Cyber Security Tools and Technologies

Dr. Arshad Ali
Associate Professor
NUCES Lahore

Networks and the Internet

- **Chapter 2 of the Book**

Computer Security Fundamentals

Network and the Internet

- **Network Basics:**
- **Connectivity**
  - **Wired (cable): IEEE 802.1 Ethernet**
  - **Wireless: IEEE 802.11**
  - **Bluetooth**
- NICs is an RJ-45 connection.
- Hub
- **The repeater** (to boost signal)
  - **Amplifiers**: simply boost the entire signal including any noise
  - **Signals**: regenerate the signal and don't rebroadcast noise

Network and the Internet

Network Basics:

- **Switch**
  - able to determine where a packet is being sent.
  - It makes this determination based on the MAC, found in the Ethernet header of the packet.
- **Router**
  - routers have interfaces allowing to configure them
  - More robust routers also offer more programming possibilities.
  - The specifics of how you program a router are different from vendor to vendor,
  - most routers are programmable, allowing you to change how they route traffic.

Network and the Internet

Network Basics:

- **Securing WiFi**
  - Wired Equivalent Privacy (WEP)
    - uses the stream cipher RC4 to secure the data and a CRC-32 checksum for error checking.
  - Wi-Fi Protected Access (WPA)
    - uses Temporal Key Integrity Protocol (TKIP), which is a 128-bit per-packet key
    - it dynamically generates a new key for each packet

Network and the Internet

Network Basics:

- **Securing WiFi**
  - **WPA2** provides the Advanced Encryption Standard (AES) using **C**ounter Mode-**C**ipher Block Chaining (CBC)-**M**essage Authentication Code (MAC) **P**rotocol (CCMP)
    - Provides data confidentiality, data origin authentication, and data integrity for wireless frames.
  - **WPA3** requires attackers to interact with your Wi-Fi for every password guess they make, making it much harder and time-consuming to crack.
    - you can connect a device by merely scanning a QR code on your phone (WPA3's "Wi-Fi Easy Connect,")
    - with WPA3, even open networks will encrypt your individual traffic.

Network and the Internet

Network Basics:

- **Data transmission protocols**
  - FTP (port 20 and 21)
  - TFTP – Trivia FTP: Fast but less reliable FTP (port 69)
  - SSH (Secure Shell – port 22): use to securely connect to a remote system
  - Telnet (port 23): remote log on
  - SMTP (port 25): sends email
  - Whois (port 43): queries a target IP address for information

Network and the Internet

Network Basics:

- **Data transmission protocols**
  - DNS (port 53): translation of URLs into web addresses
  - **HTTP** (port 80): Displays web pages
  - POP3 (port 110): Retrieves email
  - **NN**TP (port 119): used for **N**etwork **N**ews groups
  - IMAP (port 143): more advanced protocol for receiving emails – replacing POP3
  - IRC: Internet Relay Chat (port 194): used for chat rooms

Network and the Internet

Network Basics:

- **Data transmission protocols**
  - SMB (Server Message Block – port 445) – used for windows active directory
  - HTTPS (port 443): encrypted HTTP
  - SMTPS (port 465): encrypted SMTP
  - POP3S (port 995) : encrypted POP3
  - IMAPS (port 993): encrypted IMAP
  - Many more protocols
- **All these protocols are part of TCP/IP protocol suit**
- **Irrespective of the protocol is use,**
  - all communication on networks takes place via **packets**, and
  - those packets are **transmitted** according to certain protocols, depending on the type of communication that is occurring

Network and the Internet

Network Basics:

- **Ports:**
  - A *port* is a handle, or a connection point.
  - a numeric designation for a particular pathway of communications (like a channel number on TV)
  - 65535 network communication ports
  -
- **Socket:** The combination of your computer's IP address and port number
- All network communication, regardless of the port used comes into your computer via the connection on your NIC.

Network and the Internet

Network Basics:

- **Networks picture:**
  - machines connected to each other via cables, and perhaps to hubs, switches, or routers.
  - These networks transmit binary information in packets using certain protocols and ports.

Network and the Internet

Network Basics: Internet working

- **Internet** is essentially a large number of networks that are connected to each other.
- the Internet works similar to your LAN.
- Sends the same sort of data packets, using the same protocols.
- Various networks are simply connected to main transmission lines called ***backbones***.
- The points where the backbones connect to each other are called ***network access points*** (*NAPs*).

Network and the Internet

How the Internet works

- When you log on to the Internet, you probably use an *Internet service provider* (*ISP*).
  - That ISP has a connection either to the Internet backbone or to yet another provider that has a backbone.
- So, logging on to the Internet is a process of connecting your computer to your ISP's network, which is, in turn, connected to one of the backbones on the Internet.

Network and the Internet

IP addresses

- To ensure that the data packets go to the correct computer, we use IP addresses with network communications
- An IP address can be IPv4 or IPv6
- IPv4 Private addresses:

10.0.0.10 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

Loopback testing: 127.0.0.1

- NAT
- IPv4 Subnetting and CIDR
- IPv6: No subnetting but uses CIDR (i.e., /48 or /64), loopback address: ::/128

- **Uniform Resource Locator (URL)**
- **Packet?**

Network and the Internet

Basic Network utilities

- **IPConfig**
- **Ping**
- **Tracert**
- **Netstat**
- **NSLookup**
- **ARP**
- **Route**

More Network Devices

Communication Topics

- **TCP/IP protocol suit: TCP,UDP, IP**
- **OSI model**
- **MAC addresses**