6.10.2 Protocol Analyzer Facts

A *protocol analyzer* is hardware or software for monitoring and analyzing digital traffic over a network. Protocol analyzers go by other names, such as *packet sniffers*, *packet analyzers*, *network analyzers*, *network sniffers*, or *network scanners*. A protocol analyzer is a passive device. It copies frames and allows viewing of frame contents, but does not allow the capture, modification, or retransmission of frames. This is referred to as *passive interception*. Use a protocol analyzer to:

- Monitor and log network traffic as it is transmitted over the network.
- Check for specific protocols on the network, such as SMTP, DNS, POP3, and ICMP. Identifying the traffic that exists on the network helps you to:
  - Identify devices that might be using unallowed protocols, such as ICMP, or legacy protocols, such as IPX/SPX or NetBIOS.
  - Identify traffic that might be sent by attackers.
- Identify frames that might cause errors. For example, you can:
  - Determine which flags are set in a TCP handshake
  - Detect any malformed or fragmented packets
- Examine the data contained within a packet. For example, by looking at the packet data, you can:
  - Identify users who are connecting to an unauthorized website
  - Discover cleartext passwords
  - Identify unencrypted traffic that includes sensitive data
- Analyze network performance
- Troubleshoot communication problems or investigate the source of heavy network traffic

A protocol analyzer shows the traffic that exists on the network and the source and destination of that traffic. It does not tell you if the destination ports on a device are open unless you see traffic originating from that port. For example, seeing traffic addressed to port 80 of a device does not automatically mean that port 80 on the firewall is open or that the device is responding to traffic directed to that port.

You typically run a protocol analyzer on one device with the intent of capturing frames for all other devices on a subnet. Using a packet sniffer in this way requires the following configuration changes:

- By default, a NIC will accept frames addressed only to that NIC. To enable the packet sniffer to capture frames sent to other devices, configure the NIC in *promiscuous mode* (sometimes called *p-mode*). In p-mode, the NIC will process every frame it sees.
- When using a switch, the switch will only forward packets to the switch port that holds a destination device. This means that when your packet sniffer is connected to a switch port, it will not see traffic sent to other switch ports. To configure the switch to send all frames to the packet sniffing device, configure *port mirroring* on the switch. With port mirroring, all frames sent to all other switch ports will be forwarded on the mirrored port.

If the packet sniffer is connected to a hub, it will already see all frames sent to any device on the hub.

When using a protocol analyzer, you can filter the frames so that you see only the frames with information of interest.

- Filters show only those frames or packets to or from specific addresses, or frames that include specific protocol types.
- A *capture* filter captures (records) only the frames identified by the filter. Frames not matching the filter criteria will not be captured.
- A *display* filter shows only the frames that match the filter criteria. Frames not matching the filter criteria are still captured, but not shown.
- Save the results of a capture to analyze frames at a later time or on a different device.

By themselves, protocol analyzers cannot be used to perform an attack. However, protocol tools can be used with protocol analyzers for *active interception* of network traffic to perform attacks such as:

- Spoofing
- Man-in-the-middle
- Replay
- TCP/IP session hijacking
- MAC flooding

Common protocol analyzers include:

- Wireshark
- Ethereal
- Dsniff
- Ettercap
- Tcpdump
- Microsoft Network Monitor