BUILDING A CAREER IN CYBERSECURITY: ESSENTIAL NETWORKING CONCEPTS

Vaishali Shishodia

VAISHALI SHISHODIA

1. Introduction to Networking in Cybersecurity

Networking is a fundamental aspect of cybersecurity, as securing an organization's infrastructure relies heavily on understanding how data moves within a network. Cybersecurity professionals must have a strong grasp of networking concepts to identify threats, secure connections, and mitigate risks effectively. **A deep understanding of networking helps in detecting unauthorized access, mitigating attacks, and implementing security policies efficiently.**

2. Types of Networks

LAN (Local Area Network):

- Covers a small geographical area, like a home, office, or campus.
- Uses Ethernet and Wi-Fi technologies for connectivity.
- Common threats include **unauthorized access, ARP spoofing, and malware propagation.**

WAN (Wide Area Network):

- Covers a large geographical area, connecting multiple LANs.
- Uses leased communication links like MPLS, fiber optics, and satellite connections.
- Security concerns include **data interception, DDoS attacks, and unauthorized access.**

MAN (Metropolitan Area Network):

- Covers a city or a large institution, such as a university.
- Uses high-speed fiber optics for fast data transfer.
- Prone to **eavesdropping and data leaks.**

PAN (Personal Area Network):

- Used for connecting personal devices like smartphones, smartwatches, and laptops.
- Utilizes technologies such as Bluetooth and Zigbee.
- Vulnerable to **Bluetooth attacks, eavesdropping, and data theft.**

VLAN (Virtual Local Area Network):

- Segments networks logically rather than physically, improving security and efficiency.
- Used in enterprise networks to segregate user groups.
- Protects against **internal threats by restricting unauthorized access within the network.**

3. IP Address and Its Types

An **IP Address** is a unique identifier assigned to each device on a network to facilitate communication.

IPv4 (Internet Protocol version 4):

- Uses a 32-bit address format (e.g., 192.168.1.1).
- Has a limited address space, leading to the development of IPv6.

Vaishali Shishodia

- Common in legacy systems and still widely used in private networks.

IPv6 (Internet Protocol version 6):

- Uses a 128-bit address format (e.g., 2001:db8::ff00:42:8329).
- Provides a virtually unlimited address space, improving scalability.
- Supports built-in security features such as **IPSec encryption.**

Types of IP Addresses:

- **Public IP:** Used for internet-facing devices; assigned by ISPs.
- **Private IP:** Used within local networks; assigned dynamically by DHCP.
- **Static IP:** Manually assigned; useful for servers and network devices.
- **Dynamic IP:** Assigned by a DHCP server and changes over time to optimize resource usage.

4. DHCP (Dynamic Host Configuration Protocol)

How It Works:

- Automatically assigns IP addresses to devices within a network.
- Reduces administrative overhead by eliminating manual IP configuration.
- Helps in managing IP address allocation and avoiding conflicts.
- Cybersecurity risks include **DHCP starvation attacks and rogue DHCP servers.**

5. DNS (Domain Name System)

How It Works:

- Resolves human-readable domain names (e.g., google.com) into machine-readable IP addresses.
- Uses a hierarchical structure with root servers, TLDs (Top-Level Domains), and authoritative DNS servers.
- Common DNS security threats:
    - **DNS Spoofing:** Attackers manipulate DNS records to redirect users to malicious sites.
    - **DNS Tunneling:** Exploiting DNS queries to exfiltrate data or communicate covertly.

6. Subnetting

Importance in Cybersecurity:

- **Divides large networks into smaller, manageable subnetworks, reducing broadcast traffic.**
- **Enhances security by limiting lateral movement of attackers.**
- **Used to implement network segmentation, improving control over access rights.**
- **Prevents unauthorized access to sensitive areas of a network.**

Vaishali Shishodia

7. OSI Model

Layers and Their Role in Security:

1. **Physical Layer:** Deals with hardware security (cables, Wi-Fi signals); threats include **wiretapping and signal jamming.**
2. **Data Link Layer:** Handles MAC addressing; threats include **MAC spoofing and VLAN hopping.**
3. **Network Layer:** Responsible for IP addressing and routing; threats include **DDoS attacks and IP spoofing.**
4. **Transport Layer:** Ensures data delivery using TCP/UDP; threats include **session hijacking and SYN flooding.**
5. **Session Layer:** Manages sessions; vulnerable to **session hijacking.**
6. **Presentation Layer:** Encrypts and formats data; risks include **SSL stripping attacks.**
7. **Application Layer:** Provides services like HTTP, FTP, and DNS; vulnerable to **phishing and malware attacks.**

8. Network Security Devices

Firewall:

- Acts as a barrier between trusted and untrusted networks.
- Uses rules to allow or block traffic.
- Types: Packet-filtering, Stateful inspection, Next-Gen Firewalls.

Proxy Server:

- Hides client identity and filters web requests.
- Prevents malware from reaching internal systems.

Router:

- Directs network traffic and manages IP forwarding.
- Configurable with **Access Control Lists (ACLs)** to block suspicious activities.

Switch:

- Connects devices within a LAN and forwards packets based on MAC addresses.
- Can implement **port security to prevent unauthorized access.**

VPN (Virtual Private Network):

- Encrypts internet connections, securing remote access.
- Used to **prevent Man-in-the-Middle (MitM) attacks and data interception.**

9. TCP & UDP Protocols

TCP (Transmission Control Protocol):

Vaishali Shishodia

- Connection-oriented, ensuring reliable data delivery.
- Used in **HTTPS, SSH, FTP, and email communication.**

UDP (User Datagram Protocol):

- Connectionless, prioritizing speed over reliability.
- Used in **VoIP, DNS queries, and video streaming.**
- Security risks include **UDP-based DDoS attacks and DNS amplification attacks.**

10. Other Protocols Used in Cybersecurity

- **ICMP (Internet Control Message Protocol):** Used for network diagnostics; vulnerable to **ICMP flooding (Ping of Death).**
- **HTTPS (HyperText Transfer Protocol Secure):** Encrypts web communications using TLS/SSL.
- **FTP/SFTP (File Transfer Protocol/Secure FTP):** Used for secure file transfers.
- **SMB (Server Message Block):** Used in Windows networks for file sharing; targeted in **ransomware attacks.**
- **RDP (Remote Desktop Protocol):** Provides remote system access; commonly exploited in brute-force attacks.
- **SSH (Secure Shell):** Used for secure command-line access to remote devices.

Conclusion

Mastering networking concepts is crucial for cybersecurity professionals. Understanding network structures, protocols, and security devices helps in detecting vulnerabilities, securing infrastructure, and mitigating cyber threats effectively. This knowledge is essential for roles such as **SOC analysts, penetration testers, network security engineers, and ethical hackers.**

Vaishali Shishodia