網路安全 Network Security

Final

111061548 游鎮遠

1.

(a) Suppose an opponent captures an unexpired service granting ticket and modifies its network address to match that of the valid user. Is it correct that the opponent will be granted access to the corresponding service.

False. If an adversary captures an unexpired service grant ticket and modifies its network address, it is unlikely to gain access. For example, Kerberos uses a ticket-granting ticket (TGT) that contains the client's network address, and modifying it will invalidate the ticket.

(b) If the lifetime stamped on a ticket is very short (e.g., minutes) an opponent has a greater opportunity for replay.

True. If the lifetime of the tag on the ticket is short, there is a greater chance of a replay attack. Short-lived tickets limit the window of time for attackers to capture and reuse them.

(c) User certificates generated by a CA need special efforts made by the directory to protect them from being forged.

False. User certificates generated by a Certificate Authority (CA) are inherently secure, and the directory doesn't need special efforts to protect them from being forged. The CA's role is to verify and validate the identity of the certificate holder.

(d) In IPsec, authentication must be applied to the sections of the original IP packet.

True. In IPsec, authentication is applied to the entire original IP packet. This ensures the integrity and authenticity of the entire package, not just specific parts.

(e) The principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level.

True. The primary function of IPsec is the ability to encrypt and/or authenticate all traffic at the IP level, thus providing a comprehensive security solution.

(f) A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall but also records information about TCP connections.

True. Stateful packet inspection firewalls inspect the same packet information as packet filtering firewalls, but also maintain information about the status of active connections. This allows it to make more informed decisions about whether to allow or block packets.

(g) Packet filter firewalls examine upper layer data therefore they can prevent attacks that employ application specific vulnerabilities or functions.

False. Packet filtering firewalls examine lower-layer data, such as IP addresses and port numbers, and cannot prevent attacks that exploit application-specific vulnerabilities or features.

(h) The change cipher spec protocol exists to signal the transition in ciphering strategies.

True. The Change Cipher Specification protocol in SSL/TLS is used to signal encryption policy transitions during a secure connection.

(i) Transport mode in IPSec provides security to the entire IP packet.

False. In IPsec, transport mode provides security for the upper-layer protocol (such as TCP or UDP) rather than the entire IP packet. Tunnel mode is a mode that provides security for the entire IP packet.

(j) In tint fragment attack, it is possible for an intermediate fragment to pass through filter before the initial fragment is rejected.

True. In a fragment attack, an intermediate fragment may pass the filter before the initial fragment is rejected, which may cause security issues. This is a question in the context of cybersecurity.

2.

This can be done by sharing some number between Alice and Bob.
Let a number c is shared between Alice and Bob.
c should not be shared with s.

Now, Alice can share $(a\oplus c)$ with s but not to Bob.
Similarly, Bob can share $(b\oplus c)$ with s but not to Alice.
So, Now s know $(a\oplus c)$ and $(b\oplus c)$.
s can calculate $(a\oplus b) = (a\oplus c)\oplus(b\oplus c)$.

So s can calculate $(a\oplus b)$ with satisfying all constraints.

3.

(a)

i. A Requests a Session Key from KDC:

A initiates the protocol by sending a request to KDC.

A includes its identity (IDA), the identity of B (IDB), and a nonce (N1) in the request.

ii. KDC Responds with a Ticket:

KDC responds to A's request by encrypting a message with A's key (ka).

The encrypted message includes a session key (ks), the identity of B (IDB), the nonce from A (N1), and a nested encryption of the same session key (ks) along with A's identity (IDA) using B's key (kb).

iii. A Sends an Encrypted Message to B:

A, having received the ticket from KDC, sends an encrypted message to B.

The message includes the session key (ks), A's identity (IDA), and is encrypted using B's key (kb).

iv. B Responds with a Nonce:

B decrypts the message from A using its key (kb) to obtain the session key (ks) and A's identity (IDA).

B generates a new nonce (N2) and sends it back to A encrypted with the session key (ks).

v. A Sends a Function of the Nonce to B:

A sends a message to B, which includes a function (f) applied to the nonce (N2).

The message is encrypted using the shared session key (ks).

(b) Yes, this protocol is vulnerable to attacks . Like if an intruder somehow obtained the old key K, he or she could replay the message to B by pretending to be sender A.

(c) Since this is a vulnerability in the protocol, we can append a timestamp to messages sent over channels that may be vulnerable to attacks.

4. Configuring the Encapsulating Security Payload (ESP) protocol before the Authentication Header (AH) protocol is recommended in IPSec for several reasons:

Confidentiality First:
ESP provides data confidentiality primarily through encryption. By setting up ESP first, you can ensure that the payload data is encrypted before any other authentication measures are applied. This helps protect sensitive information from unauthorized access.

Flexibility in Security Associations (SA):
IPSec allows the combination of security associations so that ESP and AH can be used simultaneously. It allows for a more flexible approach when configuring ESP first. Depending on specific security requirements, users can choose to enable confidentiality, authentication, or both for a specific SA.

Adaptability to Varying Security Needs:
Different communication scenarios may have varying security needs. Configuring ESP before AH allows for the adaptation to specific requirements, providing the option to prioritize data confidentiality when needed. This adaptability is especially crucial in scenarios where privacy and encryption take precedence over authentication

.

Enhanced Efficiency:
ESP encompasses both encryption and authentication functionalities, making it a comprehensive choice for securing communication. Configuring ESP first reduces the need to implement additional authentication measures immediately, improving efficiency in the communication process.

Minimizing Overhead:
In scenarios where the primary goal is to secure data confidentiality, configuring ESP before AH minimizes the overhead associated with performing authentication on every packet. AH-style authentication covers the entire IP packet, including the outer IP header, which may be unnecessary if data confidentiality is the primary concern.

Alignment with Common Use Cases:
Many common use cases prioritize encryption for data privacy. By configuring ESP first, the protocol aligns with the typical requirements of secure communication, making it a logical and widely accepted practice.

In summary, configuring ESP before AH in IPSec is recommended to prioritize data confidentiality, provide flexibility in security associations, adapt to varying security needs, enhance efficiency, and minimize unnecessary overhead associated with authentication when it may not be the primary focus of the communication.

5. There are three types of SSH port forwarding:

Local port forwarding: Redirects traffic from a local port on the client machine to a specified port on a remote server via an SSH connection.

Remote port forwarding: Redirects traffic from a port on the remote server to a specified port on the client machine.

Dynamic port forwarding: Creates a SOCKS proxy on the client machine, enabling the forwarding of traffic from various applications through the SSH connection.