Sample Questions and Answers for CPRE 431 Final Exam

If an answer for a question is not provided, this means that the answer is straight forward and you can find it in the slides or in the provided homework solutions.

1. An IPS permits and blocks traffic by port/protocol rules.
   a. True
   b. False

2. From a security point of view, it is recommended to set the default rule of the firewall to
   a. Deny
   b. Permit

3. In 2G (GSM), the network, i.e., the BS, authenticate's the UE only, however, in 3G and beyond, the network authenticates the UE and the UE authenticates the network
   a. True
   b. False

4. Based on the U.S. legal system, Intellectual Property (IP) is an intangible asset that consists of human knowledge and ideas.
   a. True
   b. False

5. List (without explanation) three issues related to GSM security

6. Briefly explain what is SecaaS.

7. Answer the following questions:

   a. What are the two possible default policies of packet filtering firewalls?

   Answer. Accept, drop

   b. Explain which default policy from part (a) is recommended and why.

   Answer. Drop. If the firewall administrator makes a mistake when configuring the firewall (e.g. they forget to add a rule), with a drop policy then most likely that means packets that would normally be accepted will be dropped. This may cause inconvenience to normal users, but is unlikely to be a security violation. However, if the accept policy is used, then it means packets that would normally be dropped will be accepted. This may lead to a security violation.

   c. Explain how Stateful Packet Inspection (SPI) is used with a packet filtering firewall. Include in your explanation of how an SPI table is created and how it is used.

Answer. When a rule in the firewall table accepts an incoming connection (e.g. a TCP SYN packet), then an entry is added to the SPI table identifying the connection (e.g. IP address pair, port pair). Then, any subsequent packets belonging to that connection (e.g. TCP SYN/ACK in reverse direction, TCP ACK and TCP data packets) will be accepted without consulting the firewall table.

d. Assume ISU has a correctly configured firewall that prevents external users from accessing unauthorized services inside ISU, prevents internal users from accessing unauthorized services outside ISU, and stops malicious content (e.g. viruses) from entering ISU. The firewall runs on the single router that connects ISU's internal network to the internet. Consider the limitations of firewalls. Even with the firewall correctly configured, explain one method in which:

i. An internal user may access unauthorized external services.

Answer. Internal users could use alternative Internet connections (e.g. mobile phone) which the firewall does not control. Internal users could use tunneling to bypass the firewall.

ii. Malicious content can still enter ISU.

Answer. If internal users use alternative Internet connections, malicious content will not be blocked by the firewall. Similarly, if internal users use media (CD, USB) with malicious content, then it can be loaded onto internal computers.

e. Explain both an advantage and a disadvantage of using two firewalls with the DMZ, as opposed to using just a single firewall.

i. Advantage of using two firewalls:

Answer. Much easier to set up rules on firewalls (less likely for mistakes) as the first firewall must direct all incoming traffic to the DMZ; no need to create rules that allow traffic to selected internal computers. Similarly, the second firewall will block all traffic originating from outside; it only accepts incoming traffic if it is a response to requests originating from inside.

ii. Disadvantage of using two firewalls:

Answer. Require extra cost/resources; more to administer.

8. Answer the following questions

SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

Rule	Direction	Scr Addr	Dst Addr	Protocol	Dst Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

a. Describe the effect of each rule.

  i. Rules A and B ➔

  ii. Rules C and D ➔

  iii. Rule E ➔

b. Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume that a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are as shown:

  i. Indicate which packets are permitted or denied and which rule is used in each case.

Packet	Direction	Scr Addr	Dst Addr	Protocol	Dst Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	
2	Out	172.16.1.1	192.168.3.4	TCP	1234	
3	Out	172.16.1.1	192.168.3.4	TCP	25	
4	In	192.168.3.4	172.16.1.1	TCP	1357	

c. Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Typical packets are as -follows:

  i. Will the attack succeed? Give details.

Packet	Direction	Src Addr	Dst Addr	Protocol	Dst Port	Action

5	In	10.1.2.3	172.16.3.4	TCP	8080	
6	Out	172.16.3.4	10.1.2.3	TCP	5150	

d. To provide more protection, the rule set from the preceding problem is modified as follows:

Rule	Direction	Src Addr	Dst Addr	Protocol	Src Port	Dst Port	Action
A	In	External	Internal	TCP	>1023	25	Permit
B	Out	Internal	External	TCP	25	>1023	Permit
C	Out	Internal	External	TCP	>1023	25	Permit
D	In	External	Internal	TCP	25	>1023	Permit
E	Either	Any	Any	Any	Any	Any	Deny

i. Describe the change.

e. Apply this new rule set to the same six packets of the preceding problem. Indicate which packets are permitted or denied and which rule is used in each case.

Packet	Direction	Scr Addr	Dst Addr	Protocol	Dst Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	
2	Out	172.16.1.1	192.168.3.4	TCP	1234	
3	Out	172.16.1.1	192.168.3.4	TCP	25	
4	In	192.168.3.4	172.16.1.1	TCP	1357	

Packet	Direction	Src Addr	Dst Addr	Protocol	Dst Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	
6	Out	172.16.3.4	10.1.2.3	TCP	5150	

f. A hacker uses port 25 as the client port on his or her end to attempt to open a connection to your web proxy server.

i. The following packets might be generated:

Explain why this attack will succeed, using the rule set of the preceding problem.

Packet	Direction	Src Addr	Dst Addr	Protocol	Src Port	Dst Port	Action
7	In	10.1.2.3	172.16.3.4	TCP	25	8080	
8	Out	172.16.3.4	10.1.2.3	TCP	8080	25	

Answer: Packet 7 is admitted under rule D. Packet 8 is admitted under rule C.

Note that this question is the same as the homework question except that part (f) is new