Exp. 10

* Title : Using Wireshark capture live packets from LAN and capture the packets to identify the password with HTTP and HTTPs request.

* Objective: The primary aim of this experiment is to demonstrate the use of Wireshark, a network protocol analyzer, to capture live packets transmitted over LAN specifically focusing on identifying passwords transmitted via HTTP and HTTPS requests.

* Theory : 1) Wireshark is an open-source network protocol analyzer, enabling real-time inspection of data packets. With support for diverse protocols, it aids in troubleshooting, security analysis, and network understanding. The user-friendly interface displays packet-details, making it a valuable tool for administrators and researchers. Wireshark's versatility makes it essential for diagnosing network issues and comprehending data transmission dynamics.

2) HTTP (Hypertext Transfer Protocol) - Transmits data over the web and is vulnerable to interception. Wireshark can capture unencrypted HTTP traffic, allowing analysis of transmissied passwords.

3) HTTPS (Hypertext Transfer Protocol Secure)- Encrypts web traffic for security. Wireshark faces challenges in directly extracting passwords from HTTPS due to encryption, requiring additional decryption steps.

* Procedure: 1) Install wireshark on the capturing machine.
2) Connect the machine to the Internet.
3) Launch wireshark, choose the network interface.
4) Initiate live packet capture.
5) Use a web-browser for test login.
6) Fill login and password details to generate HTTP and HTTPS traffic.
7) Apply wireshark filters to isolate HTTP and HTTPS traffic.
8) Identify and select HTTP POST requests.
9) Open and inspect HTTP POST packets.
10) Locate and verify username and password fields.
11) For HTTPS, the direct password extraction is generally not possible without additional decryption steps due to encryption.

* Observation: On check post request in wireshark, the following is observed:
4) HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "Uname" = "anvai0304"
> Key: Uname
value: anvai0304
> Form item: "pass" = "01234567"
> Key: pass
value: 01234567

* Challenges: 1) Encryption - Modern encryption protocols significantly limit the ability to capture sensitive information from HTTPS, underscoring the importance of encryption for security.

2) Ethical Considerations - Experiment underlines ethical implications of capturing and analyzing network traffic, emphasizing the need for permission and legal compliance.

3) Technical Limitations - Wireshark's inability to decrypt some forms of encrypted traffic without appropriate keys highlights a technical limitation in network analysis.

* Conclusion: The experiment successfully demonstrates Wireshark's utility in capturing and analyzing network traffic ~~dtte~~ to identify passwords transmitted via HTTP.

* Questions:

1] What is a capture filter in Wireshark, and how is it different from a display filter?

Ans: A capture filter in Wireshark selects which packets are captured and stored during packet capture, while a display filter is applied after capture to selectively display and analyze captured packets within Wireshark interface. Capture filters minimize captured data based on criteria like IP addresses and port numbers, conserving storage space and reducing processing overhead. Display filters refine displayed packets for focused analysis using criteria such as protocol types of packet contents, enhancing the process.

2] How can you use Wireshark to identify the source and destination IP addresses in a captured network packet?

ANS: In Wireshark, identify source and destination IP addresses in captured packets by selecting a packet, then locating the "Internet Protocol Version 4" or "Internet Protocol Version 6" section in packet details. Source IP is listed as "source x.x.x.x" while destination IP is listed as "destination x.x.x.x".

3] Explain the term "packet sniffing" and discuss the ethical considerations associated with using Wireshark or similar tools.

ANS: Packet sniffing, like using Wireshark, involves intercepting and analyzing network traffic. Ethical concerns include privacy protection, legal compliance, security risks and ensuring transparency and accountability in data handling. Responsible use requires obtaining consent, complying with law, safeguarding data and being transparent about monitoring activities.