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.

Advanced: capture encrypted packets, using decryption process from capture discussion

Attacker Data: Kali/ Parrot

Objective

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

Lab Tasks

1. Perform active sniffing
    - 1.1. Perform MAC flooding using macof*
    - 1.2. Perform a DHCP starvation attack using Yersinia*
    - 1.3. Perform ARP poisoning using arpspoof
    - 1.4. Perform an Man-in-the-Middle (MITM) attack using Cain & Abel
    - 1.5. Spoof a MAC address using TMAC and SMAC*
2. Perform network sniffing using various sniffing tools
    - 2.1. Perform password sniffing using Wireshark*
    - ~~2.2. Analyze a network using the Omnipeek Network Protocol Analyzer~~
    - ~~2.3. Analyze a network using the SteelCentral Packet Analyzer~~
3. Detect network sniffing
    - 3.1. Detect ARP poisoning in a switch-based network
    - 3.2. Detect ARP attacks using XArp
    - 3.3. Detect promiscuous mode using Nmap ~~and NetScanTools Pro~~

*Indicates capture