Sniffers and anti-sniffers

* ZINEEDDINE BOUMRAR

1. Introduction :

Sniffing is the process of capturing and monitoring a network to capture and analyze data packets when they are travelling between devices. Network administrators often use this technique for troubleshooting, performance monitoring, and security analysis. However, attackers can also use sniffing to gather sensitive data travelled over the network.

1. What can be sniffed :

* Unencrypted Passwords
* Web Browsing Activity
* Email Contents
* File Transfers
* Instant Messaging Chats
* Voice and Video Calls
* Sensitive Data in Application Traffic
* Network Configuration Information
* Login Sessions and Session Tokens
* Network Traffic Patterns

1. Sniffing methods :
2. Promiscuous Mode

* Promiscuous mode in a network enables a network device to intercept and read each arriving network packet in its entirety. A network adapter can receive and read each data packet sent across a promiscuous mode of operation in an Ethernet local area network (LAN).

1. DNS Spoofing

* Attackers can reroute traffic to their systems by modifying Domain Name System (DNS) answers. They can use packet sniffers to capture and examine the packets after the traffic has passed through their system.
* The DNS attack often takes place in a public Wi-Fi setting, but it can happen anywhere an attacker has access to the ARP (Address Resolution Protocol) tables and can trick targeted user devices into using the attacker-controlled system as the server for a particular website. It can fool users into installing malware on their devices or disclosing personal information. It’s the initial stage of a complex phishing attack on public Wi-Fi.

1. ARP spoofing

* Attackers use the Address Resolution Protocol (ARP) spoofing technique to link their MAC address to the router’s or target device’s IP address by sending fake ARP signals. Any traffic intended for that IP address is now redirected to the attacker.
* An attacker may be able to intercept data frames on a network, change the traffic, or completely block the flow by using ARP spoofing. The assault is frequently used as an opening for other attacks like denial of service, man in the middle, or session hijacking.

1. DHCP Sniffing

* When devices (such as PCs, cellphones, or IoT devices) join a network, DHCP is used to dynamically assign IP addresses and network configuration information. During the IP address assignment procedure, DHCP messages are exchanged between the client (device) and the DHCP server.
* Attackers can grab DHCP messages as they go across the network by using packet sniffing tools. Attackers can obtain insight into the network topology, identify active devices, and potentially discover more about the organization’s infrastructure by studying DHCP traffic.

1. How to prevent

* Use Encryption:
  + Encryption protocols such as HTTPS (for websites) and SSL/TLS (for email and other apps) should be used to ensure that data carried over the network is encrypted and cannot be easily intercepted and read by sniffers.
* Use Secure Protocols:
  + Whenever possible, employ secure protocols such as SSH (for remote access) and VPN (for distant connections) to construct encrypted tunnels between your devices and the network, making critical data capture impossible for sniffers.
* Implement Network Monitoring:
  + The process of continuously monitoring a computer network for problems such as delayed traffic or component failure is known as network monitoring. This way you might be able to spot suspicious events on a network, including sniffing attempts.
* Firewalls and Access Control:
  + Setting up firewalls and access control lists (ACLs) might help you prevent sniffing attacks by blocking traffic from unknown or untrusted sources.
* Regular Updates:
  + Many vulnerabilities that lead to sniffing attacks can be prevented with patches. Therefore, keeping your software or network devices up-to-date can be helpful in preventing sniffing.
* Disable Unnecessary Services:
  + Disable or uninstall any unneeded network services and protocols that could be used by attackers.

1. Some sniffing tools

* Wireshark
* TCPdump
* Fiddler