

Real-World Scenario 13-1: Capturing and Analyzing Packets

Scenario: You are doing work for a medium-sized business with several servers. There is concern that one of the servers is running a non-secured FTP service, and is possibly being used for non-work purposes. Your task is to analyze the traffic coming in and out of the server.

What technology should you use to analyze the traffic?

What are a few examples of this technology?

Which layer of the OSI model will tell you about the ports being used by applications?

Real-World Scenario 13-1 Solution

It's a good idea to periodically analyze the traffic that is sent and received by servers. This can help when you are concerned about a potential compromise or just think that the server is being used incorrectly.

A lot of technologies are used to analyze traffic, but the best for this scenario is the protocol analyzer, otherwise known as a network sniffer or packet sniffer. Examples of these tools include Wireshark, Network Monitor, TCPdump, and so on. Wireshark is extremely common and (as of the writing of this book) is a free download.

The transport layer of the OSI model tells all. It defines the port number being used on the source computer and the destination. It also describes the transport mechanism being used (TCP or UDP). The network layer is also important because it shows the IP addresses being used by the communicating systems. The application layer shows what program is being used, but many network and security admins will jump right to the transport layer and glean that information (and much more info) from the port numbers.

Video Solution: Watch the video solution "13-1: Capturing and Analyzing Packets."

Simulation: Complete the simulation "13-1: Capturing and Analyzing Packets."