Ports and Protocols

Objectives

- Discuss what ports and protocols are used within information security
- Understand difference between secured and unsecured technology

Communication Protocols

- Typical communication methods
  - Internet traffic
  - Email
  - File transfer
- Each one can have secure or unsecure protocols and implementation methods
- Communications should always be secure

Internet Communications - HTTP

- Stands for: Hyper Text Transfer Protocol
- Used for: Transferring information between 2 computers
- Typically implemented in: web servers, web applications
- Typical communication port: 80
- Secure or Unsecure: Unsecure – meaning it can be read if it is intercepted

Internet Communications - HTTPS

- Stands for: Hyper Text Transfer Protocol - Secure
- Used for: Transferring information between 2 computers
- Typically implemented in: web servers, web applications
- Typical communication port: 443
- Secure or Unsecure: Secure – meaning it cannot be read if it is intercepted
- Secured with either SSL or TLS
- Typically very simple to secure with certificates

Email Communications – MIME

- Stands for: Multipurpose Internet Mail Extension
- Used for: Probably over 99% of all email communication sent via SMTP
- Typically implemented in: Email communication. It is a standard that defines how email is formatted so servers who are receiving the email can read it
- Typical communication port: SMTP – 25, IMAP - 143
- Secure or Unsecure: Unsecure, which means it can be read if intercepted
- Notes: This is the standard for email communication when sending

Internet Communications - SMIME

- Stands for: Secure Multipurpose Internet Mail Extension
- Used for: Transferring information between 2 computers
- Typically implemented in: end to end encrypted email exchange
- Typical communication port: SMTP – 465, IMAP - 993
- Secure or Unsecure: Secure – contents is encrypted
- Benefit of using SMIME is that the contents remains encrypted in transit and at rest.
- Downside is that webmail has a hard time processing it

File Transfer - FTP

- Stands for: File Transfer Protocol
- Used for: Transferring files from one system to another
- Typically implemented in: servers that have FTP software
- Typical communication port: 21
- Secure or Unsecure: Unsecure, which means it can be read if intercepted

File Transfer – SFTP/FTPS

- Stands for: Secure file transfer protocol
- Used for:
- Typically implemented in: servers with SFTP/FTPS software
- Typical communication port: SFTP – Port 22, FTPS 990/989
- Secure or Unsecure: Secure
- SFTP runs over Secure Shell, or SSH. FTPS is FTP implemented with SSL/TLS

Server/Network Communications- Telnet

- Stands for: Telnet
- Used for: equipment communications
- Typically implemented in: network equipment
- Typical communication port: 23
- Secure or Unsecure: Unsecure, which means it can be read if intercepted

Server/Network Communication - SSH

- Stands for: Secure Shell
- Used for: server/network communication. Typically Linux for servers
- Typically implemented in: secure text communication, but has other uses
- Typical communication port: 22
- Secure or Unsecure: Secure
- SSH within Linux can provide many advantages
  - Xwindows
  - File transfer
  - Tunnels

Overall Communication Channels - VPN

- Stands for: Virtual Private Network
- Used for: Keeping information secure
- Typically implemented in: organizations to provide a way of securely communicating
- Typical communication port: IPSec, PPTP, IKE
- Secure or Unsecure: Secure
- VPN should always be used when you do not trust the network you are connected to.
- Your organization probably has a VPN – Use it! No matter if you are at a coffee shop, the airport, another country, how can you trust your information is not being intercepted!

Other important protocols

- DNS – Port 53
- IKE/ISAKMP – 500
- RDP – 3389
- DHCP – 67,68
- Kerberos – 88
- LDAP - 389
- LDAPS – 636
- Syslog – 514
- SNMP - 161
- GRE – 1723
- PPTP - 47