

A Holistic Approach to ARP Poisoning and Countermeasures by Using Practical Examples and Paradigm

Faisal Md Abdur Rahman*, Parves Kamal**

*International Islamic University, Chittagong, Bangladesh

**University of Bedfordshire, London, United Kingdom

Corresponding Author Email: parves.kamal@gmail.com

Abstract

The main purpose of this Paper is to discuss the mechanism and detection of ARP spoofing. It can be said that an Address Resolution Protocol, simply known as ARP, plays an essential part in Computer Science and Forensics. Nowadays, there are many people who use computer hacking techniques like ARP spoofing to send fake ARP messages on a Local Area Network (LAN). Such attacks may result in traffic alteration, or even worse, in a temporary or permanent interruption of traffic. In spite of the fact that this attack is limited to networks which have Address Resolution Protocols, ARP spoofing can be the first step to being subjected to more serious attacks capable of causing much more damage. When someone wants to initiate this kind of attack, he will look for the weak points of the Address Resolution Protocol. For example, he may be seeking to exploit vulnerabilities such as its inability to successfully authenticate the person who is sending the message. This can make it particularly easy for hackers to modify or steal people's data. ARP Spoofing represents a real threat to the security of all users from the network and that is why, all the measures necessary to reduce damage must be taken.

Keywords: ARP spoofing, DHCP Snooping, Dynamic ARP Inspection, Cain and Abel, SSL Strip.

1. Introduction

The Address Resolution Protocol (ARP) is known to be very susceptible to spoofing attacks because it doesn't provide a reliable way to verify the sender's identity. Its lack of state sometimes increases the risk for more dangerous attacks. Session hijacking, denial of service or man-in-the-middle attacks represent harmful actions which are capable of causing serious damage to the Local Area Network. When it comes to detecting spoofing attacks, the existing approaches are considered to be passive and therefore, not efficient. Keeping track of the ARP traffic and searching for discrepancies in the Ethernet wastes time and as a consequence, the attack cannot be discovered in its early stages. The main purpose of this paper is discussing an active method which effectively detects ARP spoofing and explaining a very useful technique which allows forensic investigators to find proofs directly from the source computer. A presentation on how to detect ARP poisoning attacks is included in the network security practice.

1.1 Aims and objectives

Attacking a computer on a secure network environment to trace vulnerability of the network through passive ARP poisoning and find out possible way to makeover. In technical term, Address Resolution protocol will be poisoned to see what kind of information about the target computer can be detected during attack as the target computer will be convinced to send replies packets through attacker machine. As ARP is a stateless protocol (Whalen, 2001), computer updates ARP cache with the existing one if a new ARP reply is received. So this thesis is how this could lead an investigation and how after all we can take countermeasures on this.

2. Design and deployment

Virtual machine environment will be used to design the artifact where the project will be demonstrated through showing some attack mechanism on ARP poisoning, attack source detection on the network and will discussed important countermeasures (An automatic intrusion detection system) to prevent this attack on the network.

2.1 Attack outcome and analysis

Attacking tools are available. And knowledge source on this environment is getting more popular. So the security risk is increasing. However most of the people are unaware about the attack and the severity of it. The survey on current market analysis is essential in this regard that shows exactly how important it is

to study on this sector to protect users around the world. A risk analysis shows the possibility of this attack on the network and it measures the potential threat recovery rate. In the Computer Forensic investigation, metasploit and some other computer network analysis and penetration testing tools are used to access the target computer, changing, creating and deleting information as well as getting relevant information out from the file system. But ARP attack is a powerful attack in the investigation field indeed as it reveals network traffic and can subject to cause serious attack as discussed (HTTPS information revealing from SSLSTRIP, VoIP forensic etc.)

2.2 Basic Ideology of Address Resolution protocol (ARP)

Address Resolution Protocol, also known as ARP, establishes a link between an actual computer address, otherwise known as a Media Access Control or MAC, to an IP address. ARP permits the network to detect the device and incorporate it as a component of the structure. This particular method was utilized with earlier systems (Tony, 2007). More recent methods include IP 6 versions and IP 4 version which is more commonly used at present. An address in the IP 4 version is 32 bits in length. In a Local Area Network, or a LAN, however, the length of an address for all linked devices is 48 bits. Each computer has its own database called the ARP cache, which contains IP addresses for ARP requests. The ARP cache comprises Internet addresses that match them and facilitates faster and more efficient functioning of the computer by reducing the load of the bandwidth. Once a request has been made, the originating computer finds the information on the ARP cache. A request is then sent out when the necessary data are located (Tony, 2007). The entire process usually takes 15 minutes although the exact duration is determined by the type of operating system utilized. RFC 1122 deems it preferable to permit users to configure this timeout setting for every computer and device. All that is needed to perform this on Microsoft Windows, Linux or UNIX system is to key in “arp-a” (Tony, 2007). The ARP outlines the procedure for setting this up and ensures that the addresses are compatible. The ARP converts the data in every direction as well.

2.3 How ARP Works

This is recommended to all readers of this thesis report to have knowledge of ARP mechanism and this is the reason why this section is deployed. Sending information from a networked computer to a host is done via what is called a gateway. What this gateway does is as follows: after communicating with the ARP program, it requests a MAC address or location corresponding (Cox, 2005) to the IP address, an address which the ARP program attempts to verify. If verification of the IP address is completed, the information is sent back to the gateway via which data, such as type and length, can be formatted accordingly. Contrarily, when the IP address fails to be verified by the ARP program, the data is then dispersed amongst every machine connected to the network so that they may attempt to receive verification. If the IP address belongs to a particular computer, then that computer will identify itself as the intended recipient. Additionally, the IP address will be added to the ARP cache archive for further use, allowing the information to be sent to the MAC address of the particular computer. For instance, let's say Karen, who is a new employee at the business, wants a copy of all names and addresses of the entire staff to update the company roster and thus needs to use the printer in the office across the hall. Her computer's IP address is 192.148.0.15 and the printer's IP address is 192.178.0.44. Her computer will basically send out an ARP request through the entire network in order to find the exact IP address of the printer. See Figure1 for this example.

As each computer in the network receives the notice, it checks to see if it is the correct location for the ARP request. If not, it does nothing (Cox, 2005). When the actual printer receives the notice, it sends the confirmation back to let the network know it's the destination IP address 192.178.0.44 and that its MAC address is 00:90:7F:12:DE:7F, as shown in the figure. Karen's computer instantly knows where to send the information and passes it on. At the same time it stores the MAC address of 00:90:7F:12: DE: 7F and correlates it to the IP address 192.178.0.44 for the printer. This entire event only happens when the recipient of the request is part of the network. If the recipient computer is not on the same network, the host computer will check its database for the exact router that needs to be used in order to connect to another network. Once it locates the correct router, it will use the Internet address of the router in place of the other IP address in the request. The new Internet address will contain the complete information of the original IP address. As the router receives the data, it scans the information to locate the address it needs to send the information to. The router then passes on the ARP request using its own cache.

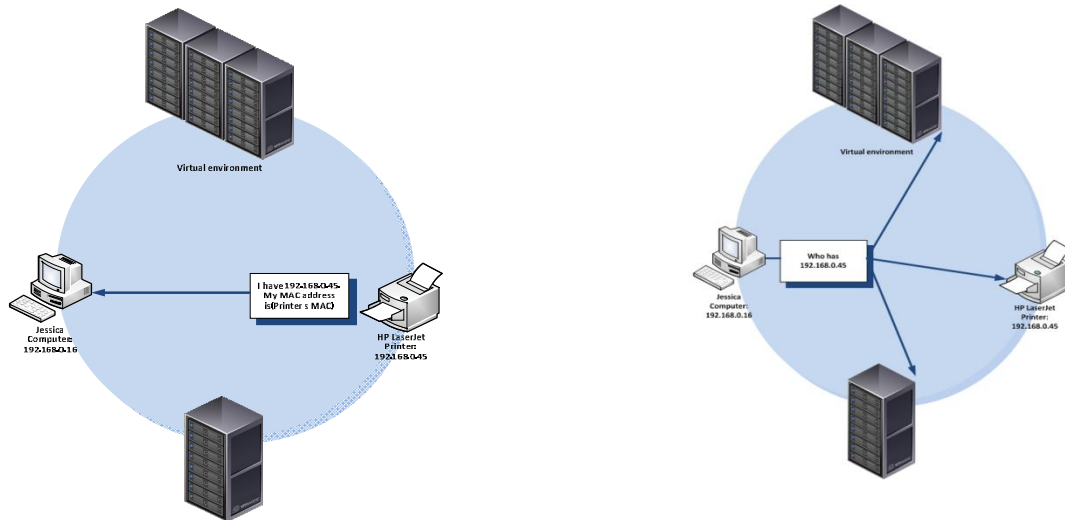


Figure 1: ARP Functionality

2.4 Frame Format

The structure of the ARP request includes the Internet title and data information (Desai, 2007). Included in the heading is the following:

- 6 byte Internet location address.
- 6 byte Internet host address.

The frame type is 0806 hexadecimal for ARP and 8035 for RARP

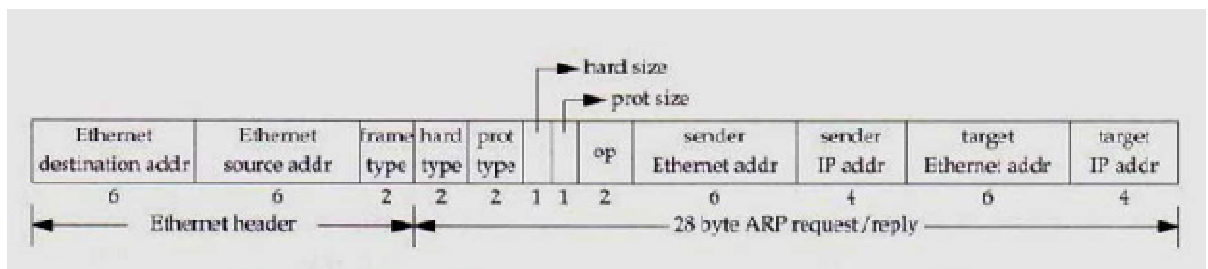


Figure 2: ARP frame format

Type of hardware addresses (2 bytes). 1=Internet.

Type of protocol address being used (2 bytes). 0800H (hexadecimal) = IP address.

Size in bytes of hardware addresses (1 byte). 6

Size in bytes of protocol address (1 byte). 4

Type of information. 1 = ARP request, 2=ARP reply, 3=RARP request, 4=RARP reply.

The sender's Internet address (6 bytes)

The sender's IP address (4 bytes)

The recipient's Internet address (6 bytes)

The recipient's IP address (4 bytes)

(At the time of the response by the ARP, the Internet address of the receiver is not provided.)

2.5 Vulnerable Operating systems for ARP attack

When an operating system is tricked by another operating system, it's called ARP spoofing. If a request is made for a certain piece of data that doesn't exist within the system, the targeted operating system is forced to add it to the database. Alternately, if the data does exist, the original system is told to overwrite it with new information. Here's a look at the types of systems and their vulnerabilities:

- Windows NT
- Windows XP
- Windows 95/98/2000
- Linux
- Netgear
- AIX 4.3 OS is not Vulnerable to ARP

2.6 Wireless Network and security

The wireless networks security has become recently of great importance topic owing to the standards included in 802.11b. They have been thoroughly studied because of the many violations that we've all heard over the years. Because they are available for anyone to see, they are an easy target for the ruthless and can be used to access computers. Wired computers, once considered very safe, become vulnerable to threats once they are open to wireless networks (Osborne, 1998). They can no longer be trusted as totally secure. They allow unlimited computers to connect to the other, as well as other cable networks via a WAN. For wireless networks to operate, they must be connected to a wired computer. This document will discuss the differences between wired and wireless networks when it comes to threats.

Some threats can only come from the same LAN via ARP, or Address Resolution Protocol. This is the cache used by the MAC. A hacker must be connected to the network to access computers in this document (Osborne, 1998). Because it occurs on a network contained, the damage that this limited number of machines connected with hubs or switches. If the network computers are connected to a router, then the tainted data would be allowed to continue on other LANs. 802.11b allow information to travel through a system comprising both wired and wireless data computers. Then contaminated would be allowed to continue on other LANs. 802.11b allow information to travel through a system comprising two wired computers and two computers without file which Complement wired and wireless.

Once the threat is through an access point, it can infect any computer connected to the system. From there, the information travelling between computers is fair game and the data can be blocked from reaching its destination (Osborne, 1998). It does not matter if the network is wired or wireless at this point, all computers are vulnerable. This brings us to the concern of a user through the Internet connected to a router. These connections are easy to hack.

3. Attack mechanism and methodologies

ARP spoofing is an acronym that stands short ARP for Address Resolution Protocol. When a computer on a local (LAN) network wants to communicate with another computer or virtual machines, it broadcasts a request in to the network (LAN) that ask which computer has this IP address in the network. The computer that is assigned that fix IP address or DHCP then responds with its MAC address (Media Access Control address), and the originating computer can then send its data over network. This works very well when all of the computers or virtual machines agree to only respond to their own requests; however, there is no check tracking in the protocol to verify that the response is correct or not. Instead, the computers just trust that nobody will respond inappropriately to this ARP requests.

3.1 Mechanism of attack

ARP attack mechanism is simple and it takes just specific software that can do the action perfectly. There are some windows and Linux based utilities those can handle the attack from the beginning. Apparently, an attacker needs to have no knowledge about ARP header and footer in the ARP frame to initiate attack using the utilities. One of the most simplified and most easy GUI based windows utilities is Cain and Abel. It has much functionality beside ARP poisoning to its post attack like it has functionality to do eavesdropping on VoIP call as part of post attack of ARP poisoning. Another sophisticated and complex mechanism of performing the same attack from the Linux Backtrack machine

that usually initiate same approach as like as Cain and Abel but has many build in utilities that can initiate a number of intelligent attack on the target computer as well as the target network (e.g. RTP flooding, RTP injection, local Denial of Services (DoS) attack etc.)

3.2 Attack approaches

3.2.1 Poisoning ARP cache

ARP poisoning is called man in the middle attack as it diverts network traffics through the attacker machine that gives the ability to over-watch the transmitted packets between two endpoints where the victim's computer cannot point out the real problem. This term is mentioned as ARP cache poisoning.

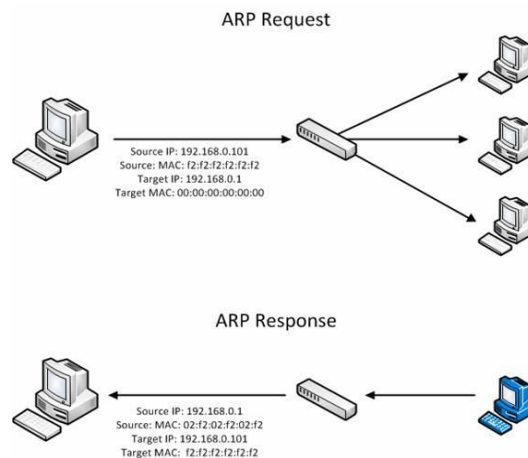


Figure 3: ARP communication process

As the ARP is stateless protocol in its nature, the computers on the network just update ARP reply each time that does not include checking the previous cache file. So the attacker have chance to poison ARP cache. When communication initiates, computer sends an ARP request to all computers on the network asking who is with this identification (includes IP address). And the correct computer responds with its MAC address. During attack, the attacker computer resolves the same identity of MAC address to the victim's computer to impersonate him and that is how the attacker goes into a listening mode where he can see all transmitted packets. So the figure 4 below shows exactly what our attacking machine does during attack.

3.3 Attack detection

Detection can be done using a professional network engineering utility: Colasoft-capsa 9.0, a new upgraded version that can be used for detecting ARP storms on the network. But detection of it needs contentious traffic monitoring. In many researches, many techniques were having been proposed to give a permanent solution that can stop further traditional ARP spoofing on the network.

3.3.1 Replacement of ARP

This is a research on S-ARP that stands for Secure ARP, propose to replacement of ARP protocol from the network stack that will provide a permanent solution for the ARP spoofing. Although it has limitations like if this technique is applied, the network will not be very scalable and will cause vendor problem during upgrade and as this use DSA, there will have some additional cryptographic algorithm will be added to it.

3.3.2 Static MAC addresses implement

This is another solution against ARP spoofing but has same limitation as it will cause difficulties in network scalability. And for wireless network this is a challenge and almost like impossible where new mobile wireless devices connect simultaneously.

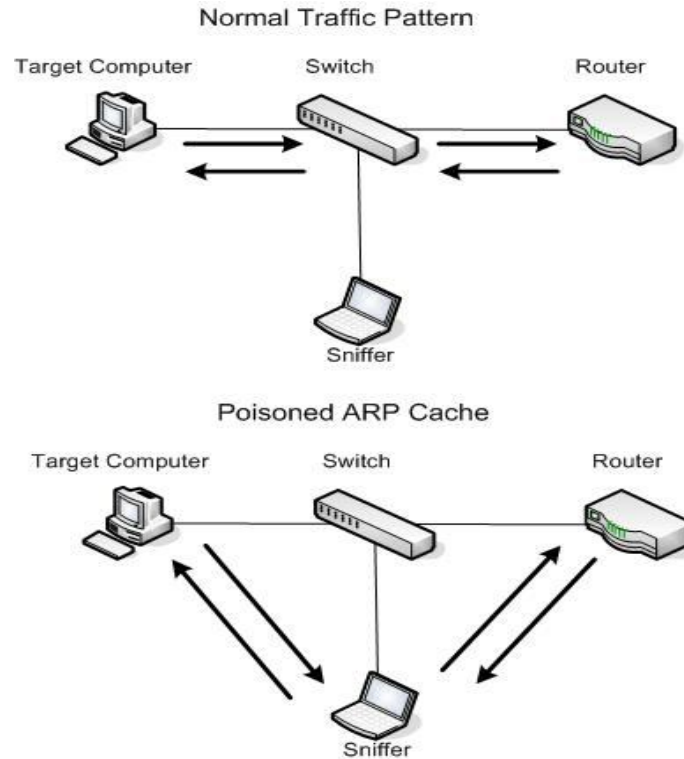


Figure 4: Intercepting Communication with ARP Cache Poisoning

3.3.3 Patching

Kernel based patches mechanism is almost expectable in preventing ARP spoofing. Utilities such as Anticap and Antidote can play a vital role in preventing this where Anticap prevent updating the ARP cache with different MAC with the existing ARP cache which actually prevent the ARP spoofing but it violates the ARP protocol specification which indeed a problem where on the other hand Antidote prevents the ARP poisoning slightly different way. It analyzes the newly received ARP reply with the existing cache. If the new cache differs with the previous then it look for the MAC address if it still alive. If it found the previous cache MAC address alive, rejects the new one and it adds the attacker MAC address in the list of banned MAC address to prevent further attempts from the ARP poisoning on the same target computer.

3.3.4 Passive detection technique

This report will show how easily a network administrator or network security manager can detect ARP attack on the network unlike active attack where ARPWATCH and another same kind of windows GUI based application like COLASOFT CAPSA 9.0 can detect active ARP poisoning on the network. In our artifact section we will show a process of how spoofed ARP reply packets can be detected in brief. (Vivek Ramachandran, S. N. (2006))

3.4 Planning background

Detection is much more important in case of any security threat. Attacking mechanism is important for a forensic investigation to get forensically more evidence from a suspect. However it is important and a very essential to protect the hosts from being a victim of ARP spoofing as it leads many serious attack on the network.

4. Artifact Planning, Design and Description

In the first section of this part of the report we will describe an artifact that clearly shows the techniques behind ARP poisoning attack both from windows based attacker machine and from Linux based attacker machine. The second part of this section will describe the passive mechanism of ARP detection on the large environment in a sophisticated and more advanced way.

4.1 The artifact

The artifact is virtualized for demonstration purpose. VMware workstation is used to create several virtual workstations. Two windows based attacker machine is created for the attack initiation and attack detection accordingly. Another Backtrack 5 based virtual workstation is used to initiate initial ARP attack as well as some other peripheral attacks using ARP spoofing. The target victim computer is a Windows operating system.

4.2 Virtual machines installation and configuration

All virtual operating systems was downloaded from the original source as ISO image file those after that were installed in VMware workstation. The installation process is not stated here as it is not a part of this thesis report. VMware workstation helpline guide gives clear instruction about how to install and virtual machines on a single host machine.

4.3 Network configuration

We used bridged network connection on each of the virtual machine. That means the VMware workstation will configure the network settings as like physical computers are using the network automatically. So the virtual machine will use the same network that the physical machines are using under the network. This configuration will provide us to do the experiment on the actual physical network. However we can use the NAT configuration that will provide us a unique virtual network environment.

The following shows a simple map of our VMware based artifact.

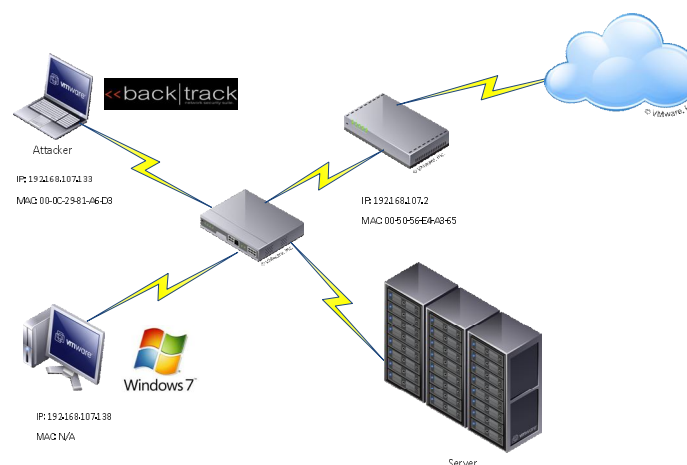


Figure 5: Artifact map

4.4 Tools and techniques

As stated before, we can use both Windows and Linux based utilities to initiate an attack. There are many windows based utilities available in open source market. On Backtrack, we have built in facilities to do ARP poisoning.

4.4.1 Windows based attack

Windows based attacking tools are GUI based and easy to use although they provide fewer utilities to the hacker, hacker can initiate easy attack with little prior knowledge on the protocol. So windows based attacking tools are comfortable for the forensic investigator to take initial scope in a short period of time. The table below shows detailed information what we used during attacking on the virtual environment.

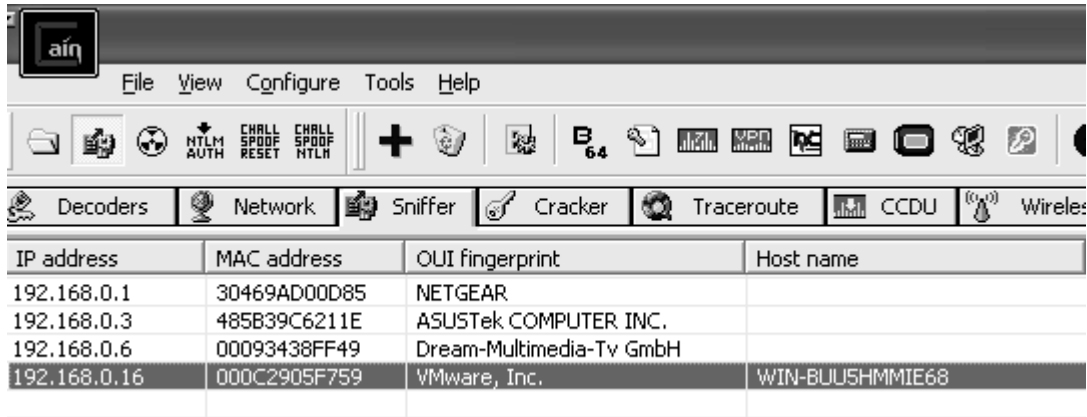
4.4.2 Short details

Subject	Description
Objective	To show how easily penetration testers and forensic investigators can use these facilities to initiate a primary attack.
Tools	Cain and Abel, Wireshark
Utilities	This is a sniffer as well as ARP poisoner.

4.4.3 Cain and Abel: Freeware network penetration utility

We used Cain & Abel as easy windows based network penetration testing utility to check the network configuration is vulnerable for the ARP spoofing attack. The following process logs were followed to initiate poisoning (see table 1).

Table 1: Process Logs

Process logs																							
Cain and Abel is a open source and freely available on http://www.oxid.it/downloads/ca_setup.exe .																							
When we are on the main panel, we will find sniffer utility on the top right menu. We have to activate to allow the software sniffing packets.																							
On the sniffer page at the software we will be able to resolve MAC address of other network computers. In this case we are attacking on a windows 7 based computer whose MAC is 00-0C-29-05-F7-59 with IP address 192.168.0.16																							
 <table border="1"> <thead> <tr> <th>IP address</th><th>MAC address</th><th>OUI fingerprint</th><th>Host name</th></tr> </thead> <tbody> <tr> <td>192.168.0.1</td><td>30469AD00D85</td><td>NETGEAR</td><td></td></tr> <tr> <td>192.168.0.3</td><td>485B39C6211E</td><td>ASUSTek COMPUTER INC.</td><td></td></tr> <tr> <td>192.168.0.6</td><td>00093438FF49</td><td>Dream-Multimedia-Tv GmbH</td><td></td></tr> <tr> <td>192.168.0.16</td><td>000C2905F759</td><td>VMware, Inc.</td><td>WIN-BUUSHMMIE68</td></tr> </tbody> </table>				IP address	MAC address	OUI fingerprint	Host name	192.168.0.1	30469AD00D85	NETGEAR		192.168.0.3	485B39C6211E	ASUSTek COMPUTER INC.		192.168.0.6	00093438FF49	Dream-Multimedia-Tv GmbH		192.168.0.16	000C2905F759	VMware, Inc.	WIN-BUUSHMMIE68
IP address	MAC address	OUI fingerprint	Host name																				
192.168.0.1	30469AD00D85	NETGEAR																					
192.168.0.3	485B39C6211E	ASUSTek COMPUTER INC.																					
192.168.0.6	00093438FF49	Dream-Multimedia-Tv GmbH																					
192.168.0.16	000C2905F759	VMware, Inc.	WIN-BUUSHMMIE68																				
Now we can access APR page of the software on the lower left corner. After that. From the top menu, we have to select add-to-list button to configure the communication segment we want to poison. The following figure will appear where on the left hand side we need to select the default gateway and on the right side we have to select the target computer.																							

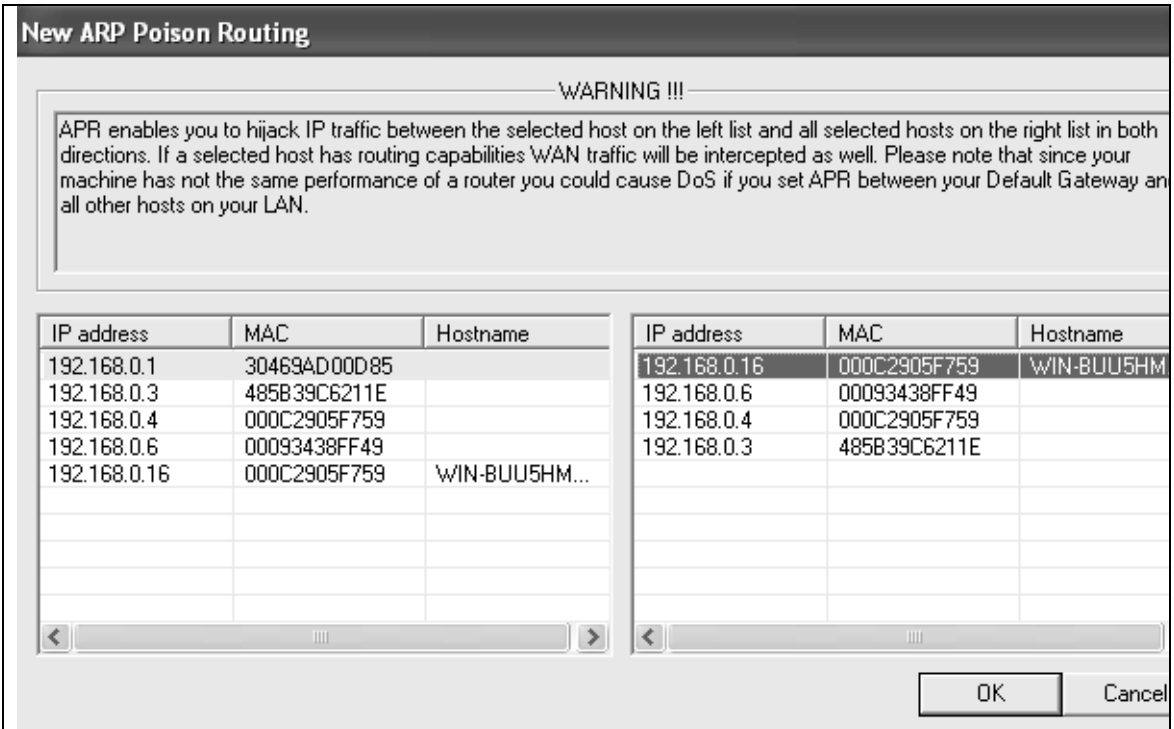


Figure 6: ARP configuration screen

The main process is done. Now we need to initiate ARP poisoning by clicking Yellow button on the top left beside sniffer button. Now we will see that the attacker computer is getting all packets and can trace the victim's network behaviour as packet. So communications are being sniffed now like as followed.

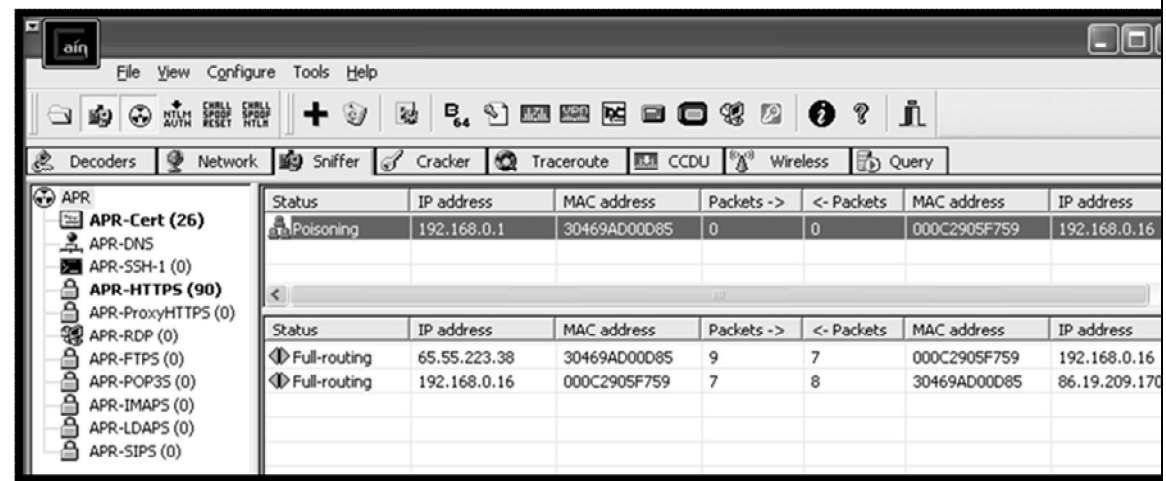
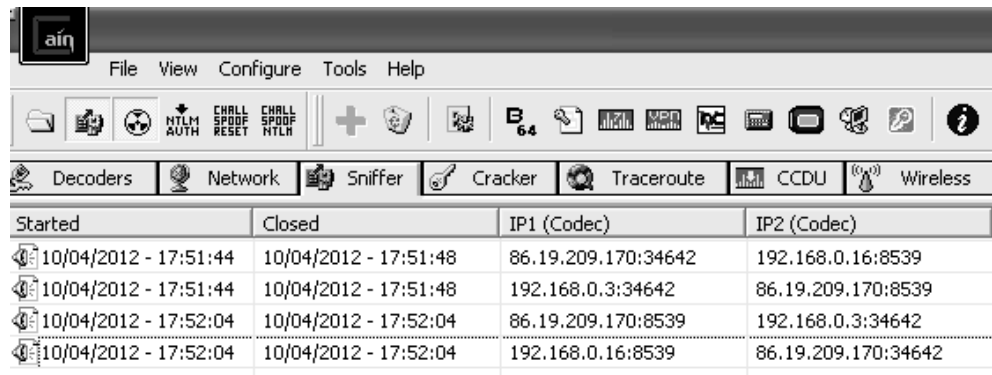


Figure 7: ARP poisoning initiated

So ARP is poisoned now on the network and all packets those are being transmitted to and from the victim's computer will be sniffed by the attacker. The next attempt of the attack which Cain & Abel does provide is VoIP sniffing attack which can record RTP packets from the VoIP communication. For this I initiated a Skype call to another network host that uses RTP packets to transmit digital audio and video on the network. As a result of successful ARP poisoning, I captured the RTP packets on the Wireshark and the Cain & Abel recorded and saved the RTP packets in .mp3 and .wmv format after successful decoding. Figures show the details.



Started	Closed	IP1 (Codec)	IP2 (Codec)
10/04/2012 - 17:51:44	10/04/2012 - 17:51:48	86.19.209.170:34642	192.168.0.16:8539
10/04/2012 - 17:51:44	10/04/2012 - 17:51:48	192.168.0.3:34642	86.19.209.170:8539
10/04/2012 - 17:52:04	10/04/2012 - 17:52:04	86.19.209.170:8539	192.168.0.3:34642
10/04/2012 - 17:52:04	10/04/2012 - 17:52:04	192.168.0.16:8539	86.19.209.170:34642

Figure 8: Recording RTP files from VoIP call through ARP attack.

4.4.4 Linux-Backtrack Attack to initiate ARP poisoning

Backtrack is an open source Linux distribution that is free to download and is a professional penetration testing tools combined with more than 400 build in penetration testing tools. Using Backtrack (Backtrack 5, the latest release) for ARP spoofing gives more reliability and so solid output instead of windows based attacking mechanism and data acquisition technique. As security professional, it is the first choice of most of the Computer security engineer. we used the build in terminal and command to initiate ARP spoofing. Then we initiated a test post attack using SSLSTRIP 0.9 to sniff the HTTPS entry from the target computer.

Important note: ARP spoofing from Backtrack machine just need single line command. But it cause sending continuous ARP packets to the victim make ARP flood or ARP storm and the victims computer act like there is connection problem or offline although the network connection indicator shows the computer is online.

ARP Storm on Victim's computer (spoof mechanism)

On our virtual machine scenario, the victim is now 192.168.0.15 (Windows). I shall initiate attack from backtrack VM which IP is 192.168.0.2. Attacking processes are as followed.

Process log

1. On the Backtrack machine "ifconfig" command will show the network information of that machine where we have to look at the IP address and the default gateway to make sure the victim is under the same network.
2. "eth0" is recorded as network adapter on Backtrack, will be used on ARP spoof command.
3. On the terminal, the following command will start ARP spoofing as well as ARP flooding at the target computer and will monitor all packets between the target host and default gateway.
4. Command: arpspoof -i (interface) eth0 -t (target) 192.168.0.15 (target pc) 192.168.0.1 (default gateway)
5. This command will initiate the attack instantly and will show continuous ARP reply information as in the figure.

```

root@bt:~# arpspoof -i eth0 -t 192.168.0.15 192.168.0.1
0:c:29:f1:fa:db 0:c:29:e9:c5:b9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:f1:f
a:db
0:c:29:f1:fa:db 0:c:29:e9:c5:b9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:f1:f
a:db
0:c:29:f1:fa:db 0:c:29:e9:c5:b9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:f1:f
a:db
0:c:29:f1:fa:db 0:c:29:e9:c5:b9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:f1:f
a:db
0:c:29:f1:fa:db 0:c:29:e9:c5:b9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:f1:f
a:db

```

Figure 9: Spoofed ARP reply initiated

Related attack

As we have stated earlier that ARP leads some serious attack on the computer users. During research study, I have found how SSLSTRIP-0.9 utility from attack can capture username and password in plain word from HTTPS pages. This is a serious threat to the internet users as most all secure websites (e.g. online banking, facebook etc.)

Test attack

To measure how serious the attack is and what is the success rate of this attack, we simulated an attack on our facebook account during experiment and the attack reveals our facebook username/email and password in plain word on Backtrack attacker machine.

Attack process

SSLSTRIP-0.9.tar.gz file needs to download and install on the Backtrack. Python and twisted-web python is pre-requisite for this installation (normally comes in default on Backtrack 5).

Running SSLSTRIP

- First of all, my attacker Backtrack machine is flipped into forwarding mode.
- Command: (echo "1" > /proc/sys/net/ipv4/ip_forward)
- Then I used to configure iptable to redirect HTTP traffic to sslstrip.
- Command: (iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port <listenPort>)
- Then this is time to run SSLSTRIP.
- Command: (sslstrip -p -l <listenPort> 1000)

```

root@bt:~# echo 1 > ./proc/sys/net/ipv4/ip_forward
bash: ./proc/sys/net/ipv4/ip_forward: No such file or directory
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@bt:~# iptables -t nat -A PREROUTING -p tcp --destination port 80 -j REDIREC
T --to-port 1000
Bad argument `80'
Try `iptables -h' or 'iptables --help' for more information.
root@bt:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIREC
T --to-port 1000
root@bt:~# sslstrip -p -l 1000

sslstrip 0.9 by Moxie Marlinspike running...

```

Figure 10: SSLSTRIP is running

LOG FILE: On a new tab: (tail -f sslstrip.log). Note: This screen will show all required user entry information (username and passwords) when I initiate ARP spoofing attack with next command.

Run arpspoof to convince a network they should send their traffic to you. (arpspoof -i <interface> -t <targetIP> <gatewayIP>)

```
root@bt:~# tail -f sslstrip.log
2012-04-17 13:07:52,114 SECURE POST Data (www.facebook.com):
lsd=AVqbbvwC&email=faisalnsu234%22gmail.com&pass=wasdesdf&default_persistent=0&c
harset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%D0%94%2C%D0%8
4&timezone=-60&lgnrnd=100733_USfs&lgnjs=1334682456&locale=en_US
```

Figure 11: SSLSTRIP log

This log shows that where the user is (www.facebook.com) and which credentials did he enter. On the second line, this is clear that the email and password is sniffed in plain word. This is indeed a danger.

4.5 Detection mechanism

Anticap and Antidote can protect the network from ARP spoofing by stopping the cache update but those violate the ARP protocol specification. Although patching mechanism is best solution for the network it is not possible for its specification violation. On the other hand, if the static MAC entries and if we replace ARP with S-ARP, the network will not be scalable.

So detection mechanism is the best solution before going for active prevention mechanism. In this thesis, we are recommending COLASOFT-CAPSA, windows based software that monitors the entire network and can give alarm notification to the network administrator about the location of the attacker computer including MAC address of the attacker almost instantly. The figure shows an example of detection of ARP storm.

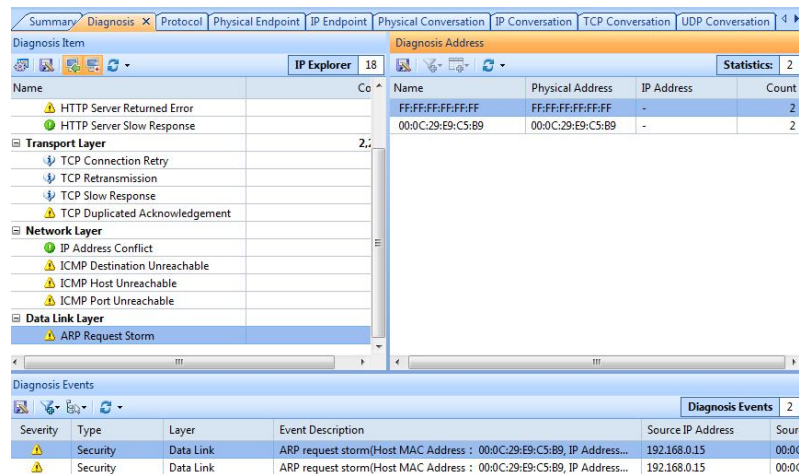


Figure 12: An example of detection of ARP storm

5. Countermeasures to ARP Attacks:

Dynamic ARP inspection in cisco systems helps prevent the man-in-the-middle attacks by not relaying invalid or gratuitous ARP replies out to other ports in the same VLAN. Dynamic ARP inspection intercepts all ARP requests and all replies on the untrusted ports. Each intercepted packet is verified for valid IP-to-MAC bindings via DHCP snooping. Denied ARP packets are either dropped or logged by the switch for auditing so ARP poisoning attacks are stopped. Incoming ARP packets on the trusted ports are not inspected. Dynamic ARP inspection can also rate-limit ARP requests from client ports to minimize port scanning mechanisms. Dynamic arp poisonings uses the information from DHCP Snooping table. (Figure -11)

```
sh ip dhcp snooping binding
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:03:47:B5:9F:AD	10.120.4.10	193185	dhcp-snooping	4	FastEthernet3/18
00:03:47:c4:6f:83	10.120.4.11	213454	dhcp-snooping	4	FastEthernet3/21

It Looks at the MacAddress and IpAddress fields to see if the ARP from the interface is in the binding, if not, traffic is blocked. (Yusuf Bhaiji)

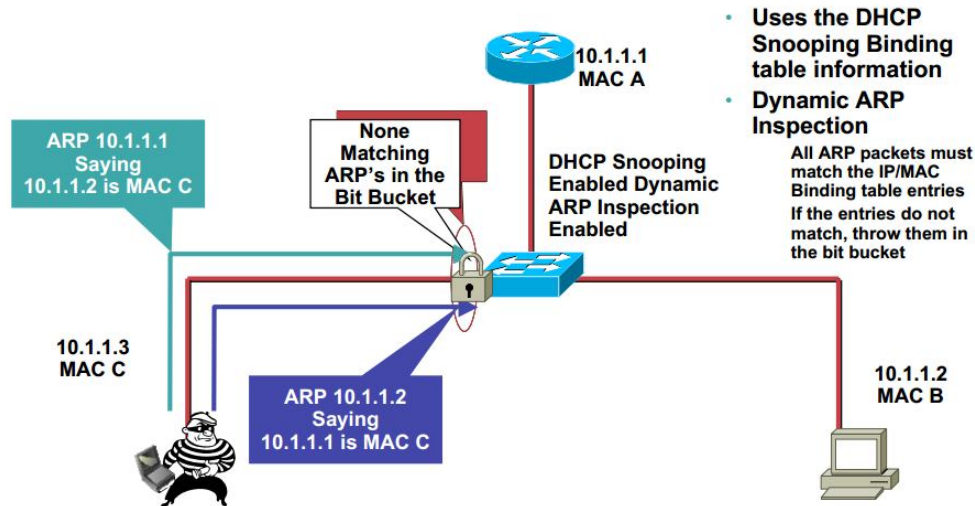


Figure 13: Dynamic ARP INSPECTION USES DHCP Snooping Table

6. Conclusion

After having substantial knowledge on Address Resolution Protocol, its functionality, packet format, reply mechanism, cache updating systems; it seems that the ARP is a vulnerable protocol on networking although this is so essential in communication and without this protocol the networking is totally useless. For its nature of functionality, it is stateless protocol and attackers use this vulnerable point to spoof the ARP reply packets to impersonate their presence to the victim. Besides this simple ARP poisoning is a base for many serious attacks. Among them, SSL Strip attack from Linux Backtrack that facilitate the attacker to get username and passwords information from HTTPS pages in plain word. Not only that attacker can read and detect every single packet that is being transmitted from the victim's computer. Such attack leads the attacker to trace victim's network behavior. VoIP call session sniffing is one of the most terrible post attacks of ARP spoofing where attacker gets RTP packets (Contains audio and video files). However from forensic point of view this vulnerability is helpful for the investigator to get extra evidences about suspect. On the other hand, network security is its limit to protect its users, especially in a corporate environment.

References

- [1] SSLSTRIP. (2009). Retrieved 2012, from [thoughtcrime.org: http://www.thoughtcrime.org/software/sslstrip/](http://www.thoughtcrime.org/software/sslstrip/)
- [2] Symantec-Norton. (2010, Nov 2). Two attacks against VoIP. Retrieved 3 14, 2012, from Symantec connect: <http://www.symantec.com/connect/articles/two-attacks-against-voip>
- [3] Vivek Ramachandran, S. N. (2006). Detecting ARP Spoofing: An Active Technique. Retrieved March 5, 2012, from [vivekramachandran.com: http://www.vivekramachandran.com/docs/arp-spoofing.pdf](http://www.vivekramachandran.com/docs/arp-spoofing.pdf)
- [4] Donato, N. (2005). Poisoning Attack and Mitigation Techniques. Retrieved from Windows ARP attack tools: <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white>

- [5] Frias, T. (1995). Cisco Security-Enabling the Self Defending Network. Retrieved from Spoofing an IP Address: <http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/>
- [6] Tony, B. (2007). Catalyst 6500 Configuration Guide. Cisco Dynamic ARP (DAI).
- [7] Cox, B. (2005). How Does ARP Work.
- [8] Desai, N. (2007). Cisco VLAN Security White Paper. Retrieved from Virtual LAN Security Best Practices: <http://www.cisco.com/en/US/products/hw/switches/ps708/>
- [9] Kirk Larsen, J. W. (2007). Vmware Security Hardening. Retrieved from Isolate the Management Network: http://www.vmware.com/pdf/vi3_security_hardening_wp.pdf
- [10] Osborne, E. (1998). Cisco Unified Wireless Network Guide.
- [11] Whalen, S. (2001, April). An Introduction to ARP Spoofing .
- [12] Yusuf Bhaiji . LAYER 2 ATTACKS & MITIGATION Techniques
<http://www.sanog.org/resources/sanog7/yusuf-L2-attack-mitigation.pdf>