First Practical Assignment

Delivery, on VirtualIPB. Deadline **22-12-2024**

---

1 Objectives and Organization

The assignment has the following main **objectives**:

- to improve knowledge about information systems vulnerabilities;
- to boost experience in creating and configuring secure solutions;
- to enhance computer systems security knowledge in students' areas of interest;
- to develop teamwork skills in a cybersecurity context.

Depending on the project's complexity and/or goals, the groups can be of 2 or 4 elements.

Students should choose a project and decide its main objectives with the professor during class. This information, jointly with group composition, should be emailed to the professor.

Considering students' areas of interest, this assignment enables them to choose a project in diverse areas, such as programming, hardening, and/or configuration of secure solutions, services, and security controls.

Students should create a technical report (see Section 2.2).

The report should be submitted jointly with attachments through the *VirtualIPB* platform by 22-12-2024. Discussion and demonstration of the project will be held on a date to be confirmed.

2 Details

Considering that students expressed interest in developing skills and competencies in diverse areas, this assignment enables them to choose a project in an area that suits them.

In the following section, suggestions are made. Students should contact the professor for each project to decide on specific objectives.

2.1 Projects

Suggestions:

1. Development
    - Animation of cryptographic algorithms
    - Repository for digitally signed documents
    - Secure Chat Rooms
    - Create a secure authentication based on RFID cards
    - Passive DNS service
    - Security Deploy for Cloud (Terraform and Ansible)
    - Homomorphic encryption with web and mobile application
    - Secure logging solution using blockchain

- Automation of computer security tasks
  - Creation of automated solutions to verify baseline security of systems
  - Automating the secure configuration of systems and services
  - Automating the check of secure configuration on systems and services
  - …
- Development of a security incident response tool
- Security monitoring dashboard with SIEM integration
- …

2. Installation of services and security controls
   - ModSecurity
   - Zeek
   - SIEM solutions
   - OWASP NAXSI Project
   - IDS / IPS
   - Honeypots / Honeynets
   - L7filter
   - Operation System Virtualization
     - FreeBSD Jail
     - Solaris Zones/Containers
     - Linux-VServer
     - OpenVZ
     - Virtuozzo
     - Docker
     - LXC
     - …
   - ESP32-based IoT devices using the MQTT protocol
   - Secure logging solutions
   - …
3. Hardening
   - Grsecurity
   - Bastille Linux
   - AppArmor
   - SELinux
   - Specific service hardening
   - …
4. Malware analysis
5. Code analysis
6. Creation of wargaming scenarios
7. Creation of security challenges
8. Creation of Labtainers activities
9. …

Students may suggest other projects.

2.2 Report

The report should reflect the work done.

It must contain an introduction explaining the project, main objectives and document structure.

Usually, next will follow a chapter describing the used tools, concepts, APIs and platforms.

The main chapter clarifies the implementation and/or the configuration that follows. The main tasks and choices made should be explained in detail. Projects involving programming must deliver the code properly commented on in the report appendix. All relevant configuration files must be commented on and incorporated in the report appendix. All attachments should be submitted jointly with the report on the platform. Full code and/or configuration files should be compressed and attached.

The following chapter describes the analysis and tests made to the created or configured solution.

The report ends with a conclusion, referring to achieved objectives, main difficulties and future work that can be done to improve the solution.

The report should contain all used bibliographies and should be correctly cited in the document.

3 Milestones and Deadlines

To help students stay on track, the following revised milestones are recommended:

1. **Group Formation and Project Selection:** *[29 October 2024]*
   Students should submit the group composition and chosen project by this date.
2. **Initial Research and Tools Selection:** *[5 November 2024]*
   A brief description of the project objectives, chosen tools, and a research plan should be presented.
3. **Initial Implementation:** *[3 December 2024]*
   Key components of the project (code or configuration) should be partially implemented by this date.
4. **Testing and Improvements:** *[15 December 2024]*
   Students should begin testing their implementation, making improvements and adjustments where needed.
5. **Final Submission:** *[22 December 2024]*
   The complete project and report should be submitted.
6. **Presentation and Demonstration:** *[TBD in January 2025]*
   Each group will present their project and demonstrate its functionalities.

4 Assessment

Grades are individual, even for group work. They take into account the following aspects:

- Quality and complexity of the work carried out;
- Clarity, structure, and depth of the report;
- Quality of the discussion and demonstration;
- Performance during the project demonstration;
- Respect for the established deadlines;

- Auto-evaluation (self-assessment of individual contribution);
- Hetero-evaluation (peer evaluation of group members' contributions).