ARP Cache Poisoning Lab Manual

Lab Objectives
This laboratory exercise demonstrates how ARP cache poisoning attack can be conducted using Cain & Abel, how password stealing and phishing can be conducted through ARP cache poisoning, how XArp is used to detect ARP cache poisoning attack, and how ARP Freeze is used to prevent ARP cache poisoning attack.

Lab Hardware and Software Requirement:
The required hardware:
- Router (to act as an isolated Access Point (AP))
- Two laptop computers with Windows XP/Windows 7 (or a laptop with two Windows XP/Windows 7) virtual machines). One is used as the attacker, the other is used as the victim.
- For the phishing lab, the router needs to be connected to the internet.
The required Software:
- Cain and Abel v4.9.43, downloaded from http://www.oxid.it/cain.html
- ARP Freeze 0.1 installed on victim computer, downloaded from http://www.irongeek.com/i.php?page=security/arpfreeze-static-arp-poisoning
- XArp 2.2.2 installed on victim computer, downloaded from http://www.chrismc.de/development/xarp/

1. ARP Cache Poisoning Attack
Two laptops or two virtual machines (attacker and victim) are connected to a router. The attacker uses Cain and Abel to launch an ARP Cache Poisoning attack on the victim.

1.1 Configuring Cain and Abel (Attacker)
(1) Run Cain and Abel and click the Sniffer tab. On the Cain and Abel menu, select Configure. The configuration dialog appears (see Figure 1).
(2) In the adapter list under the Sniffer tab, select the adapter associated with the attacker PC’s IP address (i.e., 192.168.1.100). Check “do not use promiscuous mode”, Click Apply then OK.
1.2 Discovering Hosts Connected to the AP

(1) Click the yellow and black icon which is Start/Stop APR, or ARP Poison Routing (see Figure 2). The icon to its left which is Start/Stop Sniffer will be depressed too. Now the sniffer is active.

(2) Select the Hosts tab (default selection) in the bottom left. Click the blue cross icon on the icon bar and the MAC Address Scanner dialog appears (see Figure 3). Instead of clicking the blue cross icon, you can also select File→Add to List.
(3) Click the OK button. A list of all hosts found on the subnet is displayed (Note: This list should have at least two entries to carry out this attack.)

1.3 Poisoning Host/Clients
(1) Click the APR tab at the bottom to open the poison routing page.
(2) Both panes on the right should be empty. Notice that the blue cross icon is now inactive. Click inside the top pane and the blue cross icon should become active. Click the blue cross icon to open the New ARP Poison Routing dialog (see Figure 4).
(3) On the left side, select the AP’s IP address (i.e., 192.168.1.1). Doing this tells the tool that you would like to assume the identity of the AP. The right side is now populated with the IP addresses of other clients.

(4) Select one or more clients on the right to be the victim(s).

(5) Click OK. Cain and Abel is now poisoning the selected hosts (see Figure 5).

The connection is now poisoned and any traffic sent by the victim computer to the AP will be intercepted by the attacker PC.
1.4 Intercepting Victim’s Passwords

(1) **Victim:** open a web browser and type in the router’s address http://<router’s IP>. Log into the configuration page.

(2) **Attacker:** click the Passwords tab at the bottom. Select the HTTP option on the left. The username/password information used by the victim will be shown in the list (Figure 6). This process illustrates how to intercept HTTP passwords but the same procedure can be followed for many different protocols.

![Figure 6: Intercepted username and password](image)

1.5 Phishing Lab exercise using Cain and Abel ARP Poisoning

For this lab, the router needs to be connected to the internet. After both the attacker and the victim computers are connected to the router/AP, the attacker follows the following procedure to carry out phishing attack. The victim of this laboratory exercise will be directed to a fake website.

(1) Click on the APR Tab at the bottom. On the left panel, click on “APR-DNS”

(2) Right click on the panel and click on “Add to list”

(3) Under “DNS name requested” type in the URL of the website you want to redirect from. (eg. My fake site is A&T’s webmail page so I would type in webmail.ncat.edu).

(4) Under “IP address to rewrite in response packets”, type in the IP address of where your phishing site is located and click OK. This means that whenever the victim tries to go to webmail.ncat.edu, they will go to my IP address instead. See Figure 7. (If you don’t know the IP address of the phishing site, you can click on “Resolve”. A window will pop up to resolve domain name to IP address).
2. ARP Cache Poisoning Prevention

The following steps demonstrate the ARP cache poisoning prevention method using static ARP routing.

On the victim machine:

1. Open the Command Line prompt on the user and type in “arp –a”. This will show the ARP cache of the victim and if the poisoning was successful, there should be an entry that has the IP address of the router and MAC address of the attacker.
2. After confirming a successful poisoning, type in “arp –d 192.168.1.1” to delete the poisoned entry.
3. Open a browser window and go to the router configuration page by typing in the IP address of the router. You can also just go to a webpage if you are connected to the internet. This simply updates the victim’s ARP cache with the router’s IP address again.
4. Open ARP Freeze
5. The first box will ask to keep the arpscript.bat batch file or start a new one. Click Yes to start a new one.
6. The second box asked about the “Netsh” command that is used in Windows Vista to create static entries (Figure 8). If the victim is using Vista, click Yes, otherwise if the victim is using a Windows OS older than Vista click No. If you choose yes to the Vista Netsh workaround dialog, then it will prompt you to select which adapter to set a static ARP entry for. Look for your wireless card and enter in the Idx number that corresponds to it.
(7) ARP Freeze will scan the current ARP cache and for each entry will ask if you want that entry to become static or not. Click Yes for the entry that has the router (IP gateway) IP address. For all other entries, click No (Figure 9).

(8) The next dialog box will ask to execute the Arpstaticscript.bat on every boot ensuring that the entry is static every time the computer is turned on. Click Yes.

(9) Click Ok for the next few dialog boxes which are just to confirm the changes. After this, open the command line window again and type “arp –a” to bring up the ARP cache again. This time the ARP entry of the router should be static.

(10) Repeat the steps in section 1.2 to 1.3 to conduct the ARP cache poisoning exercise again.

(11) Again, open the command line window and type “arp –a” to bring up the ARP cache. Notice that the ARP entry for the router is still there and remains static (see Figure 10). Although Cain and Abel says it is poisoning, the victim was not poisoned and therefore the attacker was unsuccessful.
3. ARP Cache Poisoning Detection

The following procedure describes how to detect ARP cache poisoning attack using XArp. Run XArp on the victim's computer, use the default settings.

1. Run Cain & Abel on the attacker’s computer. Configure the Cain & Abel Sniffer so that the wireless card of the attacker computer is selected, and “Don’t use promiscuous mode” is checked.

2. Activate Cain & Abel Sniffer function to discover clients connected to the AP (by clicking on the ARP Poison Routing icon). Press the blue cross icon and select “All Hosts in my subnet” in the MAC Address Scanner dialog box. Two IP addresses should be displayed. One is the router/gateway, the other is the victim’s computer. Write down the IP and MAC addresses of the router and the victim’s computer.

Router IP address: ______________________________ Router MAC address: ______________________________
Victim IP address: ______________________________ Victim MAC address: ______________________________

3. Click on the APR (ARP Poison Routing) tab at the bottom. Click on the top field and then click on the blue cross icon to open the New ARP Poison Routing dialog.

4. The first IP address listed to the left should be the router, click on that IP address and then on the right hand side, click on the IP address listed (this is the victim's computer). This means the attacker would intercept the traffic between the selected victim and the router. Click on OK. Now the connection between the router and the victim is poisoned. Wait a few moments until the status becomes “Poisoning”.

5. On the victim’s computer, XArp will display an alert window on the lower right hand corner of the screen, informing the user that ARP cache poisoning attack has occurred.

6. Open the Command Line prompt on the victim’s computer and type “arp –a”. The user should see an entry that has the IP address of the router and the MAC address of the attacker in the ARP cache.