

RiCSOC Penetration Test



RiCOS General Design



RiCSOC PenTest is a penetration testing tool that provides a unified terminal input handler, and is backed by three main components:

A test generation module that generates the exact penetration testing commands or operations for the users to execute.

A test reasoning module that conducts the reasoning of the test, guiding the penetration testers on what to do next.

A parsing module that parses the output of the penetration tools and the contents on the webUI.






RiCOS Function Design



The handler is the main entry point of the penetration testing tool. It allows pentesters to perform the following operations:

- Initialize itself with some predesigned prompts.
 - Start a new penetration testing session by providing the target information.
 - Ask for a to-do list, and acquire the next step to perform.
 - After completing the operation, pass the information to RiCSOC PenTest.
 - Pass a tool output.
 - Pass a webpage content.
 - Pass a human description.
- The generation module can also start a continuous mode, which helps the user to dig into a specific task.





RiCSOPentest Benefits



RiCSOC PenTest offers a number of benefits over traditional penetration testing tools, including:

Increased efficiency: RiCSOC PenTest can automate many of the tasks involved in penetration testing, freeing up pentesters to focus on more strategic and creative work.

Improved accuracy: RiCSOC PenTest uses machine learning to reason about the results of penetration tests, helping pentesters to identify and exploit vulnerabilities more effectively.

Reduced risk: RiCSOC PenTest can be used to test systems in a safe and controlled environment, reducing the risk of introducing new vulnerabilities.

