SWINBURNE UNIVERSITY OF TECHNOLOGY

TNE20003 – Internet and Cybersecurity for Engineering Applications

Introduction to Cybersecurity

Aims:

To understand the need for security and understand how to extract information from data capturing software.

Preparation:

View "Introduction to Cybersecurity"

Due Date:

Nil. In-class activity.

Using the lecture notes for week 9 please answer the following questions

rule 1: deny external hosts access inside SMTP server
rule 2: deny inside SMTP server response external hosts
rule 3: permit inside hosts access outside SMTP server
rule 4: permit external SMTP server response inside hosts
rule 5 deny any any

Question 1

What do the following set of packet filtering rules do?

Direction	Source address	Dest. Address	Protocol	Source port	Dest port	Action
In	External	Internal	TCP	>1024	25	Deny
Out	Internal	External	TCP	25	>1024	Deny
Out	Internal	External	TCP	>1024	25	Permit
In	External	Internal	TCP	25	>1024	Permit
Either	Any	Any	Any	any	Any	Deny

Question 2

Suppose we have a stateful packet filter firewall that validates the three-way handshake in a TCP connection

a. What states will the firewall record for each step of the three-way handshake?
b. Write packet filtering rules for each state.

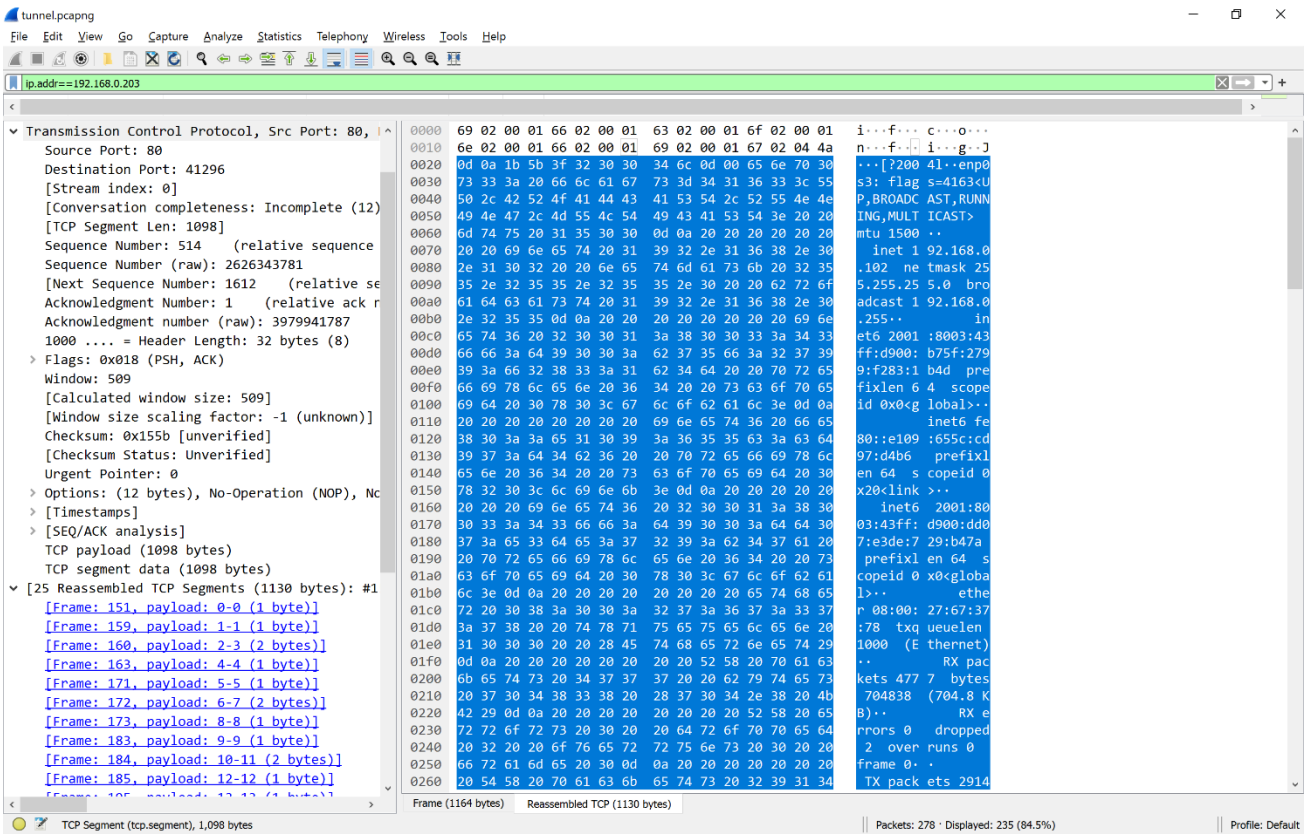
(For simplicity we do not consider direction or source address in answering this question).

Suggestion: Construct a table that has the following columns:

State	SYN set	ACK set	Action	New state

Question 3

Consider the following Wireshark extract between two hosts:



a. What port number is the source? 80 (http)

b. What application is this port number usually associated with? web page

c. Does the payload (highlighted in blue) match the port number?

d. What is the most likely explanation for what you see?

e. Would a packet filtering firewall block this packet? no

f. Would a stateful firewall block this packet?

g. Would a proxy firewall block this packet?

h. Would a deep packet inspection firewall block this packet? yes