STI 2023/2024

Practical Assignment #2

1. Goals

- Configuration of a network firewall using **NFTables/Netfilter** (filtering, NAT and integration with Snort/Suricata)
- Configuration of **Snort/Suricata** as an IDS/IPS system (intrusion detection and prevention/reaction)
- **Audit any configuration** performed in the firewall and on the IDS/IPS

2. General description

The main goal of the assignment is to configure a **network firewall** capable of detecting and **reacting** to attacks against services deployed on a protected network. For this purpose, the firewall should implement packet filtering, NAT, and 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.

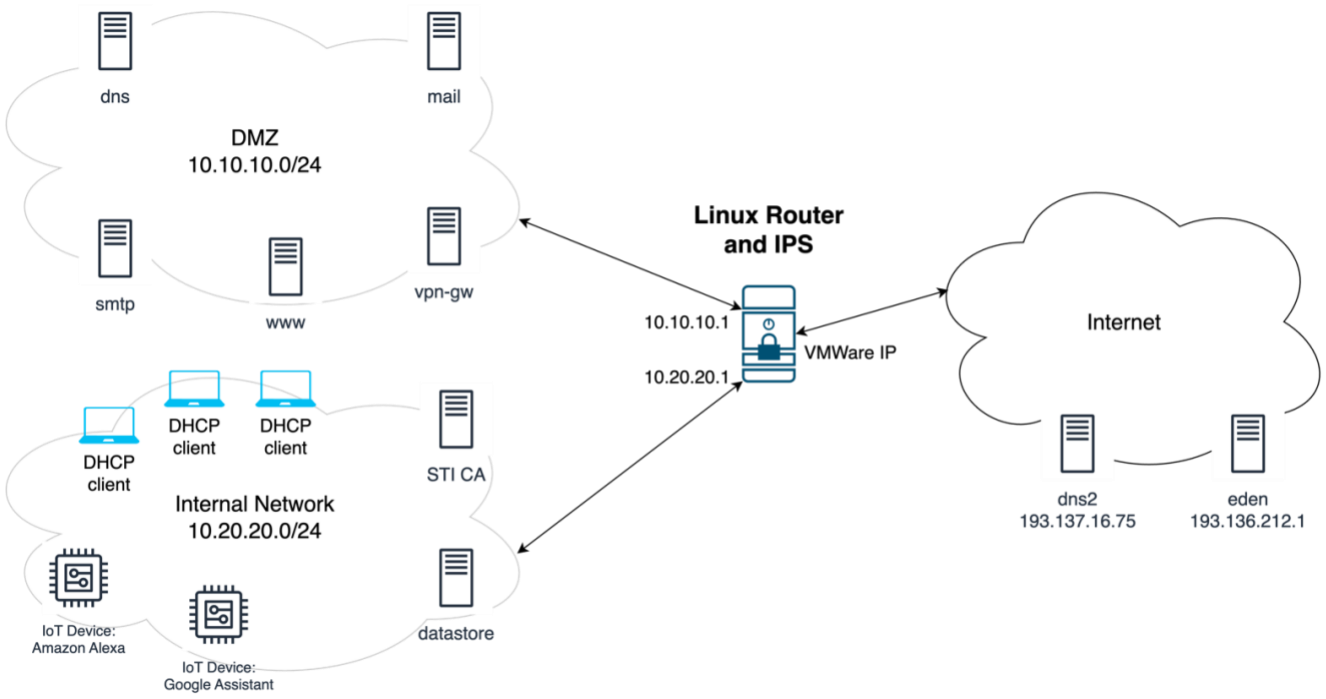

Figure 1 – Scenario for the Practical Assignment #1

As illustrated in Figure 1, we consider the usage of a DMZ and an internal network. The DMZ network is where most of the public services of the organization are placed (services which are

accessible from the outside). The goal of the internal network is to provide connectivity to users (clients with dynamic IP addresses), and support servers with specific purposes. The router interconnecting the various networks runs Linux and supports all the security functionalities described in the assignment. For all systems, you should assign IP addresses, as appropriate.

3. Packet filtering and NAT using NFtables

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***). The SSH connections should also be protected with the Port Knocking mechanism (with a minimum of 5 ports knocks). You should document the secret sequence.

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 must resolve names using DNS servers on the Internet (***dns2*** and 1.1.1.1).
- 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.

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** (identified as VMWare IP) of the firewall should be authorized and treated according to the following requirements:

- SSH connections towards the port 2021 of the Linux Router should be redirected to the SSH port of the ***datastore*** server and should be limited to 2 simultaneous connections.
- Connections towards the port 2022 of the Linux Router should be redirected to the port 2022 of the ***STI CA*** server and should only be allowed from a single IP address of Internet (this address must be documented in the report).

Firewall configuration for communications from 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 from devices with dynamic IP address (DHCP clients).

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 attacks. Attacks may be originated on the Internet and when an attack is successfully detected the firewall should be able to 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 **Snort/Suricata** and **NFtables.**
- Detect and block (at least) the following attacks:
    - One type of SQL injection
    - One type of DoS attack
    - One type of Brute Force attack
- Note: You must describe the attacks in your report.

5. Audit any modification in the firewall and IDS/IPS configuration files

Use the audit facilities in Linux to find any modification in the security files of the firewall and IDS/IPS. Any attempt to modify the permissions and any attempt to read these configuration files must be audited.

6. Certificate Authority and OCSP service (ONLY FOR MSE STUDENTS)

The ***STI CA*** server must function as a Certificate Authority that is responsible for the lifecycle of certificates, to emit, to revoke or provide information regarding their status.

The ***STI CA*** server must support the following functionalities:

- Work as a Certificate Authority, being able to emit, revoke certificates X.509.
- To provide a way to check the status of certificates through the Online Certificate Status Protocol (OCSP). OCSP must be configured to work on port 2022. All the replies of the OCSP must be signed with the respective X.509 certificate.

At least, three certificates must be created:

- One for the CA
- One for a web client with all the required extensions to be validated through OCSP.

7. Delivery of the Practical Assignment

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

- Description of all the configurations for the implementation of the previous requirements.
- A description of the application-layer attacks (SQLi, DoS, Brutr Fore) considered.
- A description of the tests performed to validate the overall configuration of the solution.
- Text files/scripts with the rules of NFtables that were created.
- Audit configurations and logs (evidences) of audited events.

To deliver the assignment, put your report, and relevant configuration files, in a single archive.

Deadline for the submission of your assignment via Inforestudante: **April 21 2024**