Project Proposal of Systems Security

Miguel Frade, Nuno Rasteiro

2019-09-19

1 Introduction

In this team work, students must design a network scenario, setup operating systems, services and security mechanisms to later demonstrate it working. Students are free to choose how to implement the network scenario, they can use real computers, local virtual machines (Virtual Box, VMware, *etc*), or cloud servers (*e. g.* Digital Ocean, Azure, Amazon Web Services [1], *etc*).

1.1 Requirements

The teams must design and setup a network with the following minimum requirements:

- setup 2 different kinds of firewalls, where at least one should be a packet filter firewall (*e. g.* iptables, pfSense, *etc*), and another a proxy firewall (*e. g.* squid, *etc*);
- setup at least one DMZ (demilitarized zone);
- teams must configure services (*e. g.* web, DNS, databases, NTP, email, *etc*) with the purpose of showing how the security mechanisms work in their scenario;
- all servers must allow remote configuration through SSH, and this service must also be protected against abuse with the fail2ban service;
- setup at least one VPN (OpenVPN, IPSec, Wireguard, *etc*)
- setup at least one service that uses digital certificates (VPN, web, email, *etc*)

Additional security services and mechanisms, will be taken into account when determining the final scores of the project. Here are some examples:

[1] Check the free Amazon service: `https://aws.amazon.com/pt/free/`

- free digital certificates through the Letsencrypt service (`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/`);
- secure DNS: DNS over TLS, or DNS over HTTPs;
- automated backup systems;
- authentication with tokens, *e. g.* citezen card (the Portuguese national identity card "Cartão de Cidadão"), YubiKey (`https://www.yubico.com/`);
- separate networks for: management, IoT devices, *etc*;

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

Diversity of operating systems will also bring added value to the project, *e. g.* Linux, Windows, Android, iOS, *etc*

2 Delivery

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

The teams must design and implement a network scenario and elaborate a report with:

- the full logical network design, including devices, IP addresses, operating systems and security services that your team wants to setup;
- detail the configuration rules of the firewalls, and what security policy they refer to;
- specify all the services that were installed, and explain the configuration customizations performed by the team;

Additionally, all configuration files must be also included, for more information read section 2.1.

This project will end with a oral presentation for all students. This presentation can be either in Portuguese, or in English, and the teams must demonstrate their implementation working.

2.1 File submission

Only one ZIP file can be submitted and must obey the following:

- the filename must be `TeamX.zip`, where `X` must be replaced by your team name (check your team name on Moodle, *e. g.* `D1`, `PL2`). Failure to comply with this rule will be penalized by 10% in the final score;
- the ZIP file must contain:
  - the report with this filename `TeamX-report.pdf`, only PDF format will be accepted for the report;
  - one folder per computer (or virtual machine) and per-service containing only the configuration files that were changed by any of the teams members.

Here is an example of the folder structure inside the ZIP file for team D7:

- `TeamD7/` – folder to store all files
- `TeamD7/TeamD7-report.pdf` – the report
- `TeamD7/server1/` – one folder per server, the server name must be clearly identified in the network diagram
- `TeamD7/server1/SSH` – one folder per service inside each server
- `TeamD7/server1/SSH/ssh_config`
- `TeamD7/server1/SSH/sshd_config`
- `TeamD7/server1/fail2ban`
- `TeamD7/server1/fail2ban/fail2ban.conf`
- `TeamD7/server1/fail2ban/jail.local`
- `TeamD7/server2/`
- `TeamD7/server2/SSH`
- `TeamD7/server2/SSH/sshd_config`
- `TeamD7/server2/fail2ban`
- `TeamD7/server2/fail2ban/jail.local`
- `TeamD7/server2/iptables`
- `TeamD7/server2/iptables/firewall.sh`
- *etc*

2.2 Evaluation

- 20% public presentation, where all team members must do part of the presentation. This presentation must include a demonstration of the services working;
- Report:
  - 40% implementation of the network design, with emphasis on configurations, technical details and why;
  - 20% implementation of the security policies from the first phase;
  - 20% complexity of the implemented network, including any additional services that may have been implemented;