

Task1: list of discovered devices, services, and open ports.

1 IP address (1 host up) scanned in 20.38 seconds

192.168.172.129(online)

Port	Protocol	Service	Version	Description
21	TCP	FTP	FTP 2.3.4	File Transfer Protocol used for transferring files between systems.
22	TCP	SSH	OpenSSH 4.7p1	Secure Shell for secure remote login and command execution.
23	TCP	Telnet	telnet	Insecure protocol for remote command-line interface access.
25	TCP	SMTP	SMTP	Simple Mail Transfer Protocol for sending emails.

53	TCP	DNS	ISC BIND 9.4.2	Domain Name System service for resolving domain names to IP addresses.
80	TCP	HTTP	Apache httpd 2.2.8	Hypertext Transfer Protocol used for web traffic.
111	TCP	RPCbind	N/A	Maps RPC services to specific ports.
139	TCP	NetBIOS-SSN	Samba smbd	Used for sharing files and printers on Windows networks.
445	TCP	NetBIOS-SSN	Samba smbd 3.0.20-Debian	Another port for Windows file and printer sharing.

3306	TCP	MySQL	MySQL 5.0.51a-3ubuntu5	Database management system.
5432	TCP	PostgreSQL	PostgreSQL 8.3.0 - 8.3.7	Relational database management system.
5900	TCP	VNC	VNC protocol 3.3	Virtual Network Computing for remote desktop access.
6667	TCP	IRC	UnrealIRCd	Internet Relay Chat service used for real-time text communication.
8009	TCP	AJP13	Apache JServ Protocol 1.3	AJP is a binary protocol used by Apache Tomcat for communication.
8180	TCP	HTTP	Apache Tomcat/Coyote JSP 1.1	Web server for Java applications.

Key Services:

1. **FTP (Port 21):** FTP is a standard network protocol used to transfer files. The scan shows anonymous FTP login is enabled, which could pose a security risk.
2. **SSH (Port 22):** Secure Shell is a cryptographic network protocol for secure data communication, shell access, and command execution.
3. **Telnet (Port 23):** Telnet allows command-line interface access but is insecure due to the lack of encryption.
4. **SMTP (Port 25):** Postfix handles mail sending. This service listens on port 25, used for email routing between servers.
5. **DNS (Port 53):** BIND DNS software is running on port 53, providing name resolution services.
6. **HTTP (Port 80 and 8180):** Apache web servers run on these ports, hosting web content.
7. **RPC (Port 111):** Provides mapping between remote procedure call services and their respective ports.
8. **MySQL (Port 3306) and PostgreSQL (Port 5432):** Both are database services with MySQL for structured data management and PostgreSQL as another robust relational database.
9. **VNC (Port 5900):** VNC allows graphical desktop sharing, enabling remote control over systems.
10. **IRC (Port 6667):** UnrealIRCd is an Internet Relay Chat server allowing text-based communication in real time.

Used Tools: Angry Scanner - NMAP

Delivered by: **Eslam Ahmed**