□ Tool Familiarity Notes

1. Wireshark

Explanation

Wireshark is a very popular network analysis tool that allows you to capture live network traffic. After capturing, you can examine the packets in detail to understand what is happening on the network. This helps in troubleshooting network problems, identifying suspicious activities, and learning how different protocols work.

Evidence

The captured network traffic file is saved as 'capture.pcap'. A screenshot of the filtered packets showing interesting communication can be included to demonstrate practical usage.

2. Nmap

Explanation

Nmap, also called Network Mapper, is a tool used to explore networks and discover devices and services running on them. It helps identify open ports, running services, and even the versions of software on those ports. This is useful for network security assessments and understanding how systems are connected.

Evidence

The results of the scan are saved as 'nmap_sV.txt'. You can also include a screenshot showing detected open ports and services for better understanding.

3. Burp Suite

Explanation

Burp Suite is a tool used for testing web application security. It works by intercepting the HTTP and HTTPS requests between your browser and the web server. This allows you to see exactly what data is being sent and received, modify requests, and test for potential security issues.

Evidence

You can attach a screenshot of intercepted traffic where you modified or analyzed a request. This shows practical usage of the tool during testing.

4. Netcat

Explanation

Netcat, sometimes called the 'Swiss Army knife' of networking, is a simple but powerful tool to read and write data over network connections. It can be used to connect to other machines, transfer files, or listen for incoming connections. It is very useful for learning how data travels over networks and practicing simple client-server setups.

Evidence

You can provide a screenshot showing a successful connection using Netcat. If a file transfer is done, a screenshot or terminal log showing the transfer can be added as proof.