Rupesh Dharme
31124

Assignment 12

Title: Study of SSL

problem statement:
To study the SSL protocol by capturing packets using wireshark but while visiting an SSL secure website. To study IPsec and protocol by capturing data packet in wireshark.

prerequisites:
knowledge of protocols and wireshark

learning objective:
learn use and importance of SSL

Theory:

a) SSL stands for ~~socket to socket~~ secure socket layer

b) It is an encryption method used to prevent anyone other than a webserver and user from was dropping on the transmission of sensitive personal or financial information

c) This encryption can secure a connection between website and a browser or client.

d) Integrating SSL into webpage improves security by reducing the risk of identity theft.

31124

SSL certificates

a) They are an essential and component of the data encryption process that make-internet tronsotions secure

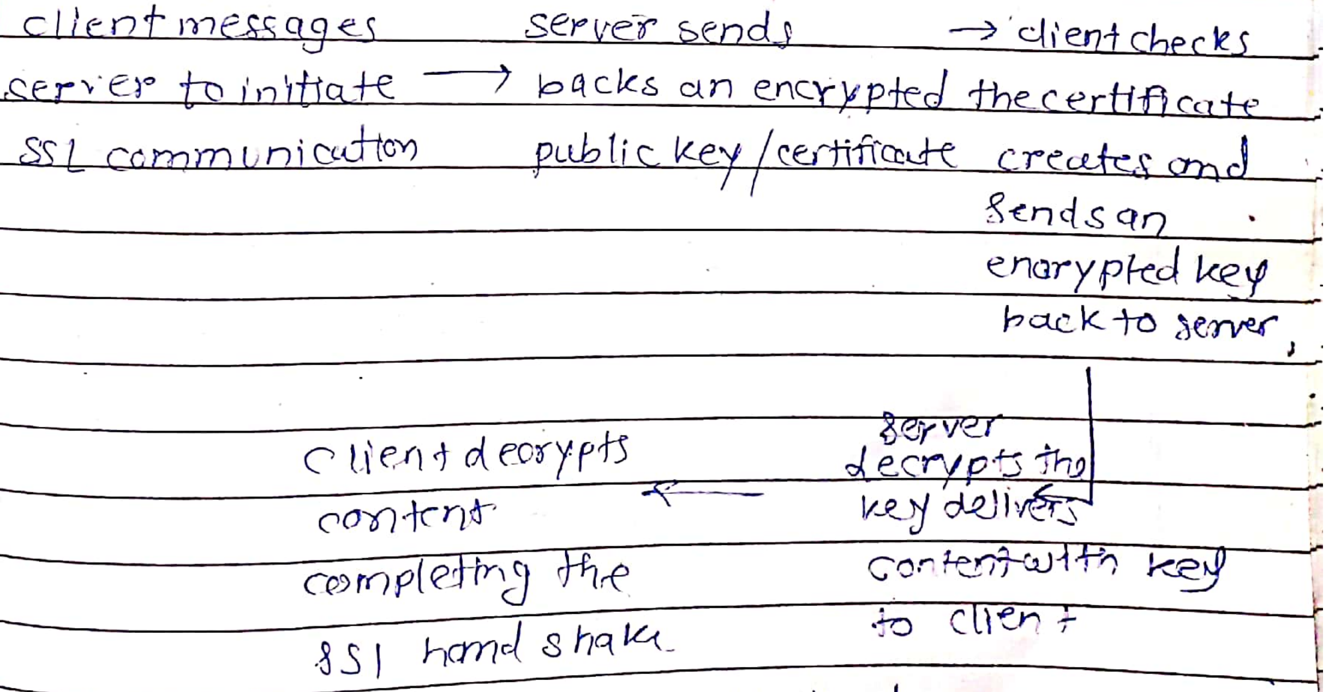
b) They are digital passports that provide authentication to protect the confidentially 4 integrity of website communication with browsers

c) The SSL certificates job is to initiate secure sessions with user's browser via the secure sockets layer (SSL) protocol

d) This secure connection cannot ie established without SSL certificate, which digitally connects company information to a cryptographic key

e) Any organisation that engages in ecommerce must have an SSL certificate on its webserver to ensure safety of customer and company information as well as the security of financial transactions.

working



client messages server to initiate SSL communication → server sends backs an encrypted public key/certificate → client checks the certificate creates and sends an encrypted key back to server,

server decrypts the key delivers content with key to client ← client decrypts content completing the SSl hand shake

conclusion- we hereby have studied SSL protocol