Network Based Attacks

Objectives

- Explain how the network can be a source of attack
- Discuss how the attacks work at a high level
- Understand options in prevention

Common Types of Attacks

- Active attacks – Attacker has ability to see/manipulate real-time traffic
  - Sniffing
  - Eavesdropping
  - Spoofing
  - Denial of service
- Passive attacks – Attacker can read data and use the data for other purposes
  - Stems from sniffing traffic
  - Compromised data

Active attacks - Sniffing

- What it is: Reading, monitoring, or capturing full packets from a device
- Well known tools used: Wireshark, tcpdump
- How common: Most network attacks come from someone being able to get into the traffic stream
- Complexity: very simple providing you have ability to actually get into the data stream
- Risk: It’s a serious threat, sniffing is non-intrusive

Active attacks - Eavesdropping

- What it is: Similar to sniffing and may be used in the same manner, but sometimes without full packets, usually synomous with 1 to 1 communications
- Well known tools used: Wireshark, tcpdump, ettercap
- How common: Most network attacks are in the form of sniffing, eavesdropping is a form of it
- Complexity: Getting into the data stream can be difficult
- Risk: It’s a serious threat, eavesdropping if done incorrectly can result in a noticeable change in connection so it’s easier to detect

Active attacks - Spoofing

- What it is: Pretending to be someone/something that you are not. ARP spoofing. Typically done with the router/gateway
- Well known tools used: ettercap
- How common: May only work on non-enterprise systems. Enterprise systems have detection mechanisms
- Complexity: Not complex because of software
- Risk: Serious threat because this is more of an active attack. Anything can be spoofed in this type of attack.

Active attacks – Denial of Service

- What it is: Effects the ability to use resources
- Well known tools used: HOIC, LOIC, botnets
- How common: Not common due to resource constraints
- Complexity: Very complex for large organizations
- Risk: You lose business because of resource availability

Passive attacks

- Most passive network attacks stem from previous active attacks
- Attacker uses information obtained via sniffing or eavesdropping for:
  - Password attacks – unencrypted password reuse
  - Replay attacks – using tokens or cookies from traffic stream
  - Use other information obtained against you

Protection

- If you are an enterprise:
  - Keep up to date on network security patches
  - Utilize enterprise grade hardware
  - Segment your network
  - Protect network equipment
- If you are a small business or and individual that cannot afford to purchase enterprise grade hardware:
  - Understand who is on your network
  - Don’t allow outsiders to connect to your private networks