CSS322 – Quiz 8 Answers

Name: _____

ID: _____ Mark: _____ (out of 10)

Question 1 [5 marks]

Consider the firewall table and Stateful Packet Inspection (SPI) table below and answer the questions. The firewall runs on a router with Interface 1 connected to the inside networks and Interface 2 to the outside networks.

Number	Interface	IPSrc	PortSrc	IPDest	PortDest	Protocol	Action
1	1	*	*	*	80	TCP	Allow
2	1	63.14.6.*	*	*	22	TCP	Allow
3	2	80.23.72.*	*	63.14.7.2	22	TCP	Drop
4	2	80.23.72.*	*	63.14.7.*	22	TCP	Allow
5	1	63.14.7.4	*	80.23.72.5	954	UDP	Allow
6	2	80.23.72.5	954	63.14.7.4	*	UDP	Allow
7	*	*	*	*	*	*	Drop

The SPI table is only used for TCP connections.

Number	Initiator IP	Initiator Port	Responder IP	Responder Port	State
8	63.14.6.28	31101	120.16.4.5	80	Established
9	63.14.7.2	40331	80.23.72.5	80	Established
10	63.14.6.1	32054	120.16.4.5	22	Established

For answers, circle YES or NO and give the Row Number that matches from which you determined the answer.

a) Can internal hosts connect to external web servers? **YES** NO Num. **_80___**

b) Can host 63.14.7.4 connect to a Secure shell server at 120.16.4.5? YES **NO** Num.**_7___**

c) Will a UDP packet with source IP address 80.23.72.5, destination IP address 63.14.7.4 and source port 954 be dropped? YES **NO** Num **_6_____**

d) Will a TCP packet with the following details be dropped? **YES** NO Num**_7__**

   - IPSrc = 120.16.4.5, PortSrc = 80; IPDest = 63.14.7.2, PortDest = 32054

e) Will a TCP packet with the following details be dropped? YES **NO** Num**_8___**

   - IPSrc = 120.16.4.5, PortSrc = 80; IPDest = 63.14.6.28, PortDest = 31101

Question 2 [2 marks]

Explain the difference between a metamorphic and polymorphic virus.

Answer

When a polymorphic virus copies the original virus to create a new virus, the new virus appears different than the original, but functions the same. For a metamorphic virus, the new virus both appears different and functions differently.

Question 3 [3 marks]

[Note: 1 mark for correct; 0 marks for no answer; -1 mark for wrong answer]

A malicious user has found a program with a function on which a buffer overflow attack may be performed.

a) One aim of the malicious user is to overwrite the current value of the Instruction Pointer with a new value that points to the memory address of the malicious code. **TRUE** FALSE

b) A buffer overflow attack can be performed by passing the source code of the malicious program as a command line argument to the original program. TRUE **FALSE**

c) The malicious user must know the exact position in memory the malicious program is inserted in order to set the new Instruction Pointer. TRUE **FALSE**