Chapter 7

2. d
4. b
6. d
8. b
10. c
12. a
14. c
16. d
18. a
20. c

Chapter 8

1.a
3. c
5. c
7. b
9. c
11. c
13. b
15. c
17. b
19. d

Case Project 7-2: Securing Email

Option	**Advantage**	**Disadvantage**
SSL (Secure Socket Layer): An application layer protocol. It encrypts data sent between two computers via the internet. TCP initiates the handshake when an email is sent or received. During this step, the client informs the server of the SSL version and compression methods.	1. The authentication ensures that no third party can access the data. 2. Payment gateways employs SSL encryption to create a secure connection for users to enter personal information.	1. An additional server is required to handle complicated proxy (caching systems). 2. It is complicated to set up and requires additional modules.
TLS (Transport Layer Security): It works in the same way as SSL, but it has more	TLS provides privacy and data integrity between two or more computer applications. It replaces	Complex network topology requiring strategies like load

powerful security measures and hence is preferred. TLS-based encryption ensures email message integrity.	the outdated Secure Sockets Layer (SSL) and provides network communication security. Many applications use the protocol, but its use as the Security layer in HTTPS is the most noticeable.	balancing to accommodate heavy website traffic.
STARTTLS: It is a server-to-server email protocol that tells the insecure web browser's email client and server to change to secure connections. The service provider implements it. When using STARTTLS for encryption, TLS is used for incoming SMTP.	It establishes an SSL connection over an existing SMTP connection, which is more efficient than SMTP.	**Because there is a middleman between the sender and the receiver, it is vulnerable to man in the middle attacks.**
MIME (Multipurpose Internet Mail Extension): It's an email encryption mechanism that uses a certificate. The MIME email certificate's public key informs the user about encryption.	Adds five additional SMTP extensions. It also has a field-value paired structure that ensures the message is only received by the intended recipient.	Compound formats are sometimes mistaken for applications.
PGP: It uses email encryption but does not use email certificates.	The middleman cannot modify the information provided and received, and the verification prevents spoofing by third parties.	It is sophisticated and has no recovery issues.

I recommend TLS for email encryption. TLS is safer than SSL. It avoids the man-in-the-middle attack of STARTTLS. In addition, TLS offers server and client authentication, validating the identities of all parties participating in the conversation. It works with most web browsers and OS. Besides, it alerts the sender and receiver about the session started during message transmission and defines the type of certificate to be sent between them. So, it's the best approach for email encryption.

Case 8-2

Mouse Jack is one of the assaults that employs remote mice and consoles, and it has been used to attack and trade off a variety of remote devices. Interlopers launch remote attacks on these distant frameworks, culminating in a total PC bargain.

The attacks are expected to mock the mouse, the console, and the blending power. This attack will occur at a distance of 345 feet, and in most cases, the remote dongle has been compromised and the infection has been transferred via it.
The flaw exploits both the entire framework and the organization to which the framework has been assigned. To ensure that the devices are functioning properly. It is best to unplug the dongle, mouse, and console after each use, and to use wired devices rather than wireless ones, as this minimizes the possibility of attacks to some amount. As a result, it is critical to always verify the dongle and remote devices thoroughly before using them.