Dr B R Ambedkar National Institute of Technology, Jalandhar

M. Tech (Computer Science and Engineering)

CS-554, NETWORK SECURITY

Submission Date: 26-March-2024

1. A host receives an authenticated packet with the sequence number 181. The replay window spans from 200 to 263. What will the host do with the packet? What is the window span after this event?
2. Show how IKE reacts to the replay attack in the quick mode. That is, show how IKE responds to an attacker that tries to replay one or more messages in the quick mode.
3. Show how IPSec reacts to a brute-force attack. That is, can an intruder do an exhaustive computer search to find the encryption key for IPSec?
4. An organization uses a Cisco router for routing between its internal networks. What feature on the router can be used to block access specifically between two internal networks.
5. An organization has a HTTPS based server behind a firewall. A website is hosted on the Web server. Which port should be open on the firewall for allowing outside users to access the HTTPS based website.
6. Two IPSEC routers are configured to communicate with each other. Pre-shared keys are used on both the routers. Are these keys used for encrypting data on the IPSEC tunnel.
7. Show how SSL or TLS reacts to a replay attack. That is, show how SSL or TLS responds to an attacker that tries to replay one or more handshake message
8. A user in an organization wishes to connect to a Web server, which is residing on the internet. The user is behind the organization firewall. What configuration should be setup on the firewall for the user to access the Web server.
9. A user receives a virus infected file in his email inbox. There is no antivirus on the system. Would the virus infect the system, if the user deletes the file from the inbox.
10. A multinational corporation operates in various countries and relies heavily on its network infrastructure for communication, collaboration, and data exchange. The company's network security team has recently detected suspicious activity indicating a potential cyber attack. Upon investigation, they discover that an unauthorized individual has gained access to sensitive company data stored on the servers located in one of their remote offices in a different country. The attacker seems to have exploited a vulnerability in the outdated firewall system at that office, allowing them to bypass security measures and access the data.

    As a network security expert tasked with addressing this incident, outline the steps you would take to mitigate the immediate threat, secure the compromised systems, and prevent similar incidents in the future. Additionally, discuss strategies for enhancing network security across the corporation's global infrastructure to better protect against cyber threats.

11. NIT Jalandhar has recently implemented an online portal for students and faculty to access academic resources, submit assignments, and communicate with each other. The portal handles sensitive information such as grades, personal details, and research papers. To ensure the security and confidentiality of data transmission, the Institute has decided to implement SSL (Secure Sockets Layer) encryption for all communications between users' devices and the portal's servers. However, the IT department has received reports from students and faculty about encountering SSL-related errors and warnings when accessing the portal from certain devices and browsers.

    As a network security specialist at NIT Jalandhar, how would you investigate and address the SSL-related issues reported by users accessing the online portal? Outline the steps you would take to troubleshoot SSL errors and ensure secure communication between users and the portal's servers. Additionally, discuss best practices for SSL implementation and management to maintain robust network security for online portals and other web-based services within the institute's infrastructure.

12. A large multinational bank, "SecureBank," operates numerous branches worldwide and relies heavily on its network infrastructure to facilitate transactions, customer interactions, and internal communications securely. To safeguard sensitive financial data and ensure compliance with regulatory requirements, SecureBank has implemented IPsec (Internet Protocol Security) across its network for secure communication between branches, data centers, and remote employees. However, the bank's network security team has detected anomalies indicating potential security breaches in some IPsec tunnels.

    As a network security expert at SecureBank, outline the steps you would take to investigate and address the anomalies detected in the IPsec tunnels. Discuss the tools, techniques, and protocols you would utilize to identify the root causes of the security breaches and mitigate the risks effectively. Additionally, describe how you would enhance IPsec configuration and management practices to strengthen network security and protect sensitive financial data across SecureBank's global infrastructure.

13. A financial institution is deploying a new application for online transactions that require high levels of data integrity, confidentiality, and flow control to ensure that transactions are processed reliably and securely.

    As a network specialist, you are asked to recommend Transport Layer protocols and mechanisms to meet the application’s requirements. Consider the following:

    • Which Transport Layer protocol(s) would you recommend for the online transaction system, and why?

    • Discuss how your chosen protocol(s) ensures data integrity, confidentiality, and flow control during a transaction process.

- Describe any potential issues that might arise with your chosen protocol(s) in terms of performance (e.g., latency, throughput) and how you would address these issues to maintain a balance between security and performance.

14. E-ShopNow, a rapidly growing e-commerce platform, experienced a surge in traffic and transactions due to its expanding product range and customer base. While business growth was promising, the platform faced increasing cybersecurity threats, including data breaches, manin-the-middle (MITM) attacks, and customer data theft. Recognizing the critical need to protect user data and transactions, E-ShopNow sought to implement robust security measures at the transport layer. E-ShopNow's challenges were multifaceted:
    - Ensuring Data Confidentiality and Integrity: Protecting sensitive customer information, such as credit card details and personal data, during transmission.
    - Building Trust with Customers: Demonstrating a commitment to security to maintain and grow customer trust and loyalty.
    - Regulatory Compliance: Meeting stringent data protection regulations to avoid legal penalties and reputational damage.
    - Seamless Integration: Upgrading security without disrupting the existing user experience or platform performance.