Network Security – Practical 2 Review

Dr. Sandra Scott-Hayward

CSC3064 Week 5 – Practical 2 Feedback

School of Electronics, Electrical Engineering and Computer Science

CSC3064 – Practical 2 Review – Tunneling

Lab2 Q1: Describe the difference(s) in the wireshark packet information between a ping via the tunnel and with no tunnel.

A1: A ping (ICMP packet) via the tunnel is appearing as a TCP packet on the network.

A ping (ICMP packet) across the network without the tunnel is appearing as an ICMP packet.

The ICMP packet is being transmitted via the tunnel and being masked as a TCP packet, whereas without the tunnel the packet type and contents are clear.

At the network interface (enp0s8), in both cases (with/without tunnel), the IP addresses that are seen in wireshark are the 192… addresses assigned to this interface. This means that the IP addresses at the endpoints of the tunnel (the 10…. Addresses) are hidden.

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Practical 2 Review – Tunneling

Lab2 Q2: The connection used in the simpletun program is a TCP connection. Why would it be better to use UDP in the tunnel, instead of TCP?

A2: UDP is faster than TCP because UDP does not offer error correction or flow control (remember the size/contents of the TCP header and the UDP header).

In the lab, you sent a ping (ICMP) via the tunnel. This was encapsulated (wrapped) in a TCP packet. If you sent TCP packets through the tunnel, then you would end up with 'TCP over TCP'.

If one TCP connection is stacked on top of another, the two layers have different timers (for retransmissions). With the timers out of sync, this can lead to one layer (e.g. TCP payload layer) queuing up retransmissions faster than the other layer (e.g. TCP tunnel layer) can process them.

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Practical 2 Review – Tunneling

Lab2 Q3: What is the average RTT for the ping via the tunnel? Note: RTT is round trip time. Comment on the difference in RTT with and without the tunnel.

A3: Average RTT with tunnel: approx. 39 ms

Average RTT without tunnel: approx. 0.3 ms

This is because of the use of TCP for the tunneling.

The encapsulation/decapsulation processes and the TCP transmission processes (e.g. flow control/packet acknowledgments) slow down the communication.

QUEEN'S UNIVERSITY BELFAST