Introduction of Assignment III

2 Oct, 2020

Pre-reading - network capture tutorial

Code

Task 1: Analyse flow data	
Tools	CoralReef, Netmate, Wireshark, TShark, tcpslice, tcpstat, tcptrace …
Step	Analyse sample pcap file and provide statics of the flow data: Total, mini, med, mean, max flow in bytes and packets
Data structure	
Analyse	Analyse sample pcap file and provide statics of the flow data: *total, mini, med, mean, max flow in bytes and packets *Top-10 host-pairs flow in bytes and packets *Plot flow number of 100 most common pairs of hosts with linear and log scale *Plot using time fixed size array Possible optimisation of the method
Hint	use /bin/time command to get resource consumption of a command, use -v for more verbose.

Task 2: Packet capture	
Tools	Private computer
Step	1. capture traffic and record interface counters and overall statistics at beginning and end of capture. (use pc in normal) – **1 h** 2. Same with 1, normal use and iperf3 test of iperf servers, ping test of iperf and research servers. (record iperf3 and ping result) **-15 min**
Data structure	
Analyse	Sanity check on the data: *Size of trace files *Packet number in trace file *Total size of packet *Value of interface counters and capture file

Task 3: Analyse captured traffic	
Tools	Private computer or SSH VM
Data structure	
Analyse	*How many IP (and IPv6 if any) hosts are communicating? *How many hosts were tried to contact to, but communication failed for a reason or another? Can you identify different subclasses of failed communications? *Top 15 hosts, byte counts. *Top 15 hosts, packet counts. *Top 10 TCP and top 5 UDP port numbers (packet count). *Top 10 fastest TCP connections *Top 10 longest (by time) TCP connections *Bit and packet rate over time (e.g. tcpstat)

Task 4: Compare ***active*** and ***passive*** measurements	
Tools	Private computer or SSH VM
Step	Extract information of iperf3 sessions. (flow tools in Task1 or tcptrace) Extract ICMP messages from traces (ping sessions), correlate requests to responses and calculate delay and identify possible packet loss.
Analyse	How much there was traffic that was not iperf or ping traffic? Compare iperf results from active and passive measurements. Provide a table. Compare ping results from active and passive measurements. Provide a table.