|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Student name  |  | ID  |  |  Section No |  |

**Question#1: 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**

****

1. **Describe the effect of each rule.**

**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**

****

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

**c. Someone from 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:**

****

**Will the attacker succeed? Give details.**

 **\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Question#2: Assume that passwords are selected from six-character combinations of 36 alphanumeric characters. Assume that an adversary requires 2 seconds to complete one attempting.**

1. **Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?**

 **b. Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Extra Credit Question: [ ONLY for students who did not participate in class or did not get full mark on the previous sheets]**

**Consider an attack using ICMP echo request (ping) packets that are 700 bytes in size (ignoring framing overhead).**

1. **How many of these packets per second must the attacker send to flood a target organization using a 200 -Kbps link?**
2. **How many of these packets per second if the attacker uses a 0.02 -Gbps link?**

**Good Luck**