Chapter 8

Sniffing

Theory

Ethical Hacking

Sniffing

Sniffing is the process of monitoring and capturing all data packets passing through a given network. Sniffing is a form of wiretap applied to computer networks. We can sniff data packets using tools like Wireshark. Any protocol that do not encrypt data are vulnerable to sniffing attacks. Attackers use sniffers to capture data packets containing sensitive information such as passwords, account information, etc.

Sniffers Works in the Datalink Layer. If the initial layer is compromised, then the rest of the layers are also compromised in the OSI model

Sniffer

A sniffer is a software tool that monitors the data flowing through computer network links in real time. It can be a self-contained software program or a hardware device with the appropriate software or firmware to perform sniffing.

Sniffers can capture copies of data packets without redirecting or altering it. Some sniffers work only with TCP/IP packets, but the more sophisticated tools can work with many other network protocols and at lower levels, including ethernet frames.

Types of sniffing

Sniffing is classified into two types based on the way they interact with the data packet to capture and provide the user the ability to alter the packet.

- Active sniffing
- Passive sniffing

Active Sniffing

Active Sniffing involves injecting address resolution (ARP) packets into the network to modify Content Addressable Memory (CAM) Table which resides in the switch; CAM keeps track of which host is connected to which port on the switched network.

Passive sniffing

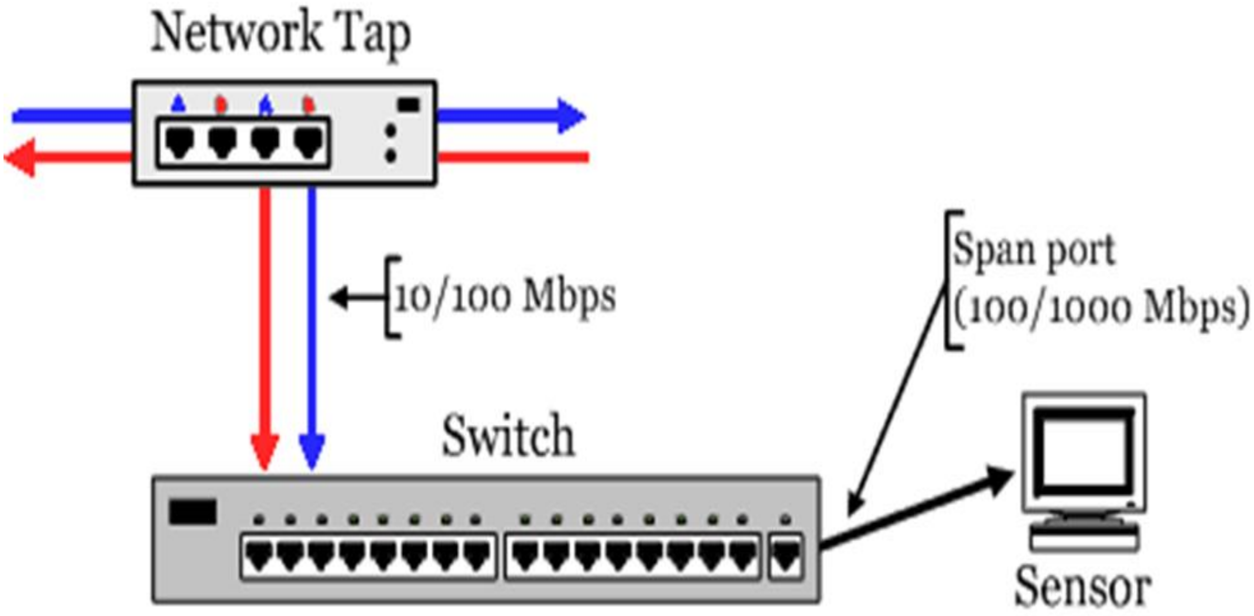
Passive sniffing involves listening and capturing traffic, in a network connected by hubs.

Protocols Vulnerable to Sniffing

HTTP - 80	FTP - 20/21
POP3 - 110	SMTP - 25
RDP - 3389	SSH - 22
NTP - 123	Telnet - 23
IMAP - 123	SNMP - 25

Port Mirroring (SPAN port)

Port mirroring is used by the network switch to send a copy of all network traffic to SPAN port on the switch. This is commonly used for monitoring network traffic by system administrators to detect suspicious activities in the network.



Address Resolution Protocol

Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given network layer address. This mapping is a critical function in the Internet Protocol suite. It is communicated within the boundaries of a single network never routed across internetworking nodes. ARP uses a simple message format containing one address resolution request or response. The size of the ARP message depends on the link layer and network layer address sizes.

ARP spoofing

In computer networking, ARP spoofing is a technique by which an attacker sends spoofed ARP messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often this attack leads to other attacks, such as Denial of service (DoS), Man in the middle (MITM), or Session hijacking attacks.

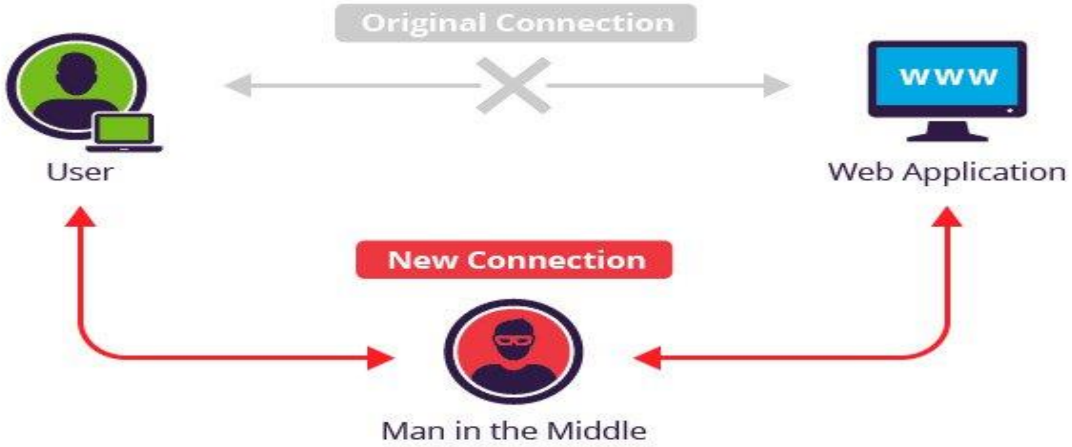
DNS spoofing

DNS spoofing is a technique of introducing corrupt Domain Name System details into the DNS resolver cache causing the name server to return an incorrect result record. This results in traffic being diverted to the attacker's computer.

A domain name system translates human-readable domain name into a numerical IP address that is used to route communications between nodes. If a DNS server is poisoned, it returns an incorrect IP address that diverts the traffic to another computer.

Man in the Middle attack

Man in the Middle attack is where an attacker positions himself in a conversation between a user and an application either to eavesdrop or to impersonate regular conversations. The attacker tries to steal personal information, such as login credentials, account details, and credit card numbers. Information obtained during attacks can be used to perform identity theft, unapproved fund transfers or an illicit password change.



Sniffing Detection Methods

1. Observing Network Traffic
2. Observing ARP Table to Detect ARP Poisoning
3. XARP Advanced ARP Poisoning Detection Tool

Countermeasures

- Use HTTPS instead of HTTP to protect usernames and passwords.
- Use switch instead of the hub as switch delivers data only to the intended recipient.
- Use SFTP, instead of FTP for secure transfer of files.
- Use PGP and S/MIME, VPN, IPSec, SSL/TLS, SSH and One-time passwords.
- Always encrypt the wireless traffic with a strong encryption protocol such as WPA and WPA2.
- Retrieve MAC directly from NIC instead of OS; this prevents MAC address spoofing.
- Use tools to determine if any NIC's are running in the promiscuous mode.

References:

1. MITM attack Image reference: (n.d.). Retrieved from https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html
2. Mitchell, B. (n.d.). What Is a Network Sniffer and How Does It Work? Retrieved from https://www.lifewire.com/definition-of-sniffer-817996
3. Address Resolution Protocol. (2018, August 02). Retrieved from https://en.wikipedia.org/wiki/Address_Resolution_Protocol
4. ARP spoofing. (2018, July 25). Retrieved from https://en.wikipedia.org/wiki/ARP_spoofing
5. DNS spoofing. (2018, July 13). Retrieved from https://en.wikipedia.org/wiki/DNS_spoofing