



TIP 255a: EPRI P183 Cybersecurity and Privacy Supplemental: Penetration Testing Tools

Context

The degree to which electric sector equipment vendors seek to identify defects and vulnerabilities in their own equipment varies widely. Some vendors go to extensive lengths, including penetration testing, to validate the security of their products. Those executing penetration testing (or paying to have it done) may at times identify such efforts as a demonstration of due diligence. However, test coverage and the vigor with which the tests are executed can be difficult to identify and full disclosure of the results of such testing is rare. This lack of information leaves gaps in the visibility of the security posture for power delivery equipment deployed in the electric sector.

To address this scarcity of information, it is prudent for asset owners to possess the capability to have penetration testing performed on equipment they intend to deploy. To perform the testing in a reasonable timeframe, it is necessary to use proven techniques and tool suites. The degree to which existing tools and techniques meet this necessity needs to be examined. Where existing tools and techniques do not provide adequate coverage, new tools and techniques need to be developed.

Description

This EPRI supplemental project identifies existing penetration test tools and techniques applicable to transmission and distribution equipment. Some of the techniques and tools identified will be chosen to undergo a gap analysis to determine high-priority protocols and technologies for which test coverage is inadequate. Results of the gap analysis will be used to identify techniques and tools that can be applied to bridge, reduce, or eliminate gaps in testing.

The project will build on the penetration testing tool developed in the EPRI Program 183 to create of a suite of tools that can be used by asset owners to better validate and improve the security posture of their transmission and distribution equipment.

Why It Matters

Participation in this supplemental project will provide:

- A better understanding of existing tools and capabilities available to malicious actors as well as security control testers
- Security tools that members can use to perform security testing
- Techniques to maximize the effectiveness of both new and existing security testing tools

Goals and Objectives

Goals of this project include:

- Identification and application of existing penetration tools to gauge effectiveness and coverage with respect to testing electric sector transmission and distribution equipment
- Development and validation of new and improved penetration testing tools and techniques targeted to transmission and distribution equipment

Deliverables

Successful completion of this project will yield the following key deliverables:

Power Delivery System Penetration Testing Tool User Manual: User manual describing the installation and use of the penetration testing tool.

Power Delivery System Penetration Testing Tool: A software tool to support a variety of standard penetration testing techniques for power delivery systems.

TIP 255a: EPRI P183 Cybersecurity and Privacy ***Supplemental: Penetration Testing Tools***

Project Start Date: September 23, 2013

Project End Date: August 23, 2014

Reports & References (Optional)

Links (Optional)

Participating Organizations

Electric Power Research Institute

Funding

BPA Membership FY2014: \$40,000

For More Information Contact:

BPA Project Manager: Andy McGuire
asmcguire@bpa.gov

