5/6/2024

Wireshark Basics:

- Capture, explore, and analyze ICMP, ARP, TCP, HTTP, FTP w/ FTP-data, and TELNET packets.
- Learned how to follow packets into the whole session.
- Learned about cookies, an alphanumeric string stored on the web browser to keep track of HTTP “sessions” (HTTP is connectionless).

Nmap Basics:

- Learned the basic usage of Nmap, such as -sT(TCP connection Scan, orFull-open scan, default w/ non-root), -sS(Half-open scan, or SYN stealth scan, default w/ root), -sV(Detects network service and versions running on a host’s open network ports), -O(Detects the OS running on the host), etc.
- Do a hand-on lab and run a scan on a network and a specific host on the network. To do a informative scan, the steps are as follows:
    - Run a quick scan with **-T5** (crazy speed) and **-sn** (Ping scan – only discovers host but does not perform scanning)
    - Identify hosts that are up. Run a scan on the host(s) interested with **-Pn** (disable Ping since we already know the host is up) **-T1/T2 -p** … to analyze the services on desired ports.
    - Also useful to fun a **-O** (OS) to gather some information about the operating system used on the server.