Systems' Security | *Segurança de Sistemas*

Project Porposal — 2024-2025

Miguel Frade

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Overview

Overview

Introduction

Introduction

This team work has two parts:

- setup a Linux server – install operating system, a firewall and other security mechanisms to make sure it is secure to be exposed to the Internet;
- testing – show all the security mechanisms working with `nmap` or other tools;

Introduction

This team work has two parts:

- setup a Linux server – install operating system, a firewall and other security mechanisms to make sure it is secure to be exposed to the Internet;
- testing – show all the security mechanisms working with `nmap` or other tools;

Students are free to choose how to implement the server, they can use:

- cloud servers (look for free options like `https://www.oracle.com/pt/cloud/free/`)
- real computers (*e. g.* a Raspeberry Pi, or a PC running at home exposed to the Internet)
- virtual machines (Virtual Box, VMware, *etc.*)

Student teams:

- each team should be composed by 3 or 4 students
  - no less than 3, and no more that 4
- each student must enroll himself on Moodle, section “Team Enrolment”

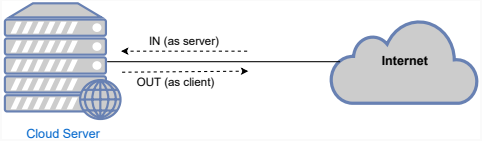
Linux Server – Requirements

Linux Server Requirements

The teams must configure the cloud server with the following minimum requirements:

- setup a web server with Wordpress (`https://wordpress.com/`)
- the web server must use digital certificates
  - such as the one provided by `https://letsencrypt.org/`, in this case it is required to buy a domain name (there are free domains for 1 year, check `http://www.dot.tk/`);
  - or, alternatively, may use the less secure self-signed certificates (but better than none)
- configure the `iptables` firewall to allow the services listed in the next slides
  - policy: deny by default

Linux Server Requirements – Firewall



List of services that must be allowed by the server firewall:

- as a server (IN)
  - HTTP versions 1.1, 2 and 3
  - SSH, protected by `fail2ban` and usage of asymmetric key login
  - `sshttp`, a SSH/HTTP(S) multiplexer to run a webserver and SSH on the same port
    - use port 443 for both HTTPs and SSH, more info: `https://github.com/stealth/sshttp`
    - SSH should also be availabe through port 22 (it must be assessible via 443 and 22)
  - ping
- as a client (OUT)
  - DNS
  - DNS over TLS
  - ping
  - SSH
  - git
  - docker
  - whois
  - http
  - https

Additional requirements:

- logging:
  - log all traffic related to the services exposed to the Internet (IN)
  - log and reject all invalid packets, in both directions: IN and OUT
- flood protection of incomming connections (IN)
  - prevent ICMP packets flood whenever higher than 5 per second
  - prevent UDP packets flood whenever higher than 10 per second, with a tolerance of 50
  - prevent TCP packets flood whenever higher than 50 per second, with a tolerance of 100
    - the SSH service must be an exception to the TCP flood protection

Additional security mechanisms:

- If your team wishes to add services, or mechanisms, that are not listed in this project proposal, please contact first the teacher to clarify the value that it may (or may not) bring to your project.

Linux Server – Testing

All firewall rules must be tested:

- a spread sheet must be created with all firewall rules and for each rule:
  - explain its purpose
  - add one or more command to test the firewall rule
  - `nmap` should be the preferred tool for testing, but other tools can be used also
- use the provided spread sheet template
- additional computers may be used to perform the tests

Report

Report

Report in PDF:

- maximum 5 pages (A4, letter size 11), including:
  - students' names and numbers
  - team number
  - description of the implementation
- and two files (no page limit):
  - bash script to implement the firewall rules
  - spread sheet with all rules and test commands

Delivery

Delivery

Delivery date

This project has only one delivery date, please check the course evaluation schedule, or Moodle, for the submission deadline.

File submission

Mandatory rules to submit the project:

- submit a single `zip` file, and only by one of the team members
- the file name must follow this format: `Team-XX.zip` *
- the `zip` must include:
  - `Report-XX.pdf` * – the report file, only PDF format is accepted
  - `firewall-XX.sh` * – script with the firewall configuration rules
  - `test-XX.xls` * – the spread sheet with the test commands, use the template available on Moodle

* `XX` must be replaced by the team number, *e. g.* `01`, `02`, *etc.*

Note

Failure to comply with these rules will result in a penalty of 10 percentage points in the final grade.

Evaluation

Oral Presentation

This project will end with a oral presentation for all students, either in Portuguese, or in English

- 20% public presentation, where all team members must do part of the presentation. This presentation must include a demonstration testing the server working and the showing the firewall rules;
- Report:
  - 20% configuration of the server, with emphasis on security mechanisms, and explanation of the technical decisions;
  - 40% testing commands to show the security mechanisms working;
  - 20% quality of the implementation, and any additional services that may have been implemented;

Evaluation

Individual evaluation of the team project

Individual Mark = TM $\times$ ICF

- Team Mark (TM) $\rightarrow$ equal to all team members
- Individual Contribution Factor (ICF) $\rightarrow$ based on self and peer evaluation quiz

Questions?