Networking

Networking Fundamentals

1.5.2 - Protocols

What are some of the common protocols and how do they differ?

Overview

The student will explain common ports and protocols, their application, and encrypted alternatives

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 1.5

- Explain common ports and protocols, their application, and encrypted alternatives
    - IP protocol types
        - Internet Control Message Protocol (ICMP)
        - TCP
        - UDP
        - Generic Routing Encapsulation (GRE)
        - Internet Protocol Security (IPSec)
            - Authentication Header (AH)/Encapsulating Security Payload (ESP)
    - Connectionless vs. connection-oriented

Protocols

TCP vs UDP?

Data can be sent across a network using many different types of protocols, however, TCP and UDP are the two most common protocols out there. ***TCP***, or ***Transmission Control Protocol***, is more common than UDP and is meant for most websites, emails, file transfers, etc.… ***UDP***, or ***User Datagram Protocol***, is lesser used than TCP, but is faster and thus used for video conferencing, streaming videos, voice calls, etc… TCP and UDP are basic standards that define the rules of the internet and are included within the standards defined by the Internet Engineering Task Force (IETF)

TCP is a ***connection-oriented*** protocol while UDP is ***connectionless***. A connection-oriented protocol means that a connection will be made between two hosts and then data will be sent back and forth between the two hosts. This is sometimes referred to as the telephone system, where two phones will connect with each other and then start communicating back and forth. A connectionless protocol does not require a connection between the hosts to send data. This is sometimes referred to as a postal system, when mail is sent via the postal service, there is no connection between the sender and receiver (and the sender never gets notified when/if the package arrives).

Teacher Notes:

A connection-oriented service is constantly checking back and forth for errors, for example when a webpage is loading an image, the image needs to be loaded correctly, so it's checking to make sure everything was transmitted properly. This constant checking is what makes a connection-oriented service, like TCP, much slower than a connectionless service. If you think of video calls, sometimes the video will lag or cut out temporarily, this is because the video calls use the connectionless service, like UDP, which does not verify that packets were received correctly.

ICMP Traffic

ICMP, or Internet Control Message Protocol, is commonly used for a network to report problems with different services. For example, if a device is attempting to reach another device, but the packets are not able to reach the other device, ICMP will send a message back notifying that the device is unreachable. Two very popular command line tools, ping and traceroute, use ICMP traffic. Ping will send an echo request to another device on the network to check connectivity between the two devices while traceroute will trace the physical route between two hosts. Two other problems that ICMP reports are if a router's memory is full and/or if the max number of hops is reached when a device is attempting to reach another device.

GRE and IPSec

GRE (Generic Routing Encapsulation) is a protocol that allows for tunneling where many different types of protocols can be used inside this tunnel. This protocol was developed by Cisco and can be used with point-to-point tunneling and/or point-to-multipoint tunnels. Tunneling is commonly used with creating VNCs between two devices, although GRE does not encrypt data, thus it provides no security.

Like GRE, *IPSec (IP Security)* creates tunnels between two devices, however it provides security for these tunnels. Thus, the VPNs created with IPSec will have encrypted packets and would be safer to use over unsecure/untrusted networks. IPSec uses two main security protocols to protect their packets, the first is the *AH (Authentication Header)*. An AH provides data integrity using a checksum (hash) generated by an authentication code. If the hashes matches with the provided hash, they know that the data was not altered in transmission. Another security of IPSec is *ESP (Encapsulating Security Payload)*.

Teacher Notes:

ESP has five parts to it, the first being that the data is encrypted using different algorithms. The data also uses checksums to make sure that the data was not tampered with, there's an authentication part to make sure the data is being sent to the proper recipient. The protocol checks for replays, helping stop a replay attack where a malicious user will resend the same packets, and finally there's traffic flow that controls all the traffic and keeps outsiders from accessing it.