08-Sniffing

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online

Advanced: Build a data file / artifact that is actionable by the contract holder. There are no instructions for this task. You must figure everything out.

Attacker Data: Kali/ Parrot

Objective

- Sniff the network
- Analyze incoming and outgoing packets for any attacks

Overview of Network Sniffing

Most networks today work on switches. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port.

Packet sniffers are used to convert the host system's NIC to promiscuous mode. The NIC in promiscuous mode can then capture the packets addressed to the specific network. There are two types of sniffing.

- **Passive Sniffing**: only captures packets flowing in the network
- **Active Sniffing**: actively injecting and redirecting traffic on the LAN

Lab Tasks

1. Perform active sniffing
    - Perform MAC flooding using macof
    - Perform a DHCP starvation attack using Yersinia
    - Perform ARP poisoning using arpspoof
    - Perform an Man-in-the-Middle (MITM) attack using Cain & Abel
    - Spoof a MAC address using TMAC and SMAC
2. Perform network sniffing using various sniffing tools
    - Perform password sniffing using Wireshark

- ~~Analyze a network using the Omnipeek Network Protocol Analyzer~~
- ~~Analyze a network using the SteelCentral Packet Analyzer~~

3. Detect network sniffing
    - Detect ARP poisoning in a switch-based network
    - Detect ARP attacks using XArp
    - Detect promiscuous mode using Nmap ~~and NetScanTools Pro~~