Volume XXIII 2020
ISSUE no.1
MBNA Publishing House Constanta 2020

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Sniffing attacks on computer networks

To cite this article: Dragoș Glăvan, Ciprian Răcuciu, Radu Moinescu and Sergiu Eftimie, Scientific Bulletin of Naval Academy, Vol. XXIII 2020, pg.202-207.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-20-I1-027

Sniffing attacks on computer networks

Dragoș GLĂVAN, Ciprian RĂCUCIU, Radu MOINESCU, Sergiu EFTIMIE

Military Technical Academy "*Ferdinand I*" – Systems Engineering for Defense and Security Doctoral School
dragos.glavan@gmail.com

Abstract. The sniffing attack or sniffer attack, in the context of network security, corresponds to data theft or interception by capturing network traffic using a sniffer (an application that aims to capture network packets). When data is transmitted over networks, if data packets are not encrypted, data in the network packet can be read using a sniffer. Using a sniffer application, an attacker can analyze the network and obtain information so that it can eventually crash or corrupt the network or read the communications that occur in the network. Sniffing attacks can be compared to touching wires and getting to know the conversation, and for this reason it is also called "wiretapping" applied to computer networks. In this paper, a sniffing attack is shared which can significantly damage the computer networks as well as methods of combating such attacks. Sniffing is usually performed to analyze network usage, troubleshoot network problems, monitor session for development and testing purposes.

1. Introduction

In the case of sniffing attacks the attacker can monitor and capture data from networks such as: Telnet Passwords, File Transfer Protocol Passwords, DNS traffic, Router Configuration, etc. Computers can be connected to the bus or switch, if the network is connected to the bus, is called shared Ethernet, and if connected via the switch, it is called switched Ethernet. In the shared Ethernet environment, if a packet is sent, it will send the packet to all machines. In switched Ethernet, the switch maintains a table that contains the MAC address of all the computers on the network, so the message is sent only to the destination machine. Although the Switch is safer than the Hub, sniffing can be done even when switching. Sniffing is classified into different types:

- MACflooding;
- DNS poisoning;
- ARP Poisoning;
- Dynamic Host Configuration Protocol (DHCP) Attacks;
- Password sniffing.

The Protocols vulnerable to sniffing are:

- Telnet;
- HTTP;
- POP;
- IMAP;
- SMTP;
- FTP.

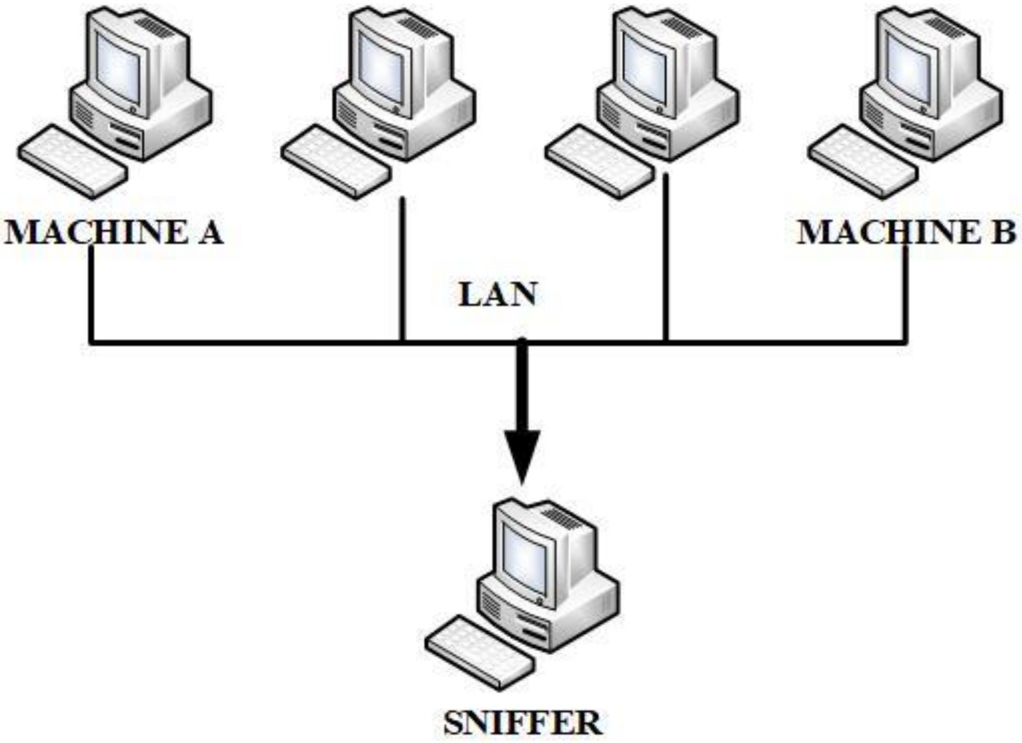

Fig.1. Sniffer in LAN

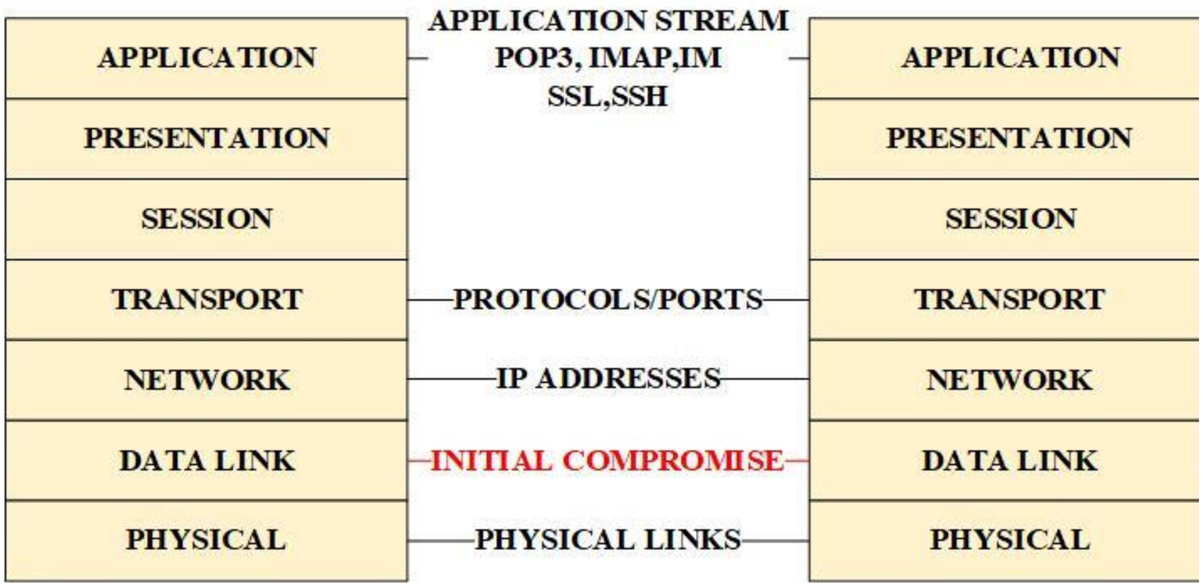

Fig.2. A Sniffer monitors network

2. MAC Flooding

MAC (Media Access Control) is a physical address that identifies each node in a computer network. CAM (Content Address Memory) stores the MAC address in the switch, the CAM size is fixed and if the CAM table is flooded with the MAC address beyond its capacity, the switch is transformed into a hub. Then the attackers can easily sniff the data. The figure below shows if the attacker uses the MAC Flooding concept to turn the switch into a hub and can easily steal sensitive data.

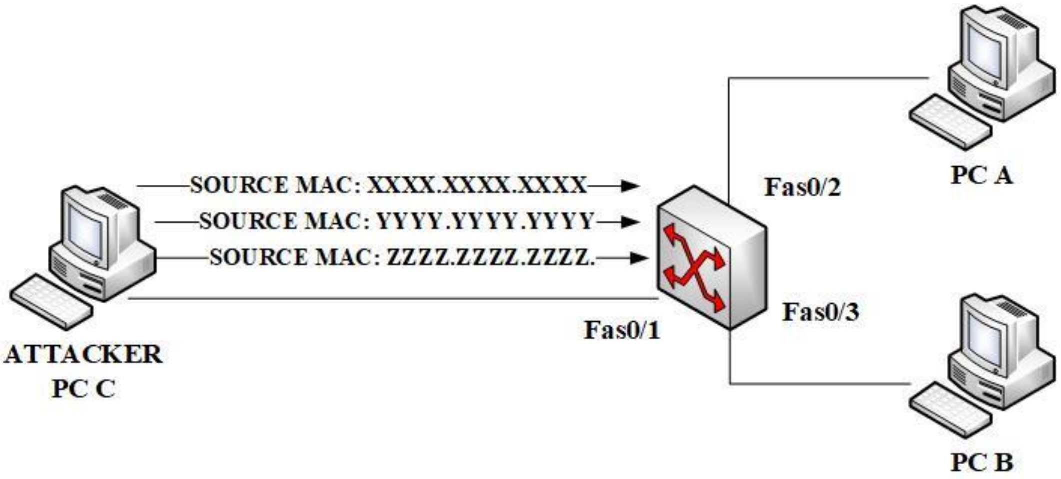
SOURCE MAC: XXXX.XXXX.XXXX
SOURCE MAC: YYYY.YYYY.YYYY
SOURCE MAC: ZZZZ.ZZZZ.ZZZZ.
ATTACKER
PC C
Fas0/1
Fas0/2
Fas0/3
PC A
PC B

Fig.3. Mac flooding

3. Dynamic Host Configuration Protocol attacks

Dynamic Host Configuration Protocol (DHCP) is a client-server protocol that provides the IP address of a gas and provides configuration information (such as default gateway, subnet mask) A DHCP relay agent, which sends DHCP requests from one LAN over another LAN, so there doesn't have to be a DHCP server on each LAN, it involves the following steps:

- DHCPDISCOVER request asking for DHCP configuration;
- DHCP Relay agent unicast this message to DHCP server;
- DHCP server unicasts DHCPOFFER;
- Relay agent broadcast DHCPOFFER in the client's network;
- Client broadcast DHCPREQUEST asking for DHCP configuration;
- Server unicasts DHCPPACK which contains configuration information

As part of the DHCP STARVATION ATTACK attack, the hacker requests a large number of DHCPREQUEST and uses all available IP address, so the DHCP server can no longer issue an IP address and in turn leads to Denial of Service (DOS) attack. In the figure below, the attacker requests a large number of IP addresses for the DHCP server, which results in the denial of service to other users.

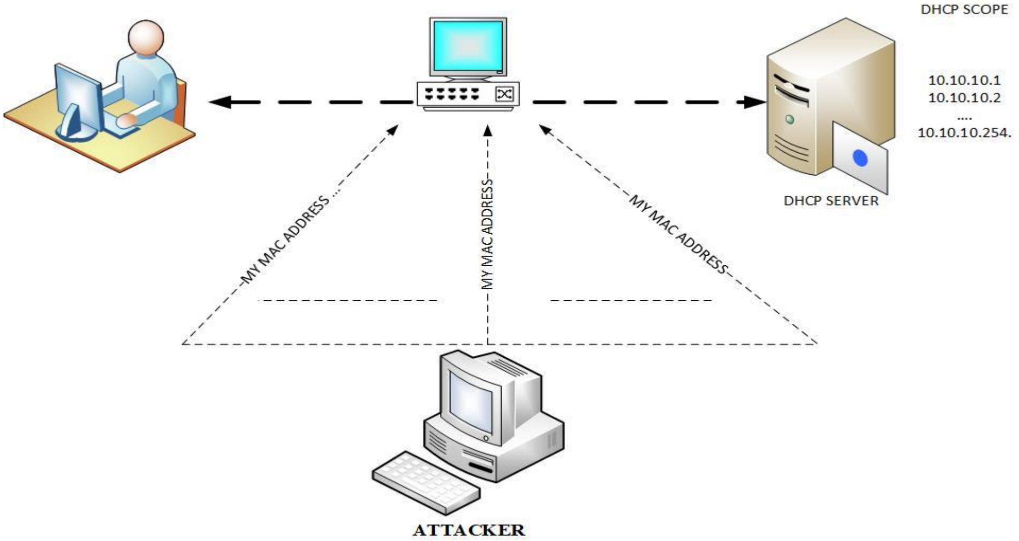

Fig.4. DHCP Starvation Attack

In the case of the ROGUE DHCP SERVER ATTACK attack, the attacker will introduce a rogue server. The DHCP server and the rogue server will respond to the client's DHCP request, the responding server will be picked up by the first one, so the rogue server will respond first. The client will send data to the dishonest server which in turn will send them to the real server. Therefore, the attacker monitors and captures all sensitive data, the client will not be aware of all these attacks.

Port security will be able to limit the maximum number of MAC addresses in the switch port, thus avoiding DHCP attacks. The DHCP snooping feature is available on switches, and to protect you from rogue DHCP servers, DHCP snooping is configured on the port on which the valid DHCP server is connected. Therefore, the switch will not allow the other ports to respond to the DHCP request.

4. Address Resolution Protocol spoofing

Address Resolution Protocol (ARP) is a stateless protocol that resolves the IP address to the MAC address. If the MAC address is not present in the ARP table, the node will transmit the ARP request, and all the nodes will compare the IP address with that one. Only one node identifies and responds to this, and ARP does not provide any means of verifying authenticity. The attacker can send any arbitrary IP and Mac address, this malicious content is stored in the victim's ARP computer. The following figure explains the concept of ARP poisoning, node 10.0.0.7 stores the IP address of 10.0.0.1 and the MAC address of the attacker and similar ARP poisonings are made for 10.0.0.1. Threats against ARP poisoning include:

- Sniffing package;
- Managing data;
- Manage in middle attack;
- Connection, resetting;
- Denial of Attacks (DOS).

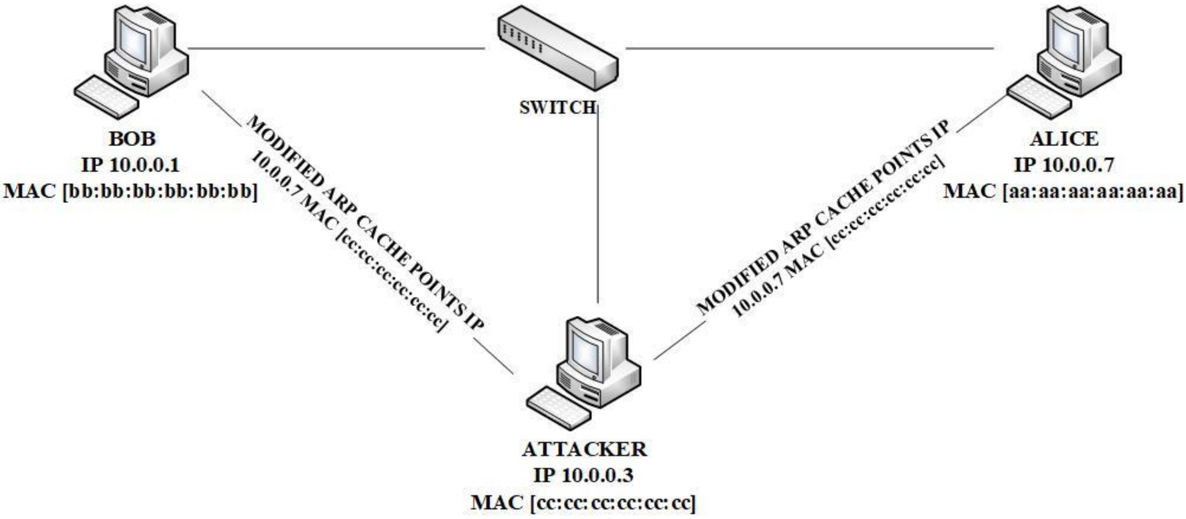

Fig.5. ARP Poisoning

Dynamic ARP Inspection (DAI) validates ARP packets on a network, DHCP Snooping must be enabled before DAI. It performs an IP address binding inspection on the MAC stored in the DHCP flagship database, and if any invalid link is found, the ARP packets are thrown, thus the MITM attack is limited.

Spoofing allows the hacker to pretend to be an authorized user. MAC spofing is nothing more than falsifying the MAC address, duplicating or spoofing one of the client's MAC addresses and reusing it. The malicious user can listen to and receive all traffic to the legitimate user. Ways to defend MAC Spoofing are as follows:

- enabling port security;

- using the DHCP snooping binding table. This table contains the MAC address and IP address of the legitimate user. It acts as a firewall between legitimate and malicious users;
- Dynamic ARP Inspection: Checks the MAC address and IP address for all packets. If an invalid address is found, they are deleted.

The IRDP protocol allows a router to identify the IP address of the active router through advertisements, it allows the nodes to listen to "Advertise router". When the node receives, this can change the routing table, and the node does not verify the authenticity of the message. A malicious user can damage the router itself, a hacker can change the default route provided by the server, so the attacker can sniff the data.

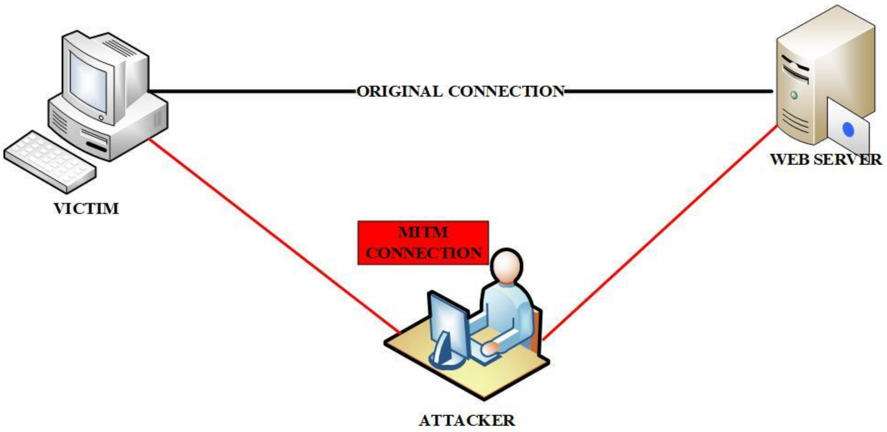

Fig.6. IRDP Spoofing

5. Sniffing tools

The sniffing tools used by hackers are as follows:

- Wireshark allows live network data capture. This data can be filtered by IP address, protocols and ports;
- The Capsa Network analyzer captures the IP address and MAC address of each host on the network;
- MSN Sniffer 2 includes MSN chats on all computers on the same LAN;
- Colasoft Packet is a package generator or package editing tool.

Steps used by sniffers are as follows:

- the hacker finds the network switch and connects to one of its ports;
- once connected, discover the network topology using hacking tools to discover the network such as Wireshark;
- analyzing the network, Sniffer receives the victim's car IP using a tool like Capsa Network Analyzer;
- once he knows the victim's IP, he sends fake messages using the tool like Colasoft Packet;
- the previous step results in the Man in the Middle Attack (MITM) attack;
- now the attacker manages to sniff the packets.

The countermeasures against sniffing are the following:

- Encryption is used to protect sensitive information;
- Static IP addresses and static ARP tables are used;
- the network is limited to authorized users only;
- IPv6 is used instead of IPv4;
- Encrypted session is used, such as SSH• HTTPS is used instead of HTTP to protect usernames and passwords;
- switches are used instead of hubs;

- the password authenticates shared folders and services• Encrypt communication between the computer and the access point.

6. Conclusions

This paper presents an approach for packet detection by packet sniffing. Sniffer is not only used for hacking purposes, but is also used for network traffic analysis, traffic / packet monitoring, troubleshooting and other useful purposes. The sniffer leaves no trace as it does not transmit data. Self-contained sniffers are hard to detect because they do not send packets. Reverse DNS lookup can be used to detect addicts who are not alone. Packet sniffers can be used to detect intrusions and there are tools that can be used to detect intrusions. Packet sniffing is a technique by which an intrusion can be created and an intrusion detected. Sniffing attacks can be compared to touching wires and getting to know the conversation, and for this reason it is also called "wiretapping" applied to computer networks.

References:

[1] S. Pandey “*Secure ContentSniffing for Web Browser: A Survey*”, 2013

[2] V. Mishra and N. Verma, “*Security against Password Sniffing using Database Triggers*”, 2014

[3] Supakorn Kungpisdan and Sumedt Jitpukdebodin “*A Novel Web Content Spoofing Technique on WLAN and Its Countermeasures*”, 2014

[4] Varsha Khokhar “*A Network Sniffer, OPEN JOURNAL OF INFORMATION SECURITY AND APPLICATIONS*”, 2014

[5] S. I. A. Qadri and K. Pandey, “*Tag Based ClientSide Detection of Content Sniffing Attack withFile*”, 2012

[6] Anubhi Kulshrestha and Sanjay Kumar Dubey “*A Literature Reviewon Sniffing Attacks in Computer Network*”, 2014

[7] Atul Verma and Ankita Singh “*An Approach to Detect Packets Using Packet Sniffing*” 2013.