (WordPress site)**

**A screenshot of a computer

Description automatically generated with low confidence**

### **Exploitation**

**Text

Description automatically generated**

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

# **Target 1**

# **flag1.txt: {b9bbcb33e11b80be759c4e844862482d}**

# **Exploit Used**

# 

# **flag2.txt: {fc3fd58dcdad9ab23faca6e9a3e581c}**

# **Exploit Used**

# 

Followed by: cat flag2.txt

# **flag3.txt: {**afc01ab56b50591e7dccf93122770cd2**}**

# **Exploit Used**

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated with low confidence

A picture containing graphical user interface

Description automatically generated

# **flag4.txt: {**715dea6c055b9fe3337544932f2941ce**}**

# **Exploit Used**

Graphical user interface

Description automatically generated

A screen shot of a computer

Description automatically generated with medium confidence

A computer screen capture

Description automatically generated with medium confidence



**Text

Description automatically generated**