COMP435 In-Class Practice 11/11/26 Name: _____

Rule	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action
A	In	External	Internal	TCP	> 1023	25	Any	Allow
B	Out	Internal	External	TCP	25	> 1023	Yes	Allow
C	Out	Internal	External	TCP	> 1023	25	Any	Allow
D	In	External	Internal	TCP	25	> 1023	Yes	Allow
E	Either	Any	Any	Any	Any	Any	Any	Deny

Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action (rule)
1	In	121.12.1.2 (ext)	222.2.2.2 (int)	TCP	25	8080	Yes	?? (?)

Question 1: Packet Filters 1.1. What is the action taken by the packet filter (Allow/Deny) and which rule is applied (A-E)?

1.2. Now consider packet 2. What is the action taken and which rule is applied?

Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action (rule)
2	In	121.12.1.2 (ext)	222.2.2.2 (int)	TCP	5051	25	Yes	?? (?)

1.3. Now consider packet 3. What is a reasonable assumption about this packet?

Packet	Dir	Src Addr	Dest Addr	Prot	Src Port	Dest Port	ACK Set	Action (rule)
3	In	121.12.1.2 (ext)	222.2.2.2 (int)	TCP	25	5055	Yes	?? (?)

- ◯ It is accessing an internal web server.
- ◯ Someone inside the organization is sending mail to someone outside
- ◯ Someone outside the organization is sending mail to someone inside

Question 2: Intrusion Detection Systems An organization installed a new intrusion detection system. The IDS boasts the following:
TPR = 99%
TNR = 98%
On a typical day the organization's network will see 50,000 events, 2 of which are intrusions. How many alarms will be raised?

Question 3: More Intrusion Detection An organization installed a new intrusion detection system. On a typical day the organization's network will see 50,000 events, 2 of which are intrusions, and the IDS will raise 100 alarms. Assuming both intrusions are detected, what is the alarm precision of the IDS?