Faculty of Business, IT, and Management

HACK2200 Hacking and Exploits

Lab 3: Scanning and Enumeration Answer File

**Syed Adil Ahmed Altaf Hussain**

**100841799**

**Part1- Network Scanning**

**Step 1: Start the lab virtual machines**

**Question 1 –** what is the IP address of your KaliVM, MS3WS2008, and MS3UBUNTU?

KaliVM IP Address: 192.168.156.130

MS3WS2008 IP Address: 192.168.156.129

MS3UBUNTU IP Address: 192.168.156.128

**Step 2: Scanning MS3WS2008 using nmap**

Insert Screenshot#1 Here (**10 marks**)

A computer screen capture

Description automatically generated with medium confidence

**Question 2 -** What is the OS reported by nmap of the target machine? (**10 marks**)

OS details:

**Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008**

**Question 3 -** List 5 of the running services with their version and the ports they are running on. (**10 marks**)

1. **21/tcp open ftp Microsoft ftpd**
2. **22/tcp open ssh OpenSSH 7.1 (protocol 2.0)**
3. **80/tcp open http Microsoft IIS httpd 7.5**
4. **4848/tcp open ssl/http Oracle Glassfish Application Server**
5. **8080/tcp open http Sun GlassFish Open-Source Edition 4.0**

**Step 3: Scanning MS3UBUNTU** **using nmap**

Insert Screenshot#2 Here (**10 marks**)

Text

Description automatically generated

**Question 4 -** What is the OS reported by nmap of the target machine? (**10 marks**)

OS details: **Linux 3.2 - 4.9**

**Question 5 -** List 5 of the running services with their version and the ports they are running on. (**10 marks**)

1. **21/tcp open ftp ProFTPD 1.3.5**
2. **22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)**
3. **80/tcp open http Apache httpd 2.4.7**
4. **445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)**
5. **631/tcp open ipp CUPS 1.7**

**End of Part 1 – Scanning Networks**

**Part 2 - Enumeration**

**Step 1: Enumerating users with snmp\_enumusers**

Insert Screenshot#3 Here (**10 marks**)

Text

Description automatically generated

**Question 6 -** List 3 user accounts that were found by the snmp\_enumusers script (**10 marks**)

1. **Administrator**
2. **anakin\_skywalker**
3. **ben\_kenobi**

**Step 2**: Repeat Step 1 while targeting MS3UBUNTU machine

Insert Screenshot#4 Here (**10 marks**)

A computer screen capture

Description automatically generated with medium confidence

**Question 7 -** List 3 user accounts that were found by the enum4linux script (**10 marks**)

1. **krbtgt**
2. **administrator**
3. **domain admins**

**End of Part 2 - Enumeration**