**Sample Questions for CPRE 431 Final Exam**

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

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

1. 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
   1. True
   2. False

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

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

1. Briefly explain what is SecaaS.

1. Answer the following questions:

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

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

* 1. 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.

* 1. 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:  
       
     1. An internal user may access unauthorized external services.

* + 1. Malicious content can still enter ISU Network.

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

* + - 1. Advantage of using two firewalls:

* + - 1. Disadvantage of using two firewalls:

1. 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 |

* 1. Describe the effect of each rule.

* + 1. Rules A and B è

* + 1. Rules C and D è

* + 1. Rule E è

* 1. 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:
     1. 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 |  |

* 1. 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:
     1. 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 |  |

* 1. 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 |

* + 1. Describe the change.

* 1. 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 |  |

* 1. 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.
     1. 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 | 5150 |  |

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