Network Security

James Foley

1. Common Ports and Descriptions

- **20 – FTP (Data):** File Transfer Protocol – data transfer in active mode
- **21 – FTP (Control):** File Transfer Protocol – control commands
- **22 – SSH (Secure Shell):** Encrypted remote login and command execution
- **23 – Telnet:** Insecure remote access protocol
- **25 – SMTP (Simple Mail Transfer Protocol):** Sends emails
- **53 – DNS (Domain Name System):** Resolves domain names to IP addresses
- **67 – DHCP (Server):** Assigns IP addresses to clients
- **68 – DHCP (Client):** Receives IP configuration from DHCP server
- **69 – TFTP (Trivial File Transfer Protocol):** Basic file transfer, often for boot files
- **80 – HTTP (Hypertext Transfer Protocol):** Unsecured web traffic
- **110 – POP3 (Post Office Protocol v3):** Downloads emails from server
- **123 – NTP (Network Time Protocol):** Time synchronization between systems
- **143 – IMAP (Internet Message Access Protocol):** Access and manage emails on server
- **161 – SNMP (Simple Network Management Protocol):** Device monitoring
- **162 – SNMP Trap:** Alert messages from SNMP-enabled devices
- **389 – LDAP (Lightweight Directory Access Protocol):** Directory services (e.g. Active Directory)
- **443 – HTTPS (HTTP Secure):** Encrypted web traffic via SSL/TLS
- **445 – SMB (Server Message Block):** Windows file and printer sharing
- **514 – Syslog:** System logging over UDP
- **3389 – RDP (Remote Desktop Protocol):** GUI remote access for Windows

2. Common Protocols and Descriptions

- **HTTP / HTTPS:** Web communication; HTTPS uses SSL/TLS encryption
- **FTP / SFTP:** File transfers; SFTP is secure over SSH
- **SSH (Secure Shell):** Encrypted command-line access to remote systems
- **Telnet:** Unencrypted remote login (deprecated)
- **SMTP / POP3 / IMAP:** Email sending (SMTP) and retrieval (POP3, IMAP)
- **DNS:** Converts domain names into IP addresses
- **DHCP:** Dynamically assigns IP addresses on a network
- **SNMP:** Monitors network devices (status, bandwidth, etc.)
- **LDAP:** Accesses and manages user directory services
- **RDP:** Remote graphical login for Windows systems
- **IPSec:** Encrypts IP traffic for VPNs (site-to-site or remote access)
- **OpenVPN:** SSL/TLS-based secure VPN solution

3. OSI Model – 7 Layers in Detail

- **7 – Application:** User-level access to network services (HTTP, FTP, DNS)
- **6 – Presentation:** Translates, encrypts, compresses data (SSL/TLS)
- **5 – Session:** Establishes and maintains connections (NetBIOS, RPC)
- **4 – Transport:** Ensures reliable delivery and flow control (TCP, UDP)
- **3 – Network:** IP addressing and routing (IP, ICMP)
- **2 – Data Link:** MAC addressing, error detection (Ethernet, PPP)
- **1 – Physical:** Transmits raw bits (Cables, NICs, Hubs)

4. Network Attacks (with Explanations & Mitigation)

- **DDoS (Distributed Denial of Service):**
  - Overloads services with fake traffic
  - *Mitigation:* Rate limiting, firewalls, CDNs, cloud DDoS protection
- **MITM (Man-in-the-Middle):**
  - Intercepts data between sender and receiver
  - *Mitigation:* HTTPS, VPNs, certificate pinning
- **SQL Injection:**
  - Injects malicious SQL into input fields
  - *Mitigation:* Input validation, parameterized queries, ORM
- **XSS (Cross-Site Scripting):**
  - Injects scripts into a webpage to run in the browser
  - *Mitigation:* Output encoding, CSP headers, input sanitization
- **Phishing:**
  - Fake emails/websites to steal login credentials
  - *Mitigation:* Awareness training, spam filters, MFA
- **Brute Force:**
  - Repeated login attempts to guess credentials
  - *Mitigation:* Lockouts, CAPTCHA, MFA
- **ARP Spoofing:**
  - Links attacker's MAC to legitimate IP via fake ARP replies
  - *Mitigation:* Static ARP tables, port security, DHCP snooping
- **DNS Spoofing:**
  - Sends fake DNS responses to redirect traffic
  - *Mitigation:* DNSSEC, secure DNS configs

5. Security Concepts & Key Terms (with Examples)

- **CIA Triad:**
  - *Confidentiality, Integrity, Availability*
  - *Example:* Encryption = confidentiality, Hashing = integrity, Redundancy = availability
- **AAA (Authentication, Authorization, Accounting):**
  - *Example:* RADIUS server controls Wi-Fi access and logs usage
- **Least Privilege:**
  - Users get only the access they need
  - *Example:* Admin tools blocked on standard user accounts
- **Zero Trust:**
  - Never trust, always verify (inside or outside network)
  - *Example:* Re-authentication for every request
- **Defense in Depth:**
  - Multiple security layers
  - *Example:* Firewall + Antivirus + IDS + Encryption
- **MFA (Multi-Factor Authentication):**
  - Two or more auth methods
  - *Example:* Password + SMS code
- **Hashing:**
  - One-way data integrity check
  - *Example:* SHA-256 hash of file = no tampering
- **Encryption:**
  - Converts data into unreadable format without a key
  - *Example:* HTTPS secures web sessions

6. Device Roles in Networking

- **Router:** Connects and routes traffic between networks (Layer 3)
- **Switch:** Connects devices in a LAN using MAC addresses (Layer 2)
- **Firewall:** Controls traffic using rules (can be software or hardware)
- **Access Point:** Provides Wi-Fi to wireless clients
- **Proxy Server:** Middle-man that handles traffic on behalf of clients
- **IDS / IPS:** Detects (IDS) or blocks (IPS) malicious activity
- **Modem:** Modulates signals for internet access via ISP

7. Command Sheet (Windows, Linux, Networking, Pen Testing)

- ipconfig – Show IP config (Windows)
- ifconfig – Show IP config (Linux/macOS)
- ping – Test connectivity
- tracert / traceroute – Trace route to host
- netstat -an – Show open network connections
- nslookup / dig – DNS lookup
- nmap -sS – TCP SYN scan (stealth scan)
- nmap -A – Aggressive scan (OS, version, script, traceroute)
- netsh advfirewall – Manage Windows Firewall settings
- Get-EventLog – View event logs (PowerShell)
- grep / findstr – Search text (Linux/Windows)
- chmod, chown – Change permissions/ownership (Linux)
- systemctl – Manage services (Linux systemd)
- tcpdump -i eth0 – CLI packet capture tool
- **Wireshark** – GUI packet analysis tool
- airmon-ng, airodump-ng – Wireless network monitoring tools
- aircrack-ng – Crack captured WPA/WEP handshakes
- msfconsole – Metasploit CLI
- searchsploit – Search local exploit database
- john – Password cracker (John the Ripper)
- hydra – Brute force login attacks