1. What command is needed on the tunnel server to accept tunnelled messages on port 80 and send them to port 23 on the local host? Include the IP addresses that you used.

Sudo hts -F 192.168.21.129:23 80

1. What command is needed on the tunnel client to tunnel messages to and from port 2323 to and from port 80?

Sudo htc -F 2323 192.168.21.128:80

1. What did Wireshark interpret the tunnelled traffic as?

They would tunnel the traffic as telnet since the communication is tunnelled over port 80

1. How did the tunnelling software attempt to hide the traffic?

By using port 80 to make it look like a regular web traffic.

1. How might tunnelling of this kind be used to subvert security policy?

By disguising the actual nature of the traffic. In this scenario, its tunnelled through port 80, which might be allowed in many network as it’s a standard web port.