

Florida International University

Knight Foundation School of Computing and Information Sciences

Cybersecurity Engineering Focus

Final Deliverable

Project Title: PantherProwl

Team Members: Jared Tracey, Valery Pena, Alejandro Terzini, Jo Johnson, Roldy Augustin

Product Owner: Jared Tracey

Instructor: Masoud Sadjadi

The MIT License (MIT)

Copyright (c) 2016 Florida International University

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Abstract

PantherProwl is an innovative learning platform designed to enhance the skills and confidence of Florida International University (FIU) students in IT and cybersecurity. By offering hands-on applications and knowledge-based assessments, PantherProwl bridges the gap between theory and practice. The project is built on a Linux-based virtual environment, divided into three primary sections: **Assessments**, **Challenges**, and **Coding**. These sections allow users to test their knowledge, tackle real-world challenges, and master coding fundamentals in Bash and Python.

With minimal setup requirements—a hypervisor capable of loading an ISO image—PantherProwl provides a versatile and accessible environment. Users can freely explore, manipulate, and even intentionally break the system, fostering a deeper understanding of troubleshooting and system recovery. Designed as both a sandbox for experimentation and a preparation tool for certifications like CompTIA A+ and Security+, PantherProwl equips students with the skills necessary for future careers in IT and cybersecurity.

Scope

PantherProwl is tailored to support aspiring IT and cybersecurity professionals at the foundational level. It provides a sandbox environment where students can experiment, learn, and grow without constraints. The project scope includes:

1. **Knowledge Assessment:** Comprehensive testing in topics aligned with certification requirements.
2. **Skill Development:** Hands-on challenges designed to simulate real-world scenarios and foster adaptability.
3. **Coding Fundamentals:** A guided approach to understanding and practicing essential programming concepts in Bash and Python.

This platform is limited to Linux-based functionality, operating within a virtualized environment through ISO deployment. It supports a wide range of users, from complete beginners to those preparing for certifications.

Statement of Work

The PantherProwl project will include the following tasks:

1. **Development of Assessment Modules:**
 - Create three 50-question tests covering A+1101, A+1102, and Security+.
 - Ensure questions simulate real-world scenarios and align with certification standards.
2. **Challenge Module Design:**
 - Develop a mini Capture the Flag (CTF) environment with escalating difficulty levels.
 - Incorporate tasks requiring the use of Linux commands, logical reasoning, and creative problem-solving to overcome obstacles.
3. **Coding Tutorial Integration:**
 - Build an interactive coding section covering printing, variables, functions, control loops, and Linux terminal commands.
 - Provide examples and functional explanations for Bash and Python coding concepts.

4. System Integrity and Recovery Options:

- Design the system to allow users the freedom to manipulate or "break" the environment as much as they please.
- Enable users to download a fresh ISO instance for seamless recovery, further promoting freedom of manipulation.

5. Testing and Debugging:

- Conduct rigorous testing to ensure stability, usability, and alignment with educational goals.

6. Documentation and Deployment:

- Create user guides for installation and operation.
- Package the PantherProwl ISO for easy deployment on hypervisors.

Cybersecurity Engineering Focus**1. Educational and Hands-On Approach:**

- The project builds tools to enhance understanding of cybersecurity concepts, Linux systems, and scripting fundamentals.
- It mirrors real-world cybersecurity challenges through the mini CTF and system manipulation capabilities, fostering an engineering mindset.

2. Secure System Design:

- The platform incorporates modular and reusable components (e.g., the database, coding environment) that mimic secure software practices.
- It emphasizes the importance of system resilience and recovery by allowing users to "break" and reset the environment without risk.

3. Cybersecurity Skill Development:

- It prepares users for certifications (like CompTIA Security+) by simulating the real-world application of cybersecurity knowledge, making it inherently tied to the cybersecurity engineering discipline.

4. Focus on Systems and Problem Solving:

- Cybersecurity engineering isn't just about protecting systems but also about building and understanding them. PantherProwl develops these engineering skills by encouraging users to adapt, troubleshoot, and learn through experimentation.

Deliverables

The following deliverables are expected upon project completion:

1. **PantherProwl ISO Image:**
 - A virtual machine-ready ISO file that hosts the PantherProwl environment.
2. **User Documentation:**
 - System navigation*, and usage instructions**.

Technical Document Overview

The technical documentation for PantherProwl provides a comprehensive guide to understanding, deploying, and operating the platform. It covers:

1. **System Requirements:**
 - A hypervisor capable of loading ISO images, such as VirtualBox, VMware, or Hyper-V.
2. **Module Descriptions:**
 - Detailed explanations of the Assessments, Challenges, and Coding sections, including their intended learning outcomes.
3. **Troubleshooting:**
 - Common issues and their solutions, including how to re-download and deploy the ISO file.
4. **Usage Scenarios:**
 - Example use cases to demonstrate how students can maximize their learning experience.
5. **Customization Options:**
 - Guidance on how users can modify the system and experiment with its features.

Database Integration

- The assessment tests are stored in a **SQLite database file (.db)**. This ensures efficient management and retrieval of test data, including:
 - Question text
 - Answer choices
 - Correct answers
 - Explanation of correct answer

Database Structure

- The database follows a structured schema, which includes tables for:
 - **Tests:** A table containing test identifiers and their associated subjects (A+1101, A+1102, Security+).
 - **Questions:** Each question is stored with fields for text, answer options, the correct answer, and an explanation behind the correct answer.

Interaction with the System

- The database is accessed directly with scripts written in Python for querying and updating records.
- Users can customize or modify the database to add new questions or tests, as the SQLite format is lightweight and user-friendly.

Requirements to Use

PantherProwl is designed to be platform-agnostic and only requires the following:

1. A **hypervisor** capable of loading ISO images, such as:
 - **VirtualBox** (open-source and widely supported)
 - **VMware Workstation Player**
 - **Hyper-V**

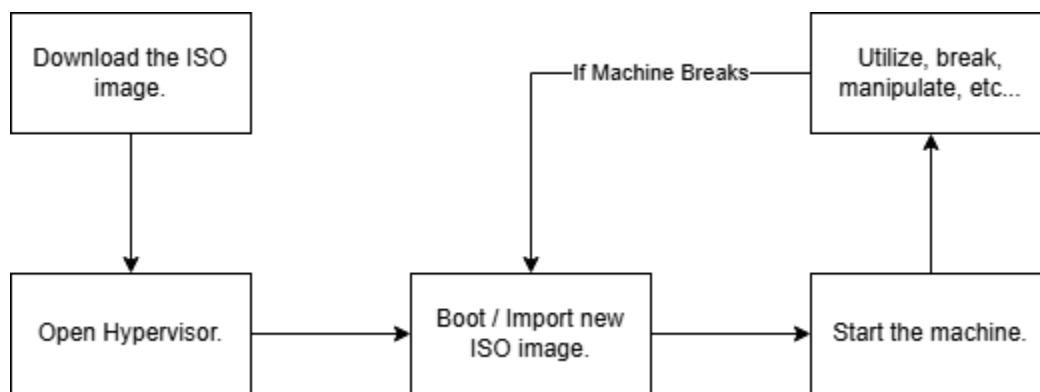
This minimal requirement ensures accessibility for a broad user base.

Installation

The installation process for PantherProwl depends on the chosen hypervisor. While specific steps may vary, the general process involves:

1. **Download the PantherProwl ISO** from the official project repository or website.
2. Open the hypervisor application and create a new virtual machine.
3. Select the PantherProwl ISO as the bootable media.
4. Configure virtual machine settings, such as allocated RAM and storage.
5. Start the virtual machine to boot into the PantherProwl environment.

Further installation details can be found in the accompanying user documentation.



Intended Usages

PantherProwl is designed as an educational tool for students and aspiring professionals to build IT and cybersecurity skills. **Key intended uses include:**

1. **Knowledge Assessment:**
 - Users can take structured tests to evaluate their understanding of certification-related topics.
2. **Skill Development:**
 - By engaging with the mini CTF challenges, users learn to adapt to dynamic situations, think critically, and solve problems efficiently.
3. **Coding Practice:**

- The guided tutorials teach foundational coding skills with practical applications in Bash and Python.

Exploration and Experimentation:

PantherProwl encourages users to experiment freely. The system's design allows users to manipulate, modify, and even "break" the environment. This approach fosters a deeper understanding of system behavior, troubleshooting, and recovery processes. Users can restore the environment easily by reloading the ISO file, ensuring a risk-free sandbox for learning.

*Appendix A: System Navigation

1. Assessments

- **Location:** Found in the main menu under the "Assessments" section.
 - **Purpose:** Provides three 50-question tests covering objectives instilled by CompTIA A+1101, A+1102, and Security+.
 - **Navigation:**
 - Select the **Assessments** directory from the main menu.
 - Run the Assessments.py script and choose one of the available tests:
 - A+1101
 - A+1102
 - Security+
 - Follow the prompts to answer the questions.
 - **Pro Tip:**
 - Each test can be restarted from the beginning, **CTRL + C** will interrupt the script, allowing you to restart.
-

2. Challenges

- **Location:** Found in the main menu under the "Challenges" section.
- **Purpose:** Offers mini Capture the Flag (CTF) challenges designed to teach Linux commands and promote problem-solving.
- **Navigation:**
 - Select the **Challenges** directory from the main menu.
 - Two categories of challenges will appear, select either to continue.
 - A list of challenge tasks will appear, ranging in difficulty.
 - The lower the task number, the less complex of a challenge.
 - Select a challenge to display its description and objective.
 - Use the terminal to execute the required commands or perform the task.
 - Submit the flag or solution when complete.
- **Pro Tip:**
 - Use the **man** command or **--help** for unfamiliar commands during challenges.

3. Coding

- **Location:** Found in the main menu under the "Coding" section.
- **Purpose:** Teaches coding fundamentals in Python and Bash with examples and interactive tutorials.
- **Navigation:**
 1. Select the **Coding** directory from the main menu.
 2. Choose a topic:
 - Printing
 - Variables
 - Functions
 - If Statements
 - Loops (While/For)
 - Running Linux Commands
 3. Try out the examples in the terminal provided within the section.

****Appendix B: Usage Instructions**

Basic Usage Guidelines

1. Starting the System:

- Launch the PantherProwl virtual machine from your chosen hypervisor.
- Wait for the main menu to load, showing the three primary sections.

2. Choosing a Section:

- Use the `cd [directory name]` command to change directories and navigate to the desired sections.
 - i. The `cd` command also allows you to navigate the whole filesystem, even outside the bounds of the product.

3. Interactive Features:

- The terminal accepts standard Linux commands.
-

Experimentation and System Manipulation

1. Freedom to Explore:

- PantherProwl is designed for experimentation. Users can explore beyond the predefined sections by:
 - Modifying files in the system.
 - Testing advanced Linux commands.
 - Writing and executing custom Python or Bash scripts.
 - Typing `exit` to leave the current user, accessing an administrative user account.

2. Breaking and Restoring the System:

- If you "break" the environment:
 - Shut down the virtual machine.
 - Reload a fresh instance of the ISO in your hypervisor.
 - No permanent damage will occur, and the system will reset to its original state.

3. Recovery Tips:

- Always back up changes in files you wish to keep (`cp [file] [backup_location]`).

- If unsure about a command, use the **man** pages or search for online Linux resources.
-

Best Practices for Usage

1. Learning Approach:

- Treat each section as an opportunity to master foundational skills.
- Take notes on the principles covered.

2. Certification Preparation:

- Use the Assessments section to measure your readiness for exams.
- Attempt the Challenges to gain hands-on problem-solving experience.

3. Customization and Experimentation:

- Create your own coding tasks in the Coding section.
 - Explore advanced features of Linux within the terminal to deepen your knowledge.
-

By following this navigation guide and usage instructions, users will maximize their experience with PantherProwl, building both confidence and competence in IT and cybersecurity fundamentals.