Information and Organisational Security

Guides for Practical Classes

João Paulo Barraca and Vitor Cunha

Department of Electronics, Telecommunications and Informatics
University of Aveiro

2018–2019

Contents

2

ARP Poisoning

Resumo:

- Manipulation of ARP caches
- Attack poisoning ARP caches
- Attacks of interception (Man-in-the-middle)
- Eavesdroping others traffic

2.1 Introduction

The ettercap[1] application is a tool for analysis of network protocols, and execution of specific security attacks. It has the possibility of intercepting traffic of a network segment, capture authentication secrets, and execute other attacks against specific protocols.

One of the possible attacks enabled with ettercap consists in the manipulation of the ARP (*Address Resolution Protocol*) caches, what is known as a poisoning attack, more specifically ARP Poisoning. This attack is executed by sending fake ARP messages, leading to the alteration of the ARP caches of the victim hosts. The final objective is to redirect the traffic sent by the victim, either to a specific host, or to a non-existing host.

If the attacker manipulates the caches in order to redirect the traffic to himself (this can be done to two victims, and intercept bidirectional traffic), he is executing an interception attach, known as *Man-in-the-Middle* (MitM). It should be noticed, that a MitM attack can be executed through many other ways, and ARP Poisoning is just a specific one.

This attack, through ARP Poisoning, implies associating the MAC address of the attacker, with the IP address of another victim. Considering three nodes (Bob, Alice and Eve), Even can poison Alices' ARP cache, by associating Bobs' IP address with Eves' MAC address. In this case, when Alice sends a packet to Bob, the packet will be sent to Eve. If Eve also poisons Bobs' ARP cache, packets from Bob to Alice, can also be sent to Eve.

The attacker (Eve) will receive the packets exchanged by the victims, and is able to forward the packets to the correct destination without any change, doing a passive attack of eavesdropping (able to see the traffic, violating the privacy of the communication). The attacker can also manipulate the packets by replacing selected contents, and can be used to other attacks, such as a downgrade attack (forces victims to use no ciphers or weak ciphers). In alternative, the attacker can also do a Denial of Service (DoS) attack, either by not forwarding packets or by poisoning victims with non-existing MAC addresses. This specific attack is known as a Black Hole attack (all traffic enters the black hole, but no traffic leaves the blackhole).

For the execution of this experiment, each group will use the network depicted in Figure 2.1. The attacker should use a Linux host, while the victims can use any other operating system. The use of a Linux systems in the vic-

[1] http://ettercap.github.io/ettercap

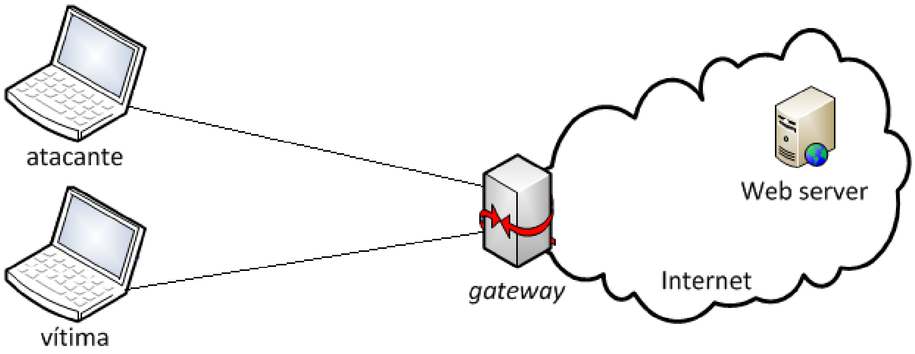

Figure 2.1: Setup to demonstrate the attack.

tims can help analyzing the attack, but the attack can be executed against any commonly existing operating system. It is recommended the use of the Virtual Machine provided by the professors, or a Linux Live distribution such as Kali[2]. In all cases, the `wireshark` application should be available.

2.2 Network setup

Create a local network (internal network in the same host) or connect to the network provided by the professor. Connect three hosts to the network (two will also work) and check if there is connectivity between the hosts (e.g. using `ping`). Also check if there is connectivity with the Internet and you can access common web pages.

Also check that `wireshark` is available, and that you can monitor the traffic of the network interface connected to the test network.

Finally, open a text console and check that you can obtain the ARP table of your hosts. This is achieved by executing `arp -a`.

2.3 Attack setup

In the victim host, do a ping to any site in the Internet. Check the ARP cache of this host, and **register the MAC address associated with the IP of the gateway**. You can obtain the IP address of the gateway using `route -n` or `ip route list`.

[2] `http://www.kali.org`

Start the `wireshark` application in both the victim and the attacker, start a ping to the same address, register the MAC and IP addresses in all ICMP packets, and identify the differences.

Edit the `ettercap` configuration file available in `/etc/ettercap/etter.conf` and edit the variables `ec_uid` and `ec_gid`, replacing the values with the user identifier and group identifier of the current user. You can obtain this using the `id` command.

A possible situation would be:

```
[privs]
ec_uid = 1000 # For the user with ID 1000
ec_gid = 1000 # For the user with Group ID 1000
```

This change will configure `ettercap` to execute with the permissions of the current user, and without requiring root access.

2.4 Execute an Interception Attack

The objective of this exercise is to poison both the ARP cache of the victim host and the ARP cache of the gateway, accomplishing a *Man-in-the-Middle* attack, between both devices. The result is that all traffic send by the victim host, and to the Internet, will be sent to the attacker. All traffic from the gateway to the victim host will also be sent to the attacker.

Please follow the following steps:

- Start `ettercap` in its graphical mode using the following command:

  ```
  sudo ettercap -G
  ```

- In `ettercap` start the *Unified Sniffing* mode (menu *Sniff/Unified Sniffing*) and select the appropriate network interface to use for the attack. It should be the network interface connected to the test network. In this mode, `ettercap` will sniff all packets arriving at the specific interface (optionally dumping secrets such as keys and passwords), and will forward all packets that have an IP address different from the current IP address of that Interface. This will correspond to packets that, although are reaching the local Interface, are not destined to the local host.

- Scan the local network for hosts, through the menu entry *Hosts/Scan* *for hosts*). Then access the Host List available at *Hosts/Host list*), select the victim ip address and click *Add to Target 1.* Then, select the gateway and click *Add to Target 2.*

- Start the ARP Poisoning attack of the two hosts by selecting the menu entry *Mitm/Arp poisoning*). In the parameter screen that is shown, select the option *Sniff remote connections* e click *Ok.*

  At this point the ARP Poisoning attack should be active.

Check the ARP cache of the victim host and register the MAC address associated with the gateway. Compare the value obtained, with the one obtained in the beginning of section 2.3. Explain what you observe.

Using `wireshark`, start a packet capture in the victim host and in the attacker host. Do a ping from the victim host to the Internet, analyse the traffic and compare the result with the one obtained in section 2.3.

2.5 Attack Exploitation

Since the moment the attack as executed, all traffic between the victim and the gateway (and the Internet), will be forwarded by the attacker. Traffic can be dropped, changed or simply observed (eavesdropping).

Simple eavesdropping is already active. `wireshark` can be used to save all traffic, and `ettercap` will extract keys and passwords, saving this to a log file. The web browsing session can also be observed in real time using the `remote_browser` plugin.

- Configure `ettercap` to use a specific web browser, by editing the file `/etc/etter.conf` and adding the following line:
  `remote_browser = "firefox -new-tab http://%host%url"`.
- While an attack is running, access the menu item *Plugins/Manage plugins*, and double click over `remote_browser` plugin.
- In the victim host, access an HTTP webpage such as the page of the Aveiro Municipality (`http://www.cm-aveiro.pt`).
- Check what happens in the attacker host.
- Explore this with other web pages.

Can you view pages accessed through a secure connection (HTTPS)? Can you explain why?

Challenge: `ettercap` has a plugin name `ssltrip` that can do a downgrade attack (HTTPS to HTTP), can you do it?

Changing the traffic between the victims can be achieved in several ways. Common ones are standard text replacements and DNS Spoof. For a DNS Spoof, edit the file `/etc/ettercap/etter.dns` and activate entries to be injected into clients. Then use the `dns_spoof` plugin while a MitM attack is being executed.

- After enabling the plugin, start `wireshark` in the attacker host.
- In the victim's host, access several webpages, including webpages present in the `etter.dns` file.
- Observe the webpages that are obtained by the vitim.
- Observe the DNS packets exchanged with the victim, and analyze the process.

Challenge: Check `ettercap` documentation and `etterfilter` and implement a Rickrolling prank [3]

Finally, the victims can be isolated from the network, making it impossible for the victims to communicate. `ettercap` has a plugin name `isolate` that will poison the victim's ARP cache with its own mac address associated with all the host it tries to contact. This way the host will not be able to contact other hosts because the packet will never reach the wire.

- To execute this attack, simply disable all other plugins, and enable the `isolate` plugin.
- In the victim's host, try to access the Internet and register what happens.
- Start `wireshark` in the victim's host and see what packets are sent into the network.

2.6 Bibliography

- ARP *poisoning*, `http://en.wikipedia.org/wiki/ARP_spoofing`.

[3] see: `https://en.wikipedia.org/wiki/Rickrolling`

- ettercap, http://en.wikipedia.org/wiki/Ettercap_%28computing%29.