Unit 4: Basic Network Investigation Using Standard Tools

Objective:

- Practice using built in utilities for network troubleshooting.
- Discuss the outputs produced by those tools.
- Read and discuss the paper in the reading list.

Outcome:

- Perform basic troubleshooting and investigations using the tools provided as part of common operating systems (tools such as ping, traceroute and so on).
- Analyze the outputs provided by the tools.
- Discuss the difference between TCP/IP and the ISO/OSI protocol stacks.

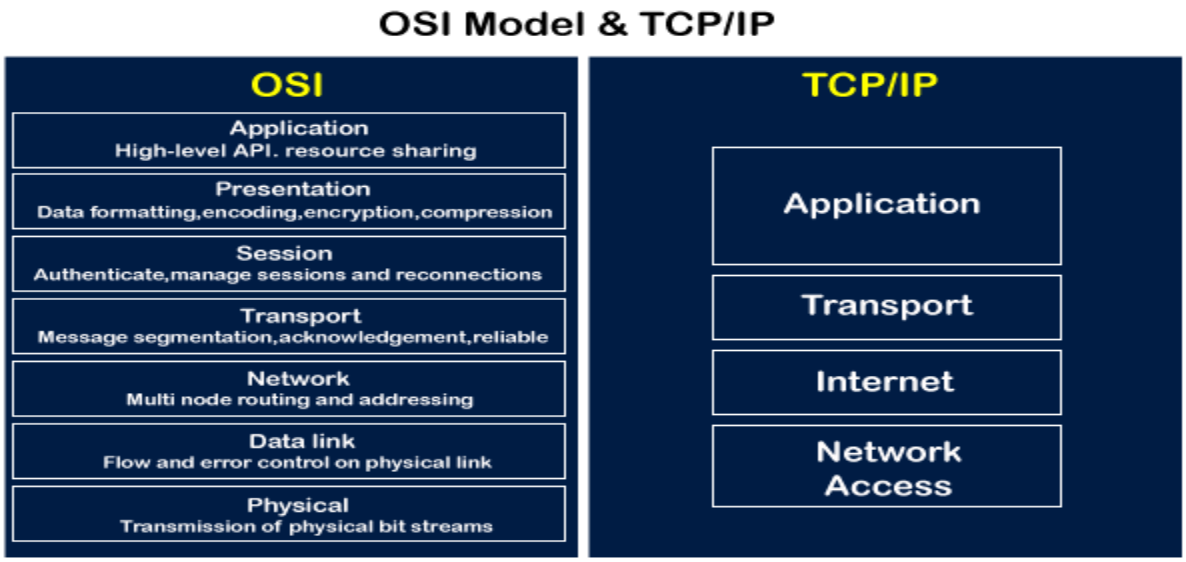
This unit provides an opportunity to learn more about network fundamentals by practicing using the basic, built in networking tools provided as standard with every computer system and discuss and analyses the output produced.

Reflection:

Network forensics is the process of collecting, recording, and analyzing network packets with the goal of determining the origin of a breach in network security. In a further step, network forensics entails the identification of patterns of penetration and the narrowing in on the particulars of an attack. It collects data from a variety of places and network devices, such as firewalls and intrusion detection systems, in order to perform an analysis of the data associated with network traffic. Network forensics may be applied both to avoid potential risks and to analyze those that may already exist LLC, L. (2020).

When examining a network, there are a total of seven procedures that must be completed, including locating and storing the evidence, gathering the evidence, evaluating the data, presenting the information, and reacting to occurrences. Here below we are explaining the network forensics tool working and flow. Investigators and administrators may use network forensic tools to look for suspicious or malicious activity on a network.

Ping is used for network troubleshooting program that comes standard with Windows. The majority of embedded network management applications as well as operating systems that are capable of using Ping as a tool for testing network reachability are referred to be Ping Network-capable. Ping is a program that measures the time length takes for messages to go from the computer that initiated them to the machine that received them and back again. Ping instructions, by default, will send out a large number of inquiries (usually between four and five), and will show the results of those requests. The results of an echo ping allow one to determine whether or not a request has been replied. The time-to-live metric is a measurement of both time it takes to get response and the number of bytes that were sent.



TCP/IP: TCP/IP, superseded Open Systems Interconnection Standards, a reference model that outlines how data is transported from one computer's software application to the software application of another computer through a physical channel. Each layer of the OSI model is responsible for a certain aspect of network operation Russell, A. (2013)

References:

LLC, L. (2020). *The Basics of Network Forensics*. [online] LIFARS, a SecurityScorecard company. Available at: https://www.lifars.com/2020/06/the-basics-of-network-forensics/ [Accessed 27 May 2022].

Russell, A. (2013) OSI: The Internet That Wasn't (How TCP/IP eclipsed the Open Systems Interconnection standards to become the global protocol for computer networking)