Network Attacks

Topics

- Objectives
- Rogue Devices
- Rogue Infrastructure Hardware Placement
- Data Theft & Malicious Insertion
- Security Feature Weaknesses &Vulnerabilities
- Denial Of Service
- Conclusion

Objectives

- Demonstrate how to recognize, perform and prevent the following types of attacks:
  - Rogue infrastructure hardware placement.
  - Denial of Service attacks.
  - Hijacking and Peer-to-peer attacks
  - MAC Spoofing
- Understand Security Vulnerabilities associated with unsecured wireless networks.

Rogue Devices

- A Rogue Device is define as any device that is not authorized to be on the network.
- An intruder might perform data theft, data insertion, peer attacks etc ,once he or she gains access to network potentially through a rogue device.
- It is common to see rogue access points, bridges, and Ad Hoc networks installed without authorization in a wireless networks.

Rogue Infrastructure Hardware Placement

- Rogue devices will be placed as if the device were designed to be there in the first place.
- Rogue Access points:
  - They will normally be placed out of site in the places like:
    - Under a desk
    - In, on top, or behind a cabinet.
    - In the ceiling
    - In a closet
    - etc
  - They will likely use a channel that will not interfere surrounding access points.

Cont…

- Encryption settings: Static WEP would be enabled if static or dynamic WEP already being used on the wireless network on which rogue is being placed.
- SSID settings: The SSID of rogue device will be set to match that of the existing wireless LAN implementation.
- Frequency: Intruders may use 900 MHz units instead of 2.4 GHz or 5 GHz Wi-fi compliant units.
- Spectrum choice: Intruders may use FHSS technology instead of DSSS.
- Antennas: Horizontally polarized antennas are often used on the rogue and the client.

Cont…

- Wireless Bridges:
  - Placement: A rogue bridge is placed with in the Fresnel zone of an existing bridge link.
  - Priority: The spanning tree priority of a rogue bridge must be set very high.
  - MAC spoofing and filter Identification: The MAC address of an authorized non-root bridge can be spoofed.
  - Antenna use: Intruders will use high-gain directional antennas.

Data Theft & Malicious Insertion

- Illegal, Unethical, or appropriate content:
  - What would be the result of a hacker obtained access to a network and deposited files on the network?
- Viruses and Spyware
- Peer to peer attacks
- Unauthorized Control

Viruses & Spyware

- Viruses are capable of disabling desktop PCs, taking web sites and even overloading email servers.
- Trojan Horse applications, Worms are specific types of viruses.
- A type of malware called spyware typically comes as a multi-featured software package that can :
  - Capture instant messenger, email, website traffic.
  - Capture sites visited.
  - Capture keystrokes and passwords.
  - And so on.
- Most widely used spware application in wireless environment is iSpyNow.
- www.symantec.com and www.mcafee.com are most popular sources dedicated to remove viruses and avoid re-infection by a virus.
- www.anti-spy.com is a popular anti-spy application.

Peer-to-Peer Attacks

- Peer-to-peer attacks are attacks instigated by one host aimed at another host, both of which are clients of the same network system.
- aim at sensitive data files, password files

Unauthorized Control

- Attacker gains access to your network, reconfigures and manages your network.
  - Network management tools
    - What's Up Gold, SNMPc, Solarwinds
  - Configuration changes
  - Third party attacks

Spamming – 3rd party attacks

- Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup.
- Some people define spam even more generally as any unsolicited e-mail.
- In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth.
- Spamming has at least two major impacts to the network and organization and they are:
  - Performance Degradation and
  - Bad Public Relations.

Source: http://www.webopedia.com/TERM/s/spam.htm

Security Feature Weaknesses and Vulnerabilities

- WEP (Wired Equivalent Privacy or Wireless Encryption Protocol) :
  - WEP was intended to provide confidentiality comparable to that of a traditional wired network.
  - Several serious weaknesses were identified by cryptanalysts, a WEP connection can be cracked with readily available software within minutes.
- Pre-shared key (PSK, also known as WPA personal mode):
  - A pre-shared key is a password which is entered to access a secure Wi-Fi system using WEP or WPA.
  - Weak PSK passphrases can be broken using off-line dictionary attacks by capturing the messages in the four-way exchange when the client reconnects after being deauthenticated.
  - Wireless suites such as aircrack-ng can crack a weak passphrase in less than a minute
  - WPA Personal is secure when used with ‘good’ passphrases or a full 64-character hexadecimal key.

Source: http://en.wikipedia.org/wiki/Wireless_security#WPA

Cont…

- LEAP (Lightweight Extensible Authentication Protocol):
  - It is a proprietary Cisco authentication protocol.
  - THC-LeapCracker can be used to break Cisco's version of LEAP
  - It can be used against computers connected to an access point in the form of a dictionary attack.
- PPTP (Point-to-Point Tunneling Protocol):
  - It was created by Microsoft in windows NT and is used in many hardware and software systems today.
  - It is inherently insecure because there are too many unauthenticated control packets that are readily spoofed.

Source: http://en.wikipedia.org/wiki/Wireless_security#WPA

Denial Of Service

- System will become unavailable to its intended users.
- It occurs when an attacker continually sends bogus requests and/or other commands.
- Wireless networks are susceptible to DoS attacks at two primary levels:
  - Physical Layer
  - MAC Layer.

Physical Layer DoS

- At the physical layer, DoS attack can be launched by generating RF energy in the same frequency as target's WLAN.
- RF Jamming:
  - Radio jamming is the (usually deliberate) transmission of radio signals that disrupt communications by decreasing the signal to noise ratio.
  - Jamming problems in a WLAN environment and they include:
    - Microwave ovens, Bluetooth devices , other RF devices and WLAN devices.
  - Administrator's only defense against this RF Jamming is the Physical Security.

MAC Layer DoS

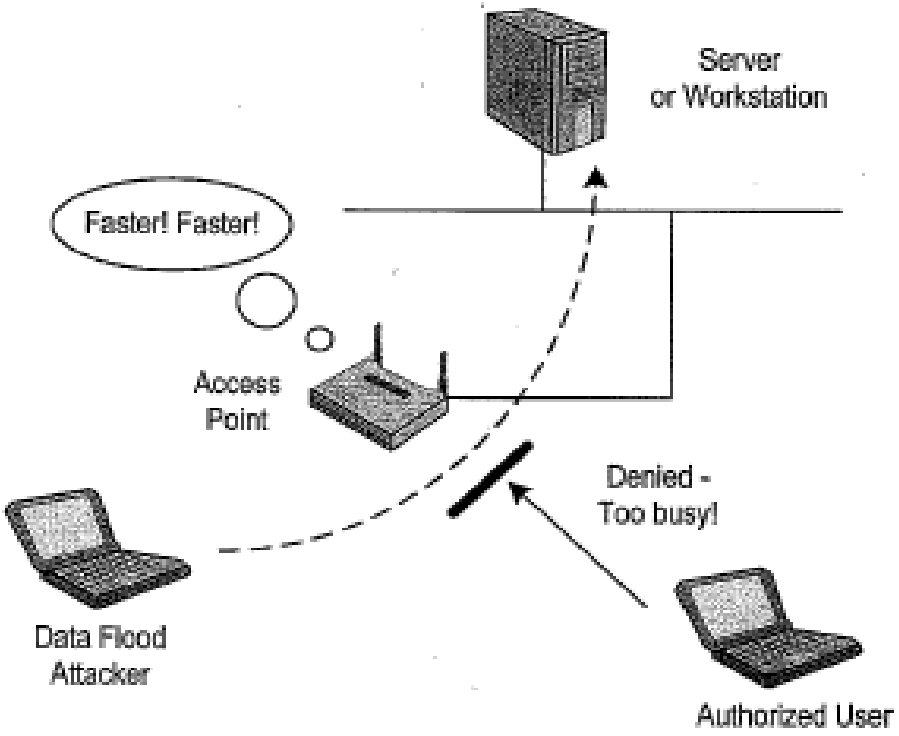
- Hijacking.
- Data Flooding
- overwhelming a computer with more data than it can process.

Cont…

- Hijacking:
  - attacker takes control of a user’s wireless LAN
    - layer 2 for denial of service
    - layer 3 for attacking purposes.

Cont…

- Data flooding illustration



Conclusion

- Different types of unauthorized access discussed are:
  - Rogue Devices
  - Data theft/insertion
  - Peer-to-peer attacks
  - Unauthorized control
- Understood the weaknesses and vulnerabilities of different security technologies.
- Three types of wireless DoS attacks discussed are:
  - RF Jamming
  - Data Flooding
  - Hijacking
- The best defense is the Physical Security.