EECS 565 Homework 4

Network Security

1. Assume an attacker controls a large botnet. He wants to attack a victim web server.

    1) First, he wants to use the TCP SYN flooding attack. Please describe how this attack works.

    2) Suppose the victim web server uses SYN cookies to protect itself. Will the attack still succeed? Why or why not.

    3) The attacker then wants to use the TCP flooding attack. Will this attack work? Why or why not.

2. What is amplification DDoS attack? Choose one UDP-based amplification attack as an example to explain how it is amplified.

3. Link-to-link encryption and end-to-end encryption can be used to protect data transmitted over networks. Which means is used by VPN?

4. What security services are provided by TLS? Choose one attack and explain how TLS prevents it.

5. What security services are provided by IPsec? Choose one attack and explain how IPsec prevents it. Can it also be prevented by TLS?

Firewall and IDS

6. The below table shows a packet firewall ruleset that allows inbound and outbound SMTP traffic.

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest 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) Please describe the effect of each rule.

2) Someone tries to send email from a remote host with IP address 192.168.3.4 to a host with IP address 172.16.1.1. Meanwhile, a user on the host may send e-mail to the SMTP server on the remote system. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on the host consisting of SMTP commands and mail. Decide if the following packets should be permitted or denied, and which rule applies.

Direction	Src Addr.	Dest Addr.	Protocol	Dest Port	
Packet 1:	In	192.168.3.4	172.16.1.1	TCP	25
Packet 2:	Out	172.16.1.1	192.168.3.4	TCP	1234
Packet 3:	Out	172.16.1.1	192.168.3.4	TCP	25
Packet 4:	In	192.168.3.4	172.16.1.1	TCP	1357

3) If an attacker (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 the local hosts (172.16.3.4), will the attack succeed?

7. Describe the differences between NIDS and HIDS. Can they be combined?

8. In the context of IDS, describe the meaning of false positive and false negative. If we have two IDS systems, IDS1 is less specific and IDS2 is more specific. Compare the alert rates of false positives in two systems. How about false negatives?