NETWORK AND SECURITY

Unit IV — Network Security Threats and Attacks

Topics Covered in this Unit

Network Security Fundamentals: CIA Triad, Threat Taxonomies, Cyber Kill Chain & Attack Surface
Reconnaissance & Discovery: Footprinting, OSINT, Port Scanning (SYN/Connect/UDP) & Enumeration
Packet & MITM Attacks: Packet Sniffing, ARP Cache Poisoning, MAC Flooding & Session Hijacking
Denial of Service (DoS & DDoS): Botnet C2 Architectures, Flooding (SYN/UDP/ICMP) & Amplification Attacks
Spoofing & Protocol Attacks: IP Spoofing, DNS Cache Poisoning, Email Spoofing & BGP Route Hijacking
Wireless & Malware Threats: Rogue APs, Evil Twin Attacks, Autonomous Worms & Ransomware Spread
Network Defense Mechanisms: Firewalls (Stateless, Stateful, NGFW), IDS/IPS (NIDS/HIDS), DMZ & Zero Trust
High-Yield University Exam Question Bank with Model Answers & Unit Summary

Compiled in a structured, easy-to-understand, textbook style format
Specially curated for B.Tech / B.E. / BCA / MCA / B.Sc Computer Science & IT Students

COURSE SYLLABUS & MAPPING

[UNIT IV SYLLABUS — PRESCRIBED UNIVERSITY CURRICULUM]

This section contains the official syllabus for Unit IV. Verify with your university curriculum mapping.

Unit IV Syllabus Breakdown:

Network Security Fundamentals: CIA triad, threat types, attack lifecycle, attack surface. Reconnaissance and Discovery Attacks: Foot printing, OSINT, scanning, enumeration, vulnerability identification; Packet and MITM Attacks: Sniffing, ARP spoofing, MAC flooding, session hijacking, and MITM; Denial of Service and Botnet Attacks: DoS, DDoS, botnets, flooding, amplification attacks; Spoofing and Protocol Attacks: IP spoofing, DNS spoofing, email spoofing, and routing threats overview. Wireless and Malware-based Threats: Rogue AP, evil twin attack overview, worm propagation, ransomware spread. Network Defense Mechanisms: Firewall, IDS/IPS, segmentation, defense-in-depth.

• Course Code: _____ • Semester / Year: _____

TABLE OF CONTENTS

4.1 Network Security Fundamentals

Definition: Network Security

Network Security encompasses the policies, processes, physical safeguards, and software technologies designed to protect the integrity, confidentiality, availability, and usability of computer networks, communication channels, and accessible digital assets against unauthorized access, misuse, modification, or destruction.

The CIA Triad & Extended Security Attributes

- **1. Confidentiality:** Guarantees that sensitive data, credentials, and network communications are inaccessible and concealed from unauthorized users, entities, or processes (enforced via AES/RSA encryption, access controls, and TLS tunnels).
- **2. Integrity:** Ensures that information and network transmissions remain completely unaltered, authentic, and accurate from sender to receiver, protecting against undetected tampering, injection, or deletion (enforced via SHA-256 cryptographic hashes and HMACs).
- **3. Availability:** Ensures that authorized users have uninterrupted, timely access to network resources, services, and communication links whenever needed (defended via redundant server clustering, DDoS mitigation, and failover topologies).
- **4. Non-Repudiation:** Prevents a communicating party from subsequently denying having originated or received a message (enforced via Digital Signatures and audit logs).
- **5. Authenticity:** Confirms the genuine identity of communicating users, hosts, and devices before granting network access (enforced via Multi-Factor Authentication MFA, Kerberos, and X.509 PKI certificates).

Taxonomy of Network Attacks

- **1. Passive Attacks:** The attacker observes, intercepts, and monitors communication channels without altering the data payload or disrupting network operations. The legitimate sender and receiver remain completely unaware of the compromise. Examples: Packet Sniffing, Eavesdropping, and Traffic Analysis (monitoring packet frequency and volume). Passive attacks are difficult to detect; primary defense is strong End-to-End Encryption.
- **2. Active Attacks:** The attacker actively injects, modifies, reorders, intercepts, or disrupts network communications, host systems, or operational services. Examples: Masquerading (Spoofing), Replay Attacks, Message Modification, and Denial of Service (DoS). Active attacks are easy to detect; primary defense is Prevention and Real-Time Detection (Firewalls, IDS/IPS).

The Cyber Kill Chain (Attack Lifecycle)

Developed by Lockheed Martin, the Cyber Kill Chain framework outlines the sequential phases of an advanced cyber attack:

- **1. Reconnaissance:** Gathering target intelligence (harvesting IP ranges, open ports, employee emails, OS versions).
- **2. Weaponization:** Coupling an exploit payload (e.g., buffer overflow) with a malicious backdoor or Trojan.
- **3. Delivery:** Transmitting the weaponized payload to the victim via phishing emails, compromised websites, or open network ports.
- **4. Exploitation:** Triggering the malicious code by exploiting a known or zero-day software vulnerability on the target host.
- **5. Installation:** Installing a persistent rootkit, backdoor, or trojan service on the compromised system.
- **6. Command and Control (C2):** The infected host reaches out across the Internet to establish a covert beaconing channel with the attacker's C2 server.
- **7. Actions on Objectives:** Executing the final mission goal (exfiltrating corporate secrets, encrypting files via ransomware, destroying databases).

4.2 Reconnaissance and Discovery Attacks

- **1. Footprinting & OSINT (Open Source Intelligence):** The passive and semi-passive discovery of an organization's publicly exposed infrastructure using search engines (Google Dorking), WHOIS databases, DNS query records, Shodan (IoT search engine), and employee social profiles on LinkedIn.
- **2. Network Scanning & Port Scanning:** Active probing of target IP ranges to identify live hosts, active listening ports, running network services, and exact operating system versions (OS fingerprinting).
  - • **TCP SYN Scan (Stealth / Half-Open Scan):** Sends a TCP SYN packet. If the target responds with SYN-ACK, the port is OPEN (attacker immediately sends RST to avoid completing the 3-way handshake and logging an established connection). If target responds with RST, port is CLOSED.
  - • **TCP Connect() Scan:** Completes the entire 3-way handshake; highly reliable but easily detected and logged by target firewalls.
  - • **UDP Scanning:** Sends empty UDP packets to ports. If an ICMP Port Unreachable error returns, port is closed; if no response, port is open or filtered.
- **3. Enumeration:** Aggressive, interactive probing to extract valid user account names, network share paths, SNMP Community Strings, NetBIOS names, and routing tables.

- **4. Vulnerability Identification:** Using automated vulnerability scanners (e.g., Nessus, OpenVAS) to cross-reference discovered service version banners against Common Vulnerabilities and Exposures (CVE) databases and evaluate risk using Common Vulnerability Scoring System (CVSS) metrics.

4.3 Packet and Man-in-the-Middle (MITM) Attacks

1. Packet Sniffing

Packet sniffing involves placing a network interface card (NIC) into Promiscuous Mode, enabling it to intercept and log all Ethernet frames passing across the local broadcast domain, regardless of the destination MAC address (using tools like Wireshark or tcpdump). Insecure legacy protocols transmitting plaintext data (HTTP, Telnet, FTP, POP3) expose passwords and session tokens directly to sniffers.

2. ARP Spoofing / ARP Cache Poisoning

Because ARP is completely stateless and lacks authentication, any device can broadcast or unicast forged Gratuitous ARP packets. An attacker sends fake ARP replies telling the Victim 'I am the Gateway' (mapping the Gateway IP to Attacker MAC) and telling the Gateway 'I am the Victim' (mapping Victim IP to Attacker MAC).

- **Consequence:** All outbound and inbound traffic between the victim and the Internet is silently routed through the attacker's machine, enabling full Man-in-the-Middle eavesdropping and packet modification. Defense: Dynamic ARP Inspection (DAI) on managed switches.

3. MAC Flooding Attack

An attacker floods an Ethernet switch with tens of thousands of fake Ethernet frames with randomized source MAC addresses. The switch's CAM (Content Addressable Memory) table quickly becomes exhausted. Once full, the switch enters a Fail-Open (Hub) state, broadcasting all subsequent incoming traffic to every single port, allowing the attacker to sniff all intra-LAN communications. Defense: Port Security (limiting MAC addresses per port).

4. Session Hijacking & MITM

- **Session Hijacking:** An attacker steals an authenticated user's active session by intercepting web session cookies (via XSS or packet sniffing) or predicting TCP Sequence Numbers, allowing the attacker to impersonate the victim without re-authenticating.
- **SSL Stripping Attack:** A MITM proxy intercepts HTTP/HTTPS requests, presenting a secure HTTPS connection to the remote web server while serving unencrypted plaintext HTTP back to the victim, capturing plaintext credentials. Defense: HSTS (HTTP Strict Transport Security).

4.4 Denial of Service (DoS) and Botnet Attacks

Definition: Denial of Service (DoS / DDoS)

A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal operation of a targeted server, service, or network by overwhelming the target system or its surrounding infrastructure with a massive flood of bogus traffic, rendering it unavailable to legitimate users.

1. Botnets & Command-and-Control (C2) Architecture

A Botnet is a vast network of thousands or millions of compromised, malware-infected internet-connected devices (PCs, cloud servers, IoT security cameras, routers) known as 'Zombies' or 'Bots'. The attacker ('Botmaster') commands the entire bot army simultaneously through a centralized C2 server (via IRC, HTTP/HTTPS) or decentralized Peer-to-Peer (P2P) control channels to launch Distributed Denial of Service (DDoS) attacks.

2. Common Flooding Attacks

- **TCP SYN Flood:** The attacker transmits a massive flood of TCP SYN packets with spoofed source IP addresses. The victim server allocates memory resources in its Half-Open Connection Backlog Queue and replies with SYN-ACK. Because the spoofed IPs never send the final ACK, the server's backlog queue becomes exhausted, causing it to reject legitimate client connections. Defense: SYN Cookies (encodes connection state in initial sequence number without allocating memory until the final ACK arrives).
- **UDP / ICMP Floods:** Overwhelms network bandwidth and router processing engines with high-volume UDP or ICMP echo requests.

3. Amplification & Reflection Attacks

- **DNS Amplification Attack:** The attacker sends small DNS queries (e.g., 60 bytes requesting `ANY` record) with a spoofed Source IP set to the VICTIM'S IP address to publicly accessible open recursive DNS resolvers. The resolvers respond with huge DNS responses (up to 4000 bytes) sent directly to the unsuspecting victim, achieving an amplification factor of 50x to 70x!
- **NTP / Memcached Amplification:** Exploits vulnerable NTP `monlist` commands (500x amplification) or unprotected UDP Memcached servers (up to 50,000x amplification factor!).
- **Smurf Attack:** Attacker broadcasts ICMP Echo Requests with the victim's spoofed source IP to a local broadcast address, prompting every machine on the subnet to flood the victim with replies.

4.5 Spoofing and Protocol Attacks

- **1. IP Spoofing:** Forging the Source IP address field in the IPv4 packet header to conceal attacker identity or bypass IP-based firewall authentication. Defense: BCP 38 / Ingress and Egress network filtering (verifying that source IPs belong to the originating subnet).
- **2. DNS Spoofing / Cache Poisoning:** Injecting forged IP address mappings into the cache of a local recursive DNS resolver (e.g., mapping `bank.com` to an attacker-controlled phishing IP). Defense: DNSSEC (Domain Name System Security Extensions) using cryptographic digital signatures.
- **3. Email Spoofing & Phishing:** Forging SMTP `From:` header lines to make emails appear from trusted executives or banks. Defenses: (a) SPF (Sender Policy Framework: lists authorized sending IPs in DNS), (b) DKIM (DomainKeys Identified Mail: signs emails with private key), (c) DMARC (enforces strict rejection policies).
- **4. Routing Attacks & BGP Hijacking:** A malicious Autonomous System (AS) broadcasts illegitimate BGP route advertisements claiming ownership over IP prefixes belonging to other entities (e.g., hijacking cryptocurrency or government traffic). Defense: RPKI route validation.

4.6 Wireless and Malware-Based Threats

1. Wireless Threats: Rogue APs and Evil Twin Attacks

- **Rogue Access Point (RAP):** An unauthorized wireless access point plugged directly into an enterprise wired Ethernet wall jack by an employee or intruder, bypassing perimeter firewall security and exposing the corporate intranet.
- **Evil Twin Attack:** An attacker configures a rogue Wi-Fi AP broadcasting the exact same SSID (network name) and MAC address as a legitimate public Wi-Fi hotspot (e.g., 'Airport_Free_WiFi') with higher radio signal power. Unsuspecting devices connect automatically, and the attacker captures plaintext traffic and credentials via a captive portal.

2. Malware Propagation Mechanisms

- **Network Worms:** Self-replicating, standalone malicious programs that spread autonomously across networks by scanning for and exploiting unpatched network vulnerabilities without requiring human interaction (e.g., SQL Slammer, Conficker, Blaster worm).
- **Ransomware Networks:** Malicious software that traverses network file shares (SMB) using exploits (e.g., WannaCry leveraging the EternalBlue SMBv1 exploit), encrypts local and networked hard drives using AES-256 and RSA-2048, and demands cryptocurrency ransom for decryption keys.

4.7 Network Defense Mechanisms & Architectures

1. Firewalls (Classification by Generation)

- **Stateless Packet Filtering Firewall (1st Gen - Layer 3/4):** Inspects individual packets in isolation against static rule tables (filtering on Source/Dest IP, Protocol, Source/Dest Port). High speed, low memory; vulnerable to spoofing and cannot track connection state.
- **Stateful Inspection Firewall (2nd Gen - Layer 3/4):** Maintains an active State Table tracking established TCP/UDP connections. Automatically permits return traffic for legitimate outbound requests and drops unsolicited inbound packets.
- **Next-Generation Firewall (NGFW) / Application Firewall (3rd Gen - Layers 4–7):** Performs Deep Packet Inspection (DPI) into application payloads, decrypts TLS/SSL streams, integrates real-time Intrusion Prevention (IPS), and identifies specific applications (e.g., blocking BitTorrent while allowing HTTPS).

2. Intrusion Detection and Prevention Systems (IDS / IPS)

- **IDS vs IPS:** An IDS (Intrusion Detection System) operates out-of-band in passive listening mode, generating alerts when suspicious activity occurs. An IPS (Intrusion Prevention System) sits in-line directly in the traffic pathway, actively dropping malicious packets in real time.
- **Detection Methodologies:**
  - Signature-Based Detection: Compares packet patterns against a database of known attack signatures (fast and accurate; fails against zero-day attacks).
  - Anomaly-Based Detection: Establishes a baseline profile of normal network traffic using machine learning; flags statistical deviations as potential attacks (detects zero-days; higher false-positive rate).
  - NIDS (Network IDS) monitors entire subnet traffic; HIDS (Host IDS) monitors system call logs and file integrity on a single host.

3. Network Segmentation, DMZ & Zero Trust Architecture

- **Demilitarized Zone (DMZ):** A physical or logical subnetwork that exposes an organization's external-facing public services (Web, Mail, DNS servers) to the untrusted Internet, while isolating the sensitive internal corporate LAN behind a secondary firewall. If a public web server is compromised, the internal LAN remains protected.
- **Zero Trust Architecture (ZTA):** Security framework based on the core tenet: 'Never Trust, Always Verify'. Eliminates implicit trust based on physical network location. Enforces continuous multi-

factor authentication, end-to-end encryption, and least-privilege micro-segmentation for every access request.

- **Defense-in-Depth:** A multi-layered defense strategy ensuring that if one defensive layer fails (e.g., perimeter firewall breached), subsequent layers (IDS, segmentation, endpoint EDR, data encryption) stop the adversary.

4.8 High-Yield University Exam Question Bank

Part A: Short Answer Questions (2 to 5 Marks)

Q1. What is the CIA Triad in Network Security? [3 Marks]

- **Answer:** Confidentiality (preventing unauthorized disclosure via encryption), Integrity (preventing unauthorized modification via hashing/checksums), and Availability (ensuring authorized users have uninterrupted access to services).

Q2. How does an ARP Spoofing attack work? [4 Marks]

- **Answer:** Because ARP lacks authentication, an attacker sends fake ARP replies to a victim associating the default gateway IP with the attacker's MAC address, and to the gateway associating victim's IP with the attacker's MAC. This positions the attacker as a Man-in-the-Middle to intercept all traffic.

Q3. Explain the mechanism of a TCP SYN Flood and how SYN Cookies defend against it. [4 Marks]

- **Answer:** Attacker sends thousands of SYN packets with spoofed source IPs. The server reserves memory in its backlog queue waiting for final ACKs that never arrive, exhausting resources. SYN Cookies defend by encoding connection parameters into the Initial Sequence Number (ISN) without allocating server memory until a legitimate final ACK arrives.

Part B: Long Answer Questions (10 to 15 Marks Outline Guides)

- **Q4. Explain various Reconnaissance and Discovery attacks (Footprinting, OSINT, Port Scanning techniques, and Enumeration) in detail. [10 Marks]**
- **Q5. Compare DoS and DDoS attacks. Explain DNS Amplification, Smurf attacks, and Botnet C2 architectures with diagrams. [15 Marks]**
- **Q6. Discuss Network Defense Mechanisms: Firewall generations (Packet Filter, Stateful, NGFW), IDS vs IPS (Signature vs Anomaly), and DMZ Architecture. [12 Marks]**

- **Q7. Explain Wireless Security threats (Rogue APs, Evil Twin) and Malware propagation mechanisms (Worms vs Ransomware) with real-world mitigation strategies. [10 Marks]**

4.9 Unit Summary & Key Takeaways

- Security relies on the CIA Triad (Confidentiality, Integrity, Availability) plus Authentication and Non-repudiation.
- Reconnaissance includes Footprinting, OSINT, Port Scanning (SYN, Connect, UDP), and Enumeration.
- Packet & MITM attacks exploit unencrypted traffic (Sniffing), ARP poisoning, MAC flooding (CAM overflow), and SSL stripping.
- DoS/DDoS attacks exhaust bandwidth and server resources via SYN floods, UDP floods, and Amplification attacks (DNS/NTP).
- Spoofing threats: IP spoofing (defended by BCP 38), DNS cache poisoning (DNSSEC), and Email spoofing (SPF, DKIM, DMARC).
- Wireless & Malware threats include Rogue APs, Evil Twin attacks, autonomous Worms, and Ransomware (WannaCry).
- Defenses incorporate Next-Gen Firewalls, in-line IPS, DMZ architectures, Defense-in-Depth, and Zero Trust Architecture.