

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**.

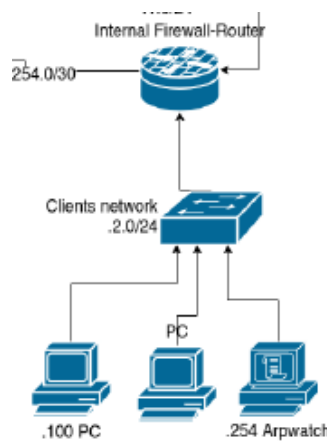


Figure 1: The **Clients network**, scope of the assignment.

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**. 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;

The screenshot shows the 'Services: DHCPv4: [CLIENTS]' configuration page. It includes a table with the following settings:

Services: DHCPv4: [CLIENTS]	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on the CLIENTS interface
Deny unknown clients	<input type="checkbox"/>
Subnet	100.100.2.0
Subnet mask	255.255.255.0
Available range	100.100.2.1 - 100.100.2.254

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

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 5**, the **dhclient** command was run so that the machine could obtain a new

The screenshot shows a configuration window for a DHCP service. It has two main sections. The first section, titled 'Range', contains two input fields: 'from' with the value '100.100.2.101' and 'to' with the value '100.100.2.253'. The second section, titled 'Additional Pools', contains a table with the following data:

Pool Start	Pool End	Description	
100.100.2.2	100.100.2.99	exclude .100	✎ 🗑

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

The screenshot shows a configuration window for MAC address control. It has a section titled 'MAC Address Control' with two input fields. The first field is labeled 'Enter a list of partial MAC addresses to allow, comma-separated, no spaces, such as 00:00:00,01:E5:FF' and contains the value 'E6:80:50,36:CA:37,20:82:5D'. The second field is labeled 'Enter a list of partial MAC addresses to deny access, comma-separated, no spaces, such as 00:00:00,01:E5:FF' and is empty.

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

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 6**. The **dhclient** command was run again, and this time no offer was received, thus confirming that the service is only leasing IP addresses to machines having the desired **MAC addresses** on their interfaces.

```
user@kali: ~  
File Actions Edit View Help  
For info, please visit https://www.isc.org/software/dhcp/  
  
Listening on LPF/eth0/e6:80:50:76:15:46  
Sending on LPF/eth0/e6:80:50:76:15:46  
Sending on Socket/fallback  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8  
DHCPOFFER of 100.100.2.102 from 100.100.2.1  
DHCPREQUEST for 100.100.2.102 on eth0 to 255.255.255.255 port 67  
DHCPACK of 100.100.2.102 from 100.100.2.1  
bound to 100.100.2.102 -- renewal in 2761 seconds.  
root@kali:~# ip addr show  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group d  
efault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc pfifo_fast state  
UP group default qlen 1000  
    link/ether e6:80:50:76:15:46 brd ff:ff:ff:ff:ff:ff  
    inet 100.100.2.101/24 brd 100.100.2.255 scope global dynamic noprefixro  
ute eth0  
        valid_lft 7120sec preferred_lft 7120sec  
    inet 100.100.2.102/24 brd 100.100.2.255 scope global secondary dynamic  
eth0  
        valid_lft 7137sec preferred_lft 7137sec
```

Figure 5: Kali machine with right MAC address on eth0 receiving a new IP address.

```
valid_lft forever preferred_lft forever  
user@kali:~$ sudo su -  
root@kali:~# dhclient -v  
Internet Systems Consortium DHCP Client 4.4.1  
Copyright 2004-2018 Internet Systems Consortium.  
All rights reserved.  
For info, please visit https://www.isc.org/software/dhcp/  
  
Listening on LPF/eth0/12:00:15:b7:36:92  
Sending on LPF/eth0/12:00:15:b7:36:92  
Sending on Socket/fallback  
DHCPREQUEST for 100.100.2.103 on eth0 to 255.255.255.255 port 67  
DHCNPAK from 100.100.2.1  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 10  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 19  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 14  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 11  
No DHCPOFFERS received.  
No working leases in persistent database - sleeping.  
root@kali:~#
```

Figure 6: Kali machine unable to receive a DHCP offer due to its modified MAC address (not allowed).

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.*