Developing a Sniffer Detector for Windows Operating Systems

Dr. Mumtaz AL-Mukhtar
Information Engineering Faculty, Nahrain University
e-mail: mumtaz_almukhtar@yahoo.com

Yasir Ahmed Abdullah
Information Engineering Faculty, Nahrain University
e-mail: reditman@yahoo.com

Abstract

This paper presents the design and implementation of a sniffer detector system which can be used to detect any host running a sniffer on an Ethernet network. The proposed detection system is based on two effective detection techniques: the ARP (Address Resolution Protocol) detection technique and the Three-way Handshaking detection technique. The first technique, the ARP detection, attempts first to send trap ARP request packets with faked hardware addresses, to a suspicious sniffing host. Then, based on the generated responses of the suspicious sniffing host, a decision is made on whether or not the suspicious host is running a sniffer. In case of no response the second technique, the Three-way Handshaking detection, is used to detect active sniffer which did not respond to the first technique by sending trap TCP-SYN packets with faked IP address, to a suspicious sniffing host. Based on the generated responses of the suspicious host, a decision is made on whether or not it is running a sniffer. The two techniques are implemented in a system that automatically gives the system administrator a helping hand regarding the detection of sniffers on an Ethernet network. The proposed system is tested in comparison with three other available anti-sniffers (L0pht AntiSniff, PromiScan, and PromiscDetect). The results showed its enhanced performance.

Keywords: *Sniffers, Promiscuous Mode, Address Resolution Protocol, Anti-Sniffers.*

1. Introduction

The explosive growth of the networks and the Internet has been bringing about revolutionary changes in the ways daily activities are conduct such as government, business, education, entertainment, etc. It has made possible e-commerce, e-banking and e-government. The Internet phenomenon has saved the way for a new era of humanity: the information society. Such a technological development has also its downside. Internet has experienced an unprecedented growth in security incidents and attacks on computers systems, networks, etc [1]. In addition, attacks have grown in sophistication as well, using a very large set of tools and techniques. Sniffing is one of these tools. A sniffer is a program or a device that eavesdrops on the network traffic by capturing all packets traveling over a network. To achieve this, the sniffer sets the Network Interface Card (NIC) of the computer into a mode called "promiscuous mode". Then the NIC will blindly receive all packets and pass them to the system kernel. Packets that are not supposed to arrive at that computer are no longer blocked by the NIC [2]. Sniffers work because the Ethernet was built around a principle of sharing. Most networks use broadcast technology wherein messages for one computer can be read by another computer on that network. In practice, all the other computers except the one for which the message is meant, will ignore that message. However, computers can be made to accept messages even if they are not meant for them [3]. Sniffers were originally developed due to the need for a tool to debug networks. Essentially they capture, interpret and store network data for later analysis. However, just like most powerful tools used by network administrators, sniffers became subverted over the years and are now often used as malicious means to attack various systems [4]. By using sniffers, malicious users can easily steal confidential data, passwords, and anyone's privacy. This can be done simply by downloading free sniffer software from the Internet and installing it on a computer. Many basic services, such as File Transfer Protocol (FTP), Telnet, and Simple Mail Transfer Protocol (SMTP) send clear text data in the packets [5]. This underlines the importance of a reliable sniffer detector that can aid network administrators in detecting malicious sniffing activities.

2. Sniffers detection

The sniffing attack on a network is usually difficult to detect because it does not interfere with the network traffic at all, don't generate unusual traffic and only requires a standard machine, which becomes very apparent when reviewing the state of the research in the domain [6]. System administrators are facing difficulties in detecting and dealing with this attack. There are a few ways in which a system administrator can detect that a sniffer is running on his network. Packet sniffer detection normally consists of three different types of techniques. MAC (Media Access Control) based techniques, decoy based techniques, and network and machine latency based techniques [7,8]. Today, tools for sniffer detection should be a standard part of the security toolkit, used to protect computing assets from hostile attacks [9]. However, it is important to understand that the installation of a sniffer detector is a second-tier defense. If the sniffer detector detects any unidentified sniffing activities, it means the network has already been penetrated. By receiving and responding to a sniffer detector alert, the intrusion can be limited in scope and halted before further serious damage is incurred. In addition, the sniffer detector alert can aid

in computer forensics, and help make attackers more accountable for their actions. Hence, sniffer detectors and Intrusion Detection Systems (IDS) in general, may act as a deterrent to attacks [10].

3. Types of sniffers

According to sniffers functions and responses, sniffers can be categorized into two types: (i) passive sniffers and (ii) active sniffers.

i. A passive sniffer is a sniffer that captures solely packets in the network, and does not alter and block any networking activities and traffic. Any host running a passive sniffer can be detected just by using any detection techniques but mainly the ARP detection technique.

ii. An active sniffer is a sniffer that captures packets in the network but can alter and block network activities and traffic to stay undetectable by anti-sniffers. That is, most current anti-sniffers rely on the generated outgoing ARP, ICMP (Internet Control Message Protocol) or DNS (Dynamic Name System) Reply messages, by the suspicious hosts, to detect whether or not they are running sniffers. Consequently, while sniffing the network, active sniffers attempt to block all outgoing ARP Reply, ICMP Reply and DNS messages so that the anti-sniffers cannot detect them [11].

4. Proposed system: detection sniffers in a LAN

The proposed detection system is a combination of the two detection techniques: the ARP detection technique and the Three-way Handshaking detection technique. The proposed detection system consists of two stages:

1. To map a particular IP (logical) address to a given MAC (physical) address so that packets can be transmitted across the network, systems use the ARP protocol. Each host in a network segment has a table, called ARP mapping table, which maps IP addresses with their MAC addresses. New entries in the ARP mapping table can be created or already existing entries can be updated by ARP Request or Reply messages.

In the first stage, the ARP detection technique will be applied. The ARP detection technique consists of checking whether or not a suspicious host responds to ARP request packets that are not supposed to be treated by the suspicious host. Since the sniffing host receives all the packets, including those that are not targeting to it, it may make mistakes such as responding to a packet, which originally is supposed to be filtered by the host's NIC. Therefore, the detection is performed by checking the responses of ARP reply packets, when ARP request packets are sent to all hosts on the network. Also in this stage the ARP mapping table of each sniffing host in the LAN will be corrupted with a deliberate fake entry (IP-X and MAC-X), using ARP mapping table attack. Only the ARP mapping table of the hosts running sniffers will be corrupted, and this attack on the ARP mapping table will not cause any damage to the attacked hosts.

2. In the second stage, Three-way Handshaking detection technique will be applied. The Three-way Handshaking detection technique consists of establishing a TCP connection with each host in the LAN by using the fake addresses (IP-X and MAC-X) used in the first stage to corrupt the ARP mapping tables of sniffing hosts. Then the LAN is sniffed in an effort to capture any packet containing the fake entry. The hosts that send TCP or ICMP packets containing the fake entry are running sniffers. However, the hosts that send ARP Request packets are not running sniffers.

The following sub-sections describe in details the two stages. The use of a host in the LAN called the source host is assumed to do all the actions needed in the two stages.

5. ARP detection and ARP mapping table attack

In this stage the first detection technique will be applied to discover any host running a passive sniffer and the ARP mapping table of each sniffer will be corrupted by a fake entry.

5.1 ARP Detection Technique

When the NIC is set to promiscuous mode, packets that are supposed to be filtered by the NIC are now passed to the system kernel. Therefore, an ARP Request packet is first configured such as it does not have a broadcast address as the destination address. The source host sends this packet to every host on the network and discovers that some hosts respond to it, then those hosts are running sniffers. When the NIC is in promiscuous mode, the NIC does not perform any filtering operation. That this packet is able to pass to the system kernel. In the system kernel there exists some sort of software filter. The packet is actually filtered again by the software filter; therefore the destination MAC address of the ARP Request packet must be set to a value that can pass both the NIC filter and the software filter. It has been tested that if the destination MAC address is set to the fake broadcast address B47 (FF:FF:FF:FF:FF:FE), then any host with any windows operating system set to the promiscuous mode will accept the ARP Request message.

Consequently ARP Request message with fake broadcast address B47 set as the destination MAC addresses must be sent to all hosts in the LAN. Normally, such a packet is discarded. But when in promiscuous mode, the operating systems will grab these packets as legitimate packets since the MAC address is checked insufficiently, and respond accordingly. If the target machine replies to the ARP request packet with an ARP reply packet, it can be concluded that the target machine is running a sniffer. If the host is set to the normal mode, this ARP Request message will be blocked at the Ethernet layer because the destination MAC address is neither a unicast address, a broadcast address, nor a multicast address.

5.2 ARP Mapping Table Attack

The aim of this attack is to corrupt only the ARP mapping table of the sniffing hosts in a LAN. In principal, to corrupt the entries in the ARP mapping table of a target host, source host generates ARP request or reply packets including fake IP and MAC addresses. However, in practice, the success of this malicious activity depends on the operating system of the target host. The source host

may attempt to send fake ARP reply packet to a target host even though the malicious host did not receive any ARP request packet from the target host. If the operating system of the target host accepts the fake ARP reply packet from the source host without checking whether or not an ARP request packet was generated before, then the received ARP reply packet will corrupt the ARP mapping table of the target host with fake MAC/IP entries. However, some operating systems are not any more vulnerable to this attack. Alternatively, the source host may attempt to send ARP request packets, instead of ARP reply packets. Three popular operating systems have been tested and the results are shown in Table 1. The obtained results show which operating systems with entries in the ARP mapping table were vulnerable to the ARP mapping table attack.

Table (1) Creation and Updating entries in the ARP mapping table using ARP Request and Reply packets.

	Windows XP		Windows 2000		Windows Server 2003	
Does the entry exist in the ARP mapping table	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**
ARP Request packet	√	√	√	√	√	√
ARP Reply Packet	√	X	√	√	√	X

√= the ARP request or reply packet is accepted by the system and therefore allows the update or the creation of an entry.

X = the ARP request or reply packet is rejected by the system and therefore does not allow the update or the creation of an entry.

Table 1 indicates clearly that:

- If the entry does not exist in the ARP mapping table, all the tested operating systems, except Windows 2000 do not allow the creation of a new entry by an ARP reply packet.
- If the entry does not exist in the ARP mapping table, all the tested operating systems allow the creation of a new entry by an ARP request packet.
- However, if the entry already existed in the ARP mapping table, all the tested operating systems allow its update by an ARP reply or ARP request packet.

Therefore, when using ARP reply packets, the ARP mapping table attack becomes difficult to realize against most operating systems. However, it remains indeed possible when using ARP request packets. Source host can first use ARP request packets to create fake MAC/IP entries in the ARP mapping tables of the target hosts. Then, fake ARP reply packets are used to maintain the existence of fake MAC/IP entries in the ARP mapping tables of the target hosts.

Consequentially the source host sends an ARP Request packet, with fake source IP and MAC addresses (IP-X and MAC-X), to all hosts in the LAN. Hence, the source host needs to choose the values of the fields in each header so as to let only the sniffing host process the ARP Request packet. If the destination MAC address in the Ethernet layer header is set to a broadcast address (FF:FF:FF:FF:FF:FF), then all the ARP mapping tables of the hosts in the LAN will be corrupted by the ARP mapping table attack. Such a destination MAC address is discarded. However, if the destination MAC address is a fake broadcast address, then a target host set to the promiscuous mode will accept the ARP request packet and send it to the ARP layer. If the destination MAC address is the fake broadcast address B47 (FF:FF:FF:FF:FF:FE), then any host with any operating system set to the promiscuous mode will accept the ARP Request packet and its ARP mapping table will be corrupted by the fake entry. If the host is set to the normal mode, this ARP Request packet will be blocked at the Ethernet layer because the destination MAC address is neither a unicast address, a broadcast address, nor a multicast address.

One ARP Request packet represents the ARP detection technique and the ARP mapping table attack will be send by the source host to each host in the LAN as illustrated in fig.1. The values of the main fields of the ARP Request packet used to detect and corrupt the sniffing hosts are listed in Table 2.

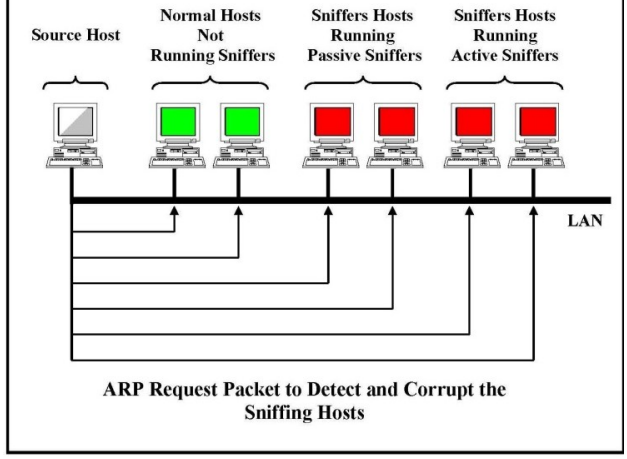

Figure (1) ARP Request Packet Sending.

Table (2) Fields of the ARP Request Packet used to detect and corrupt the sniffing host.

Ethernet header	
Source MAC address =	Source host's MAC address
Destination MAC address =	FF:FF:FF:FF:FF:FE
Ethernet Type =	ARP Packet
ARP header	
Source IP address =	Fake IP address IP-X
Destination IP address =	IP address of a target host
Source MAC address =	Fake MAC address MAC-X
Destination MAC address =	00:00:00:00:00:00
Operation code =	1 (ARP request)

After sending the ARP Request packet to each node in the LAN, the source host must sniff the network in an effort to capture any host responding to it. The normal hosts will discard the ARP Request packet because the destination MAC address is neither a unicast address, a broadcast address, nor a multicast address. While the sniffing hosts will accept this packet. There is an expect of two types of responses from the sniffing hosts as shown in fig.2. This depends on whether the sniffing hosts running a passive or an active sniffer:

i.The Target Host Is Running a Passive Sniffer. In this case the sniffing host will accept the ARP Request packet and respond to it by an ARP Reply packet targeted to the source host, then the source host can easily detect these host running sniffers.

ii. The Target Host Is Running an Active Sniffer. In this case the sniffing host will accept the ARP Request packet and does not respond to it, but the ARP mapping table of the sniffers hosts will be corrupted by the fake entry (IP-X and MAC-X).

The source host must sniff the network to capture any ARP reply packet on the LAN that has those fake IP and MAC addresses (IP-X and MAC-X) as the destination addresses. All hosts that sent such ARP reply packets are consequently running sniffers, and their IP addresses can be easily identified.

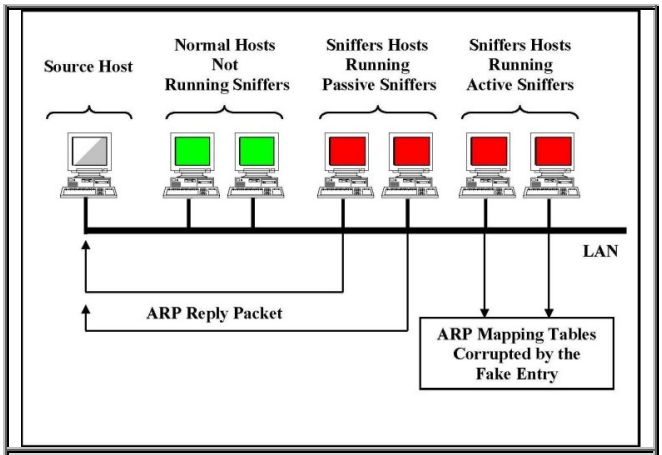

Figure (2) The Detection of the Passive Sniffers.

6. Three-way handshaking detection technique

The hosts running passive sniffers will be detected in the first stage because these sniffers hosts respond to the source host by an ARP Reply packet, while the hosts they did not respond to the ARP Request packet are either hosts running active sniffers or normal hosts. Hence the second stage of the proposed system will detect any active sniffers on the network.

In this stage The Three-way Handshaking detection technique will be applied to discover any host running an active sniffer. The Three-way Handshaking detection technique consists of establishing a TCP connection with each host in the LAN that did not respond to the source host in the first stage by using the fake address. Then the LAN is sniffed in an effort to capture any packet containing the fake addresses. To do that, the source host sends one TCP packet with the bit SYN set to each host in the LAN as shown in fig.3. The values of the main fields of the TCP packet used to establish a TCP connection with each host in the LAN are listed in Table 3. The source IP address in the IP header of the TCP packets is not the source IP address of the source host, but it is the fake IP address (IP-X) that used in the first stage to corrupt the ARP mapping table of the sniffers hosts. Each host in the LAN will process the received TCP packet.

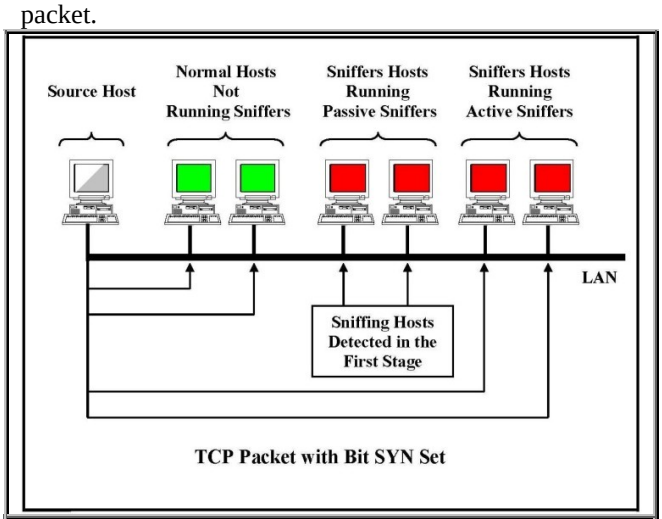

Figure (3) TCP Connections Establishing.

Table (3) Fields of the TCP Packet used to detect the sniffing host

Ethernet header	
Source MAC address =	The source host's MAC address
Destination MAC address =	The target host's MAC address
Ethernet Type =	IP Packet
IP header	
Source IP address =	Fake IP address IP-X
Destination IP address =	IP address of a target host
IP Type =	TCP Packet
TCP header	
Source Port =	Any number between 1 and 65535
Destination Port =	Any number between 1 and 65535
SYN-Bit =	True

After an establishment of a TCP connection with each host in the LAN, the source host must sniff the network in an effort to capture reply packets from those hosts. There is an expect of two types of possible reply packets to be generated by the hosts as illustrated in fig.4. This depends on whether the hosts running active sniffers or not running sniffer:

i. The Target Host Is Running an Active Sniffer. In this case, there are two possible Reply packets. A TCP packet indicating that the connection can be established (the SYN and ACK bits are set) or an ICMP error message indicating that the connection cannot be established because the port destination is inaccessible.

ii. The Target Host Is Not Running a Sniffer. In this case, there is a possible reply packet. It will be an ARP Request message sent by the host to look for the MAC address of the fake source IP address IP-X.

The source host must sniff the network to capture any TCP or ICMP packet on the LAN that has those fake IP and MAC addresses (IP-X and MAC-X) as the destination addresses. All hosts that sent such TCP or ICMP packets are consequently running sniffers, and their IP addresses can be easily identified.

However, any host whose ARP mapping table is not corrupted would generate an ARP Request message to get the MAC address of the fake IP address IP-X. This MAC address will be used later to send the Reply message, which is expected to be a TCP or ICMP packet. Therefore, any host in the LAN that will send ARP Request message looking for the MAC address of the IP address IP-X is not running a sniffer.

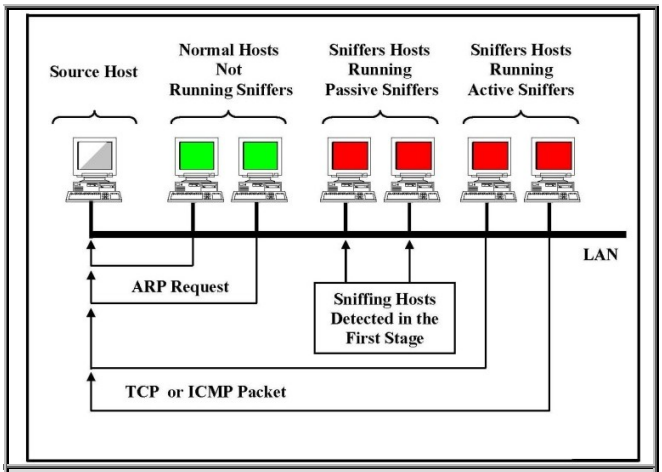

Figure (4) The Detection of the Active sniffers.

7. Implementation

Based on the proposed detection system, an anti-sniffer with a graphical user interface (GUI), called AAT (ARP detection, ARP mapping table attack, Three-way handshaking detection) anti-sniffer, has been developed using C# and Winp-Cap Library. The AAT anti-sniffer integrates an ARP and TCP packet generator and a sniffer with filtering capabilities. The AAT anti-sniffer allows one to generate ARP Request packet and TCP packet with fake source IP and MAC addresses. In addition, it is able to sniff the network and capture packets based on filtering rules defined by the users. The detection capability of the AAT anti-sniffer allows the administrator to detect all types of sniffers in his network.

7.1 ARP Detection and ARP Mapping Table Attack Application

This application represents the first stage of the proposed detection system and has four main responsibilities:

1. Generating an ARP request packet with fake addresses and sending it to the suspected host.
2. Creating a filter that allows only reply to the sent ARP request packet to pass and sniff the network according to it.
3. Alerting the administrator if the suspected host is running a passive sniffer.
4. Corrupting the ARP mapping table of the suspected host if it is running an active sniffer.

When the application is launched, the main window of the ARP detection and ARP mapping table attack will appear as shown in fig.5.

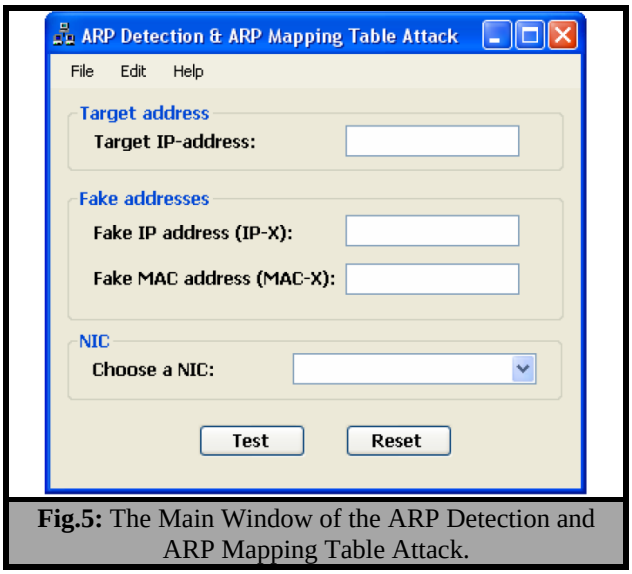

Fig.5: The Main Window of the ARP Detection and ARP Mapping Table Attack.

As the main window appears, the administrator can test any host on his network. If the suspected host is running a passive sniffer, the detection system will alert the administrator as shown in fig.6.

If the suspected host did not respond to the ARP request packet, this means that the host is either running an active sniffer or a normal host. In case of an active sniffer, the second stage of the proposed detection system must be performed to detect the active sniffer.

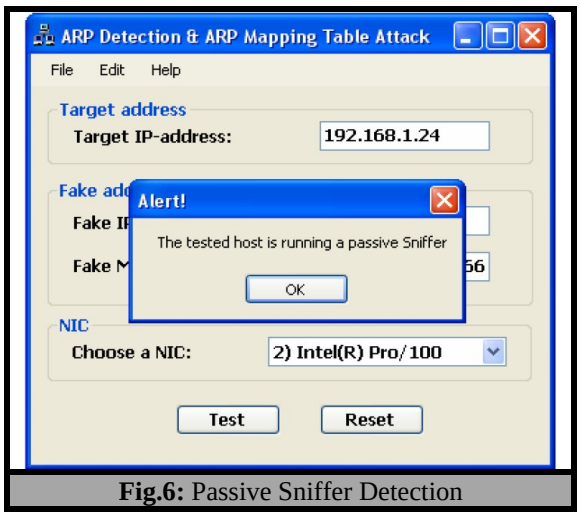

Fig.6: Passive Sniffer Detection

.

7.2 Three-way Handshaking Detection Application

This application represents the second stage of the proposed detection system and has three main responsibilities:

1. Generating a TCP packet with fake IP address and sending it to the suspected host.
2. Creating a filter that allows only replies to the sent TCP packet to pass and sniff the network according to it.
3. Alerting the administrator if the suspected host is running an active sniffer.

When the application is launched, the main window of the Three-way Handshaking Detection will appear as shown in fig.7.

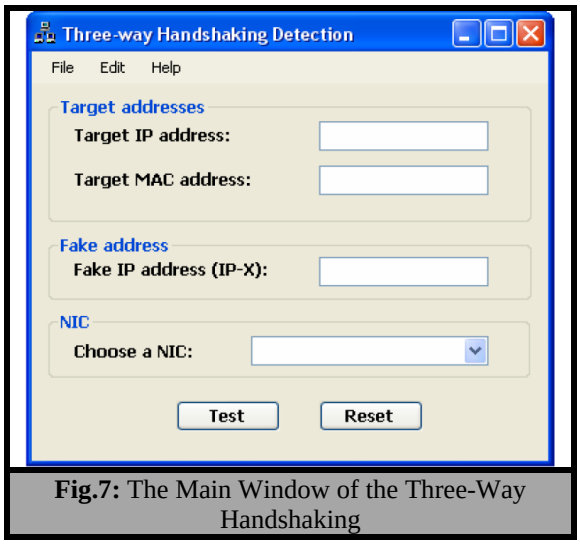

Fig.7: The Main Window of the Three-Way Handshaking

.

As the main window appears, the administrator can complete testing the suspected host. If the suspected host is running an active sniffer, the detection system will alert the administrator that this host is running an active sniffer as shown in fig.8.

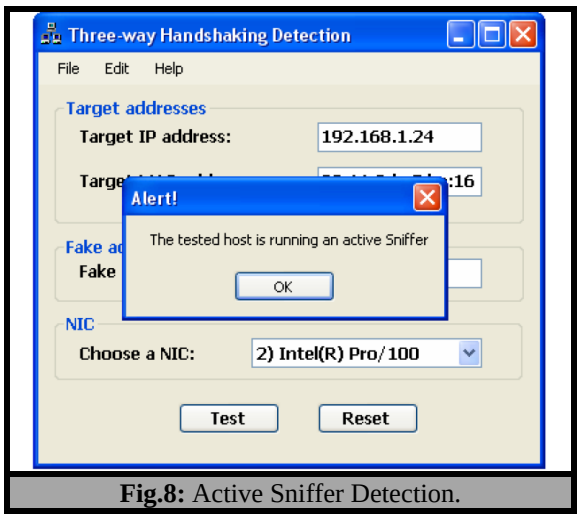

Fig.8: Active Sniffer Detection.

8 EVALUATION

Current anti-sniffers are based on three detection techniques: (1) the ARP detection technique, (2) the DNS detection technique, and (3) the RTT (Round Trip Time) detection technique. However, sniffers are becoming very advanced so that anti-sniffers are unable to detect them. In fact, the main drawbacks of these detection techniques is that they rely on the ARP, ICMP, DNS reply messages generated by the sniffing hosts. Therefore, to stay undetectable by the anti-sniffers, well designed and implemented sniffers (active sniffers) do not generate such reply messages while sniffing. AAT anti-sniffers does not rely on such messages. Even active sniffers which does not generate any ARP Reply and DNS messages, or put continuously heavy traffic on the network cannot stay undetectable by AAT anti-sniffers. Four anti-sniffers L0pht AntiSniff, PromiScan, PromiscDetect, and AAT anti-sniffers were tested and the evaluation results showed that AAT anti-sniffers succeeded in detection both the passive and active

sniffers. The other anti-sniffers performances are quite similar to each other; they succeeded in detecting the passive sniffer and failed in the detection of active sniffer.

9 CONCLUSIONS

Current anti-sniffers use many detection techniques, primarily the RTT, DNS, and ARP detection techniques. These techniques have many drawbacks, so that well designed and implemented sniffers can stay undetectable by current anti-sniffers. When the sniffing hosts do not generate any Reply ARP and DNS messages, or put heavy traffic on the network, these detection techniques become useless.

The proposed system presented a developed sniffer detection system which is effective in detecting sniffers running on remote hosts. The proposed detection system is based on two integrated techniques, the ARP detection technique and the Three-way Handshaking detection technique, that allow the administrator to detect sniffers efficiently.

Although sniffers are difficult to detect, the proposed technique can provide system administrators with a consistent decision. However, by combining two detection techniques in a single anti-sniffer system, administrators will have more results that confirm whether or not a target host is running a sniffer.

The developed system would not require an extra overhead to detect promiscuous applications, starting and ending without increasing the network load. That it is sufficient to send only one packet in each detection stage.

Implemented tests showed that when sniffers do not generate any ARP Reply and DNS messages, or put continuously heavy traffic on the network, only the proposed detection system could detect such sniffers.

REFERENCES

[1] S. Mcclure, J. Scambray, and G. Kurtz, Hacking Exposed: Network Security Secrets and Solutions, McGraw-Hill, 2007.

[2] J. Birnbaum & R. Kline, “Project ifchk: Host Based Promiscuous Mode Detection and Handling”, Proceedings of Research Day, CSIS, Pace University, May 2004.

[3] Z. Trabelsi, H. Rahmani, K. Kaouech, and M. Frikha, “Malicious Sniffing Systems Detection Platform”, Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT’04), PP. 110-117, January 2004.

[4] A. Orebaugh, G. Morris, E. Warnicke, and G. Ramirez, Ethereal Packet Sniffing, Syngress Publishing, 2004.

[5] M. Jipping, A. Bugaj, L. Mihalkova, and D. Porter, “Using Java to teach networking concepts with a programmable network sniffer”, SIGCSE 2003, Reno, Nevada, USA, pp. 120-124, February 2003.

[6] M. Jakobsson, S. Stamm, “Invasive Browser Sniffing and Countermeasures”, Proceeding of the 15th International Conference on World Wide Web, May 2006.

[7] H. AbdelallahElhadj, H. M. Khelalfa, and H. M. Kortebi, “An Experimental Sniffer Detector: SnifferWall”, Basic Software Laboratory, CERIST, 2002.

[8] Victor A. Clincy, Nael Abu-Halaweh, “A Taxonomy of Free Network Sniffers for Teaching and Research”, Journal of Computing Science in Colleges, Volume 21, Issue 1, October 2005.

[9] Mic Bauer, “Paranoid Penguin: Stealthful Sniffing, Intrusion Detection and Logging”, Linux Journal, Volume 2002, Issue 102, pp. 17-23, October 2002.

[10] S. LIU, J. SUN, X. ZHAO, and Z. WEI, “A General Purpose Application Layer IDS”, CCECE 2003 - CCGEI 2003, Mantrial, May 2003.

[11] Thomas King, Mikkel Baun Kjoergaard,”Composcan: Adaptive Scanning for Efficient Concurrent Communications and Positioning with 802.11”, Proceeding of the 6th International Conference on Mobile Systems, Applications, and Services, pp. 67-80, June 2008.

الخلاصة

يقدم هذا البحث تصميم وتنفيذ نظام كشف ضد إستراق المعلومات الذي يمكن استخدامه لاكتشاف اي مستخدم يدير برنامج إستراق المعلومات على شبكة Ethernet. نظام الكشف المقترح يستند على تقنيتي الكشف الفعالتين: تقنية كشف Resolution (ARP) Address Protocol وتقنية كشفThree-Way Handshaking. التقنية الاولى ARP ترسل اولا رزمة طلب Trap ARP Request بعناوين حاسبات مزيفة، الى المستخدم المشتبه به. ثم استناداً الى الردود المولدة من المستخدم المشتبه به، يتم تحديد فيما اذا كان المستخدم يدير برامج إستراق المعلومات. في حالة لا ردود، التقنية الثانية Three-way Handshaking سوف تستخدم لكشف برامج إستراق المعلومات المتقدمة التي لم تستجب للتقنية الاولى بارسال رزمة Trap TCP-SYNبعنوان IP مزيف الى المستخدم المشتبه به. ثم استناداً الى الردود المولدة من المستخدم المشتبه به، يتم تحديد فيما اذا كان المستخدم يدير برامج إستراق المعلومات. تم جمع التقنيتين في نظام يعطي مدير النظام الياً يد المساعدة بخصوص كشف برامج إستراق المعلومات على شبكة Ethernet. النظام المقترح اختبر بالمقارنة مع ثلاثة انظمة اخرى متوفرة مضادة لاستراق المعلومات. النتائج اظهرت انه الافضل اداءاً.