eJPT Certification

Section: Networking/Tools

08/18/2020

**Tool**: Wireshark

**Purpose**: Wireshark is a network sniffer and protocol analyzer. This mean that you can use it to analyze every packet, traffic stream, or connection that hits your computer network interface(s).

**Who uses it?** Widely used by network administrators, networking protocol researchers, and hackers.

**Notes**:

* Wireshark can capture all of the traffic seen by a network interface card on the computer running it.
  + Most network cards can run on promiscuous or monitor mode
* During normal operations a NIC discards any packet addressed to another NIC.
* Promiscuous mode
  + A NIC will accept and process any packet it receives.

Basic Capture Filters

A screenshot of a cell phone

Description automatically generated

Display Filters

A screenshot of a cell phone

Description automatically generated

Example Display Filters

A screenshot of a cell phone

Description automatically generated