OTLab 10

TCP/IP and Three-Way Handshake

Prof. Dr. Luiz Fernando Freitas-Gutierres (a.k.a. substationworm)

linkedin.com/in/lffreitas-gutierres

github.com/substationworm/OTLab

luiz.gutierres@ufsm.br

Problem Overview

Containerized Hosts

- `client`.
- `server`.
- `sniffer`.

Tasks

1. Access the `client` host and verify network connectivity with the `server` using the command: `ping -c 3 server`.

2. From the `client`, clear the ARP cache using the command `ip neigh flush all`. Subsequently, force ARP discovery by executing `ping -c 1 server`. Then, verify the MAC address associated with the `server` by running `ip neigh show`.

3. Access the `server` and start an HTTP service using the following command: `python3 -m http.server 80`. In a separate terminal session, access the `client` host and issue the request: `curl -v http://server`. Record and analyze the response returned by the web service.

4. On the `sniffer` host, use `tcpdump` to monitor TCP traffic between the `client` and the `server` by executing: `tcpdump -i any 'tcp and host <client_IP> and host <server_IP>' -n -vv`. In another terminal session on the `server`, execute: `nc -l -p 8080`. Then, from the `client`, establish a connection using `nc server 8080` and transmit a text message. Analyze the captured packets and describe the observed TCP three-way handshake process.

5. After completing the previous step, execute the following command on the `client`: `nc -vz server 9090`. A connection failure is expected. Examine the packet capture in `tcpdump` during this process and describe the observed TCP behavior.

6. From the `client`, perform a port scan against the `server` using the following command: `nmap -Pn -p 80,8080 server`. Evaluate the open ports and associated services based on the scan results.

Tools

The following tools are available for completing OTLab 10: `curl`, `ifconfig`, `ip`, `ipcalc`, `nc`, `nmap`, `ping`, `python3`, `tcpdump`, and `traceroute`.

Nomenclature

- ARP: Address resolution protocol.
- HTTP: Hypertext transfer protocol.
- IP: Internet protocol.
- MAC: Media access control.
- TCP: Transmission control protocol.