Networking Overview

A network enables two computers to communicate. There are various topologies (mesh, tree, star), mediums (ethernet, fiber, coax, wireless), and protocols (TCP, UDP, IPX) used to facilitate networks. Understanding networking is crucial for security professionals as silent failures may lead to undetected issues.

Flat vs Segmented Networks

- **Flat Network**: Easier to set up but vulnerable, like a house with only a front door lock.
- **Segmented Network**: Adds multiple layers of defense, similar to a house with fences, lights, and bushes.

Examples

1. **Access Control Lists (ACLs)**: Like fences creating controlled entry points.
2. **Network Mapping & Documentation**: Like lighting the property.
3. **Intrusion Detection Systems (IDS)**: Like bushes deterring entry through windows.

Flat /24 networks may allow unrestricted communication, leading to risk.

Story Time: A Pentester’s Oversight

Penetration testers often default to a /24 subnet (255.255.255.0), which can lead to missing other network segments:

- **/24 Network**: All devices in 192.168.1.xxx can talk to each other.
- **/25 Network**: Splits the /24 in half. Devices can only talk to their half.

Example Setup:

- Server Gateway: `10.20.0.1/25`
- Domain Controller: `10.20.0.10/25`
- Client Gateway: `10.20.0.129/25`
- Client Workstation: `10.20.0.200/25`
- Pentester IP: `10.20.0.252/24`

Pentester missed high-value targets due to incorrect subnetting.

Basic Networking Overview

Diagram: Shows Home and Company networks connected to ISP.

- Home devices communicate with the company website.
- **FQDN vs URL**:
  - FQDN: `www.hackthebox.eu` (building address)
  - URL: `https://www.hackthebox.eu/example?floor=2&office=dev&employee=17` (complete address)

Router: Acts as the "post office".

- Sends packets to ISP (main post office)
- ISP uses DNS to resolve FQDN to IP
- Sends packets to destination webserver
- Server responds back to your IP via the same route

Extra Points: Network Segmentation

1. **Web Server → DMZ**:

   - Internet-exposed
   - Separate from internal network for added security

2. **Workstations → Own Network**:

   - Isolated from servers
   - Prevents lateral movement attacks

3. **Switch/Router → Administration Network**:

   - Prevents unauthorized snooping
   - Protects routing protocols (e.g., OSPF)

4. **IP Phones → Dedicated Network**:

   - Prevents eavesdropping
   - Enables traffic prioritization

5. **Printers → Separate Network**:

   - Prevents credential theft via NTLM
   - Printers are difficult to secure and store sensitive info

---

Key Takeaway: Proper network segmentation enhances security, detectability, and manageability. Always verify network masks and avoid flat designs where possible.