FSI LEI 2025/2026

Practical Exercises #2

Use IPTables to configure a Linux system firewall

1. **Clear** all the rules on the system's firewall configuration

2. Create a firewall rule to ignore incoming **ping** requests from another host (can be tested using the localhost address – 127.0.0.1), while authorizing all the remaining IP packets. Note: ping uses ICMP packets of types 8 (**echo request**) and 0 (**echo reply**)

3. Create firewall rules to authorize the following incoming TCP connections (filter table, INPUT chain), while rejecting (only) other TCP communications:
    a. **SSH** connections originated at the server student.dei.uc.pt
    b. **POP3** and **IMAP4** connections originated at any other hosts.

4. Add to the previous configuration firewall rules to authorize the following outgoing TCP connections (filter table, OUTPUT chain), while rejecting (only) other TCP communications:
    a. **HTTP** and **HTTPS** connections destined to the server student.dei.uc.pt
    b. **SSH** connections destined to any other hosts.

5. **Clear** all the firewall rules defined in the previous exercises

6. Use IPTables to authorize the following communications, while denying the remaining IP traffic (policy DROP on both the INPUT and OUTPUT chains):
    a. Incoming **SSH** and **HTTP** connections
    b. Outgoing **SSH**, **HTTP** and **HTTPS** connections
    c. **DNS** queries sent to the server dns.dei.uc.pt and dns2.dei.uc.pt
    d. Incoming **ping** requests from the server student.dei.uc.pt
    e. All IP communications to or from the **localhost** (127.0.0.1, or interface **lo**)

7. Activate the previous firewall configuration **permanently** on the system

Goals

Configure a system firewall using IPTables in Linux

Materials

- Segurança Prática em Sistemas e Redes com Linux, Jorge Granjal, FCA 2017, "Capítulo 17. Proteção de Servidores"
- Red Hat Enterprise Linux Security Guide: 2.8 Firewalls
- The netfilter.org Project
- Linux 2.4 Packet Filtering HOWTO