Network Security

1. Network Vulnerability
2. What makes network vulnerable?
   * Unknow attacks
     + Attacks may be launched from thousands of miles away.
     + Hack a machine from another hacked machine.
   * Many points of attack: from any machine to any machine
   * Sharing
   * System/Network complexity
   * Unknown perimeter (host on multiple networks)
   * Unknown paths (packets may travel over many different paths to a destination)
3. Hazy network perimeter:

* HAPPENED when it’s difficult to def the boundaries of a network due to factors such as cloud-based services and mobile access.
* PROBLEM: can create vulnerabilities and make it harder to control and monitor activity.
* SOLVE: use tools and strategies suck as network segmentation, access controls, and monitoring to improve network security.

1. Attacks
2. **Threat Precursors**

* Are techniques or activities that can be used by potential attackers to gather information about a network, system, or organization.
* COMMON THREAT: Port scan, war dialers, social engineering, dumpster diving, network mapping, vulnerability scanners, vendor documentation.

1. **Eavesdropping, Wiretapping**

* DEF: techniques used to intercept and monitor communications between devices on a network
* TECHNIQUE can be done by using:
  + Packet sniffers: wiretaps, Ettercap
  + Cable-based
  + Insecure wireless networks

1. **Packet sniffing**

* DEF: is a technique used to intercept and analyze network traffic.
* Ethernet frame structure
* When a packet is sent over a subnet
* Promiscuous mode

1. Protocol Flaws
2. Spoofing

* At Network Layer
* At Transport Layer
* After Spoofing
  + Packet sniffing
  + Spoofing: SYN spoofing, how would anti spoofing help?
  + Flooding: UDP flood, SYN flood
  + Smurf attack
  + DoS attacks: reflection, amplification

1. Controls
   * Design: separation, single point of failure, redundancy, recovery, encryption