Sniffing Attack (Wireshark with the Url Target)

A sniffing attack using Wireshark involves capturing and analyzing network traffic to gather sensitive information, such as login credentials or other data transmitted over the network. Here's a brief overview of how to perform a sniffing attack using Wireshark:

Install Wireshark: If you don't have Wireshark installed on your system, you can download and install it from the official Wireshark website.

Select the network interface: Launch Wireshark and select the network interface you want to sniff. This can be a wireless network connection or a local area network interface.

Capture network traffic: Start capturing network traffic by clicking on the "Capture" button in Wireshark. This will start capturing packets transmitted over the network.

Filter for specific traffic: Use display filters in Wireshark to filter and isolate specific packets or protocols that you are interested in. For example, you can filter for HTTP traffic by using the filter expression http.

Analyze captured packets: Wireshark provides a detailed view of captured packets, including the source and destination IP addresses, protocols used, and the contents of the packets. Analyze the captured packets to uncover potentially sensitive information, such as login credentials or other data.

Follow HTTP stream: Wireshark allows you to reconstruct and analyze a full conversation between two systems by following the HTTP stream. Right-click on a packet and select "Follow" > "HTTP Stream" to view the complete conversation and the Seletc “POST”.