UNIVERSITY OF MILAN-BICOCCA

Computer Science

Master in

DATA SCIENCE

Vulnerability - Dynamic Host Configuration Protocol

Alessio Giannelli

Academic 2022/2023

Indice

1. Dynamic Host Configuration Protocol

DHCP (Dynamic Host Configuration Protocol) is a dynamic IP addressing program. Once a DHCP server has been defined on the network, it is notified of the list of addresses it must assign and a DHCP database is created: when a host is switched on, it enters into communication with the DHCP server requesting the network parameters for carry out the auto-configuration.

The generation of the IP address is done by the server randomly, in the range of its available addresses, and as soon as a new address is created, a uniqueness check via the ARP protocol is required.

1.1 How DHCP works

There are two possible ways DHCP works:

- **automatic allocation**: DHCP permanently assigns an IP address;
- **dynamic allocation**: DHCP assigns an IP address for a limited amount of time.

Both use the same mechanism for assigning addresses:

- **DHCPDISCOVER**: suppose a host, PC1, is turned on: its network interface broadcasts a DHCP-DISCOVER message looking for a DHCP server;
- **DHCPOFFER**: any existing DHCP servers on the network they respond to the host with a message DHCPOFFER with which each proposes an IP address.
- **DHCPREQUEST**: the host accepts only one of the offers that reach it, and it always broadcasts a DHCPREQUEST message asking the PC/SERVER to send it the complete configuration.
- **DHCPACK**: DHCP server replies to host with a DHCPACK message specifying the configuration parameters, which are: the IP address, the Subnet-mask, the broadcast address, the default gateway; and the DNS server.

DHCP, whose main advantage is an efficient use of IP addresses that are assigned only to machines running and connected, is essential if you have only a few valid IP addresses available on the Internet.

Furthermore, this eliminates possible host configuration errors as nothing is done manually. In conclusion there is a technique that takes the name of DHCP LEASING: when a host is shut down or disconnected, it must release the address and make it available for a new allocation: the release can be explicit (DHCPRELEASE) or take place at the end of the lease period (parameter supplied by the server in the DHCPOFFER).

1.2 DHCP Server Manual Configuration - CISCO Packet Tracer

In the figure below we consider the A2 class C network with IP address 192.168.5.64, subnet-mask 255.255.255.224, and the default gateway (router) 192.168.5.65 (remember that it is customary to assign the internal network interface of the router the first available IP address immediately after that of the Subnet). For the physical configuration of the DHCP server, a Cisco PT server was chosen, equipped with an ethernet port and connected to the switch of the A2 network, so that it can communicate both with the router and with the other devices on the subnet.

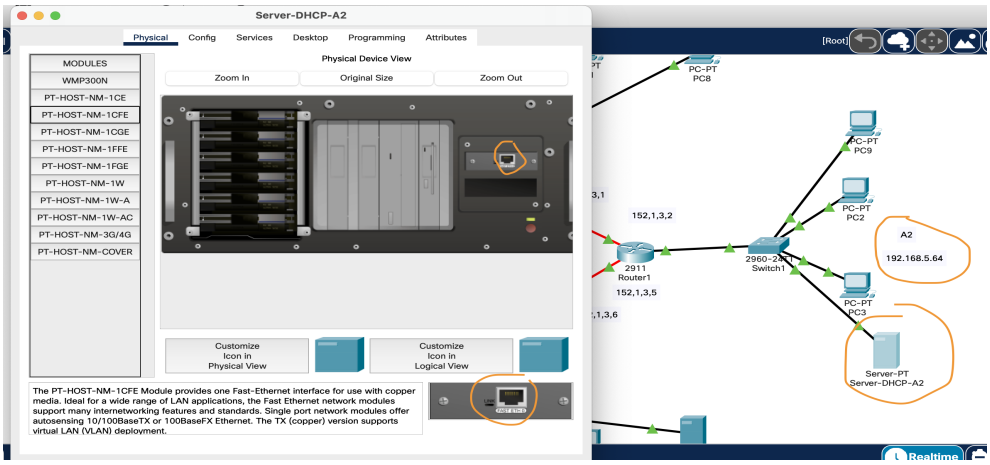

Figura 1.1: Physical Configuration

in the following figure, a manual configuration of the parameters of the SERVER device interface is carried out: the IP address, SUBNET and MAC address:

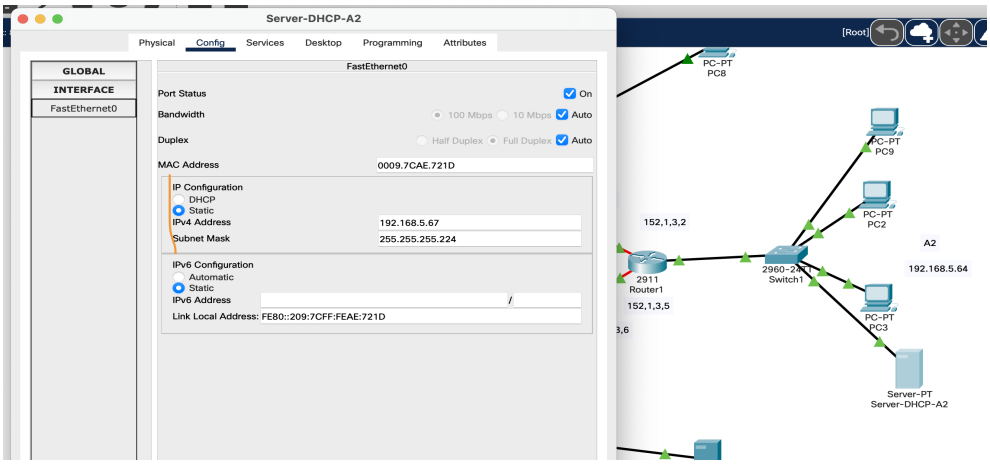

Figura 1.2: Server Configuration

In conclusion, we go on to configure the type of service that our server will have to perform, i.e. DHCP service. Starting from the top you choose the type of interface, in our case ethernet, the name of the Pool or rather the environment in which our server will work and then enter the address of the network gateway. Secondly, the initial IP address of the range of possible assignments, the size of the latter and the subnet mask to which the addresses belong were set.

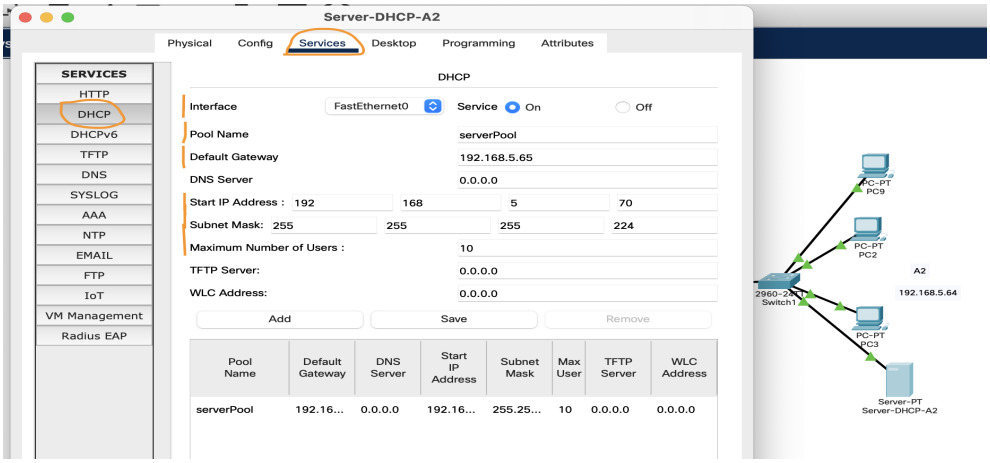

Figura 1.3: Server DHCP Configuration

2. DHCP Vulnearbility

2.1 Rogue Server

This vulnerability is based on the fact that a client is not aware of the DHCP server address, in fact to request the configuration during the dhcp-discover phase the message is sent in broadcast. By exploiting this, the attacker can set up a malicious DHCP server which, however, must respond before the legitimate server during the dhcp-offer phase, communicating an incorrect network configuration in which the rogue server replaces the gateway, allowing all traffic passing through to be intercepted . Here is an example of a dhcp server configuration on router from CLI to route traffic:

```
Router>enable
Router#configure terminal
Router(config)#ip dhcp pool PIPPO
Router(dhcp-config)#network 192.168.5.64 255.255.255.224
Router(dhcp-config)#default-router 192.168.5.79
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.5.65 192.168.5.70
```

A further example is given in which it is possible to implement the DHCP service from the Ettercap software using the DHCPspoofing tool in which the pool is created and by inserting the default dns which, however, must match the default gateway to ensure that the traffic is diverted to our own machine. An example of configuring the pool using Ettercap follows:

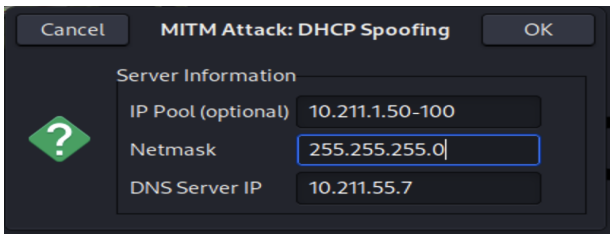

Figura 2.1: Pool Creation

Spoofing is a type of cyber-attack that employs identity spoofing in various ways. Spoofing can occur at any level of the TCP/IP stack and can also involve falsifying application information.

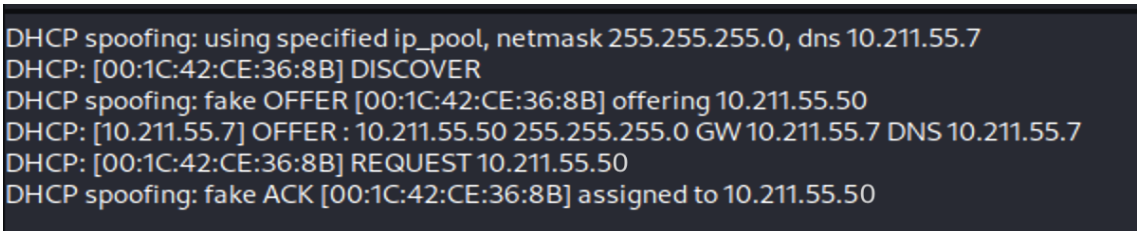

Figura 2.2: Hooked Target

By opening a software like wireshark or directly on ettercap it will be possible to see the traffic that has just been diverted to our machine. Furthermore, if the default gateway that the victim is used to using offers DHCP service, it will be very difficult for the attacker's DHCPOFFER to be accepted, in fact it is more noticeable in public places with high network traffic.

These two cases cause a violation of network security policies and user privacy, thus undermining the Confidentiality (man in the middle) feature.

2.2 Address Starvation

This vulnerability is based on the lack of authentication between client and server during the dhcp-discover phase; due to this lack an attacker can send multiple requests through fake MAC addresses. In this way the server, forced to respond to all the requests received, saturates all the possible configurations to send. Legitimate clients will then not have the ability to connect to the network and will therefore be banned. This DOS attack case causes a violation of the Availability property as it takes the server offside making it impossible to configure any host within the network. It is possible to use tools like Yersina built into linux operating systems to perform a DOS attack after issuing the following commands from CLIi:

```
sudo apt-get install yersinia
sudo yersinia -G
```

The last command launches the following GUI:

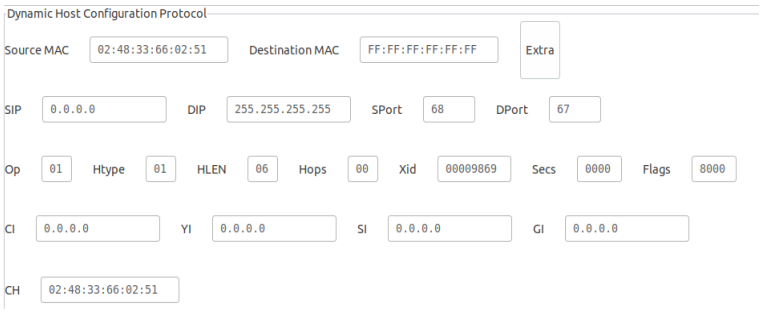

Figura 2.3: Dos

The IP set to 0.0.0.0.0 is set to make the server understand that it is a new host, the mask 255.255.255.255 to send the broadcast message throughout the network, after which the type of DOS attack is specified:

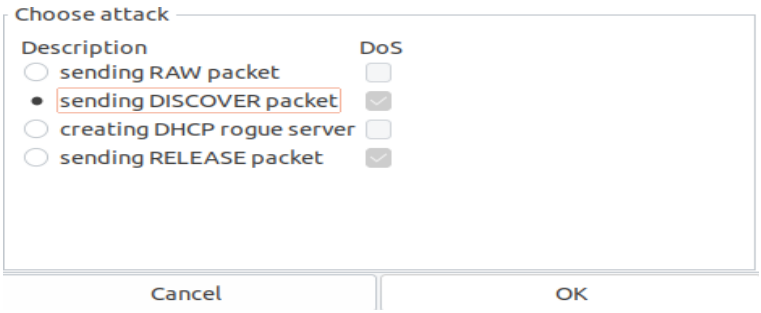

Figura 2.4: Dos

It will then be possible to monitor the attack via wireshark until it runs out:

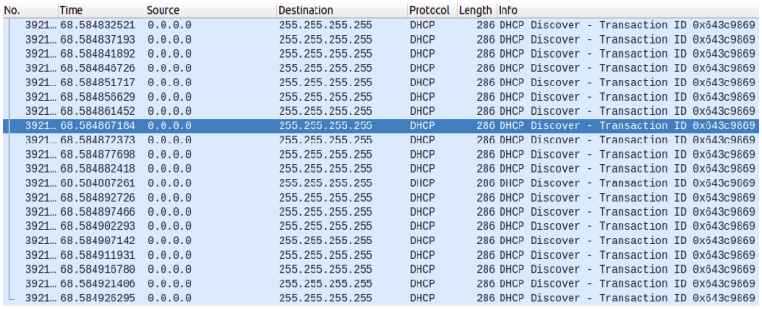

Figura 2.5: Attack Monitoring