Red Team: Summary of Operations Chad Skeen

#### Table of Contents

- Exposed Services

- Exploitation

- Critical Vulnerabilities

-----------------------------------------------------------------------------------------------------------

#### Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

```

$ nmap -A 192.168.1.0/24

Starting Nmap 7.80 (<https://nmap.org>)

Nmap scan report for 192.168.1.1

Host is up (0.00058s latency)

Not shown: 995 filtered ports

PORT |STATE |SERVICE |VERSION

----------------------------------------------------------

135/tcp |OPEN |msrpc |Microsoft Windows RPC

139/tcp |OPEN |netbios-ssn|Microsoft Windows Netbios-ssn

445/tcp |OPEN |Microsoft-ds?

2179/tcp|OPEN |vmrdp?

3389/tcp|OPEN |ms-wbt-server Microsoft Terminal Services

----------------------------------------------------------

```

#### Exploitation

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

- Target 1

- `flag1.txt`: flag1{b9bbcb33e1b80be759c4e844862482d}

- \*\*Exploit Used\*\*

- We were able to view hardcoded flag information

- \*right click\* --🡪 view source \*ctl+F\* “flag1”

- `flag2.txt`: flag2{fc3fd58dcad9ab23faca6e9a36e581c}

- \*\*Exploit Used\*\*

- We exploited the poor password practices used by Michael.

- find . -iname \*flag\* 2>&1 |grep -v “Permission denied”

- `flag3.txt`: flag3{afc01ab56b50591e7dccf93122770cd2}

- \*\*Exploit Used\*\*

- We created a sql dump by exploiting the password located in the vulnerable ‘wp-config’ file

- mysql -u root -p

- `flag4.txt`: flag4{fc3fd58dcad9ab23faca6e9a36e581c}

- \*\*Exploit Used\*\*

- We created a sql dump by exploiting the password located in the vulnerable ‘wp-config’ file

- mysql -u root -p

#### Critical Vulnerabilities

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

- Target 1

- 22 SSH

- 80 HTTP

The following vulnerabilities were identified on each target:

- Target 1

- Having the port 22 and 80 seriously opens up the server to entry and critical data breach and loss.