Cybersecurity Daily Dairy

Day 6: Network Security, Hierarchy & Subnetting Basics

Date: June 24, 2025

Topics Covered:

- Cybersecurity hierarchy and layers
- Network security concepts (AAA, IAM)
- Network architecture (Access, Distribution, Core Layers)
- Role of a Network Administrator
- Firewall concepts and packet filtering
- Access rules in firewalls
- Subnetting fundamentals
- IP addressing, private IPs, subnet mask, broadcast address

What I Did:

Today I studied the **hierarchical structure of cybersecurity tasks**, focusing on how different responsibilities fit into various layers of the security framework. I also explored **network security basics** like AAA, IAM, and firewall configuration.

Hierarchy in Cybersecurity:

- **Application Layer:**
    - Penetration Testing
    - Vulnerability Assessment
    - Threat Handling
- **Network Security Layer:**
    - Network Design
    - Firewalls and Access Rules
    - AAA (Authentication, Authorization, Accounting)
    - IAM (Identity and Access Management)

Network Design Layers:

1. **Access Layer** – Connects end-user devices (PCs, printers, etc.) to the network
2. **Distribution Layer** – Enforces policies and forwards data between access and core layers

3. **Core Layer** – Acts as the backbone, providing high-speed data transfer across the network

---

Key Roles:

- **Network Administrator:**
  Responsible for setting up, maintaining, and securing the network infrastructure.
  Tasks include configuring switches, routers, applying firewall rules, managing subnets, and monitoring traffic.

Firewall Concepts:

- **Packet Filtering Firewall:**
  Filters traffic based on IP addresses, ports, and protocols. Each packet is examined and either allowed or blocked based on predefined rules.
- **Access Rule Configuration:**
  Rules define what kind of traffic is permitted or denied, usually based on source/destination IPs, ports, or services.

Subnetting Concepts:

- **IP Address:**
  A numerical label assigned to each device on a network (e.g., 192.168.1.1)
- **Private IP Addressing:**
  IP ranges reserved for use in private networks (e.g., 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12)
- **Broadcast Address:**
  An IP address used to communicate with all devices in a subnet (e.g., 192.168.1.255 for 192.168.1.0/24)
- **Subnet Mask:**
  A 32-bit number that splits the IP address into network and host parts (e.g., 255.255.255.0)

Key Learnings:

- Cybersecurity involves multiple layers, each requiring specialized knowledge and tools
- AAA and IAM frameworks are essential for securing access
- Proper network design improves both performance and security
- Subnetting helps in efficient IP address allocation and managing traffic flow