CNS Mid-Term Lab Exam 2024-25

Set A

1) Implement a secure communication system using OpenSSL and RSA. Complete the following tasks:

a. Generate RSA keys and certificate
b. Encrypt and decrypt messages using RSA
c. Set up a secure communication using RSA-based SSL/TLS

2) Write a C program that demonstrates a format string vulnerability . Modify the program to safely handle user input and prevent format string attacks. You can use any one format specifier to exploit the vulnerabilities.

3) Download file from the class room. (File_name: Wireshark.pcap)
The trace shows that at least one of the clients makes HTTPS connections to sites other than Facebook. Pick one of these connections and answer the following:

a. What is the domain name of the site the client is connecting to?
b. During the TLS handshake, the client provides a list of supported cipher suites. List the first three cipher suites and name the crypto algorithms used in each.
c. What is the broadcast Ethernet address, written in standard form as Wireshark displays it?
d. Which bit of the Ethernet address is used to determine whether it is unicast or multicast/ Broadcast?

Set B

1) You have an existing RSA signature scheme that signs 256-bit messages using OpenSSL. However, you need to sign 512-bit messages. Using OpenSSL, how would you adapt your signature process by hashing the message before signing it? Provide the command to generate and verify a signature for a 512-bit message using SHA-256 as the hash function.

2) Explain using a program how an attacker can overwrite a return address using a stack overflow.Name some mitigation techniques against this attack.

3) Download file from the class room. (File_name: Wireshark.pcap)

The trace shows that at least one of the clients makes HTTPS connections to sites other than Facebook. Pick one of these connections and answer the following:

a. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.
b. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation.
c. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment.
d. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? Give the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the RTT value for each of the six segments? What is the EstimatedRTT value.

Set C

1) The password can be encrypted using DES or MD5. If the field containing the password starts with 1, the password is encrypted using MD5, otherwise it is encrypted with DES. The salt (which is an additional randomness) used for the password occurs before the next $. Finally, the encrypted password follows the last $. Implement a program that attempts to crack a hashed password using brute-force and complete the following tasks.

a. Use OpenSSL to create an MD5-encrypted password with a four-letter lowercase password and a known salt.
b. Extract the salt and encrypted password.

2) Create a vulnerable C program demonstrating a buffer overflow.Compile the program and observe the output.Then, recompile the program with **stack canaries enabled** and highlight the difference in behavior.

3) Download file from the class room. (File_name: Wireshark.pcap)

The trace shows that at least one of the clients makes HTTPS connections to sites other than Facebook. Pick one of these connections and answer the following:

a. What is the largest possible source port number?
b. What cipher suite does the server choose for the connection?.
c. What is the broadcast Ethernet address, written in standard form as Wireshark displays it?

d. Establish TCP connection and name the 3 packets involved in the connection (TCP handshake). Determine what is the IP address of the client (the initiator of this TCP connection), and what is the server's IP address? From which port the client initiates the connection, and what is the port number used for this connection on the server side?

Set D

1) Implement Message Authentication Codes (MAC) using OpenSSL. Using OpenSSL to generate and verify **CMAC** and **HMAC** authentication codes. Complete the following tasks:

a. Compute CMAC using AES-128-CBC
b. Compute HMAC using SHA-256
c. Verify CMAC and HMAC

2) Write a C program that demonstrates a **use-after-free** vulnerability and analyze the output. Now modify your program to prevent this vulnerability.Provide the detailed steps for the same.

3) Download file from the class room. (File_name: Wireshark.pcap)
The trace shows that at least one of the clients makes HTTPS connections to sites other than Facebook. Pick one of these connections and answer the following:

a. Execute the command "ping www.mnit.ac.in" in terminal, Use WireShark to capture the generated ICMP packet (you can use filter "icmp") and answer why is it that an ICMP packet does not have source and destination port numbers?
b. Apart from the ICMP headers, what is in the data field of these ICMP packets? Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer? And Which fields stay constant?
c. Is there a display filter you could have used to rule out the localhost as either a source or destination?
d. Design a display filter that will help you see DHCP request and response traffic for when another machine first connects to the network.