Name : Binod kumar

Roll no. : 23203006

Class : M-Tech (CSE)

Subject : Network security

Semester : 2nd

Assignment : 01

Q.1> A host receives an authenticated packet with 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?

Ans:

- Since, the sequence numbes of the packet 181 is out of the window 200 to 263. The Packet is discarded.
- It is either duplicate or its arrival time has expired.
- The window span does not change. The host only discard the specific out-of-order packet, not entire window

Q.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.

Ans: . To protect against a replay attack, IKE uses nonces.

- Diffe-Hellman is vulnerable to a replay attack; the information from one session can be replayed in a future session by a malicious intruder
- To prevent this, we can add nonces to the third and forth messages to preserve the freshness of the message.

N-I : Initiator's nonce
N-R : Responder's nonce

The exchange of encrypted N-I and N-R in the first and second messages protects these messages from being replayed. The inclusion of these values again in the encrypted hash or signature in the third message gives the whole session together and protect the session against replay.

- Nonce is an arbitrary number used only once. It's often a random or pseudo-random number generated specially for that communication session.

There are following strategies to counter the replay attack in IKE quick mode.

i) An attacker intercepts a legitimate IKE quick mode message during the exchange and attempts to replay it later.

ii) The replayed message will have the same sequence number as the original.

iii) Each party verifies the nonce received from the other party during the quick mode. The inclusion of nonces in the negotiation ensures that each negotiation is unique and replayed message with the same nonce are detected.

iv) IKE implements anti-replay windows, which track the sequence number of received messages. Outside the acceptable window consider as replay attack and reject the packet.

Q:5> Show how IPSec reacts to a brute-force attack. That is can intruder do an exhaustive computer search to find the encryption key for IPSec?

Ans: - The effectiveness of the brute-force attack depends on the size of the secrets exchanged between two parties.

- Since IKE allows the concatenation of key to create a larger key, brute-force can be protected by creating a larger key.

- IPSec doesn't directly address brute force attack but relies on the internet key exchange protocol to establish secure keys.

i) IKE support strong cryptographic algorithms for key generation and exchange. The algorithm like Diffie-Hellman key exchange make it computationaley infeasible to guess the key through brute-force.

- key size >, 2048 (Generally).

ii) Hash functions play a crucial role in IPSec for integrity verification and authentication. The use of strong hash functions such as SHA-256, ensure that it is computationaly infeasible to find two different inputs that produce the same hash value.

iii> IPSEC implementation may include rate limiting and lockout mechanisms to mitigate against brute-force attack.
for example, after a certain number of failed authentication attempts, a system may impose delays, temporary lockouts

iv> continuous monitor network traffic and log suspicious activities.

v> IPSEC can use pre-shared key or digital certificate for authentication.

Q.4> An organization uses a cisco router for routing between its internal networks. What feature on the router can be used to block access specially between two internal networks.

Ans: You can use Access control lists (ACLs) on a cisco router to restrict access between two internal network.

i> You can create an ACL to specify which traffic you want to allow or deny.

ii> within the ACL, you can define rules that specify the source and destination networks you want to restrict communication between.

iii> Then, ACL is applied to the relevant interface on the router. This interface could be the one connecting the two internal networks you want to isolate.

Q.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.

Ans: • Outside user can safely access the website over HTTPS by opening port 443 on the firewall and forwarding incoming traffic on that port to the internal IP address of the web server hosting the website.

- This guarantees secure and encrypted data transmission between the user's browser and the web server.
- A firewall acts as a security barrier, controlling incoming and outgoing traffic on a network. By opening port 443, you allow for HTTPS traffic to reach the web server behind the firewall.

Q.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 encryption of data on the IPSEC tunnel

Ans: Yes, the pre-shared key on the IPSEC routers can be used for encrypting data on the IPSEC tunnel, but with some nuances.

IKE Negotiation:

- The pre-shared keys are primarily used for authentication during the IKE negotiation process
- IKE establishes a secure chanel for exchanging additional keys used for actual data encryption.

Key Derivation:

- During the IKE negotiation, both routers use the pre-shared key along with random numbers (nonces) to derive a set of encryption and decryption keys specific to that IPSec session.
- These keys should be more secure than the pre-shared key itself.

Here are some steps

i) Both IPSec routers are pre-configured with the same identical pre-shared key.

ii) the router initiate the IKE exchange using pre-shared key to prove their identies to each other.

iii) During the secure IKE channel, both routers use the pre-shared key along with nonces. to mathematically derive a unique set of encryption and decryption keys for the IPSec session.

iv) The actual data transmitted through the IPSec tunnel is encrypted using the derived keys.

Q.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.

Ans: - The handshake protocol uses the idea of symmetric key-agreement for establishing session secrets between two parties. If strong key exchange algorithm such as RSA, Emphemeral Diffie-Hellman is used for key agreement.

- The protocol is more immune to the man-in-the-middle attack.
- If weak key exchange algorithms such as Anonymous Diffie Hellman is used for key agreement, the protocol is less immune to the man-in-the-middle attack.

- Both the client and server generate nonces during handshake process. It included in specific handshake messages.
- During the handshake, the client and server use their respective nonces with a key exchange algorithm to derive pre-Master secret. This key is used to generate the session key encryption and message authentication.
- Each handshake messages carries a unique sequence number. This allow the receiver to identify message that are out of order or have been replayed.

Q.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.

Ans: To allow a user behind the organization's firewall to access a web server on the internet, you need to configure the firewall to permit traffic to the web server.

Here are some steps

i> Identify the web server Port

Most website use HTTPS, which operates on Port 443 by default. check the website documentation.

ii> Open the Port on the firewall

You need to create well rule on firewall so that allows outbound traffic on the specific Port to the internet.

iii> Stateful packet inspection

A lot of firewalls have this feature, which automatically permits internet response to go back to the internal user who initiated it.

iv> If the company employs NAT, make sure that when a user connects to the internet, their internal IP address is converted to a working external IP address. This enables the internet web server to correctly reply to the user's queries.

v) Implement suitable security measures such as web filtering, malware scanning and intrusion detection/prevention systems, to safeguard the network of the company against nefarious online activity.

vi) continuous monitoring web traffic and identify any suspicious activity or unauthorised access attempts. set up logging and monitoring the firewall

Q.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.

Ans: It is not guaranteed that the virus will not spread throughout the system if the infected file is delete from the inbox.

Here's the reason

i) Automatic execution

- Some viruses have the ability to lunch automatically when an email is opened, even the attachment is not downloaded.
- The virus might use the email client's Preview plane, which renders attachments like images automatically, to infect the system.

ii> Macros in Documents:

- Malicious macros embedded in word or Excel documents can lunch when an email is opened, even if the attachment is not downloaded or saved.
- one way to lessen this risk is to disable macros in the email client settings.

Improved safety procedures:

i> Never open suspicious Emails:
It's best to delete emails that seem suspicious or that come from senders you don't recognize.

ii> Don't Enable Macros:
To stop automatic execution of attachments, turn off macros in the setting of your email.

iii> set-up antivirus program:
To identify and stop malware infections. it's essential to have a reliable antivirus software installed.

iv> scan Downloaded files:
Prior to opening an attachment, if you must download one, make sure it has been scanned by a reliable antivirus programme.

Q.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 sensitiver 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.

Ans: For addressing a cyber attack incident and enhancing network security aacross a multinational corporation's global infrastructure. I would like to perform following steps.

There are following steps should be taken to mitigate the immediate threat and secure the compromised systems.

i) Containment:

- Isolate the compromised system from the rest of the network to prevent further unauthorized access to sensitive data.
- This could entail segmenting impacted network segments, blocking suspicious IP addresses or deactivating compromised accounts.

ii) Forensic Analysis

- To determine the scope of the breach, locate the point of entry and obtain information for prospective legal actions, conduct a comprehensive investigation.
- Save system snapshots, logs & any other information for forensic examination.

iii) Password reset and Access control

Change the passwords on any compromised accounts and use multi-factor authentication or other more robust authentication methods.

iv) Interaction

Inform all the relevant parties about the situation such as senior management, the legal departments and the impacted staff.

v> Updation

You must ensure that all the systems and software across the network are up-to-date with the latest security.

Now,

To perform operation in order to prevent similar incidents in future. Here are some strategies.

i> continuous Monitoring

- To detect and react to security incidents instantly.
- Use cutting-edge security monitoring tools like security information and Event management systems.
- Use anamoly detection and behavioural analytics to find odd activity patterns.

ii> Risk assessment and management

- Conduct regular risk assessments to identify potential vulnerabilities.
- Implement a risk management framework to proactively address security threats.

iii> Network segmentation

- To prevent attackers from moving laterally, divide the network into discrete areas or zone with restricted access controls.
- To enforce segmentation, put intrusion detection systems (IDS), firewalls and network access control solutions into place.

iv) Employee Education and Awareness

Inform staff members about social engineering techniques, password hygiene and cyber security best practices.

v) Roles and responsibilities

Assign roles and responsibilities, create channels of communication and specify protocols for co-ordination with relevant stakeholders.

Q.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 encryption for all communications between user's 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 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 would you take to troubleshoot SSL errors and ensure secure communication between user and portal servers. Additionaly discuss the 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.

Ans:

I would take the following actions to look into and resolve the SSL-related problems that users of NIT Jalandhar online portal have reported.

i> Examining SSL Errors:

- Gather information about the errors that have been reported, such as the precise error messages, the impacted hardware, browsers and network settings.
- Find out if the problems are specific to a device or location or if they affect many users at once.

ii> SSL certificate verification

- verify and examine the SSL certificate that is installed on the portal's servers to make sure it is current, valid and set up correctly.
- To look for problems like expired certificates, mismatched domains or broken certificate chains, use online SSL certificate validation tools.

iii> Review SSL configuration

verify that the server's SSL/TLS configuration supports the most recent encryption standards and cypher sets.

iv) Debugging SSL Handshake

Record and examine the SSL handshake process that takes place between user's devices and the portal's servers using network analysis tools such as Wireshark.

v) Browser compatibility

- To find any SSL compatibility issues that may be unique to a particular web browser, test the portal using a variety of web browser versions.
- The SSL/TLS protocol and encryption algorithms that are supported by some older browsers may be limited or restricted.

vi) Client-side Troubleshooting

Give instruction to users who are encountering SSL errors, like how to diagnose and fix problems on their end.

For example

- cleaning browser cathes
- Upgrading browsers.
- modify security setting.

These are following steps I would take to troubleshoot SSL errors.

i) Revise the SSL configuration:

Modify the SSL configuration on the server as needed to resolve incompatibilities and guarantee widespread support for contemporary encryption standards.

ii> Renew or Replace SSL certificate

If the SSL certificate is out-of-date, invalid or incorrectly configured, you can either replace it with a newly issued, correctly configured certificate issued for appropriate domain or you can renew it with a reliable certificate authority.

iii> Deploy Redirects:

Implement HTTP or HTTPS redirects to ensure all traffic is encrypted with SSL. That leads to secure communication.

iv> Updation

- To help users solve SSL-related problems successfully update support materials and documentation.
- Provides instructions on how to set up browsers to work with SSL and how to fix common SSL errors.

Here, There are following best practices for SSL implementation and management to maintain robust network security for online portal.

i> Employ Robust Encryption

Use robust encryption protocol or algorithm (TLS 1.2 or higher) to protect user and server data transmission.

ii> Frequent inspection and upkeep:

Make sure to conduct routine inspections and monitoring of SSL certificates, including their expiration dates, to guarantee prompt renewal and avoid service interruptions brought on by expired certificates.

iii> Implement HSTS.

Tell browsers to always communicate with the portal over HTTPS by turning on HTTP strict Transport security (HSTS), which enforces secure connections and guards against downgrade attacks.

iv> Security Awareness

Inform users. Faculty and student about the significance of SSL and security and the proper way to identify and handle error or warnings connected to SSL.

Q.12> A large Multinational bank, "secureBank" operates numerous branches worldwide and relies heavily on it.s network infrastructure to facilate transactions customer interactions and internal communication securely. To safeguard sensitive financial data and ensure compliance with regulatory requirements, securBank has implemented IPsec 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 investigate and address the anomaries 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 risk effectively. Additionaly describe how you would enhance IPSEC configuration and management practices to strengthen network security and protect sensitive financial data across secureBank's global infrastructure.

Ans:

In order to look into and fix any anomalies found in secureBank's IPSEC tunnels, I would take the following.

1) Examining the disturbances in IPSEC Tunnels:

i) Examine the log from intrusion detection/ prevention systems, routers, firewalls and IPsecf devices to find any oddities in the behaviours or occurences connected to IPsec tunnels.

ii) capture the packet and analyze them. use tools for packet capture such as wireshark. keep an eye out for anamoly that might point to security flows or configuration errors such as packet drops, retransmission or unexpected payloads.

iii) To find probable indicators of compromise (IOCs) or attack patterns directed at IPsec tunnels, correlate security events originating from different sources.

iv) Perform vulnerability scans and penetration tests in order to find possible vulnerabilities in the IPsec implementation such as out-of-date software versions or incorrect configuration.

v) Check that router, firewall and VPN gateway IPsec configurations adhere to security standards and best practices.

These are following tools, technique and protocol, I would like to utilize.

i) Forensic Tools.

- Utilize forensic tools such as Encase, FTK to analyze compromised systems and gather evidence.

ii) Network Monitoring tools.

Implement network monitoring tools like Wireshark, Snort to detect anomalous network traffic pattern indicative of potential security breaches.

iii) Review existing security controls and configuration to ensure adherence to industry best practices and compliance standards.

iv) vulnerability scanning tools

conduct a regular vulnerability assessment using tools like Nessus, Qualys or openVAS to identify weakness in systems and applications.

v> Penderation testing

Perform regular penetration tests using tools like Metasploit, BurpSuite to simulate real world cyber attacks and identify potential security loopholes.

vi> Endpoint Detection and Response (EDR)

- Deploy EDR solution like Carbon Black, crowdstrike or sentinelone to monitor endpoint devices for suspicious activities and behaviours.
- EDR tools provide visibility into endpoint activities and facilate rapid response to security incidents.

To enhance IPSec configuration and Management

i> Enforce strong authentication techniques such as digital certificate or multi-factor authentication. To safeguard the integrity and confidentiality of data. use strong encryption algorithm and key exchange algorithm.

ii) To simplify the configuration management, monitoring and troubleshooting, implement centralized management and monitoring solutions for IPSec devices.

iii) Logging and reporting should be centralized to make security analysis and incident response easier.

iv) To find vulnerabilities and fix them early, perform routine audits and security evaluations of IPSec configurations.

v) Educate network administrators and staff members on a regular basis about incident response protocols, security risks and IPSec best practices.

Q.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 the transactions are processed rapidly and securely.

As a network specialist, you are asked to recommend transport layer protocols and mechanism to meet the application's requirement consider the following:

- Which transport layer protocol 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 and how you would address these issues to maintain a balance between security and performance.

Ans: I would suggest utilizing the Transport layer security (TLS) protocol, more specially TLS 1.3, for an online transaction system that needs to have very high standards of data integrity, confidentiality and flow control.

This is the reasons for why.

i> Strong encryption

ii> Perfect forward secrecy (PFS)

- PFS is supported by TLS 1.3 and guarantees that previous communications are secure even in the event that a session key is comporomised in the future.
- Data confidentiality and integrity are improved by this.

iii> Effective mechanism for session resumption are included in TLS 1.3, which lower the overheads of creating new connections and boosts transaction throughput.

iv> Decreased Handshake latency.

TLS ensure Data Integrity, confidentiality and flow control.

i) Data Integrity

- Through cryptographic integrity check, TLS 1.3 guarantees data integrity and guards against data modification and tempering during transmission.
- During the handshake procedure, cryptographic hash functions are used to acomplish this.

ii) confidentiality:

- TLS 1.3 uses robust encryption algorithms to encrypt data being transfered over the network, shielding it from prying eyes and illegal access.
- This guarantees the confidentiality of sensitive transaction data.

iii) Flow control

- TLS 1.3 Provides effective data transmission and congestion control mechanisms, although flow control is essentially the responsibility of the underlying transport protocol such as TCP.
- It ensures dependable delivery by reducing latency and optimising the handling of data packets.

Potential performance issues and Mitigation strategies:

1> Latency

- TLS 1.3 seeks to reduce handshake latency, creating secure connections may still come with overhead, particularlly for quick transactions.
- Technique like session resumption and TLS false start can be used to minimise handshake overhead and help with latency issues.

ii> Throughput:

- Transaction throughput may be impacted by extra processing overhead that TLS encryption and decryption may cause.
- Hardware acceleration, carefully choosing cypher suites and fine-tuning TLS configurations can help to increase throughput without sacrificing security.

iii> Resource Utilisation

- CPU and Memory resources are used during the TLS handshake and encryption/decryption process, particularly on servers that handle large volumes of transactions.
- Resource exhaustion problem can be avoided by efficiently allocating the workload and implementing load balancing TLS offloading and scaling resources.

Q.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 cyber security threats, including data breaches, man-in-the-middle attacks and customer data theft. Recognizing the critical need to protect user data and transactions. 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.

Ans: Various measures can be put in place to address the complex security challenges that E-ShopNow faces at the transport layer.

1. Implementation of Transport layer security (TLS).

- Implementing TLS protocol, ideally TLS 1.3.

i) Integrity and confidentiality of Data

- Data is encrypted by TLS while it is being transmitted, guaranteeing confidentiality.
- To stop manipulation, it also offers cryptographic integrity checks.

ii) Developing customer Trust!

- E-ShopNow can show its dedication to security by using extended validation certificates and prominently displaying SSL/TLS certificates.

iii) Regulatory compliance

In order to compile with data protection low like GDPR, PCI DSS, TLS encryption is a basic necessity.

iv) Seamless interaction

- The user experience can be substantially interrupted less than if TLS implementation is smoothly incorporated into the current infrastructure.
- performance effect can be reduce with appropriate configuration and optimisation

2. Employing protocols for secure communication

- Promote the use of HTTPS and othe secure communication protocol in all client-server interactions.

i> sensitive information is protected from evasdroping and manipulation by HTTPS, which encrypts data transferred between clients and servers by using TLS over HTTPS.

ii> Customers's trust can be increased by the pedlock icon and "https://" in the URL, which reassure them that their data is secure.

iii> By securing online transactions and safeguard user privacy, HTTPS adoption complies with legal requirements.

iv> E-ShopNow's web servers are capable of implementing HTTPS with ease, guaranteeing secure communication without compromising user experience.