ARP Spoofing:
A Comparative Study for Education Purposes

Zouheir Trabelsi
College of Information Technology,
UAE University, Al Ain, UAE
trabelsi@uaeu.ac.ae

Wassim El-Hajj
College of Information Technology,
UAE University, Al Ain, UAE
welhajj@uaeu.ac.ae

ABSTRACT
ARP spoofing attack, one of the most important security topics, is usually taught in courses such as Intrusion Detection in Local Area Networks (LANs). In such a course, hands-on labs are very important as they facilitate students' learning on how to detect ARP spoofing using various types of security solutions, such as intrusion detection and prevention systems (IDS/IPS). The preparation of these hands-on labs are usually the task of Security Instructors who are required to select and use efficient security solutions for their hands-on experiments; the problem that presents itself is that most of these security instructors lack the sufficient hands-on experience and skills. For this reason and because of the diversity of the available security solutions, the security instructors are having much difficulty when selecting the adequate security solutions for their hands-on labs.

This paper is a comparative study for educational purpose. It provides analysis based on practical experiments carried out on a number of security solutions regarding their ability to detect ARP spoofing. Our analysis provides means for security instructors to evaluate and select the appropriate security solutions for their hands-on labs. In addition, we clearly show that ARP spoofing has not been given enough attention by most tested security solutions, even though this attack presents a serious threat, is very harmful and more dangerously it is easy to conduct. As a solution, we propose the requirements for an ideal algorithm that can be used by security solutions to detect effectively any ARP spoofing attack.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – *Security and protection*. K.4.4 [**Computers and Society**]: Electronic Commerce – *Security*. K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *Unauthorized access.*

General Terms
Performance, Experimentation, Security.

Keywords
ARP spoofing, ARP spoofing detection, Denial of Service (DoS), Man-in-the-Middle (MiM)

InfoSecCD '09, September 25-26, 2009, Kennesaw, GA, USA.

1. INTRODUCTION
Intrusion detection is one of the major security topics taught in network and information security courses. These courses cover several lectures describing the common security attacks, the corresponding detection and prevention techniques, and extensive hands-on labs. It is to be noted that there are various types of attacks, such as Denial of Service (DoS) attacks, Man-in-the-Middle (MiM) attacks, ARP spoofing, buffer overflow, malicious sniffing, etc. ARP spoofing, also called ARP Cache poisoning, is one of the hacking methods that spoofs the contents of an ARP table of a remote computer on a LAN. Using ARP spoofing, malicious users can corrupt the ARP caches of target hosts in order to perform MiM or DoS attacks. Hence, ARP spoofing based attacks are very common LAN attacks that can be easily performed and thus they present a very serious under looked threat. For this reason, such dangerous attack along with its countermeasures should be well described and demonstrated to students during lectures and hands-on lab experiments.

However, usually security instructors lack sufficient hands-on expertise and skills to be able to evaluate and select the appropriate security solutions to detect ARP spoofing for the hands-on lab experiments. There are many available security solutions, and are implemented mainly in hosts (for instance host IDS), switches, IDS hardware appliances and software tools, or Unified Threat Management (UTM1) appliances.

In this paper, which serves educational purposes, we conducted many experiments to test whether the most commonly used security solutions can detect ARP spoofing or not; the surprising results are presented and analyzed. Our analysis provides means for security instructors to be able to efficiently and effectively evaluate and select the appropriate security solutions for their hands-on labs.

It is worth mentioning that experiments show clearly that even thought, ARP spoofing is known to be a very harmful attack, it has not been given serious attention by most available security solutions. In fact, despite the fact that some security solutions claim to fully and efficiently deal with most common network intrusions, they are still incapable of detecting a dangerous attack such as ARP Spoofing. On the other hand, we found out that other

[1] *UTM (Unified Threat Management):* is used to describe a security device that has many features in one box, including a firewall, an intrusion detection (or prevention) system (IDS or IPS), e-mail spam filtering, anti-virus capability, and World Wide Web content filtering

security solutions use algorithms that deal with this attack only partially. In sum, this work proposes the requirements for an ideal algorithm that can be implemented in any security tool or device to effectively detect ARP spoofing attack.

The rest of the paper is organized as follows. Section 2 introduces briefly the ARP protocol Section 3, describes the ARP spoofing attack. Section 4 lists and illustrates all possible abnormal ARP packets. Section 5 depicts the experiments carried out on various security solutions designed to deal with network intrusions. Section 6 discusses and analyses the experiments' results. Section 7 proposes the requirements for an ideal algorithm for detecting ARP spoofing. Finally, section 8 concludes the paper.

2. Background

2.1 ARP protocol

To map a particular IP address to a given MAC address so that packets can be transmitted across a LAN network, systems use the ARP protocol [5]. Address Resolution Protocol (ARP) messages are exchanged when one host knows the IP address of a remote host and wants to discover the remote host's MAC address. For example, to get the MAC address of Host 2, Host 1 sends first a broadcast ARP request message. Then, Host 2 sends to Host 1 a Unicast ARP reply message containing its MAC address. Figure 1 shows the main fields in ARP packet.

ARP header
Operation code =1 (Request), or 2 (Reply)
Source IP address
Source MAC address
Destination IP address
Destination MAC address
Ethernet header
Source MAC address
Destination MAC address
Ethernet Type (=0x0806 for ARP message)
Hardware type = 1 (Ethernet)
Protocol type = 0x0800 (IP)

Figure 1. The main field of an ARP packet

The ARP protocol specifies no rules to maintain consistency between the ARP header and the Ethernet header. This means that one can provide uncorrelated addresses between these two headers. For example, the source MAC address in the Ethernet header can be different from the source MAC address in the ARP message header.

2.2 ARP cache

Each host in a network segment has a table, called ARP cache table, which maps IP addresses with their corresponding MAC addresses. There are two types of entries in an ARP cache, namely: Static entries and Dynamic entries. Static entries remain in the ARP cache until the system reboots. Dynamic entries remain in the ARP cache for few minutes (this depends on the operating system (OS)) then they are removed if they are not referenced. Static entries mechanism is used unfortunately in small LAN networks only. However, in large networks, the deployment and update of static entries in the ARP caches are not common practice.

New entries in the ARP cache can be created or already existing entries can be updated by ARP request or reply messages as follow. Refer to the work in [11] for more details on the process of creating and updating entries in ARP caches for various OSs.

3. ARP Spoofing

ARP spoofing, also called ARP Cache poisoning, is the malicious act, by a host in a LAN, which introduces a spurious IP address to MAC address mapping in another host's ARP cache. This can be done by manipulating directly the ARP cache of a target host, independently of the ARP messages sent by the target host. To do that, the malicious host can either add a new fake entry in the target host's ARP cache, or update an already existing entry by fake IP and MAC addresses. These two methods are explained as follow:

Create a new fake entry: To do that, an ARP request message with fake source IP and MAC addresses in the ARP header, is sent to a target host. When the target host receives the ARP request message, it believes that a connection is going to be performed, and then, creates a new entry in its ARP cache utilizing the fake source addresses (IP and/or MAC) provided in the message's ARP header. Consequently, the target host's ARP cache becomes corrupted with fake IP/MAC entries.

Update an entry with a fake entry: To do that, an ARP reply message with fake IP and MAC addresses can be sent to a target host. Thus, even if the entry already exists in the target host's ARP cache, it will be updated with the fake IP/MAC addresses.

3.1 ARP spoofing based MiM and DoS attacks

In LAN networks, MiM and DoS are very common attacks that can be easily performed. These attacks use usually spoofed ARP packets to corrupt the ARP caches of victim hosts. The MiM attack consists of re-routing (redirecting) network traffic between two target hosts to a malicious host (usually the attacker host). Then, the malicious host will forward the received packets to its real destination, so that the communication between the two target hosts will not be interrupted and the two hosts' users will not notice that their traffic is being redirected and sniffed by a malicious user.

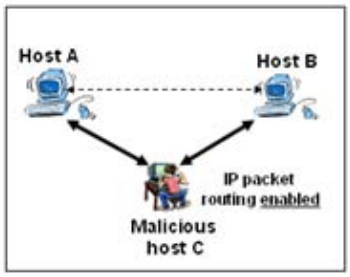

Figure 2. A presentation of the MiM attack

In such attack, the malicious user first enables the host's IP packet routing, in order to become a router and be able to forward the redirected packets. Then, uses an ARP cache poisoning attack, the malicious user corrupts the ARP caches of the two target hosts, in order to force the two hosts to forward all their packets (Figure 2).

It is important to notice that if the malicious host corrupts the ARP caches of the two target hosts without enabling its IP packet routing, then the two hosts will not be able to exchange packets and it will be a Denial of Service (DoS) attack. In this case, the malicious host does not forward the received packets to their

legitimate destination as shown in Figure 2. This is extremely potent when we consider that not only can hosts be poisoned, but routers/gateways as well. All Internet traffic for a host could be intercepted by performing a MiM attack on the host and the LAN's router.

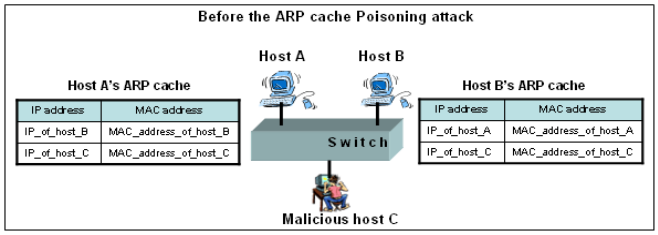

Figure 3. The entries of the ARP caches of hosts A and B before the ARP cache poisoning attack

In Figure 2, host C is the malicious host and hosts A and B are the two target hosts. To perform MiM attack, host C enables its IP packet routing and corrupts the ARP caches of hosts A and B, using ARP cache poisoning attack. Figure 3 shows the initial entries in the ARP caches of hosts A and B, before the ARP cache poisoning attack. Host C sends a fake ARP request packet to hosts A in order to damage its ARP cache with the fake entry IP_Host_B/MAC_Host_C (Figure 4). Also, host C sends a fake ARP request packet to hosts B in order to distort its ARP cache with the fake entry IP_Host_A/MAC_Host_C (Figure 5).

ARP header
Operation code =1 (Request)
Source IP address = **IP_Host_A**
Source MAC address = **MAC_Host_C**
Destination IP address = IP_B
Destination MAC address = 00-00-00-00-00-00
Ethernet header
Source MAC address = Any
Destination MAC address = **MAC_B**
Ethernet Type (=0x0806 for ARP message)

Figure 4. Fake ARP request sent to host B by the malicious host C

ARP header
Operation code =1 (Request)
Source IP address = **IP_Host_B**
Source MAC address = **MAC_Host_C**
Destination IP address = IP_B
Destination MAC address = 00-00-00-00-00-00
Ethernet header
Source MAC address = Any
Destination MAC address = **MAC_A**
Ethernet Type (=0x0806 for ARP message)

Figure 5. Fake ARP request sent to host A by the malicious host C

After the attack, as shown in Figure 6, host A associates host B's IP with host C's MAC, and host B associates host A's IP with host C's MAC. All packets sent by host A to host B will first go to host C. Then, host C forwards them to host B, since IP packet routing in host C is enabled. Moreover, all packets sent by host B to host A will first go to host C, then, host C forwards them to host A.

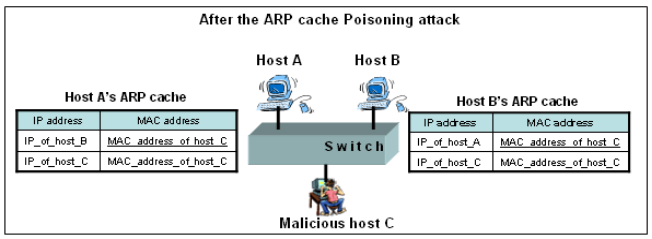

Figure 6. The entries of the ARP caches of hosts A and B after the ARP cache poisoning attack

However, in DoS attack (Figure 7), target hosts are denied from communicating with each other, or with the Internet. This is done simply by corrupting their ARP caches with fake entries including nonexistent MAC addresses, or by disenabling the IP packet routing option in the malicious host, so that received redirected traffic will not be forwarded to its real destination.

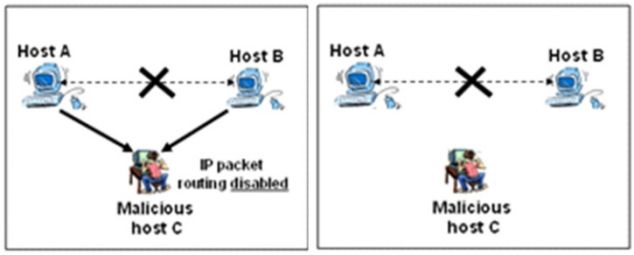

Figure 7. A presentation of the DoS attack

3.2 ARP spoofing tools

Malicious users do not need to know deeply how ARP spoofing attack works and are generated. In fact, there are many available easy-to-use tools to perform ARP spoofing attack, namely: ARP Spoof Tool [1], Winarp [8], SwitchSniffer [7], WinArpSpoof [10], WinArpAttacker [9], and Cain & Abel[2].

4. Abnormal ARP packets

There are many security solutions claiming to be able to cope with ARP spoofing. These solutions are found usually in highly-cost switches, network IDS/IPS hardware appliances, and IDS/IPS software tools.

ARP spoofing uses abnormal ARP packets to corrupt ARP caches of target hosts. The detection process consists of detecting those abnormal ARP packets sent over the LAN network. However, most abnormal ARP packets do not damage the ARP caches (Tables 1 and 2), but they may produce DoS situations in target hosts. Consequently they should be detected. Tables 1 and 2 identify exhaustive two lists of all possible abnormal ARP request and reply packets, respectively.

We identified 4 possible types of abnormal ARP request packets and 6 possible types of abnormal ARP reply packets, as follows:

- P#1, P#5, and P #7: Security devices should keep track of IP-to-MAC address mappings. Every ARP packet contains a mapping of IP-to-MAC address. ARP requests contain the IP-MAC mapping of the sender. ARP replies contain the IP-MAC mapping of the machine resolved. Every mapping is inserted into a database. If a mappings is monitored that breaks current mappings, an alert is generated. IP-to-MAC mappings database can filled either automatically or manually.

Table 1. List of possible abnormal ARP request packets

Packet number	P#1	P#2	P#3 (Unicast ARP request)	P#4 (Unexpected IP or MAC address in ARP request packets*)
ARP Header				
ARP Operation	1	1	1	1
Source IP	IP_A*	IP_A		0.0.0.0 255.255.255.255 Multicast Not in the network subnet
Source MAC	MAC_X*	MAC_A*		00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Destination IP				0.0.0.0 255.255.255.255 Multicast Not in the network subnet
Destination MAC				
Ethernet Header				
Source MAC		MAC_X		00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast MAC
Destination MAC			Unicast	00-00-00-00-00-00 Unicast or Multicast
Does the packet corrupt the ARP cache?	Yes	No	No	No

- *IP_A*: is the IP address of a host A*
- *MAC_A*: is the MAC address of a host A*
- *MAC_X*: is a MAC address of a nonexistent host*
- *Unexpected IP or MAC address in ARP request packets*: These addresses are considered unexpected and consequently ARP request packets should not have such addresses*

- P#2, P#6, and P #8: ARP packets have special restrictions. In an ARP request and reply packet, the Ethernet source MAC address has to match the ARP source MAC address. In ARP reply, the Ethernet destination MAC address has to match the ARP destination MAC address.
- P#3: A normal ARP request needs to be sent to the broadcast MAC address, and not to a Unicast MAC address. Such packets are used by ARP spoofing software to spoof only a specific machine and not all machines on a network.
- P#9: A normal ARP reply needs to be sent to Unicast MAC address, and not the broadcast MAC address. Such packets are used by ARP spoofing software to spoof only a specific machine and not all machines on a network.
- P#4 and P#10: There are fields in the ARP packet that have restrictions regarding the values they can adopt. This module checks these values for correctness. ARP mappings may not contain certain IP addresses. These include broadcast and multicast as well as null addresses.

Moreover, some MAC addresses in ARP packets are highly suspicious. No IP-to-MAC mapping should, for example, have the MAC broadcast, multicast or null address assigned. Every ARP packets IP addresses need to be in the same subnet. An ARP packet with IP addresses that are not in the network interfaces configured subnet are suspicious and will be alerted.

Tables 1 and 2 show that only abnormal packets P#1 and P#5 can corrupt ARP caches of target hosts with fake IP-MAC entries. The remaining abnormal ARP packets do not corrupt ARP caches. However, they may still be harmful and should be detected since they can carry DoS attacks.

Table 2. List of possible abnormal ARP reply packets

	P#5	P#6	P#7	P#8	P#9 (Broadcast ARP reply)	P#10 (Unexpected IP or MAC address*)
ARP Header						
Operation	2	2	2	2	2	2
Source IP	IP_A	IP_A				0.0.0.0 255.255.255.255 Multicast Not in the network subnet
Source MAC	MAC_X	MAC_A				00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Destination IP			IP_B*	IP_B		0.0.0.0 255.255.255.255 Multicast Not in the network subnet
Destination MAC			MAC_X	MAC_B*		00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Ethernet Header						
Source MAC		MAC_X				00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Destination MAC				MAC_X	ff-ff-ff-ff-ff-ff	00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Does the packet corrupt the ARP cache?	Yes	No	No	No	No	No

- *IP_B*: is the IP address of a host B*
- *MAC_B*: is the MAC address of a host B*
- *Unexpected IP or MAC address in ARP reply packets*: These addresses are considered unexpected and consequently ARP reply packets should not have such addresses.*

5. Experiments

Various types of security solutions have been used during the experiments that can be classified into 4 categories, namely:

1. LAN switches
    a. Cisco switch 3560 Series
    b. Juniper Switches EX3200 Series
2. Software IDS/IPS
    a. Snort IDS
    b. XArp 2 tool
    c. Sax2 NIDS
3. IDS/IPS hardware appliances
    a. Cisco IPS 4255 Series
    b. TopLayer Model 5000
    c. IBM ISS Proventia Model GX4004C
    d. SourceFire
    e. TippingPoint 50
4. Unified Threat Management (UTM*) devices
    a. Juniper Netscreen 50

Table 3 shows the identified security solutions that perform ARP inspection on ARP packets regardless of the type of inspection.

Table 3. Security solutions performing ARP inspection

	Type	Performing ARP inspection (Yes or No)?	Detection or prevention solution?
Cisco Switch 3560 Series	Switch	Yes	Prevention
Juniper Switches EX3200 Series	Switch	Yes	Prevention
Snort IDS	IDS software tool	Yes	Detection
XArp 2 tool	IDS software tool	Yes	Detection
Sax2 NIDS	IDS software tool	Yes	Detection
Cisco IPS 4425 Series	IPS appliance	Yes	Detection
TopLayer Model 5000	IPS appliance	No	Detection
IBM ISS Proventia Model GX4004C	IPS appliance	No	Detection
SourceFire	IPS appliance	No	Detection
TippingPoint 50	IPS appliance	Yes	Detection
Juniper Netscreen 50	UTM	No	Detection

In the upcoming experiments, we excluded from the above list, the IPS TippingPoint 50 since it includes ARP inspection that is not concerned with the detection of ARP spoofing attack. TippingPoint 50 uses three ARP signatures to check whether or not the Hardware Type and Protocol Type fields in the Ethernet header contain valid values (figure 1). This type of inspection does not allow detecting ARP spoofing.

Among the security solutions that include ARP inspection mechanisms (table 3), table 4 shows the ones that can totally or partially detect the abnormal ARP packets listed in tables 1 and 2.

Table 4. Detection of abnormal ARP request and reply packets

	P#1	P#2	P#3	P#4	P#5	P#6	P#7	P#8	P#9	P#10
Cisco Switch 3560 Series	Detected	Detected	Not detected	Not detected	Detected	Detected	Detected	Detected	Not detected	Not detected
Juniper Switches EX3200 Series	Detected	Detected	Not detected	Not detected	Detected	Detected	Detected	Detected	Not detected	Not detected
Snort IDS	Detected	Detected	Detected	Not detected	Detected	Detected	Detected	Detected	Not detected	Not detected
XArp 2 tool	Detected	Detected	Detected	Partially detected[1]	Detected	Detected	Detected	Detected	Detected	Partially detected[2]
Sax2 NIDS	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected
Cisco IPS Series 4255	Detected	Not detected	Not detected	Partially detected[2]	Detected	Not detected	Detected	Not detected	Not detected	Partially detected[2]

Using the data in Table 4, we can easily notice that no system offers an ideal solution for the problem of ARP spoofing detection. Out of the detection systems, the XArp 2 tool seems ideal in terms of the number of detected abnormal ARP packets. Snort IDS seems to be a good alternative, but both of them perform only detection and are not enable to prevent ARP spoofing attack. The prevention/blocking systems, such as Cisco switches 3560 Series [3] or Juniper switches EX3200 Series [6], are the most ambitious ones, but require usually complex installations. In addition, the high costs of these switches make this solution prohibitive for many companies [4]. Cisco IPS is a prevention system and is a limited alternative solution since it can deal with few types of abnormal ARP packets (P1 and P5). Nevertheless, it is important to remember that the packets P#1 and P#5 are the most used ARP packets during ARP spoofing, since they are the only packets that can corrupt the ARP caches of target hosts. .

Sax2 NIDS cannot detect any abnormal packet described in Tables 1 and 2. However, it can detect ARP request storm traffic and ARP scanning traffic. This type of traffic uses normal ARP packets and it will be described in Section 5.3.

5.1 Cross-layers ARP inspection

In order to be able to detect the abnormal ARP packets P#2, P#6, and P #8 described in Tables 1 and 2, a security solution requires including an ARP inspection mechanism that can perform cross-layers ARP inspection between the Ethernet and ARP headers. In an ARP request and reply packet, the Ethernet source MAC address has to match the ARP source MAC address. However, in ARP reply, the Ethernet destination MAC address has to match the ARP destination MAC address. Table 5 shows the security solutions that include cross-layers ARP inspection mechanism.

Table 5. Security solutions performing cross-layers ARP inspection

	Performing cross-layers ARP inspection?
Cisco Switch 3560 Series	Yes
Juniper Switches EX3200 Series	Yes
Snort IDS	Yes
XArp 2 tool	Yes
Sax2 NIDS	No
Cisco IPS 4425 Series	No

5.2 ARP statefull inspection

ARP replies should normally follow ARP requests. A statefull detection process should remember all ARP requests originating and match them to ARP replies. Many ARP spoofing tools send ARP replies that are not requested. Table 6 shows the list of security solutions that perform ARP statefull inspection on ARP requests against ARP replies. ARP inspection mechanism might give false positives in some cases as machines want to distribute their IP-to-MAC mapping to other machines that did not request it. Among the above tested security solutions, XArp 2 tool and Sax2 IDS are the only solutions that perform ARP statefull inspection.

Table 6. Security solutions including ARP statefull inspection

	Performing ARP stateful inspection?
Cisco Switch 3560 Series	No
Juniper Switches EX3200 Series	No
Snort IDS	No
XArp 2 tool	Yes
Sax2 IDS	Yes
Cisco IPS 4425 Series	No

5.3 ARP request storm and ARP scan

ARP request storm: Dynamic ARP entries remain in the ARP cache for few minutes then they are removed if they are referenced. Consequently, to keep the ARP cache of a target host corrupted with fake entries, malicious users may storm the target host with ARP request packets. In other words, the malicious host keeps sending continuously fake ARP request packets to the target host. If the number of ARP request packets per second exceeds the ARP request threshold, then this is an indication that an ARP request storm is taking place. Table 7 shows the security solutions that include mechanisms to detect ARP request storm and/or ARP scanning. Among the above tested security solutions, Sax2 IDS is the only solution that is able to detect ARP request storm and ARP scanning.

ARP scan: The possible reason of ARP scanning in LAN networks is surveillance software running, host infected with virus, or the virus is doing ARP scanning.

Table 7. Security solutions including ARP request storm and/or ARP scan detection mechanisms

	Detect ARP Request Storm?	Detect ARP Scan?
Cisco Switch 3560 Series	No	No
Juniper Switches EX3200 Series	No	No
Snort IDS	No	No
XArp 2 tool	No	No
Sax2 IDS	Yes	Yes
Cisco IPS 4425 Series	No	No

6. Experiments' Results Analysis

The experiments in this work show clearly that ARP spoofing is not fully detected by most common security solutions. This is because of the absence of an efficient ARP spoofing detection algorithm. There are abnormal ARP packets that do not corrupt ARP caches. However, they are still harmful and should be detected, since they can carry DoS attacks.

In addition to detecting some abnormal ARP packets such as P#2, P#6 and P#8, cross-layer ARP inspection is required. Among the tested security solutions, only Cisco switch 3560 Series, Juniper switch EX3200 Series, Snort IDS, and XArp 2 tool perform cross-layers ARP inspection.

On the other hand, security solutions should be able to remember all ARP request originating and match them to ARP replies. This can be achieved by using ARP statefull inspection. XArp 2 tool and Sax2 IDS are the only security solutions that perform ARP statefull inspection.

Security solutions should also be able to cope with ARP request storm traffic and ARP scanning traffic. This type of traffic is used usually to keep target hosts' ARP caches corrupted or produce DoS attack. Sax2 IDS is the only security solution that is able to detect ARP request storm and ARP scanning.

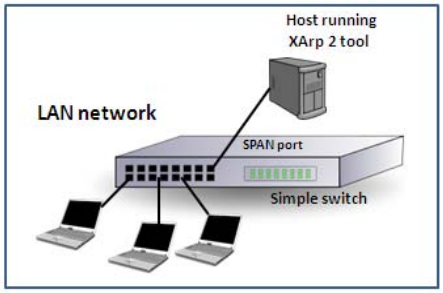

Figure 8. A LAN network with simple switch and XArp 2 tool

According to the conducted experimental results, XArp 2 tool is the most efficient available security solutions to cope with ARP spoofing. However, it needs minor improvement, compared to the other tested security solutions, by adding mechanisms to detect ARP request storm and ARP scanning. Figure 8 shows a LAN network that uses a simple switch without any security features and a host running XArp 2 tool to detect ARP spoofing attack. The host running XArp 2 tool is connected to a SPAN port (mirroring port) in order to be able to receive and analyze all the LAN network traffic. This network architecture is considered ideal in terms of its low cost and its efficiency regarding the detection of ARP spoofing. However, this network architecture cannot prevent ARP spoofing, unless the simple switch is replaced by a more costly switch that integrates advanced security features. Cisco switch 3560 Series [3] and Juniper switch EX3200 Series [6] are examples of highly cost switches that can prevent ARP spoofing using a feature called Dynamic ARP Inspection (DAI).

7. Requirements for Ideal Algorithm for ARP Spoofing Detection

Based on the experiments results, our work concludes that any security system claiming to cope with ARP spoofing, should use an efficient algorithm. We compiled six requirements that any Security analyst should follow in order to get an ideal algorithm that deals with ARP spoofing on switched LANs:

1. Perform a cross-layer ARP inspection between the Ethernet and ARP layers
2. Perform ARP statefull inspection
3. Detect non expected IP and MAC addresses
4. Detect ARP storm
5. Detect ARP scanning
6. Build manually (in case of non DHCP environment) or automatically (in case of DHCP environment) IP-MAC

mapping table, in order to be able to detect invalid IP-MAC pairs.

8. Conclusion

In this study, we conducted an extensive work to know which Security Solutions are able to detect a very dangerous MAC layer attack called ARP Spoofing. It is to be noted that ARP Spoofing constitutes the beginning of many attacks, one of which is, the destructive MiM attack. We were able to show throw testing and experimentation that the current Security Solutions has many shortcomings and defects when it comes to detecting ARP Spoofing. XArp 2 tool was the most efficient available security solution that can cope with ARP spoofing attacks. However, it needs minor improvements, compared to the other security solutions, by adding mechanisms to detect ARP request storm and ARP scanning.

The experimental results discussed in our work can be used to assist security instructors in selecting the appropriate security solutions to be used during the hands-on labs, as well as for building secure LAN network. In addition, Security courses that deal with intrusion detection in LAN networks can use our experimental results as additional/supporting material to describe ARP spoofing and the available detection and prevention mechanisms. As a conclusion of our study, we suggested 6 basic and crucial requirements that any algorithm should follow in order to detect ARP spoofing on switched LANs.

9. REFERENCES

[1] ARP Spoof Tool, http://www.imfirewall.com/en/arp-spoof.htm.

[2] Cain & Abel, http://www.oxid.it/cain.html.

[3] Cisco Catalyst 3560 Series Switches, http://www.cisco.com.

[4] Cristina L. Abad, Rafael I. Bonilla, "An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks", Proceedings of the 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), June 22 - 29, 2007.

[5] D. Plummer. An Ethernet Address Resolution Protocol, Nov 1982. RFC 826.

[6] Juniper Switches EX3200 Series, http://www.juniper.net

[7] SwitchSniffer, http://www.nextsecurity.net/software/SwitchSniffer.html

[8] Winarp, http://www.arp-sk.org

[9] WinArpAttacker, URL: http://www.xfocus.net/tools/200606/WinArpAttacker3.50.rar

[10] WinArpSpoof , http://www.nextsecurity.net/software/Windows_ARP_Spoofer.html

[11] Zouheir Trabelsi, and Khaled Shuaib, "A Novel Man-in-the-Middle Intrusion Detection Scheme for Switched LANs", the International Journal of Computers and Application, ACTA Press, Vol. 3, No. 3, 2008.