Project MITS: A Prototype to Demonstrate SSH Vulnerabilities

Research Document

Alexandros Karayiannis, Anton Reunovs, Bence Mohr, Carlos Schaap García, David Corodeanu, Nick Grahovskis, Sara Kiani Nejad

For NHL Stenden University of Applied Sciences

Maritime IT Security (MITS) Research Group

October 2025 (Version 1.0)

Table of contents

1. Background of the project

This project is carried out in collaboration with the Maritime IT Security (MITS) research group, which operates at NHL Stenden University of Applied Sciences. MITS focuses on raising awareness and improving resilience against cyber threats in the maritime sector through research, simulations, and applied projects.

By pairing a deliberately misconfigured SSH server with an attacker testing environment, the prototype will serve as an educational tool to raise awareness of how quickly insecure setups can be exploited, and why strong configurations and credential management are essential in cybersecurity. This directly supports the research group’s plan to create a workshop setting where participants can see and experience how easily misconfigured SSH systems can be compromised.

2. Fishbone diagram

A fishbone diagram, also known as an Ishikawa diagram, has been derived from the current problem we are trying to tackle. “Insecure and exploitable SSH system” is the target goal we are trying to achieve, and so many 6 categories have also been derived to visually represent the subproblems we need to think about.

People: Human choices and behaviour, mistakes, habits or shortcuts by users and administrators that unintentionally create risks (for example using easy passwords or not following guidance).

System: How things are set up and connected, technical setups or defaults that make systems easier to reach or misuse when not configured carefully.

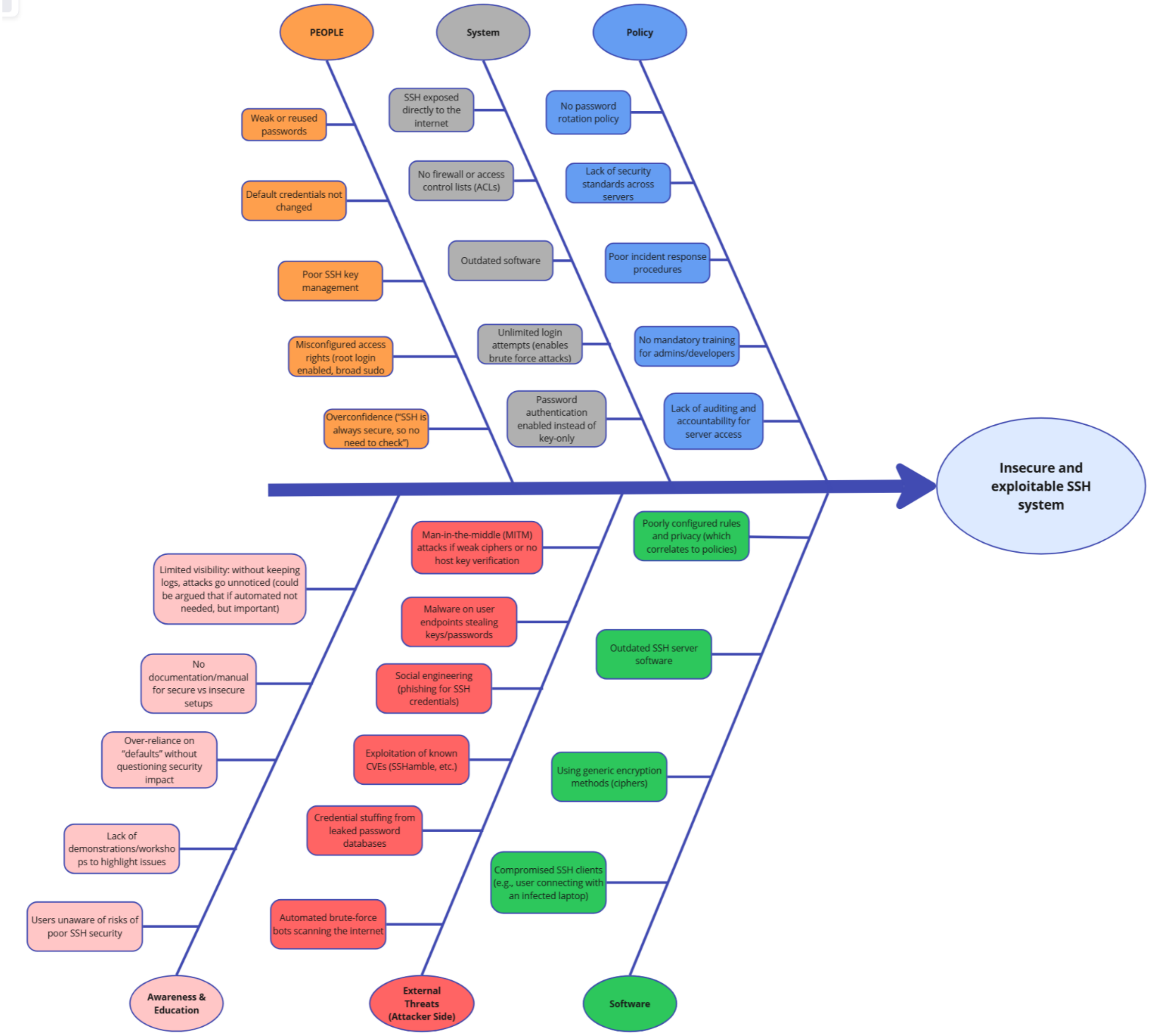
Policy: The organisation’s rules and processes, whether there are clear instructions, responsibilities and checks in place to keep systems secure over time.

Awareness & Education: Staff and student knowledge, how well people understand the risks and whether training, guides or demonstrations exist to show them what to look for.

External Threats: What attackers do; the automated tools and tricks used by outsiders (e.g., mass scanning or stolen passwords) to find and exploit weak systems.

Software: The applications and tools in use, whether software is kept up to date and configured sensibly so it doesn’t become a source of vulnerability.

A clear showcase of the fishbone diagram can be viewed below (in the next page).



Insecure and exploitable SSH system

PEOPLE

Weak or reused passwords

Default credentials not changed

Poor SSH key management

Misconfigured access rights (root login enabled, broad sudo

Overconfidence ("SSH is always secure, so no need to check")

System

SSH exposed directly to the internet

No firewall or access control lists (ACLs)

Outdated software

Unlimited login attempts (enables brute force attacks)

Password authentication enabled instead of key-only

Policy

No password rotation policy

Lack of security standards across servers

Poor incident response procedures

No mandatory training for admins/developers

Lack of auditing and accountability for server access

Awareness & Education

Limited visibility: without keeping logs, attacks go unnoticed (could be argued that if automated not needed, but important)

No documentation/manual for secure vs insecure setups

Over-reliance on "defaults" without questioning security impact

Lack of demonstrations/worksho ps to highlight issues

Users unaware of risks of poor SSH security

External Threats (Attacker Side)

Man-in-the-middle (MITM) attacks if weak ciphers or no host key verification

Malware on user endpoints stealing keys/passwords

Social engineering (phishing for SSH credentials)

Exploitation of known CVEs (SSHamble, etc.)

Credential stuffing from leaked password databases

Automated brute-force bots scanning the internet

Software

Poorly configured rules and privacy (which correlates to policies)

Outdated SSH server software

Using generic encryption methods (ciphers)

Compromised SSH clients (e.g., user connecting with an infected laptop)

3. Research question

How can a misconfigured SSH server and attacker simulation environment be designed and implemented to effectively demonstrate common security vulnerabilities and raise cybersecurity awareness among students in maritime IT workshops?

4. Research patterns and cards

Pattern:

Our group chose the Choosing fitting technology pattern for our project, according to ICT Research Methods (2018) it is important to decide which tools, languages, and existing components can be used in our project. This pattern can make the development process easier and more efficient, because during designing and prototyping phases, our group will evaluate and test whether the chosen tools are sufficient. This will help to understand and decide which tools can be used in the final product and which need to be replaced. By using this pattern, our group will ensure that we are using correct tools in the final version of the product.

Cards:

Library:

Available product analysis: Our group chose this method to make our development easier and faster, because there are many available tools for usage that we need to research, on which can save time during the development phase.

Field:

Explore User Requirements: This method will help our group to understand what our users need. We will ask the client several questions about who will use it, what features must be in the product, why it is important, and how we should deliver the final product.

Stakeholder analysis: Our group chose this method to understand important stakeholders of our product, understand who will use it, and possibly develop it in the future.

Workshop:

Brainstorm: Our group chose this method because we need to come up with ideas and possible implementations during the design and development process.

Prototyping: Our group chose this method because, as we develop different versions of the product, we will evaluate whether the chosen tools are sufficient and think what features can be implemented in the next prototype.

Lab:

Security test:

Our group chose this method because, for our project, it is important to have different vulnerabilities, so it is essential to research the most common vulnerabilities for the SSH server, implement, and check

System test:

Our group chose this method because, as we develop our software, we should verify every component to ensure it works as expected before adding it to the prototype.

4.1. Library

The library phase focuses on gathering existing knowledge and available technological solutions before beginning development. The goal is to identify and evaluate relevant research, tools, and technologies that could support the project's objectives. This ensures that the design is based on proven methods and that unnecessary work is avoided by reusing reliable existing solutions.

Available Product Analysis

In this stage, the team explored existing tools, frameworks, and technologies to find those best suited for demonstrating SSH vulnerabilities in a controlled, educational environment. Each option was analyzed based on compatibility, usability, and support within cybersecurity education.

Tool / Library	Purpose	Evaluation Summary
Docker & Docker Compose	Containerization and orchestration	Enables isolated, reproducible environments for both attacker and victim systems.
Kali Linux (Docker image)	Attacker simulation	Includes penetration testing tools like nmap, hydra, and ssh-audit, ideal for hands-on security exercises.
Ubuntu (Docker image)	Victim SSH server	Stable, lightweight, and easy to configure for multiple SSH vulnerability profiles.
Python (Questionary, Rich, PyYAML)	CLI interface development	Used to create a user-friendly, interactive

		experience for workshop participants.
GitHub & Jira	Collaboration and project tracking	Supports version control, documentation, and sprint-based coordination.

After analyzing these tools, Docker and Python were chosen as the main technologies due to their reliability, open-source nature, and educational relevance. These tools form the technical foundation of the prototype and support future workshop implementation.

Why the Library Method?

The library method (ICT Research Methods, 2025) was chosen because it supports structured knowledge gathering before implementation. It allows the team to make well-informed design decisions by exploring existing academic and technical sources. This method ensures that the project builds upon established best practices rather than starting from scratch, saving time and increasing the technical quality of the final product.

4.2. Field

To ensure that our project — the *Containerized Vulnerable SSH Prototype* — was developed in a structured and evidence-based way, we applied two research methods from the ICT Research Methods Card Library:

- **Explore User Requirements**
- **Stakeholder Analysis**

These cards were selected because they provided a solid foundation for understanding the problem context, defining project requirements, and identifying key stakeholders who influence or benefit from the project.

Explore User Requirements

Description of the card

The *Explore User Requirements* card is a field research method used to identify what users expect from a product or system and to ensure that the final design meets their needs. According to ICT Research Methods (HBO-i, 2018), this method involves gathering insights from users or stakeholders to understand their goals, challenges, and expectations before and during development.

How We Conducted the Research

To explore user requirements our team gathered input from the client and its organization. Through informal interviews and feedback sessions, we identified what users needed from the SSH vulnerability prototype:

- The environment must be safe.
- It should be easy to deploy
- It should simulate real vulnerabilities without risk to actual systems
- It should be educational, allowing students to observe, exploit and understand vulnerabilities.

We documented and validated these requirements in weekly meetings with the client and during project reviews with supervisors.

Result of the Research

The exploration revealed that the most important user needs centred around safety, simplicity and educational effectiveness. These requirements directly influenced our design choices; using Docker Compose for isolation, SSHamble for controlled vulnerability simulation, and detailed documentation to support users.

By exploring user requirements early, we ensured the final prototype was relevant, usable and aligned with both technical and educational goals of the project.

Stakeholder Analysis

Description of the card

The *Stakeholder Analysis* card is used to identify, categorize, and understand all people or organizations that influence or are influenced by a project. The ICT Research Methods (2018) guide emphasizes mapping stakeholders' interests, influence, and importance, often visualized through a Mendelow Matrix or similar tools. This method ensures that project communication and priorities are aligned with stakeholder expectations.

How We Conducted the Research

We conducted the Stakeholder Analysis after exploring the user requirements to clarify who was involved in the project and how their roles impacted our decisions. The steps we took included:

- Listing all potential stakeholders from the project scope (client, team members, educators, MIWB, etc.).
- Categorizing each stakeholder as direct or indirect, and internal or external.
- Assessing their level of importance and influence using a Mendelow diagram.
- Discussing these relationships as a team and validating them with the client and supervisor.

The analysis was summarized in our official Stakeholder Analysis document, which structured relationships, communication plans, and influence levels for each stakeholder group.

Result of the Research

The Stakeholder Analysis clarified the project's social and organizational structure. It showed that:

- The Client had very high influence and very high importance because they set the project's goals and evaluate the results.
- Team members and the Team leader had high influence through direct implementation and coordination.
- End users and MIWB had high importance, as they represent the main educational and industry beneficiaries.
- Teachers, supervisors, and future trainees had lower influence but remained essential for future project adoption.

This analysis improved communication, allowing the team to plan meetings, reviews, and deliverables according to each stakeholder's influence level. It also helped ensure the project remained relevant to both academic and maritime cybersecurity contexts.

4.3. Workshop

After applying field-research methods (Problem Analysis and Stakeholder Analysis) to understand the context and identify the key actors, we moved into workshop-based methods to generate ideas and shape the design of our prototype. The two selected cards from the ICT Research Methods toolkit are Brainstorm and Prototyping. They support creativity and tangible exploration of solutions.

Brainstorm

The brainstorm is a creative thinking technique that can help generate new ideas and solutions to include in the project during different phases.

Our team had several brainstorming sessions during which we discussed possible improvements and features. During different project phases, our team discussed the visualisation, implementation, and debugging to come up with the best scenario to meet both the client's and future users' requirements.

The brainstorming method helped our team to understand what the must-have, should-have, and could-have features and tools in our project are, to correctly prioritise them during the project development. Additionally, it helped our group to create a well-developed architectural design, realise possible solutions for bugs, and minimise time waste.

Prototyping

Its goal is to develop, evaluate or communicate a concept, design or problem solution by making it concrete. According to ICT Research Methods (2018) prototyping is all about developing, evaluating or communicating a concept, design or a problem to make ideas concrete.

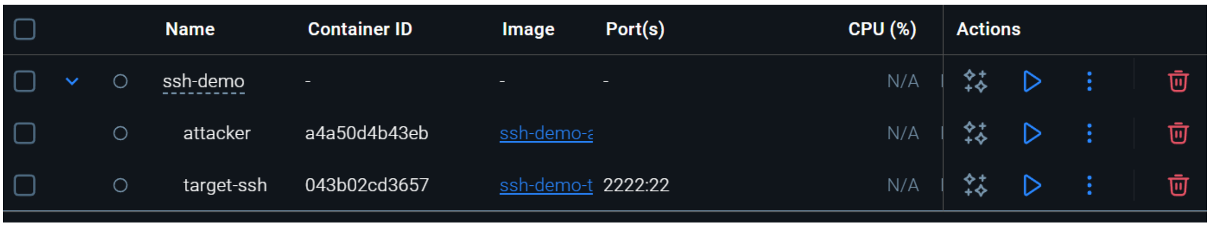
How We Conducted the Research

After brainstorming and selecting a design direction, we developed simple prototypes of the environment. We built a minimal Docker Compose setup with attacker and target containers, configured one basic SSH misconfiguration, and created a demo for educators. We then presented these prototypes to the client and collected feedback.

Result

The prototyping phase flagged several design issues early: the initial deployment was too complex for workshop instructors, the vulnerability scenario lacked visual feedback for learners, and the attacker environment needed clearer separation.

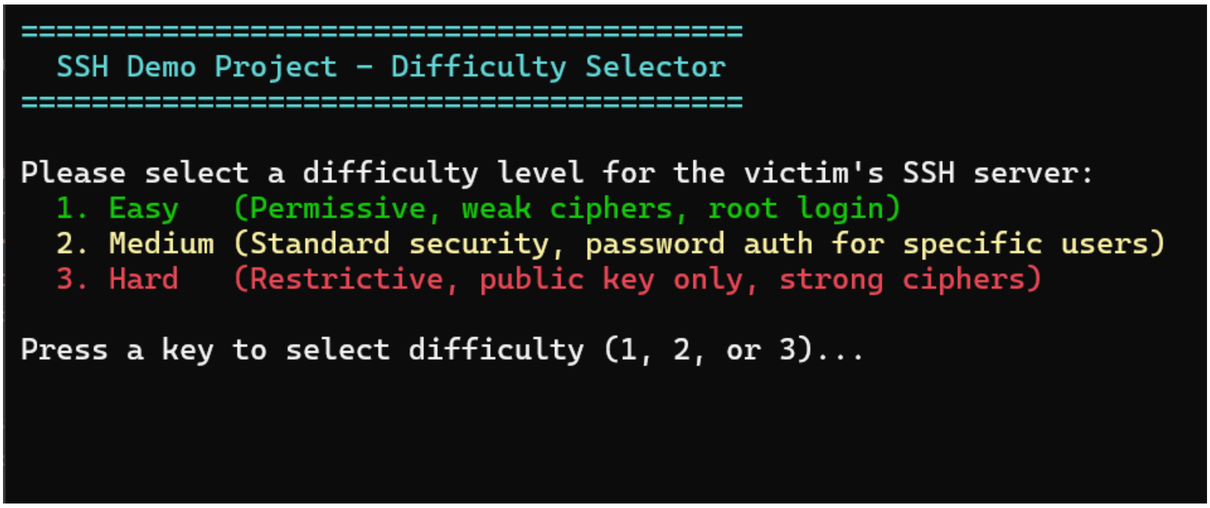
Docker Containers Image *(nothing critical changed here throughout the iterations)*



☐			Name	Container ID	Image	Port(s)	CPU (%)	Actions
☐	⌄	○	ssh-demo	-	-	-	N/A	▷ ⋮
☐		○	attacker	a4a50d4b43eb	ssh-demo-a		N/A	▷ ⋮
☐		○	target-ssh	043b02cd3657	ssh-demo-t	2222:22	N/A	▷ ⋮

In the next page is a showcase of how each iteration of the application is resembled only looks-wise (no practical demo), but it paints an overall image of the product – with iteration 3 being the release version that was delivered to the client.

CLI App Iteration 1

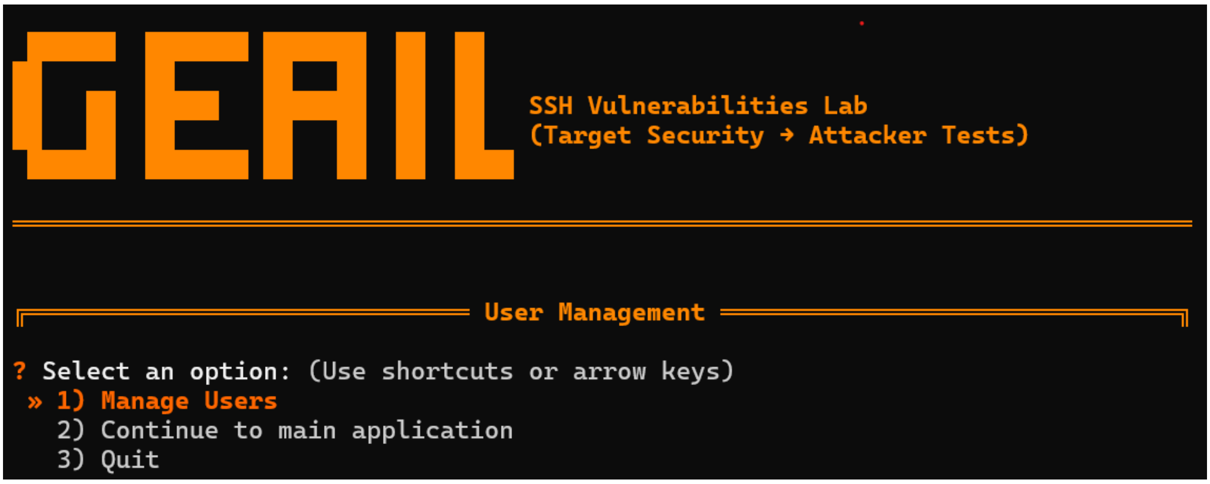


```
=========================================
  SSH Demo Project - Difficulty Selector
=========================================

Please select a difficulty level for the victim's SSH server:
  1. Easy   (Permissive, weak ciphers, root login)
  2. Medium (Standard security, password auth for specific users)
  3. Hard   (Restrictive, public key only, strong ciphers)

Press a key to select difficulty (1, 2, or 3)...
```

CLI App Iteration 2

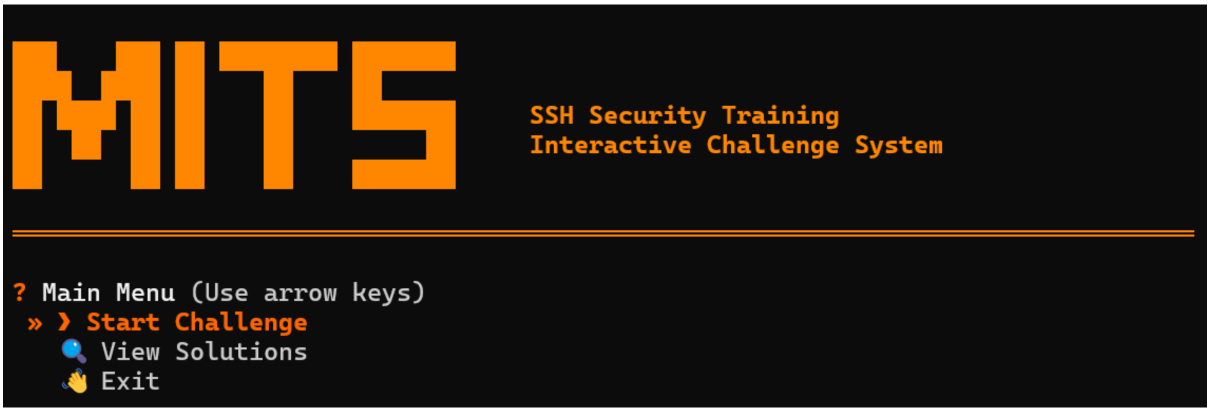


```
SSH Vulnerabilities Lab
(Target Security → Attacker Tests)

╔═══════════════════════ User Management ═══════════════════════╗

? Select an option: (Use shortcuts or arrow keys)
 » 1) Manage Users
   2) Continue to main application
   3) Quit
```

CLI App Iteration 3



```
SSH Security Training
Interactive Challenge System

? Main Menu (Use arrow keys)
 » ❯ Start Challenge
   🔍 View Solutions
   👋 Exit
```

4.4. Lab

Security Test

The security test is the process of finding and researching common vulnerabilities in systems and testing them through different penetration tests.

First, our team did research on popular vulnerabilities that can be found and used this information to create different levels for our project. Later, our team made system tests based on the configuration files that we made for different levels to confirm that all the vulnerabilities are present and set up correctly.

The security testing helped our team to find all the common vulnerabilities in SSH servers and verify that all the configuration files work as expected, showcasing how bad configurations can affect the security of the server.

System test

The system test is the process of creating a testing plan with expected outcomes and the testing process itself, where all the expected outcomes are checked for each system component.

Our team created a test plan with all the components that we need to check and debug and assumed possible positive and negative outcomes. First, our team started by building and composing all the Docker containers. If something went wrong, we have made a debug session. Later, our team checked whether logging into different containers is sufficient and whether all the tools work as they are needed.

The system testing process helped in spotting and fixing all the big bugs that we had during the development of our prototypes and upgrading them.

5. Conclusion

This research demonstrates the feasibility and educational value of utilising a misconfigured SSH server and attacker simulation environment to enhance cybersecurity awareness among students engaged in maritime IT workshops. Guided by the ICT Research Methods framework, we employed Library, Field, Workshop, and Lab approaches to ensure a structured and evidence-based process. The library phase informed our technology selections, resulting in the development of a containerised environment using Docker Compose. Field research elucidated user requirements pertaining to safety, simplicity, and educational efficacy, while workshop methodologies facilitated brainstorming and iterative prototyping to improve usability. Lab testing verified the presence of realistic misconfigurations—such as weak passwords, outdated cryptography, and absent access controls—and confirmed system reliability. Through the application of research techniques and iterative prototyping, we constructed a containerised SSH vulnerability environment utilising Docker Compose and SSHamble. This environment intentionally incorporated common misconfigurations, enabling participants to safely observe and comprehend how such vulnerabilities can be exploited. An isolated, reproducible, and interactive setup proved vital for effective learning, allowing students to experiment securely with attack strategies and mitigation techniques. By providing a controlled environment for testing attacks and defences, the tool translates abstract cybersecurity concepts into practical experience. In summary, the research indicates that such a simulation environment not only augments technical understanding but also fosters critical thinking and responsible security practices. This methodology offers a scalable framework for maritime IT education and can be expanded to encompass additional attack vectors or defence mechanisms in future training or research initiatives.

6. Bibliography

HBO-i. (2018). *Brainstorm*. ICT Research Methods. https://ictresearchmethods.nl/workshop/brainstorm

HBO-i. (2018). *Choosing fitting technology*. ICT Research Methods. https://ictresearchmethods.nl/patterns/choose-fitting-technology

HBO-i. (2018). *Explore user requirements*. ICT Research Methods. https://ictresearchmethods.nl/field/explore-user-requirements

HBO-i. (2018). *Prototyping*. ICT Research Methods. https://ictresearchmethods.nl/workshop/prototyping

HBO-i. (2018). *Stakeholder analysis*. ICT Research Methods. https://ictresearchmethods.nl/field/stakeholder-analysis