Network Sniffing, Technique T0842 - ICS

Archived: 2026-04-05 13:17:39 UTC

Network sniffing is the practice of using a network interface on a computer system to monitor or capture information [1] regardless of whether it is the specified destination for the information.

An adversary may attempt to sniff the traffic to gain information about the target. This information can vary in the level of importance. Relatively unimportant information is general communications to and from machines. Relatively important information would be login information. User credentials may be sent over an unencrypted protocol, such as Telnet, that can be captured and obtained through network packet analysis.

In addition, ARP and Domain Name Service (DNS) poisoning can be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.
