Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Impediments

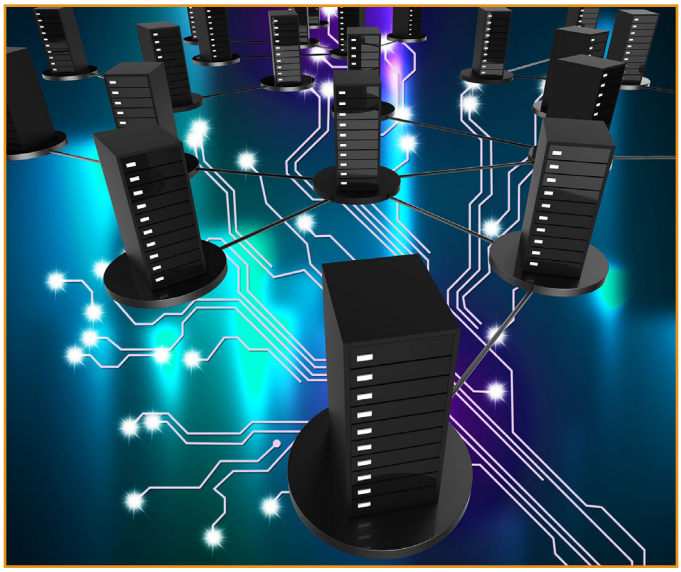
CHALLENGE

Existing penetration testing tools, red team processes, and security testing can not cope with continuous and resilient systems. This project provides realistic, relevant, and appropriate attacks, faults, and disruptions for the Demonstration Integration effort.

What happens when something goes wrong? Will the lights stay on and the system continue to run?

CURRENT PRACTICE

Current practice for penetration testing uses a slice-in-time methodology for tracking vulnerabilities and how the environment looks and behaves. We are using these snapshots as reference for building attack maps and guidance for crafting the method of attack into a network. Since these don't drastically change often, the maps can be used for long periods of time and maintain accuracy. After that point, the rest of the cyber kill chain is executed.



APPROACH

Forthcoming architectures create an ever-changing landscape of targets and vulnerabilities. We are taking the traditional penetration testing schemas and ideas and identifying the faults that they have, as well as what will work for use in the next generation architectures. Once the strengths and weaknesses in the current state of practice are identified, the strengths will be incorporated into the new design for a penetration testing framework. This framework will be designed to work on the new landscape that will be constantly shifting and moving once attacks are successful at compromising the systems in an effort to self heal.

While designing the framework, the Impediments project will also play many different roles to simulate what can happen to a live network, such as the role of user, attacker, as well as the environment. This will validate the testing and verify the conditions for an ARC project to be deemed as successful.

IMPACT

All of the projects under ARC will benefit from the penetration testing that will be available to them. The framework that is being developed will help automate the testing required for an ever-changing defense. Indirectly, the framework for doing penetration testing will allow for more dynamic and up-to-date information and tactics.

ABOUT PNNL

The Pacific Northwest National Laboratory, located in southeastern Washington State, is a U.S. Department of Energy Office of Science laboratory that solves complex problems in energy, national security and the environment, and advances scientific frontiers in the chemical, biological, materials, environmental and computational sciences. PNNL currently has approximately 4,900 staff members and a business volume of more than $1.1 billion. The Laboratory has been managed by Ohio-based Battelle since 1965.

Contact

David Manz
Principal Investigator
(509) 372-5995
david.manz@pnnl.gov

Nathan Krussel
Co-Lead
(509) 375-6421
nate.krussel@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*