ENSEA
Ecole Nationale
Supérieure
de l'Electronique
et de ses Applications

3RTS – Architecture & Protocols

TP #3 - room D055
Security Operations

C. BARÈS

Objectives : Understand the potential hacking mechanisms at LAN level.

Warning

The manipulations that you are going to perform today are not trivial. The network of the room at our disposal (D055) has been specially configured to allow these manipulations without risk of interfering with the rest of the ENSEA network.

The reproduction of these manipulations outside this room, on a network that does not belong to you, may be considered an infraction under articles 323-1 and seq. of the French Penal Code :

Article 323-1

> *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.*
>
> *Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.*
>
> *Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.*

1 – Setting up the layout

In order to carry out this exercise, you need to set up a group of two computers, and decide on an attacker *Mallory* and a victim *Alice*. Don't try to attack each other, that wouldn't be very effective ! The principle of the network used for the attack is presented in diagram 1 on the following page.

- Check your configuration using the `ip addr` command (configuration of the machine's IP and its mask).

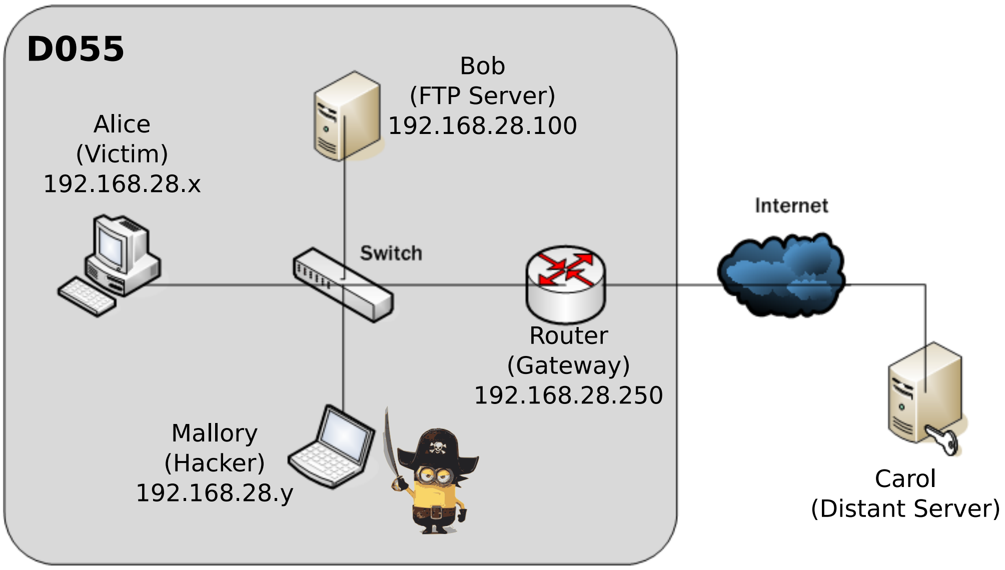

FIG. 1 : Operating diagram

2 – NMAP

The nmap (network map) utility allows you to scan the network and detect available services.

- Launch a scan on your network with the command nmap 192.168.28.1-10 (be patient, it's a bit long).
- Interpret some elements of the result.
- What is the purpose of the command nmap -sP 192.168.28.1-10 ?

3 – ARP POISONNING

The ettercap tool allows you to easily perform a number of operations on packets incoming and outgoing from a network interface.

- In a command window as root, run ettercap with the command sudo ettercap -G (graphical mode).
- In the sniff menu, launch "unified sniffing" on the enpXsY interface in order to discover the surrounding world.
- Next choose "host", "scan for host" and "host list" so that you can choose your target. Determine the "target1" and "target2", between which your hacker will insert himself.
- On the target (Alice) and on PC100 (Bob) (in ssh), look at the ARP table before going further.
- Now launch the man in the middle attack ("mitm" by "arp poisoning" by checking the "sniff remote connections" option.

- Look at the ARP table of your two targets. Comment on it. Also look at the ARP traffic using wireshark.
- During an FTP session between the victim and the server, capture and comment the traffic on your hacker computer (password, among other things).

4 – Utilisation d’un filtre

Ettercap permet également de ne pas « simplement » réémettre le trafic, mais de le modifier au cours de la ré-émission. Ainsi, il est possible de modifier des éléments de la réponse. Par exemple, sur la session FTP, on peut modifier l’invité de commande (« 220 ProFTPD 1.3.2 Server (ProFTPD Default Installation) »).

5 – Use of an Ettercap filter

Ettercap also makes it possible to not ”simply” retransmit the traffic, but also to modify it during the retransmission. Thus, it is possible to modify elements of the response. For example, on the FTP session, you can modify the command prompt (”220 ProFTPD 1.3.2 Server (ProFTPD Default Installation)”).

- To do this, it is necessary to pre-compile our action (in order to go as fast as possible). The filter can be written in a text file named ” filter_file ” as follows :

```
if (tcp.src == 21 && search(DATA.data, ”vsFTPd”)) {
replace(”vsFTPd 3.0.3”,”RTS’s are the best”);
}
```

- The filter must then be compiled on the command line as follows :

```
  $ etterfilter filter_file -o compile_file
```

  You can then load the filter into Ettercap (Filter / Load a filter).
- Test with wireshark the result of your manipulation by restarting an ftp session on the target. Pretty cool, isn’t it ?

6 – Spying with driftnet

Driftnet is a small tool that simply displays multimedia streams in a window, without formatting.

- Start your ARP Poisoning again,
- Run driftnet in parallel...
- ...and recover an image for example.
- Look at the result during a standard web access.

7 – DNS Poisonning

ARP Poisonning is already powerful, but it can be made even better. Given that our pirate PC is at the centre of all victim's communications with the internet, we can go further by modifying the responses to its requests, in particular DNS : it is the DNS Poisonning.

- Modify the file /etc/ettercap/etter.dns according to the examples given, so as to redirect the request of your choice to the desired service (for example, http://www.cyu.fr/ redirected to 193.51.47.207).
- This is to insert itself between your machine and the DNS server. So start your ARP Poisoning again (by restarting ettercap).
- Activate the DNS Poisonning plugin in ettercap. To do this, plugins->manage then double-click on the dns_spoof plugin.
- Don't forget to monitor the result with wireshark.
- Look at the effect of your victim's DNS cache on the operation.