American University of Beirut

EECE 655

Assignment 1: ARP Posisoning and Defence

Author:
Ali Hojaij
Mehiar Dabbagh

Supervisor:
Prof. Imad ElHajj

March 20, 2011

1 How to Run the Program

You can only run the deffender and the poisoner from the command line on a linux shell and these are the required steps to do:

1. Make sure that you have the latest version of libpcap and java sdk.
2. From the command line, change the current directory to the directory of the .class file(defend/poison).
3. For the poisoner execute: sudo java poison -ipsrc=<spoofed IP source> -ipdst=<destination IP> -hardsrc=<source MAC address> -harddst=<destination MAC address> -intf=<0 for eth0 or 1 for wlan0>. The source IP and destination IP are mandatory fields, all others are optional. The default value for the interface is eth0, for the hardsrc is the interface's MAC and broadcast for the harddst.
4. For the defender execute: sudo java defend -intf=<0 for eth0 or 1 for wlan0> -timeout=<timeout in seconds>. Both fields are optional and the default value for interface is eth0 and the default for timeout is 10 seconds.

2 ARP Cache Poisoning Methods

Three methods were used to poison the cache:

1. **ARP request attack:** an ARP request packet is sent with the spoofed IP (i.e the stolen IP address) as the source IP and with the MAC address of the attacker as the hardware source address. The destination IP address is that of the machine to be poisoned. If no destination hardware address is specified, the packet is broadcasted.
2. **ARP reply attack:** an ARP reply packet is sent with the spoofed IP (i.e the stolen IP address) as the source IP and with the MAC address of the attacker as the hardware source address. The reply is broadcasted.
3. **ARP gratuitous attack:** an ARP reply packet is boadcasted with the spoofed IP as the source and destination protocol address.

3 Detection Approach

The detection approach maintains a list of all the IPs and their associated MAC addresses. This is done by creating an entry for each received ARP packet with a new IP source. Once a new entry is created, an ARP request is sent to the source address of the received packet to make sure that this address is reachable and that no other machine has the same IP address (to detect ARP poisoning attacks). In the normal case, an ARP reply is received with the same source IP and source MAC address as the stored entry. An attack will be flagged if we receive an ARP reply with a different MAC address. If no ARP reply is received then this means that this IP address is unreachable and that it is possible that the attacker is trying to claim that he has a different non-existing IP address. In this approach, no false alarms should be generated. Also, the ammount of traffic created by this defence mechanism is not large since we don't send ARP requests if the entry already exists. The defence system maitains a log file that contains all attacks.

4 Results

The attack was successful when tested against Windows 7 and Ubuntu 10.10 (Kernel 2.6.37). When tested agaisnt our poisoning system, the deffence was 100% successful with no false alarms. The following figures show screenshots of the attack against Windows 7 and the defence.

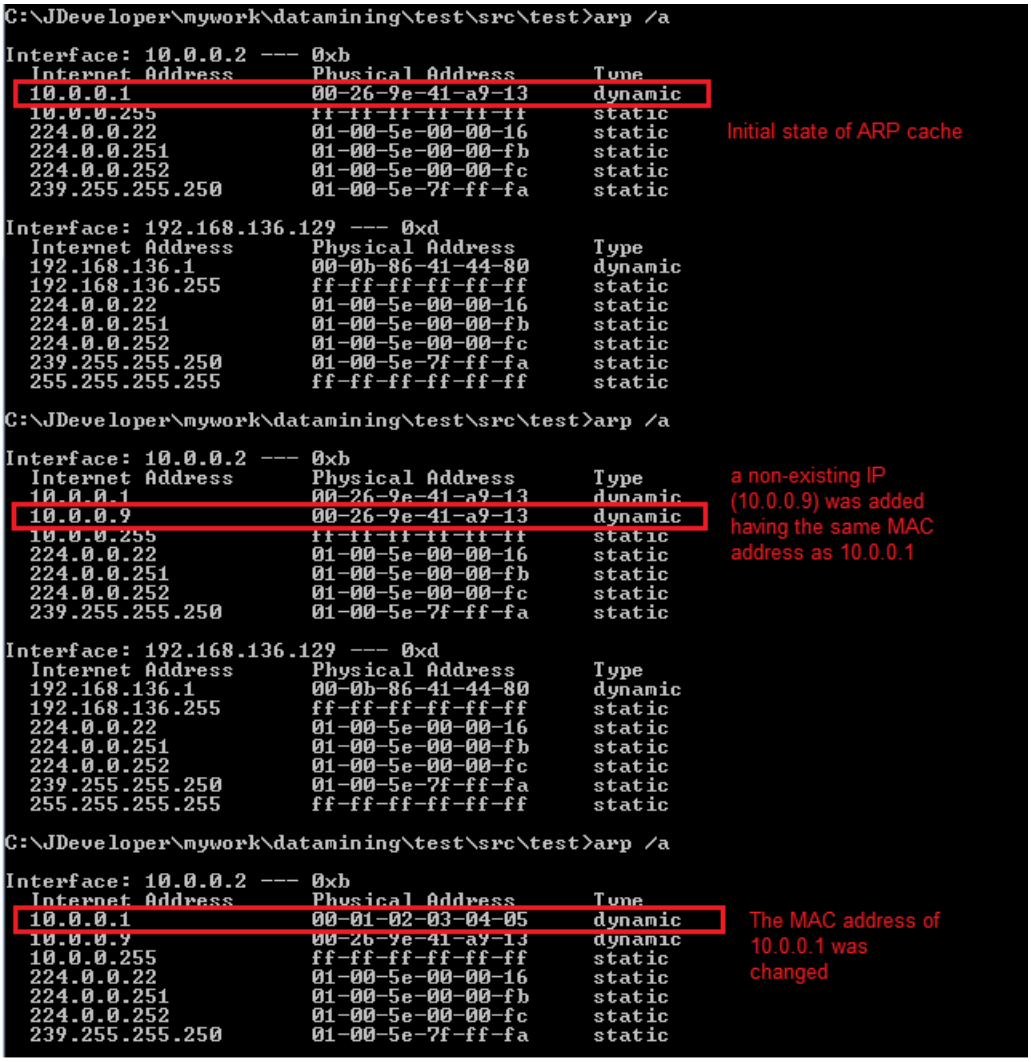

Figure1. Windows 7 poisoned ARP table

```
Defending started
ARP REQUEST 00:26:6c:72:52:62(/10.0.0.9) -> 00:00:00:00:00:00(/10.0.0.1)
        Entry was added to the list 10.0.0.9
        ARP Request is sent to: 10.0.0.9
ARP REPLY 00:26:9e:41:a9:13(/10.0.0.1) -> 00:26:6c:72:52:62(/10.0.0.9)
ARP REQUEST 00:26:9e:41:a9:13(/10.0.0.1) -> 00:00:00:00:00:00(/10.0.0.9)
10.0.0.9 is unreachable!!!!!!!!!!!!!!!!!! and could be a spoofed IP
        10.0.0.9 was removed from the list
ARP REQUEST 00:01:02:03:04:05(/10.0.0.2) -> 00:00:00:00:00:00(/10.0.0.1)
        Entry was added to the list 10.0.0.2
        ARP Request is sent to: 10.0.0.2
ARP REPLY 00:26:9e:41:a9:13(/10.0.0.1) -> 00:01:02:03:04:05(/10.0.0.2)
ARP REQUEST 00:26:9e:41:a9:13(/10.0.0.1) -> 00:00:00:00:00:00(/10.0.0.2)
ARP REPLY 00:26:6c:72:52:62(/10.0.0.2) -> 00:26:9e:41:a9:13(/10.0.0.1)
        10.0.0.2 already exists in database
!!!!! ARP POISONING ATTACK!!!!!!
10.0.0.2 has 2 MAC addresses: 00:26:6c:72:52:62 00:01:02:03:04:05
```

Figure2. Defence system detecting poisoning attacks