Computer Security - IV10113

Quiz 2

1,

Masquerade - An individual who is not authorized to use the computer and who exploits a legitimate user's account.

Misfeasor - is a legitimate user who access data, programs or resources for which such access is not authorized.

Clandestine - is a user who seize supervisory control of the system (can be both a insider or outsider)

2,

Q. What is ARP spoofing?

A. A man-in-the-middle attack against ARP.

3,

Q. The IPsec standards define two modes of use. Which are these IPsec modes?

A. Transport mode and tunnel mode

4,

Q. Which of the following statements about security associations are correct?

A. The SA specifies what cryptographic algorithm to use.
The SA can be manually configured.

5,

Q. What does IP spoofing mean?

A. That an attacker sends an IP packet with a fake source address.

6,

Q. Which of the following pieces of information must you supply when creating a policy that configures IPsec to use tunnel mode between two routers over the Internet?

A. The IP address of the router at the far end of the tunnel

7,

Q. Secure tunneling is a technique in which the IP datagram is first **ENCAPSULATED** and then **ENCRYPTED**.

A. Encapsulated in another datagram; encrypted

8,

Q. You use a URL that starts with "https:" to contact a web server. What assumptions are reasonable to make about the communication with the web server?

A. The server is authenticated.
The communication with server is confidential.
The communication is integrity protected.

9,

Q. Which of the following actions are reasonable ways to try to deal with IP spoofing?

A. Block incoming packets from the external network with source addresses belonging to the internal network.

Block outgoing packets from the internal network with source addresses from outside the internal network

---

10,

Q. Which of the following statements about the capabilities and configuration of firewalls are true?

A. When a firewall has the "Default discard" policy, it needs to be explicitly configured for each service or destination that you want the firewall to allow.

When a firewall has default forward policy you typically do not need to change the configuration when you want to use a new service from your protected network (everything not expressly prohibited is permitted)

Application level gateway firewalls can support applications using TCP as well as applications using UDP

11,

Q. Which of the following statements about TCP vulnerability is (most) correct?

A. TCPs way of establishing connection makes it vulnerable to a denial of service attack(TCP SYN attack)

12,

Q. Which one of the following is *not* an example of a well-known TCP attack?

A. TCP FIN flooding

13,

Q. You set up a connection to a web server with your browser, and as part of this process, the web server sends its certificate. What information can you find in the certificate?

-domain name
-name of the CA that issued the certificate
-the certificates expiration date
-the servers public key
- A globally unique serial number

14,
Q. One of the following statements about packet filter firewalls is true. Which one?

A. Packet filter firewalls can block or allow packets based on information both in the IP header and in the transport level header.