Assignment 2: Network Scanning [40 points]

**Part 1: Scan Analysis: scan1.pcapng**

Q1: What are the two protocols being used by nmap to scan? [2 points]

TCP and ARP.

Q2: What is the range of scanned addresses? [2 points]

192.168.56.1 - 192.168.56.254

Q3: Based on Q1 and Q2, what nmap command did the attacker use? (provide the complete command, not just the scan type) [3 points]

Nmap -sn 192.168.56.0/24

Q4: What are the results of the scan? (Your answer doesn’t need to specifically look like nmap output, but it should contain the same information) [4 points]

|  |
| --- |
| 192.168.56.1 is at 0a:00:27:00:00:00 |
| 192.168.56.205 is at 08:00:27:69:83:b2 |
| 192.168.56.112 is at 08:00:27:69:83:b2 |
| 192.168.56.100 is at 08:00:27:a6:ba:7f |
| 192.168.56.111 is at 08:00:27:7a:ee:d2 |
| 192.168.56.111 is at 08:00:27:7a:ee:d2 |

**Part 2: Scan Analysis: scan2.pcapng**

Q1: What is the scan type used in this packet capture? [2 points]

Full Connect Scan

Q1: Which ports are open on the target machine? [4 points]

80, 22, 3306, 21

Q2: What services are most likely to be running on those ports? Can you be sure those are the services which are actually running? Why? [4 points]

Port 80 – HTTP Server

Port 22 – SFTP

Port 3306 – MySQL

Port 21 – FTP

I cannot be sure that these are the services running on the ports as these are just the common services for those ports.

Part 3: Sandbox Scanning

Warning: one of the services on the target server can be very slow to start up. If you have to restart your server machine give it 5-10 minutes to start all the services.

Q1: perform a port scan of the server.cs491 machine. Provide a list of each open port, the service running on that port, and the software / software version listening on the port. For each service, describe the purpose of that service in a few words. Note that there is one service where you will not be able to find the software version. [16 points]

Example: Port: 80. Service: http. Software: apache server 2.4.46. Purpose: web server.

Port: Service: Software: Purpose:

Port: 21 Service: ftp Software: vsftpd Purpose: transfer files

Port: 53 Service: domain Software: dnsmasq 2.80 Purpose: DNS caching

Port: 145 Service: http Software: nginx 1.17.10 Purpose: web server

Port: 2202 Service: ssh Software: OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0) Purpose: Communicate with another computer

Port: 3306 Service: mysql? Software: Purpose: relational database

Port: 5000 Service: http Software: Werkzeug httpd 1.0.1 (Python 3.8.5) Purpose: web server

Port: 5553 Service: domain Software: ISC BIND 9.16.1 (Ubuntu Linux) Purpose: DNS server

Port: 5553 Service: mongodb Software: MongoDB 4.4.3 Purpose: non-relational database

Q2: One of the ports is behind a firewall. Which port is this? [3 points]

Port: 1234