Practical Network Defense

First Assignment - University "La Sapienza"

Group 27: Nicola Bartoloni ******* - Roja Lakshmi Perla ******* - Valerio Trenta 1856471

2020-13-04

1 Scope of the assignment

1.1 Our network

The target network belongs to the fictitious **ACME co.**, which requires a series of tools and security checks to be implemented in the hosts of the network itself.
All the hosts can be reached through a **VPN**. Though the network is quite large and comprehends a number of more than ten hosts, in this paper we will focus only on a specific subnet, that is the one where the security measures are to be implemented according to the scope of this assignment.
Thus, from now on we will not refer to the topology of the whole network, but only on the topology of the **Clients network**.

1.2 Our scope

The aforementioned **Clients network** is pictured in **Figure 1**, and is assigned the corresponding IP address **100.100.2.0/24**.

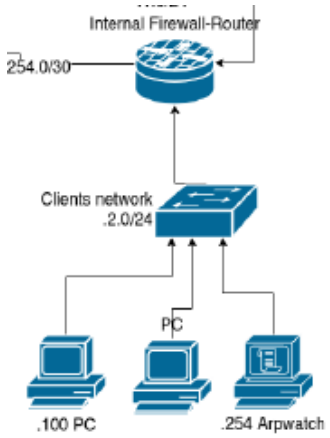

Figure 1: The **Clients network**, scope of the assignment.

The scope of the assignment is to enable the **DHCP service** on the *Internal Firewall-Router*, in order to provide the clients of the target network with dynamic IPv4 addresses. Furthermore, the clients should be protected against **link-local attacks** by implementing security measures and tools on the **Arpwatch** machine with IP address **100.100.2.254**.

1.3 Goals

How do we plan to achieve the goals of this assignment? General ideas.

2 DHCP Setup

This section describes how the **DHCP service** was set up in the *Internal router* machine, the one reachable at address **100.100.2.1**.
The router was accessed via web browser in the **Kali machine** (**100.100.2.100** as static IP address) through the given credentials, and then the desired service was configured through the **OPNSense** administration panel.
The following steps were taken to give the service the proper configuration provided by the assignment:

- the service was enabled on the router, as pictured in **Figure 2**, with the option **"Deny unknown clients"** checked in order to prevent undesired clients (the ones with a MAC address that is different from the ones specified and thus without ARP entries registered) from obtaining a dynamic IP address in the network. Keep also in mind that the subnet mask was already specified in the **CLIENTS** interface for the router, and the same goes for other services - such as **Unbound DNS**, so that these settings were not required to be configured again;
- the address range was initially specified as **100.100.2.101 - 100.100.2.253** so to avoid a re-assignment of known static IP addresses in the network - that is to say, those belonging to the Kali machine, the Arpwatch machine and, of course, the router itself. Later on, as pictured in **Figure 3**, a new pool of addresses was specified in the range **100.100.2.2 - 100.100.2.99** so to comprehend all the addresses that are not known to be assigned in the network;
- as pictured in **Figure 4**, the partial **MAC addresses** pointed out in the assignment as allowed to make use of the service were specified in the configuration, so that the only machines able to receive DHCP offers from the router will be the ones exhibiting these MAC addresses;
- as pictured in **Figure 5**, the six desired MAC addresses were then specified in the **DHCP Static Mappings** and a **Static ARP entry** was created for each of them so to remember their MAC address and mark them as known clients.

Once the **DHCP service** was confirmed running on the router, it was tested directly from the **Kali machine** by deleting the IP address set by default on **eth0** and thus trying to obtain a new one through the **DHCP service** of the router. First, as pictured in **Figure 6**, the **dhclient** command was run so that the machine could obtain a new dynamic IP address on the interface **eth0** - the machine has by default a **MAC address** on interface **eth0** which falls under the allowed addresses specified in the configuration. A **DHCP offer** was received by the router, and a new IP address was obtained, positively assessing the functioning of the service so far.
Again from the **Kali machine**, the **MAC address** of **eth0** was then changed to one that should not be allowed to request a new IP to the service, as pictured in **Figure 7**. The **dhclient** command was run again, and this time no offer was received, thus

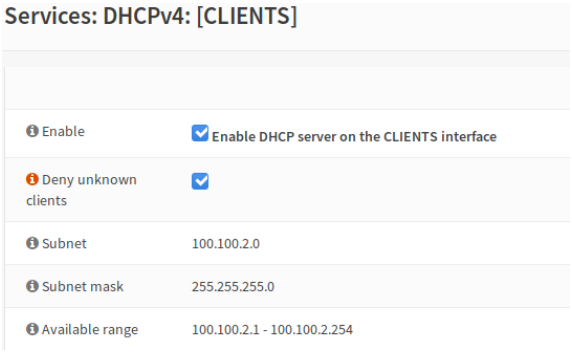

Figure 2: Enabling the DHCP service on the Internal Router.

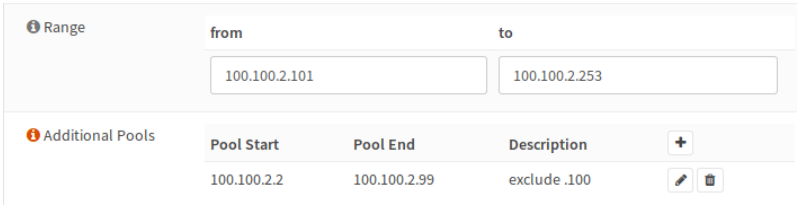

Figure 3: The specified range for assignable addresses on the DHCP service.

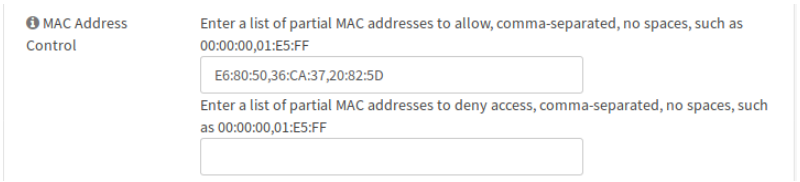

Figure 4: The partial MAC addresses specified in the configuration.

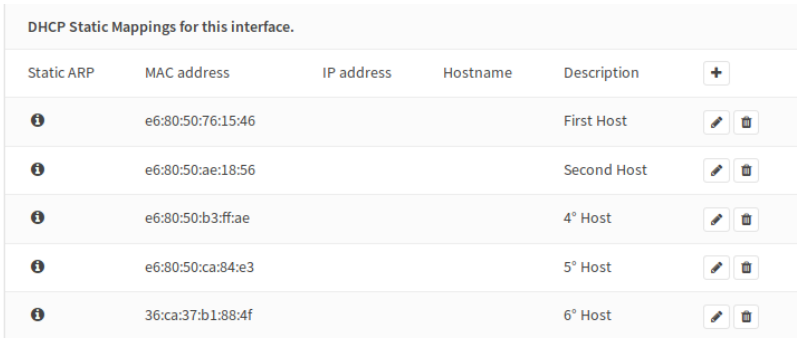

Figure 5: DHCP Static Mappings for the desired addresses - one is missing due to screen resolution on openVNC.

confirming that the service is only leasing IP addresses to machines having the desired **MAC addresses** on their interfaces. Since the machine had already received a lease by the service in the previous step, though, it was able to re-use the one previously obtained, but if it hadn't then no IP address would have been obtained.
Same test was run by slightly changing the original **MAC address** maintaining the first three bytes (**e6:80:50**), so to obtain a partial match of the address; as we can see from **Figure 8**, again no DHCP offer was received, confirming the desired behavior of the service.

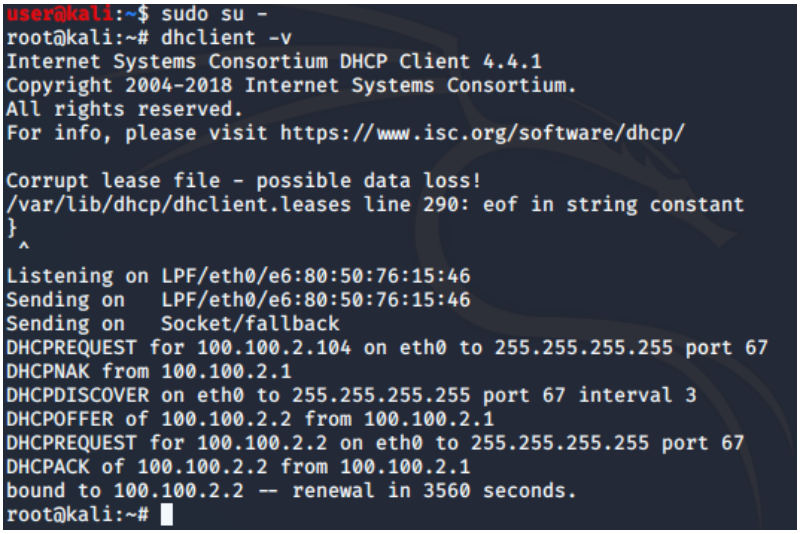

Figure 6: Kali machine with right MAC address on eth0 receiving a new IP address.

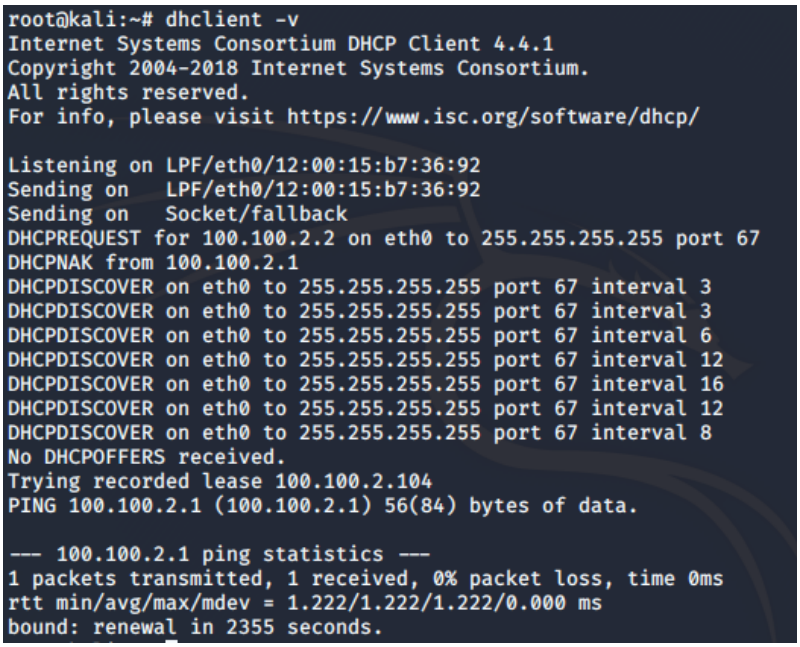

Figure 7: Kali machine unable to receive a DHCP offer due to its modified MAC address.

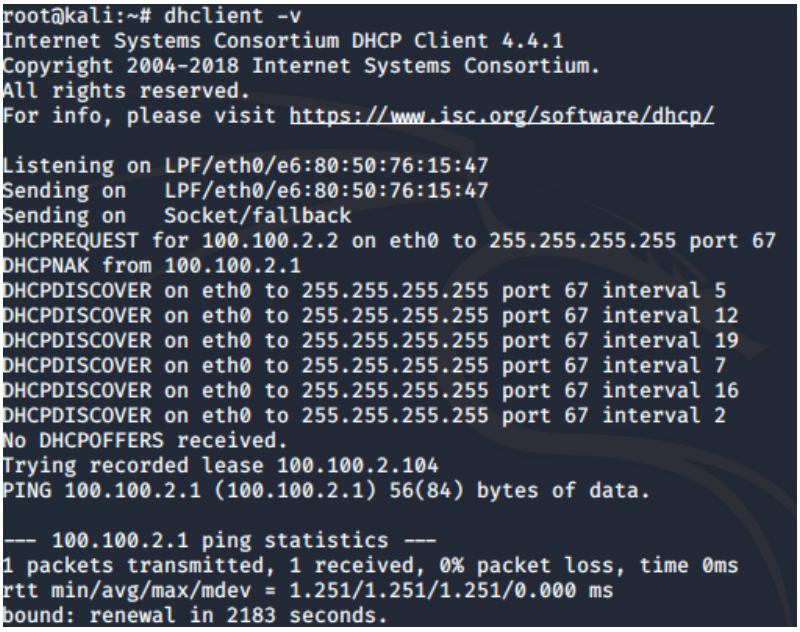

Figure 8: Kali machine unable to receive a DHCP offer due to its slightly modified MAC address.

3 Arpwatch tool configuration

How we performed the configuration of the Arpwatch tool on the Arpwatch machine.

4 Other tools configuration

Did we implement other tools to improve security? If yes, we describe them here.

5 Testing our security measurements

We did test x test y and test z and everything is cool.

6 Final remarks and possible improvements

blablabla

References

[1] *Just a placeholder.*