Practical Network Defense

Second Assignment - University "La Sapienza"

Group 27: Nicola Bartoloni ******* - Valerio Trenta 1856471

2020-13-06

1 Scope and Initial Considerations

The scope of this assignment comprehends the whole target network: a series of services provided by different machines in several subnetworks in the **ACME** environment are listed, and we focus on how to enable these services to the clients of our network by exposing them on a controlled manner through firewall rules specified in the **OPNSense** service provided by the two main routers of the network.
By catching a quick glimpse of the policy proposed by the assignemnt, we can tell the scope is to provide our network of a series of *white-listed* services that we want to be enabled and reachable from certain machines in the network itself, thus reducing the *attack surface* of the network by also excluding from this white list every other service that is not of interest.
Our analysis should begin with the services that we want to provide in the target network, and then on the firewall rules that make it possible to reach each service on each different machine.
Please notice that, since IPv6 addresses are not part of the scope of this assignment, we will ignore them during the configuration of the firewall rules in section 4.

2 Infrastructure Setup

We identify four main services which require machine-to-machine communication and, thus, are susceptible to the firewall rules that we'll define:

- an **Apache** web server reachable through **TCP** ports **80** (HTTP) and **443** (HTTPS) at **100.100.6.2**;
- a **DNS service** reachable through standard **UDP** port **53** at **100.100.1.2**;
- a **syslog server** reachable through standard **UDP** port **514** at **100.100.1.3**;
- a **proxy server** reachable through port **3128** at **100.100.6.3**, to be configured later on Assignemnt 3.

We thus identify two new subnetworks: the **Internal Servers** subnetwork **100.100.1.0/24** and the **DMZ** subnetwork **100.100.6.0/24**, and for the sake of defining the scope of this assignment and the setup of the whole infrastructure, we should also consider two additional details:

- Two of the four services - web server and syslog server - are already setup and running in the system: they do not need to be configured or launched;
- the **proxy server** is to be configured on the next assignment: for now, knowing from the **zentyal** portal that it is provided on port 3128 is enough.

This leaves us with the only **DNS service** to be configured at the moment. This step has been performed by following the instructions provided with the assignment: by accessing the **zentyal** portal at **100.100.1.2** on port **8843** - credentials have been changed - we added as forwarders the suggested IP addresses and specified the domain name - **acme.group27**. Then, the file located at **/etc/zentyal/dns.conf** on the aforementioned machine was modified including the target subnetworks (Clients and DMZ, that are the ones which will exploit the service).
At this point, pairs of IP addresses and hostnames were specified in the portal, so that the well-known machines of the network can now be associated with the following names:

- **kali**.acme.group27;
- **watchdog**.acme.group27;
- **dc**.acme.group27;
- **web**.acme.group27;
- **proxy**.acme.group27;

only the machines in the target subnetworks were actually included - so machines in the External subnet did not receive a hostname, and as suggested in the assignment were provided with an external DNS service such as 8.8.8.8 in their DHCPv4 configuration. Please notice also that the *logserver* was not given a name since it is only meant to be accessed by the SPOCK environment or by SSH and is not offering any browser-related service - and the same reasoning could be applied to the first two machines, *kali* and *arpwatch*, which we could exclude from this pairing list.
Last step was to actually modify the DHCPv4 settings in the two main routers to set the **dc** machine as the **DNS server** in the Internal Servers network, after having disabled the **Service Unbound DNS** in both routers.
The **DNS service** configuration is tested in section 5.

3 Policy Evaluation

4 Policy Implementation

5 Tests

5.1 Testing the DNS Service

5.2 Testing the policy

6 Final remarks

References

[1] *Just a placeholder.*