STI 2023/2024

Practical Assignment #2

1. Goals

- Configuration of a network firewall using **IPTables/Netfilter** (filtering, NAT and integration with Suricata)
- Configuration of **Suricata** as an IDS/IPS system (intrusion detection and prevention/reaction)

2. General description

The main goal of the assignment is to configure a **network firewall** capable of detecting and **reacting** to security attacks against services deployed on a protected network. For this purpose, the firewall should implement packet filtering, NAT and also intrusion detection, as well as mechanisms to react against attacks from hosts on the outside (Internet). Figure 1 illustrates the scenario considered for the practical assignment.

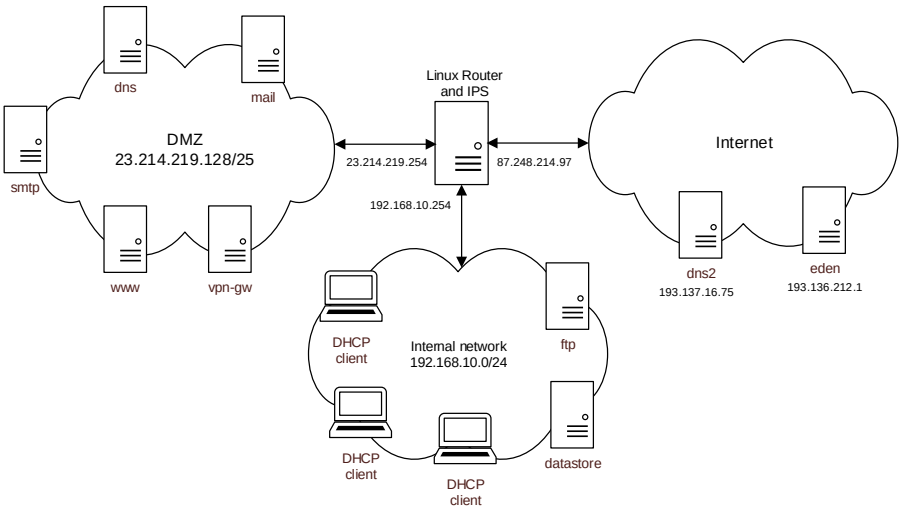

Figure 1 – Scenario for the Practical Assignment #1

As illustrated in Figure 1, we consider the usage of a DMZ and internal networks. The DMZ network is where most of the public services of the organization are placed (services which are contactable from the outside), while the goal of the internal network is to provide connectivity to users (clients with dynamic IP addresses), while also supporting servers with specific purposes. The router interconnecting the various networks runs Linux and should support all the security functionalities described in the assignment. For all systems in the scenario, you should assign IP addresses, as appropriate.

3. Packet filtering and NAT using IPTables

Firewall configuration to protect the router:

The firewall configuration should **drop** all communications **entering** the router system, except those required for the normal operation of the following services:

- DNS name resolution requests sent to outside servers.
- SSH connections to the router system, if originated at the internal network or at the VPN gateway (***vpn-gw***).

Firewall configuration to authorize direct communications (without NAT):

The firewall configuration should **drop** all communications **between networks**, except the ones required for the normal operation of the following services:

- Domain name resolutions using the ***dns*** server.
- The ***dns*** server should be able to resolve names using DNS servers on the Internet (***dns2*** and also others).
- The ***dns*** and ***dns2*** servers should be able to synchronize the contents of DNS zones.
- SMTP connections to the ***smtp*** server.
- POP and IMAP connections to the ***mail*** server.
- HTTP and HTTPS connections to the ***www*** server.
- OpenVPN connections to the ***vpn-gw*** server.
- VPN clients connected to the gateway (***vpn-gw***) should be able to connect to all services in the Internal network (assume the gateway does SNAT/MASQUERADING for communications received from clients).

Firewall configuration for connections to the external IP address of the firewall (using NAT):

The connections originated on the outside (Internet) and destined to the **external IP address** of the firewall should be authorized and treated according to the following requirements:

- FTP connections (in passive and active modes) to the ***ftp*** server.
- SSH connections to the ***datastore*** server, but only if originated at the ***eden*** or ***dns2*** servers.

Firewall configuration for communications from the internal network to the outside (using NAT)

The following communications from the internal network to the **outside** (Internet) should be authorized using NAT:

- Domain name resolutions using DNS.

- HTTP, HTTPS and SSH connections.
- FTP connections (in passive and active modes) to external FTP servers.

4. Intrusion detection and prevention (IDS/IPS)

Other goal of the assignment is to enable, in the firewall system, the capability to detect and react to security attacks. Attacks may be originated on the Internet and when an attack is successfully detected the firewall should block it. Thus, intrusion detection and prevention should be implemented in your firewall considering the following requirements:

- The firewall should be able to detect and block attacks, using **Suricata** and **IPtables.**
- Detect and block (at least) the following attacks/scans:
    - Two types of SQL injection.
    - Two types of DoS (Denial of Service) attacks.
    - OS fingerprinting attempts.
- Note: You must describe in your report how the attacks work and how Suricata is able to detect and block them.

5. Delivery of the Practical Assignment

With the assignment please deliver also a report, containing the following information:

- Description of all the configurations required for the implementation of the previous requirements.
- A description of the attacks considered in your configuration.
- A description of the tests performed to validate the overall configuration of the solution.
- A text file/script with all the IPtables rules that have been configured.

For the delivery of the assignment, put your report, as well as the relevant configuration files, in a single archive. This archive should be signed using your PGP key and encrypted using the PGP key of your PL teacher.

Note: Assignments without PGP will be accepted, although with a discount of 5% in the final grade.

Deadline for the submission of your assignment via Inforestudante: **April 28 2024.**