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

1. He wants to use the TCP SYN flooding attack. Please describe how this attack works.
   * TCP SYN flooding uses large number of TCP data packets that do not belong to known connections.
   * The attacker sends a large number of TCP SYN packets to the victim web server, with the aim of consuming its network bandwidth and resources.
   * The web server will respond to each SYN packet by sending a SYN-ACK packet back to the source IP address.
   * This will cause the target system to continuously wait for the response to the SYN packets, that will never arrive.
   * The web server will be overwhelming the system with trafic and will not be able to respond to legitimate requests.
   * The attacker can also use spoofed IP adresses in order to make the attack more difficult to trace.
   * The attacker can take down the web server when the number of SYN packets is large enough.
2. Suppose the victim web server uses SYN cookies to protect itself. Will the attack still succeed? Why or why not?
   * The answer is yes, the attack can still succeed.
   * SYN cookies will make the web server less vulnerable to SYN flood attacks. Make it harder for the attacker to take down the web server. But it is possible for the attacker to overwhelm the server’s network bandwidth or other resources, which can result in a denial of service.
   * So if the attacker has enough resources that can overwhelm the server’s network bandwidth, the attack can still succeed.
3. The attacker then wants to use the TCP flooding attack. Will this attack work? Why or why not?
   * The answer is yes, the attack will work.
   * While SYN cookies can prevent the server from becoming overwhelmed by half-open connections, they do not necessarily protect the server from the volume of traffic generated by a TCP flooding attack.

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

* Amplification DDoS attack is a type of DDoS attack that relies on amplification factor to increase the amount of traffic sent to the victim.
* DNS amplification attack: is a UDP-based amplification attack
  + Selects a large number of legitimate DNS serves as intermediary amplifiers.
  + Creates a series of DNS requests to containing the spoofed source address of the victim.
  + Send the requests to the selected DNS servers.
  + This will cause amplification by increasing the size of the response packets.

### 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?

* VPN uses end-to-end encryption to protect data transmitted over networks. Since link-to-link encryption only protects data transmitted over a single link.
* VPNs use link encryption between the end-user and VPN server.

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

* TLS provides the following security services:
  + Confidentiality: TLS uses symmetric encryption to provide confidentiality.
  + Integrity: TLS uses HMAC to provide integrity.
  + Authentication: TLS uses digital signatures to provide authentication.
  + Replay protection: TLS uses sequence numbers to provide replay protection.
  + Perfect forward secrecy: TLS uses Diffie-Hellman key exchange to provide perfect forward secrecy.
* Eavesdroppers
  + TSL uses a combination of symmetric and asymmetric encryption algorithms to encrypt the data and ensure that only the intended recipient can decrypt 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?

* IPsec provides the following security services:
  + Confidentiality: IPsec construct a secure channel upon the IP layer to provide confidentiality.
  + Integrity: IPsec uses HMAC to provide integrity.
  + Authentication: IPsec uses digital signatures to provide authentication.
  + Replay protection: IPsec uses sequence numbers to provide replay protection.
  + Perfect forward secrecy: IPsec uses Diffie-Hellman key exchange to provide perfect forward secrecy.
* Man in the middle attack:
  + IPsec use digital certificates or pre-shared keys as a way to authenticate the communicating parties. Once both endpoint have been authenticated, they can use the Diffie-Hellman key exchange to generate a shared secret key. This key is used to encrypt and decrypt the data.
  + Yes, TLS can also prevent this attack. TLS also uses digital certificates or pre-shared keys as a way to authenticate the communicating parties to prevent this attack. ## Firewall and IDS ### 6. The table below shows a packet firewall ruleset that allows inbound and outbound SMTP traffic.

| Rule | Direction | SRC Address | 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 | Internal | Internal | TCP | >1023 | Permit |
| E | Either | Any | Any | Any | Any | Deny |

1. Describe the effect of each rule.
   * Rule A: Allow inbound SMTP traffic from external sources to internal servers is permitted through TCP port 25.
   * Rule B: Allow outbound SMTP traffic from internal sources to external server is permitted to use any TCP port number above 1023.
   * Rule C: Allow inbound SMTP traffic from internal sources to external server is permitted through TCP port 25.
   * Rule D: Allow outbound SMTP traffic from external sources to internal server is permitted to use any port number above 1023.
   * Rule E: Deny all other traffic.
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.

| Packet | Direction | SRC Address | Dest Address | Protocol | Dest Port |
| --- | --- | --- | --- | --- | --- |
| 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 |

* From: 192.168.3.4
* To : 172.16.1.1
* Packet 1: Allow, Rule A
* Packet 2: Allow, Rule B
* Packet 3: Allow, Rule C
* Packet 4: Allow, Rule D

1. 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?

* Packet 1: A TCP packet from 10.1.2.3 to 172.16.3.4 and port 8080 will be allowed by D;
* Packet 2: A TCP packet from 172.16.3.4 to 10.1.2.3 and port 5150 will be allowed by B.
* So, the attack will succeed.

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

* NIDS is a network-based intrusion detection system that monitors and analyzes network traffic for suspicious activity.
* HIDS is a host-based intrusion detection system that monitors and analyzes the internals of a computing system as well as the network packets on its network interfaces.
* Yes they can be combined. Since NIDS and HIDS have different roles in monitoring and analyzing network and host activity, and can be combined to provide a more comprehensive approach to intrusion detection and prevention.

### 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?

* False positive: is an alert that incorrectly indicates that some attack is taking place.
* False negative: is an alert that fails to indicate that some attack is taking place.
* IDS1 is less specific, so it will have a higher chance of generating false positive alerts.
* IDS2 is more specific, so it will have a higher chance of generating false negative alerts.
* This mean IDS1 will generating more alerts, some of which will be false alarms, while IDS2 will generate fewer alerts, but they are more likely to be true alerts. However, IDS2 is more likely to miss potential attacks than IDS1.