

Penetration Testing Toolkit

Software Manual

3002005804



DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

ELECTRIC POWER RESEARCH INSTITUTE, INC. ("EPRI") RESERVES ALL RIGHTS IN THE PROGRAM AS DELIVERED. THE PROGRAM OR ANY PORTION THEREOF MAY NOT BE REPRODUCED IN ANY FORM WHATSOEVER EXCEPT AS PROVIDED BY LICENSE, WITHOUT THE CONSENT OF EPRI.

A LICENSE UNDER EPRI'S RIGHTS IN THE PROGRAM CAN BE OBTAINED DIRECTLY FROM EPRI.

THE EMBODIMENTS OF THIS PROGRAM AND SUPPORTING MATERIALS MAY BE INDEPENDENTLY AVAILABLE FROM ELECTRIC POWER SOFTWARE CENTER (EPSC) FOR AN APPROPRIATE DISTRIBUTION FEE.

ELECTRIC POWER SOFTWARE CENTER (EPSC)
9625 RESEARCH DRIVE
CHARLOTTE, NC 28262

THIS NOTICE MAY NOT BE REMOVED FROM THE PROGRAM BY ANY USER THEREOF.

NEITHER EPRI, ANY MEMBER OF EPRI, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

1. MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS OF ANY PURPOSE WITH RESPECT TO THE PROGRAM ; OR
2. ASSUMES ANY LIABILITY WHATSOEVER WITH RESPECT TO ANY USE OF THE PROGRAM OR ANY PORTION THEREOF OR WITH RESPECT TO ANY DAMAGES WHICH MAY RESULT FROM SUCH USE.

RESTRICTED RIGHTS LEGEND: USE, DUPLICATION, OR DISCLOSURE BY THE GOVERNMENT IS SUBJECT TO RESTRICTION AS SET FORTH IN PARAGRAPH (G) (3) (I), WITH THE EXCEPTION OF PARAGRAPH (G) (3) (I) (B) (5), OF THE RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE IN FAR 52.227-14, ALTERNATE III.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION(S), UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Southwest Research Institute

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2015 Electric Power Research Institute, Inc. All rights reserved.

ACKNOWLEDGMENTS

The following organization(s), under contract to the Electric Power Research Institute (EPRI), prepared this report:

Southwest Research Institute
6220 Culebra Rd.
San Antonio, TX 78238

Principal Investigator
T. Do

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Penetration Testing Toolkit: Software Manual. EPRI, Palo Alto, CA: 2015. PT1.0.

SOFTWARE DESCRIPTION

The “Penetration Testing Toolkit” provides a unified interface for a user to perform a variety of penetration testing activities against a power systems device.

Description

The Penetration Testing Toolkit is a software tool to aid end users in the security assessment of power systems sector specific embedded devices. The PT² provides the end user with a centralized interface for managing and executing penetration test activities. The PT² gives the end user the ability to execute the full range of penetration test activities such as: script execution, data collection, data analysis, traffic injection, and fuzzing. Additionally, the PT² provides access to a variety freely available open source security penetration testing tools in an easy to use interface. The benefit of this approach is that it minimizes the amount of setup required in order to execute a penetration test. In the initial release of the software, support for the OpenADR 2.0a protocol was provided. The OpenADR 2.0a protocol is an XML based HTTP protocol, therefore, the toolkit may also be utilized to test protocols which are similar in structure to the OpenADR protocol. In version 2.0 of the software, preliminary support for the Distributed Network Protocol 3.0 (DNP3) protocol has been provided. The DNP3 protocol is a binary-based protocol that is used primarily in industrial control system environments. DNP3 works across a variety of physical links such as RS-422 and Ethernet. This release of the software supports the Ethernet variant of the protocol.

The features supported for OpenADR are:

- OpenADR Specific Test Cases
- OpenADR Packet Sniffer and Analyzer
- An HTTP Proxy
- An XML Fuzzer

The features supported for DNP3 are:

- DNP3 Specific Test Cases
- DNP3 Packet Sniffer and Analyzer
- A DNP3 Proxy

Please note that there are some limitations of this software with regard to DNP3, specifically the software does not currently support:

- Rule-based DNP3 packet modification
- Server or client emulation
- Application layer packet decoding
- Secure DNP3 packet decoding
- Secure DNP3 authentication (DNP3 SAV5)

Please note that there are performance limitations when using the software with a large number of packets stored in the database and limited machine memory. As currently designed, all packets are stored in an in-memory database. As a result, a large number of packets can exhaust the amount of virtual memory allocated to the software and cause a performance slowdown. The issue is most commonly seen when trying to clear the packets from the sniffer interface screen. With the current structure of the software architecture, there is no feasible way to limit the size of the dynamically allocated packet database. This may be reviewed and modified in future revisions. When using the sniffer function, we recommend the following:

- Do not leave the sniffer function running for long periods of time.
 - Use the sniffer for less than 30 minutes at a time and clear packets when you are finished to prevent a large growth in packets. Please note that actual time to trigger the software limitation will vary more or less depending on machine memory and the rate at which network traffic is generated.

The PT2 has been developed with extensibility in mind and may support the addition of protocols such as: IEC 61850, Smart Energy Profile 2.0, and DLMS-COSEM in future revisions.

Benefits and Value

Values and benefits provided by the PT² are that it provides:

- A power systems sector specific tool for performing penetration testing.
- A tool targeting power systems specific protocols.
- A unified interface for performing multiple penetration testing activities

Platform Requirements

At a minimum the supported platforms for this software are: Windows Vista/7/8 (32-bit and 64-bit), Ubuntu Linux 32-bit and 64-bit, and Kali Linux 32-bit and 64-bit.

The following experimental feature is only supported under Kali Linux 32-bit and 64-bit:

- OpenADR Proxy

Under the Windows Platform, only the following features are supported:

- OpenADR Packet Sniffer, OpenADR Fuzzer

The “Test Script Execution” functionality is not supported under the Windows platform.

It is recommended that the user install the “Kali Linux” distribution as this software has been designed to interoperate with a number of third-party packages included in that particular Linux distribution. Kali Linux can be obtained from the following website:

<https://www.kali.org/downloads/>.

The Ubuntu Linux distribution can also be used given that the following software packages are installed.

- Nmap: <http://nmap.org/>
- Arpspoof: <http://arpspoof.sourceforge.net/>

These packages can be installed on Ubuntu linux with the following command:

- `sudo apt-get install dsniff nmap`

If you are using virtual machines to execute this software ensure the following:

- Network adapters are configured in bridged networking mode
- The “server” and “client” virtual machines are on physically separate machines
- The host operating system is not running Microsoft Hyper-V as it may prevent ARP poisoning attacks

Keywords

Penetration Testing, Smart Grid, OpenADR, DNP3

CONTENTS

1 INSTALLING PREREQUISITES.....	1-1
Operating System Prerequisites.....	1-1
Software Prerequisites	1-1
Installing Prerequisites	1-1
2 BUILDING FROM SOURCE	2-1
Building the Software	2-1
3 INSTALLATION AND USAGE INFORMATION.....	3-1
Recommended Test Environment for OpenADR	3-1
Recommended Test Environment for DNP3.....	3-2
Introduction to the User Interface	3-2
Starting the Software.....	3-3
Windows Instructions.....	3-3
Linux Instructions	3-3
4 TEST CASES FOR OPENADR	4-1
Scenario 1: Creating a Workspace and a Project	4-1
Scenario 2: Host Discovery	4-4
Scenario 3: ARP Poisoning	4-5
Scenario 4: Traffic Sniffing	4-6
Scenario 5: Using the Proxy	4-8
Using the Filters	4-10
Using the Interceptor	4-10
Scenario 6: Using the Fuzzer	4-11
Adding New Fuzz Test Cases	4-15
5 TEST CASES FOR DNP3.....	5-1
Scenario 1: Creating a Workspace and a Project	5-1
Scenario 2: Host Discovery	5-4
Scenario 3: ARP Poisoning	5-5
Scenario 4: Traffic Sniffing	5-7
Scenario 5: Using the DNP3 Proxy.....	5-9
Using the Interceptor	5-10
6 ADVANCED USAGE	6-1
Removing the Database.....	6-1
Removing Projects	6-1
Adding Test Cases.....	6-1
Manual Editing Files	6-1
Adding and Removing Test Cases Using the GUI	6-2
Removing all Packets from the Sniffer.....	6-2
Filtering Packets in the Sniffer Window	6-2

Customizing Columns in the Sniffer Window/Fuzzing Window	6-2
Controlling the Packets Captured by the Sniffer	6-3
Loading a PCAP capture	6-3
Enabling SSL Support in the Proxy	6-3
Uninstalling the Software.....	6-3

LIST OF FIGURES

Figure 1 – OpenADR Test Environment	3-1
Figure 2 – DNP3 Test Environment.....	3-2
Figure 3 - Workspace Wizard	4-1
Figure 4 - Project Workspace View	4-2
Figure 5 - Create New Project Dialog.....	4-3
Figure 6 - Add New Device Dialog	4-3
Figure 7 - Test Case Properties	4-4
Figure 8 - Test Script Console.....	4-4
Figure 9 - Arp Poison Properties	4-5
Figure 10 - Arp Poison Console	4-6
Figure 11 - Sniffer Options Panel	4-7
Figure 12 - Sniffer Packets.....	4-8
Figure 13 - Proxy Configuration Options	4-9
Figure 14 - Proxy Interceptor Panel.....	4-11
Figure 15 - Sending Packet to Fuzzer	4-12
Figure 16 - Fuzzer Panel.....	4-12
Figure 17 - Fuzzer Options Panel	4-13
Figure 18 - Fuzzer Test Case Selection	4-14
Figure 19 - Fuzz Packet Display	4-14
Figure 20 - Fuzzer Options Panel	4-15
Figure 21 - Add Fuzz Test Panel.....	4-16
Figure 22 - Workspace Wizard	5-1
Figure 23 - Project Workspace View	5-2
Figure 24 - Create New Project Dialog.....	5-3
Figure 25 - Add New Device Dialog	5-3
Figure 26 - Test Case Properties	5-4
Figure 27 - Test Script Console.....	5-5
Figure 28 - Arp Poison Properties	5-6
Figure 29 - Arp Poison Console	5-6
Figure 30 – IP Forwarding Console.....	5-7
Figure 31 - Sniffer Options Panel	5-8
Figure 32 - Sniffer Packets.....	5-9
Figure 33 – DNP3 Proxy Options	5-10
Figure 34 - Proxy Interceptor Panel.....	5-11
Figure 35 - Customize Columns.....	6-3

MANDATORY SOFTWARE INSTALLATION INFORMATION

Installation of EPRI Software at Client Site

EPRI develops software using a number of third party software products and tools that run on various operating systems and server platforms. Reports from the software industry suggest there are known security issues with some products and systems. EPRI recommends that, if you are using EPRI software, you review its use with your Information Technology (IT) department and their overall strategy to ensure that all recommended security updates and patches are installed as needed in your corporation. If you have any concerns please call the EPRI Customer Assistance Center (CAC) at 1-800-313-3774 (or email askepri@epri.com).

If you experience difficulties accessing the application

If you experience difficulties accessing the application after standard installation on Windows, please consult your IT department personnel to have proper access permissions setup for your use. If the problem can not be resolved, please call the EPRI Customer Assistance Center (CAC) at 1-800-313-3774 (or email askepri@epri.com).

1 INSTALLING PREREQUISITES

In this section we will review how to install the software prerequisites.

Operating System Prerequisites

- Ubuntu Linux 14.04
- Kali Linux
- Windows Vista/7/8

Please note that the “Test Script Execution” functionality is not supported on the Windows platforms as this functionality relies on Third Party Software packages that may be incomplete or not available on the Windows platform. The preferred operating system environment is Kali Linux.

Software Prerequisites

- Java SE JRE 6u45
- Apache Maven 2.2.1 build system
- Apache Ant 1.9 build system
- Winpcap (for Windows)
- Libpcap (for Linux)
- Redsocks (for Linux)

Installing Prerequisites

1. Install the development kit of Java SE 6 for your platform
 - 1.1. Windows: <http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-419409.html>
 - 1.1.1. Download Java SE Development Kit 6u45 from above link
 - 1.1.2. Modify System Environment Variable Path to include path to Java SE Development Kit 6u45 binary (e.g. C:\Program Files\Java\jdk1.6.0_45\bin)
 - 1.1.3. Verify install by issuing the following command and observing reported version
`> java -version`
 - 1.1.4. Create another System Environment Variable named JAVA_HOME with the path to your Java Development Kit 6u45 (e.g. C:\Program Files\Java\jdk1.6.0_45)
 - 1.2. Ubuntu Linux:
 - 1.2.1. `sudo apt-get install openjdk-6-jdk`

```
> java -version
```

2. Install the Apache Maven 2.2.1 build system

2.1. Windows: <http://archive.apache.org/dist/maven/binaries/>

2.1.1. Download Apache Maven 2.2.1 zip from above link

2.1.2. Modify System Environment Variable Path to include path to Apache Maven 2.2.1 binary (e.g. C:\Program Files\apache-maven-2.2.1\bin)

2.1.3. Verify install by issuing the following command and observing reported version

```
> mvn -v
```

2.2. Ubuntu Linux:

2.2.1. `sudo apt-get install maven2`

2.2.2. Verify install by issuing the following command and observing reported version

```
> mvn -v
```

3. Install the Apache Ant 1.9 build system

3.1. Windows: <http://ant.apache.org/bindownload.cgi>

3.1.1. Download Apache Ant 1.9 from above link

3.1.2. Modify System Environment Variable Path to include path to Apache Ant 1.9 binary (e.g. C:\Program Files\apache-ant-1.9.4\bin)

3.1.3. Verify install by issuing the following command and observing reported version

```
> ant -version
```

3.2. Ubuntu Linux:

3.2.1. `sudo apt-get install ant`

```
> ant -version
```

4. Install libpcap for Winpcap for your platform:

4.1. Windows: <http://www.winpcap.org/install/default.htm>

4.1.1. Download Winpcap and run executable from above link

4.1.2. Follow instructions on the screen to install correct drivers

4.1.3. Verify install by navigating to Control Panel and to Add/Remove Programs and an entry with “WinPcap” should exist

4.2. Linux:

4.2.1. `sudo apt-get install libpcap0.8-dev`

4.2.2. Verify install by issuing following command and observing the following libraries installed: libpcap.so.0.8, libpcap.so.1.5.3, libpcap.a, and libpcap.so.

```
> sudo find / -name 'libpcap*' -print
```

5. Install the redsocks package for Linux

5.1. `sudo apt-get install redsocks`

5.2. Verify install by issuing the following command and observing reported version

```
> redsocks -v
```

After installing all software prerequisites restart the operating system.

2 BUILDING FROM SOURCE

These instructions are only to be used if the user wishes to build the software from source. If a binary distribution is available for the user's system, the user should skip this step and proceed to the usage instructions section. Before attempting to build from source the user needs to install the software prerequisites covered in Section 1.

Release Date: 6/10/2015

Contact Information: Tam Do, Southwest Research Institute, tam.do@swri.org

Third Party Software Used: antlr, dom4j, h2, hibernate, jboss, jgoodies, jnetpcap, junit, miglayout, owasp-proxy, rsyntaxtextarea, swingx, hexlib, redsocks

System Requirements: Ubuntu Linux, Kali Linux, Windows Vista/7/8

Lines of Code: ~21,200

Building the Software

1. Extract the source binary package for PT2.
 - 1.1. Please ensure you extract the correct source binary package for your operating system. Do not extract the Linux binary package on a Window's platform or attempt to use Linux binaries compiled on a Window's platform.
 - 1.2. Please ensure that if you are building the software on a Window's platform, you must ensure that the file path does not include any spaces. For example building the software in the folder "C:\Software Development\PT2" will not work. You will need to place it in a folder as such "C:\Software_Development\PT2". This also applies to any subdirectory folder leading up to the project source code. This is a known issue that may be resolved in later software releases.
2. Navigate to the source package directory from the command line
3. Issue the following command to download all dependencies and build the packages
 - 3.1. mvn clean package
4. If the build is successful, you should see a "BUILD SUCCESSFUL" response
5. If the build is not successful, please make sure you have an internet connection and try again.
6. The compiled binaries should now be present within the target/ directory
 - 6.1. Please note that compiled binaries will exist for each of the following platforms:
 - 6.2. Windows 32-bit (.zip file)
 - 6.3. Windows 64-bit (.zip file)
 - 6.4. Linux 32-bit (.tar.gz file)
 - 6.5. Linux 64-bit (.tar.gz file)

3 INSTALLATION AND USAGE INFORMATION

Recommended Test Environment for OpenADR

The recommended testing environment for OpenADR devices is depicted below:

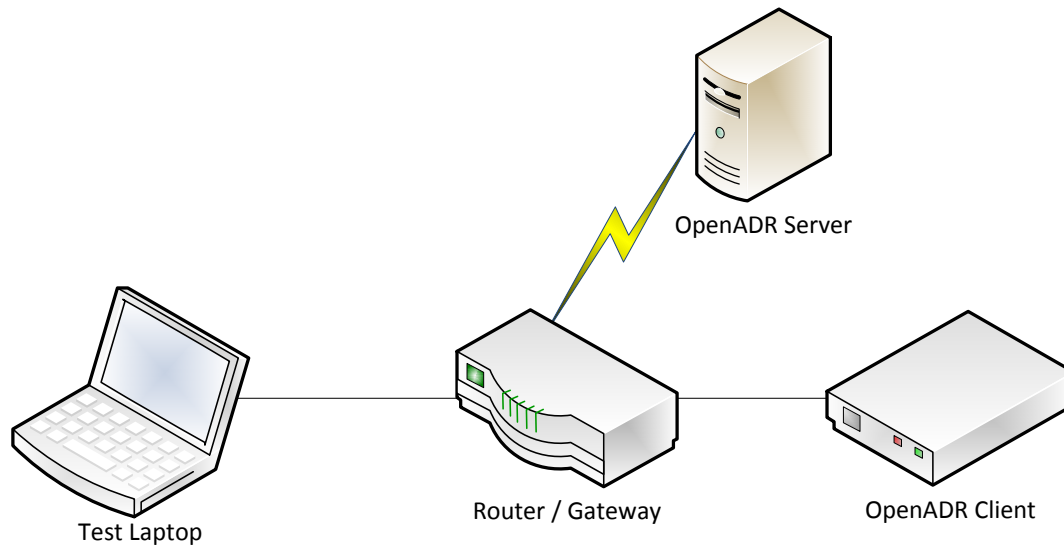


Figure 1 – OpenADR Test Environment

The test laptop and the OpenADR client are connected to the same router/gateway. The router/gateway has a remote connection to an OpenADR server. The remote connection may be represented by an internet connection or virtual private network. Please note that if the software is running in a virtual machine (VM) then the virtual network adapter of the VM must have promiscuity mode enabled.

Recommended Test Environment for DNP3

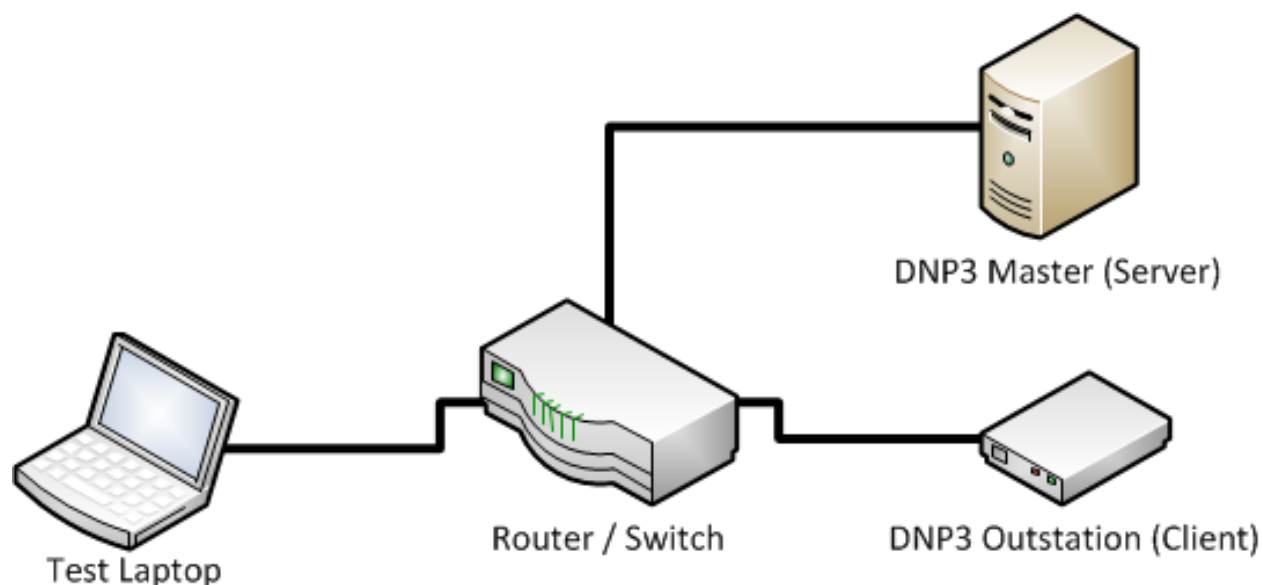


Figure 2 – DNP3 Test Environment

The test laptop and the DNP3 outstation are connected to the same router/switch. The router/switch has a remote connection to a DNP3 server. The remote connection may be represented by an Internet connection or Virtual Private Network (VPN). Please note that if the software is running in a virtual machine (VM) then the virtual network adapter of the VM must have promiscuity mode enabled.

Introduction to the User Interface

The PT2 is a graphical-user-interface (GUI) based program that leverages a “workspace” centric design, where a user can at any given time manage multiple projects within the workspace.

From the “workspace” view the user is be able to:

- Create a new workspace
- Open an existing workspace
- Remove an existing workspace
- View all projects within a workspace
- Create a new project
- Remove a project
- Select a project
- Start the proxy
- View the fuzzer

Each project within a workspace operates independently of all other projects existing within the workspace, or other workspaces. Projects are created with the “project wizard dialog”. The user is required to specify a project name and description before proceeding. Next, the user is asked

to name the device, provide a device description, and select an interface and the protocol. Upon adding the device to the project, the project will be populated with a set of protocol specific test cases. These test cases contain respective test scripts, which will aid the end user in testing the device.

For example, if an end user is testing a Smart Meter, the device would have several interfaces such as: RF, ZigBee, and Optical. Additional, per each interface a specific protocol would be assigned such as: C12.22, ZigBee Smart Energy, or C12.18.

When the user has finished adding creating a project and adding devices to it, the user can access the project from the workspace view. When selecting the project, the user will notice that the sniffer options tab now contains the list of devices associated with the project. Upon selecting the device from the list, the user is able to initiate a packet capture or load a set of previously captured packets.

In addition to the sniffer, the user will have access to a proxy and a fuzzer. The proxy is used for man-in-the-middle security tests, and must be active when fuzzing OpenADR 2.0a responses. The fuzzer is used for “fuzz” testing to test the how a device or server handles invalid or malformed data.

Starting the Software

To ease the process of executing the software, binary distributions have been provided. In this section we will review how to execute the software from the binary distribution.

Windows Instructions

In this section we will review how to execute the software on Windows.

1. Locate the software distribution for your version of Windows (32-bit or 64-bit). The software distributions are located in the pt2/targets directory if you have received the software source distribution.
 - 1.1. 32bit: pt2-0-0.2-<DATE/TIME>-SNAPSHOT-win32.zip
 - 1.2. 64bit: pt2-0-0.2-<DATE/TIME>-SNAPSHOT-win64.zip
2. Extract the software to a location on your hard disk.
3. In a Windows command prompt, navigate to the folder where the software was extracted.
Note: If you are using Windows, please run the Command Prompt as Administrator.
4. Execute the “runPT2.bat” file from the command prompt to start the software.

Linux Instructions

In this section we will review how to execute the software on Linux.

1. Locate the software distribution for your version of Linux (32-bit or 64-bit). The software distributions are located in the pt2/targets directory if you have received the software source distribution.
 - 1.1. 32bit: pt2-0-0.2-<DATE/TIME>-SNAPSHOT-linux-x86.tar.gz
 - 1.2. 64bit: pt2-0-0.2-<DATE/TIME>-SNAPSHOT-linux-x86_64.zip

2. Extract the software to a location on your hard disk
 - 2.1. `tar -xvzf <software name>`
3. In a terminal window, navigate to the folder where the software was extracted
4. If you are using Kali Linux, execute the “runPT2.sh” file from the terminal to start the software.
5. If you are using Ubuntu Linux, you will need to execute the software as a root user. To run this software as a “root” user execute the following command. You may be prompted to enter your password.
 - 5.1. `sudo ./runPT2.sh`

4 TEST CASES FOR OPENADR

In this section we will describe the different usage scenarios for the software.

Scenario 1: Creating a Workspace and a Project

1. Launch the software.
2. You will be presented with the following screen.

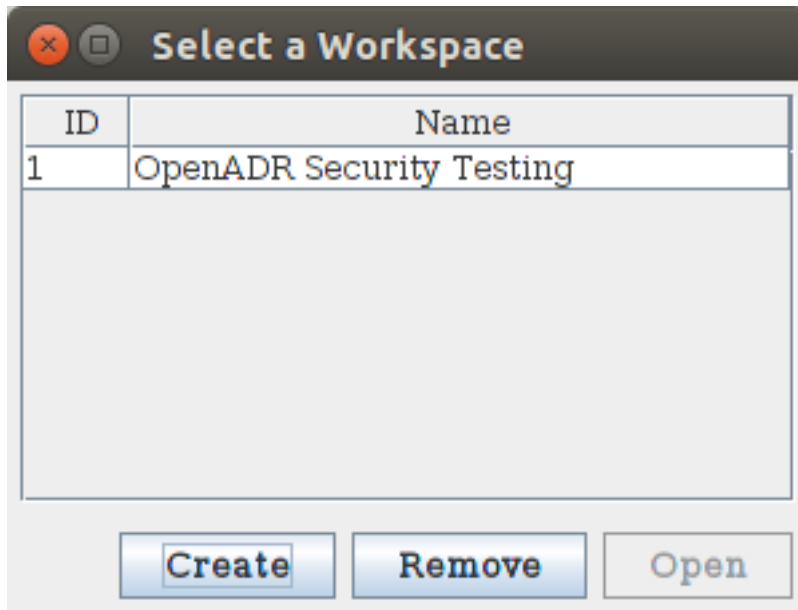


Figure 3 - Workspace Wizard

3. If this is the first time you are launching the software, the workspace list will be empty.
 - 3.1. In this case, click the “Create” button to create a new workspace.
 - 3.2. You will be presented with a dialog to give a name to your workspace.
 - 3.3. Please give a meaningful name to your workspace that you will remember.
4. A workspace encompasses a set of projects that may be used to test different devices.
 - 4.1. An example of a name is “OpenADR Security Testing”
5. Upon clicking OK, the workspace will appear in the list.
6. Select the workspace and click the “Open” button to open the workspace.
7. Upon opening the workspace you will be presented with the following screen.

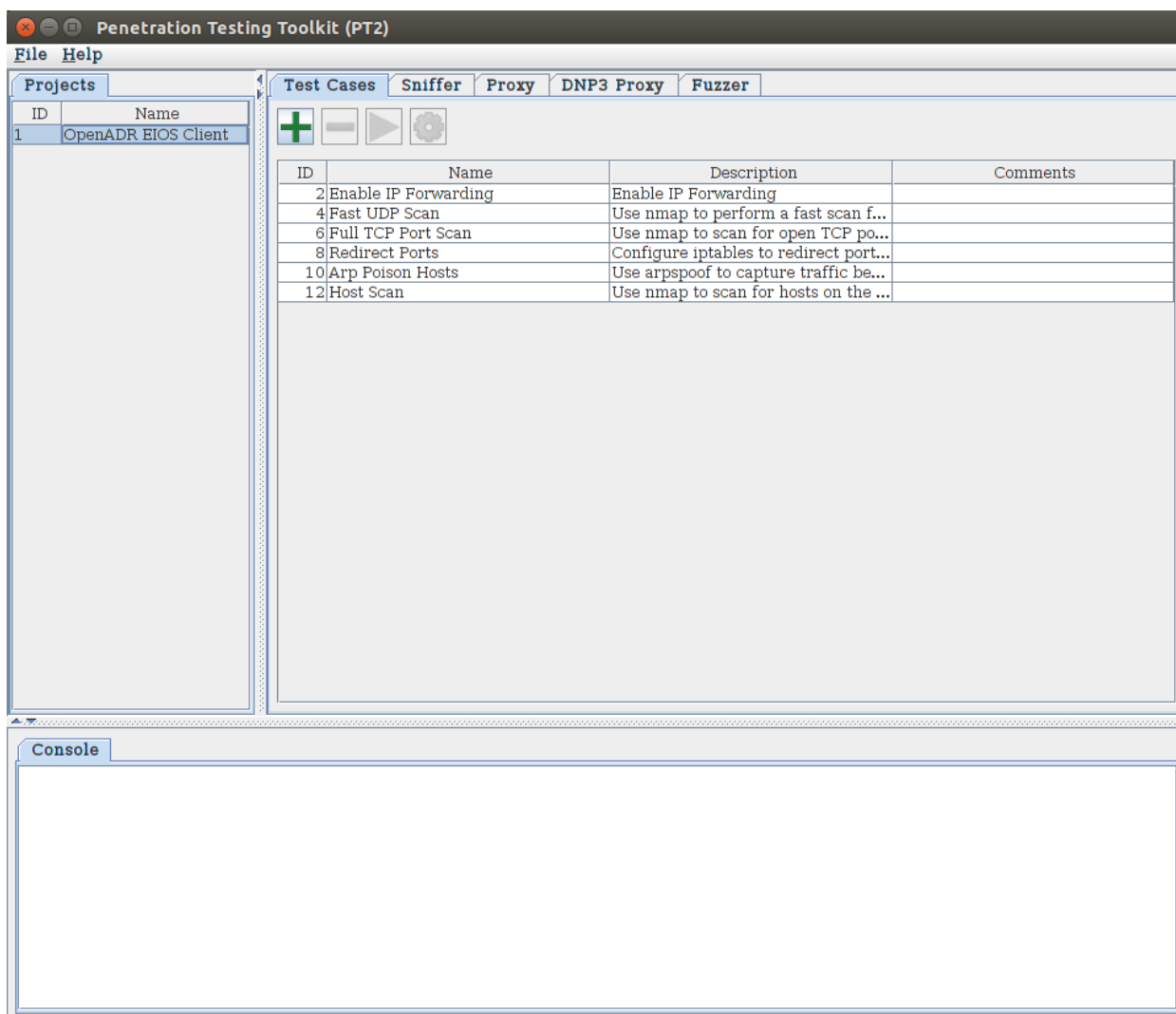
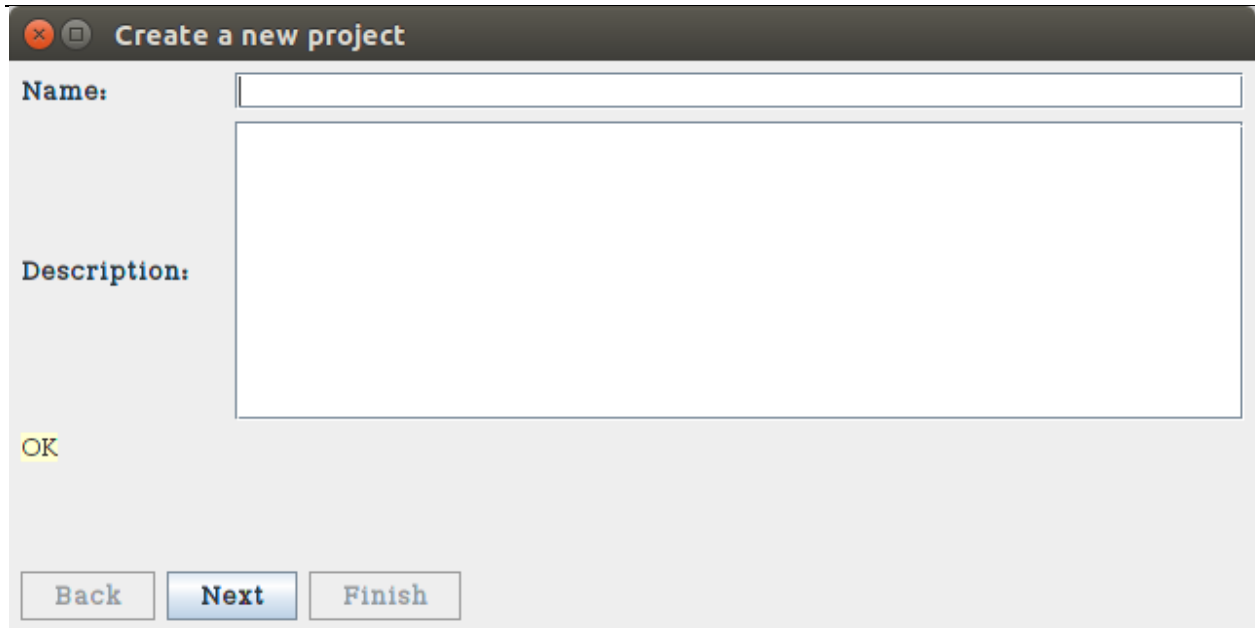


Figure 4 - Project Workspace View

8. If this is the first time you are running the software, this screen may be empty.
9. To add a project to the workspace, from the “File” menu selected the “New Project” option.
10. You will be presented with the following dialog:



Create a new project

Name:

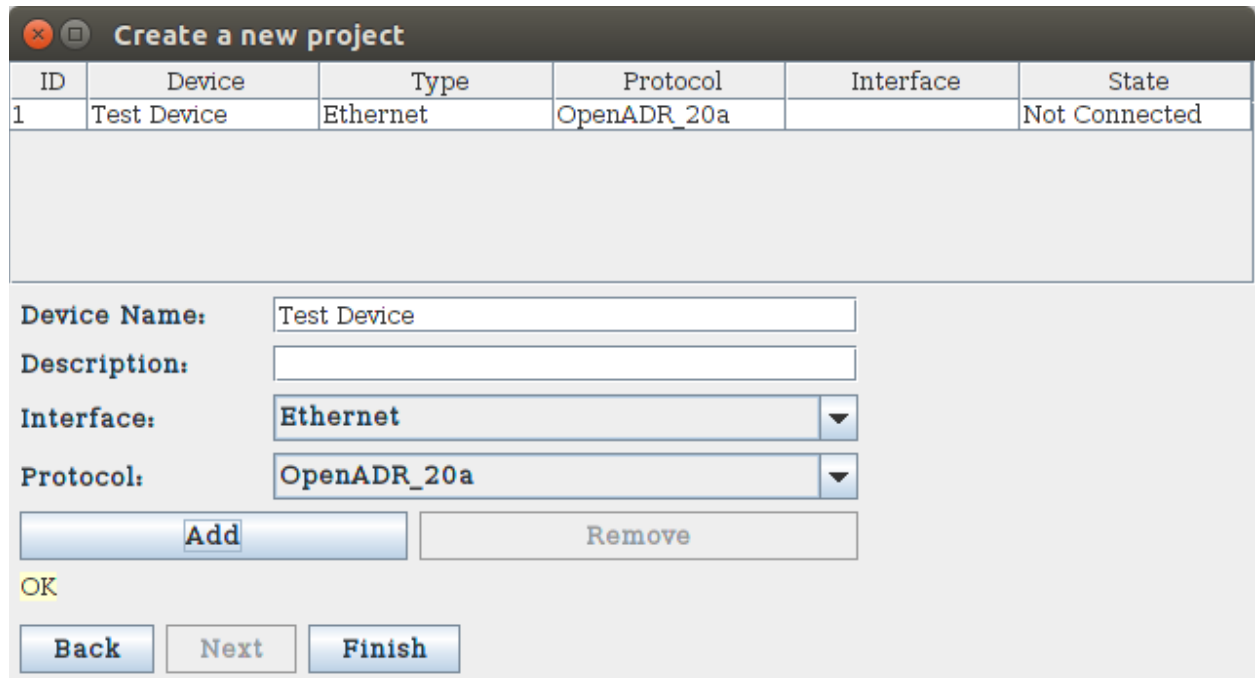
Description:

OK

Back Next Finish

Figure 5 - Create New Project Dialog

11. Please provide a meaningful name and description for your project and click next.
12. Upon clicking next, a new project will be added to the workspace.
13. The next step is to add a device, interface, and protocol to the project.



Create a new project

ID	Device	Type	Protocol	Interface	State
1	Test Device	Ethernet	OpenADR_20a		Not Connected

Device Name:

Description:

Interface:

Protocol:

Add Remove

OK

Back Next Finish

Figure 6 - Add New Device Dialog

14. Please provide a device name and description, and the select the desired interface and protocol.

- 14.1. In the current version, only the “Ethernet” interface is supported.
15. Click Add to add the device to your project.
16. Click Finish to exit the dialog.
17. If you now select the project, you will notice that the project has been populated with a list of default test cases.
18. These test cases are added based on the protocol that you selected.

Scenario 2: Host Discovery

This section assumes that the user has followed “Scenario 1: Creating a Workspace and a Project” to create a new workspace and project. This section also assumes that the user is running a “Linux” operating system, the Windows environment is not supported, with the PT2 software started under a root user, and also that the user has network access to the device they are evaluating.

1. Select the project from the project list panel on the left.
2. A set of default test cases will be populated in the GUI.
3. Select the test with the name “Host Scan” from the list of test cases.
4. Click the settings button “indicated by the gear symbol” above the list of test cases.

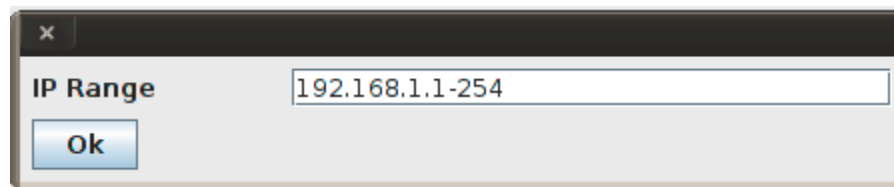


Figure 7 - Test Case Properties

5. Enter the IP range that is desired to be scanned.
6. Click the OK button.
7. Make sure the test case is selected and click the green run triangle.
8. The script will execute in a new window next to the console at the lower portion of the screen.

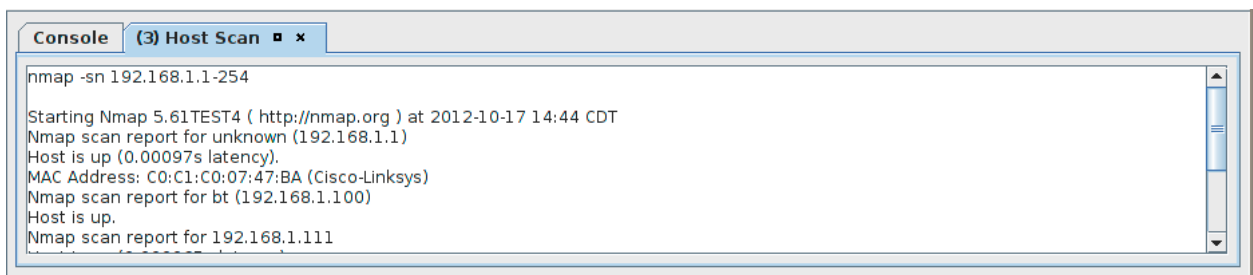


Figure 8 - Test Script Console

9. Please note that the console window displays the current test case ID in the tab, and the test script command and output in the text area below the tab.

10. Please take note of the hosts that have been detected.
11. Of particular interest are the IPs of the targeted device and the IP of the gateway device.
12. These can be found by correlating the MAC address to the discovered IP.
 - 12.1. How to locate the MAC address is out of scope of this manual, however these are typically found on the device label.

Scenario 3: ARP Poisoning

This section assumes that the user has followed “Scenario 1: Creating a Workspace and a Project” and “Scenario 2: Host Discovery” and has the following information available:

- IP Address of the Gateway or OpenADR Server
- IP Address of the Device

The user performs the following:

1. Select the test named “Arp Poison Hosts” from the test case list.
2. Click on the gear icon to configure the test.

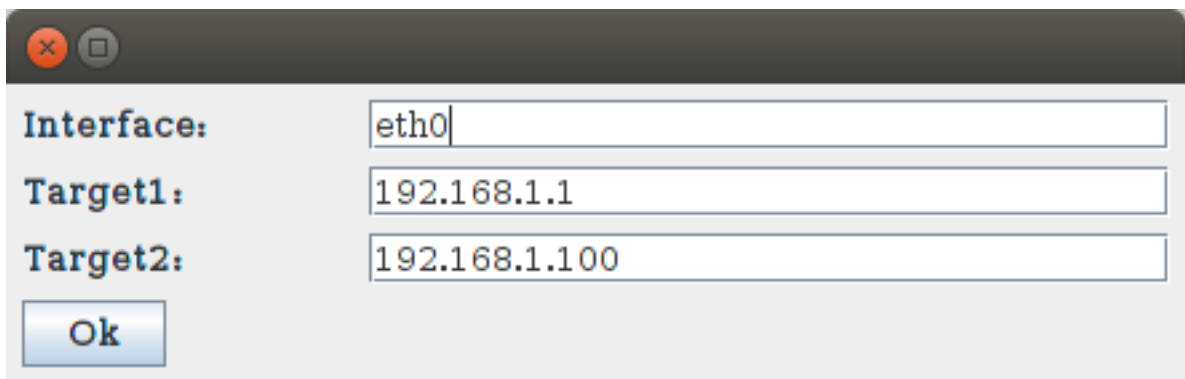


Figure 9 - Arp Poison Properties

3. If the OpenADR Server and device reside on the same physical network switch then enter the IP address of the OpenADR server in Target1 otherwise enter the IP address of the gateway in Target1.
4. In Target 2 enter the ip address of the device.
5. Click OK to save the settings.
6. Click on the green run triangle to execute the test.
7. Please note that the test is now running and is available in the tab below the list of tests.

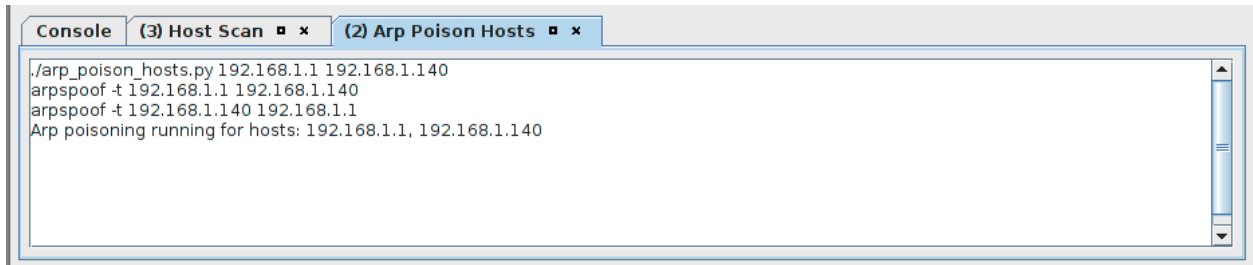


Figure 10 - Arp Poison Console

8. Since the ARP poison attack is an active test, the test will continue to run until the user stops the script by clicking on the square-shaped symbol to the left of the “X” in the tab, or exits the program.
9. The user must now enable IP forwarding to allow the packets to be forwarded to the remote host.
10. Select the test named “Enable IP Forwarding”.
11. Click on the green run arrow to execute the test.

Scenario 4: Traffic Sniffing

This section assumes that the user has successfully performed “Scenario 3: ARP Poisoning” and now wishes to view the intercepted packets.

The user performs the following:

1. Select the project from the project list.
2. Select the Sniffer Tab.
3. Click on the Options Panel.

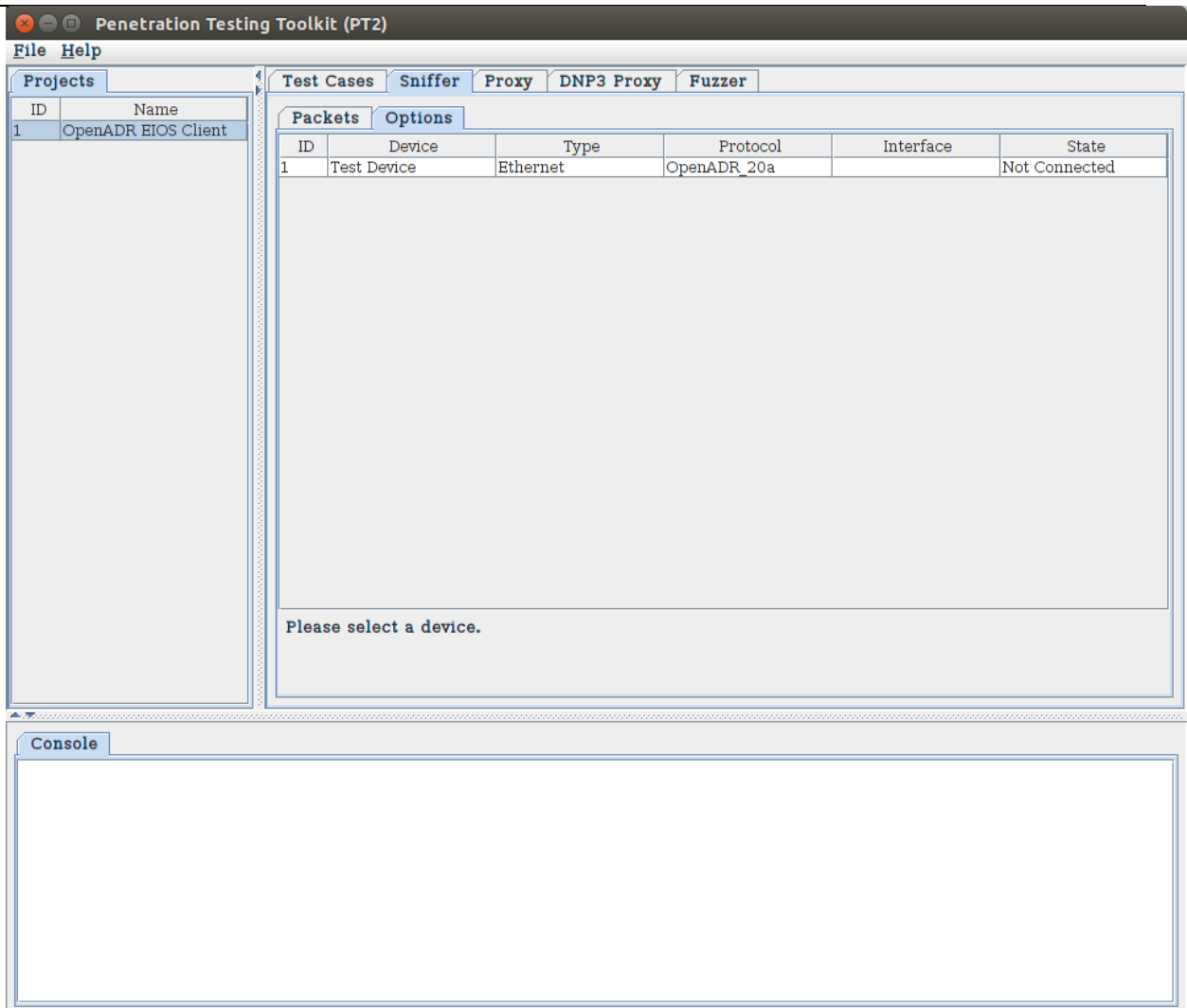


Figure 11 - Sniffer Options Panel

4. Select the physical interface from the dropdown list.
 - 4.1. Please note that this feature is supported only if you are running as an administrator or root user.
 - 4.1.1. On a Linux machine the Ethernet interface should be selected (e.g., eth0). Please note that using any interface aside from eth0 may cause the packet sniffer to not work correctly until the program is restarted
5. Click the Enable Sniffer button.
6. Click on the Packets tab.
7. As packets are sent between the OpenADR Client and the Server, they will be captured in the Packets tab.

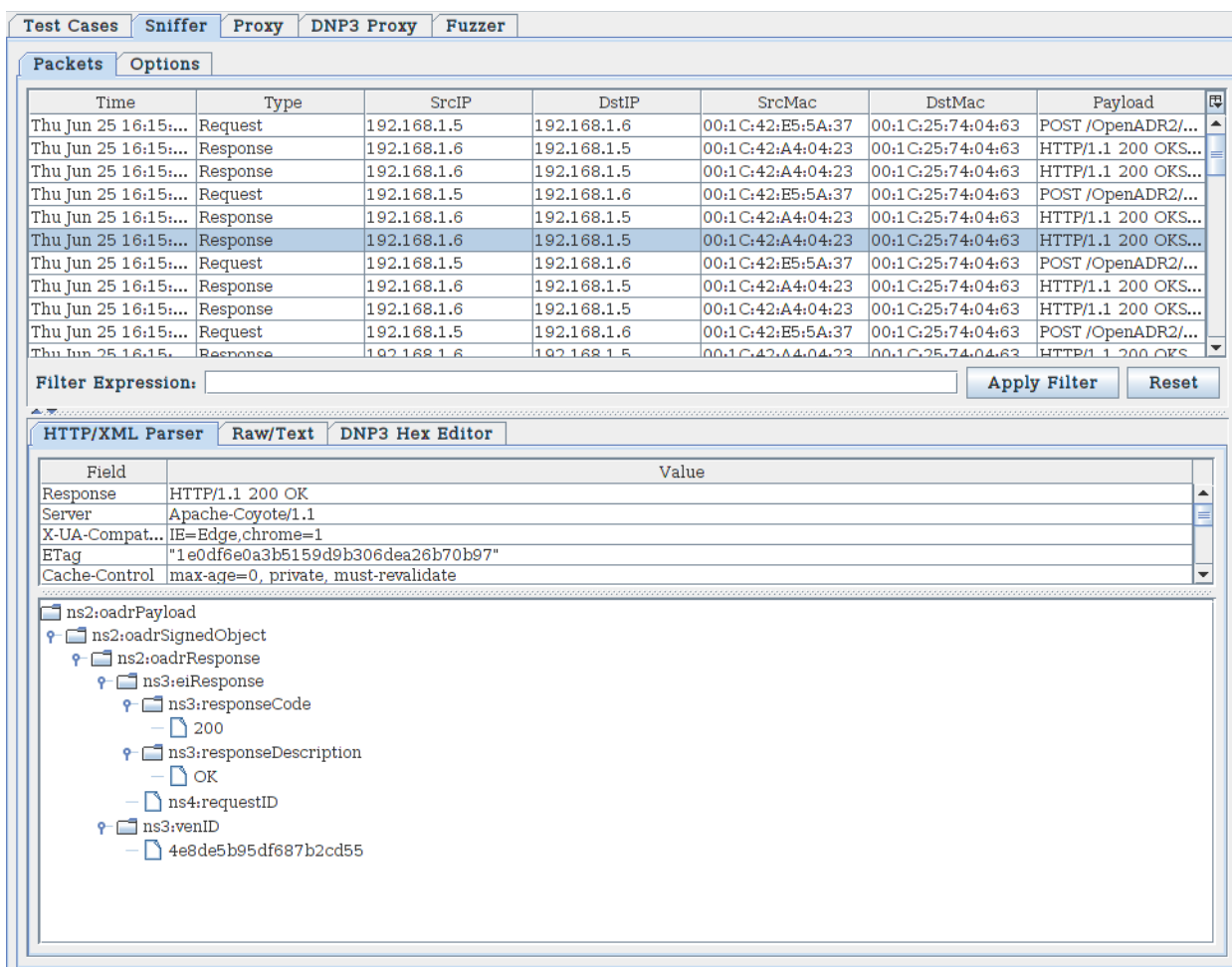


Figure 12 - Sniffer Packets

8. When you select a packet, the contents will be displayed in the analyzer panel.
9. The parser view allows you to browse the XML content in a tree view.
10. The Raw/Text panel allows you to see the raw html text.

Scenario 5: Using the Proxy

This section assumes that the user has successfully performed “Scenario 3: ARP Poisoning Scenario 3” and now wishes to modify the intercepted packets. OpenADR Proxy is an experimental feature only supported under Kali Linux 32-bit and 64-bit; please note, due to this restriction Scenario 5 will not work with an Ubuntu 14 machine. This feature has been confirmed to work with targets where the original port of intercepted packets is either “80” or “8080”; intercept on other ports are not supported. Please note, if the OpenADR Proxy begins to not work correctly it can be fixed by restarting the operating system.

The user performs the following:

1. Select the project from the project list.
2. Click on the Proxy Tab.

Test Cases Sniffer Proxy DNP3 Proxy Fuzzer

Configuration Interceptor

Enable Proxy: ☐

Enable SSL: ☐

Proxy Address:

Proxy Port:

OK

Enable Filters

Type:

Match Rule:

Replace Text:

Add Remove Raise Priority Lower Priority

Type	Rule	Replacement
------	------	-------------

OK

Figure 13 - Proxy Configuration Options

3. In the Proxy address field, enter a proxy address of 0.0.0.0 on the tester laptop.
4. In these instructions the original port is “80” and proxy port is “8080”. If you are using a different original port, replace the original port “80” with the new original port, for example “8080”.
5. Enter the desired proxy port in the Proxy Port field.
 - 5.1. The chosen proxy port cannot be equal to the port you’re trying to intercept. In the instructions below modify the proxy port “8080” with the new port that you are using, for example “8081”.
6. Click the “Enable Proxy” radio button.
 - 6.1. If an error occurs, ensure that you have entered a valid IP address and that no other programs are utilizing the specified proxy port.
7. Select the test cases tab.
 - 7.1. Ensure that the IP tables rules are clear by running the “Flush IP Tables” test to flush all the IP tables before setting up IP table rules.

8. Select the test named “Redirect Ports”.
9. Click the properties button.
10. Make sure that the Original port is 80 and the Proxy port is 8080.
 - 10.1. If there is more than one field labeled Original port and Proxy port, enter the same value into the corresponding fields.
11. Click OK.
12. Click the Run button to forward the packets from port 80 to port 8080.
13. At this point the packets are being sent through the proxy on port 8080.
14. The user has a couple of options for performing different types of security tests.

Using the Filters

The filters are regular expressions that can be applied to various parts of an HTTP request or response (e.g., the header or the body). The filters can be used in this particular instance, to replace specific parts of an XML packet to test the robustness of an OpenADR protocol implementation.

In this case we will demonstrate how to replace the Price Field within an OpenADR packet.

1. The user selects the “Response Body” under the type combobox.
2. The user enters the following regular expression into the match rule field.
 - 2.1. `(?<=<ei:value>)([-+]?[0-9]*\.[0-9]+)(?=</ei:value>)`
3. This rule replaces any floating point number between the `<ei:value>` tags in an XML packet.
4. The user enters the replacement text in the replacement text field.
 - 4.1. 0.75 for example
5. The user clicks add to add the current rule to the filter chain.
6. The user clicks enable filters to begin filtering of the traffic.

In this case the user would observe the price change on the OpenADR client.

The user may chain multiple filters together to make more complex modifications. The filters are processed in the order in which they are displayed. They filters can be reordered using the raise and lower priority buttons.

Using the Interceptor

The interceptor can be used to selectively modify individual requests or responses, drop, or pass through packets through unmodified.

In order to use the Interceptor the user performs the following:

1. Click on the interceptor tab within the proxy tab.
2. Click on intercept enabled to turn on the interceptor.
3. Wait for a packet to arrive.

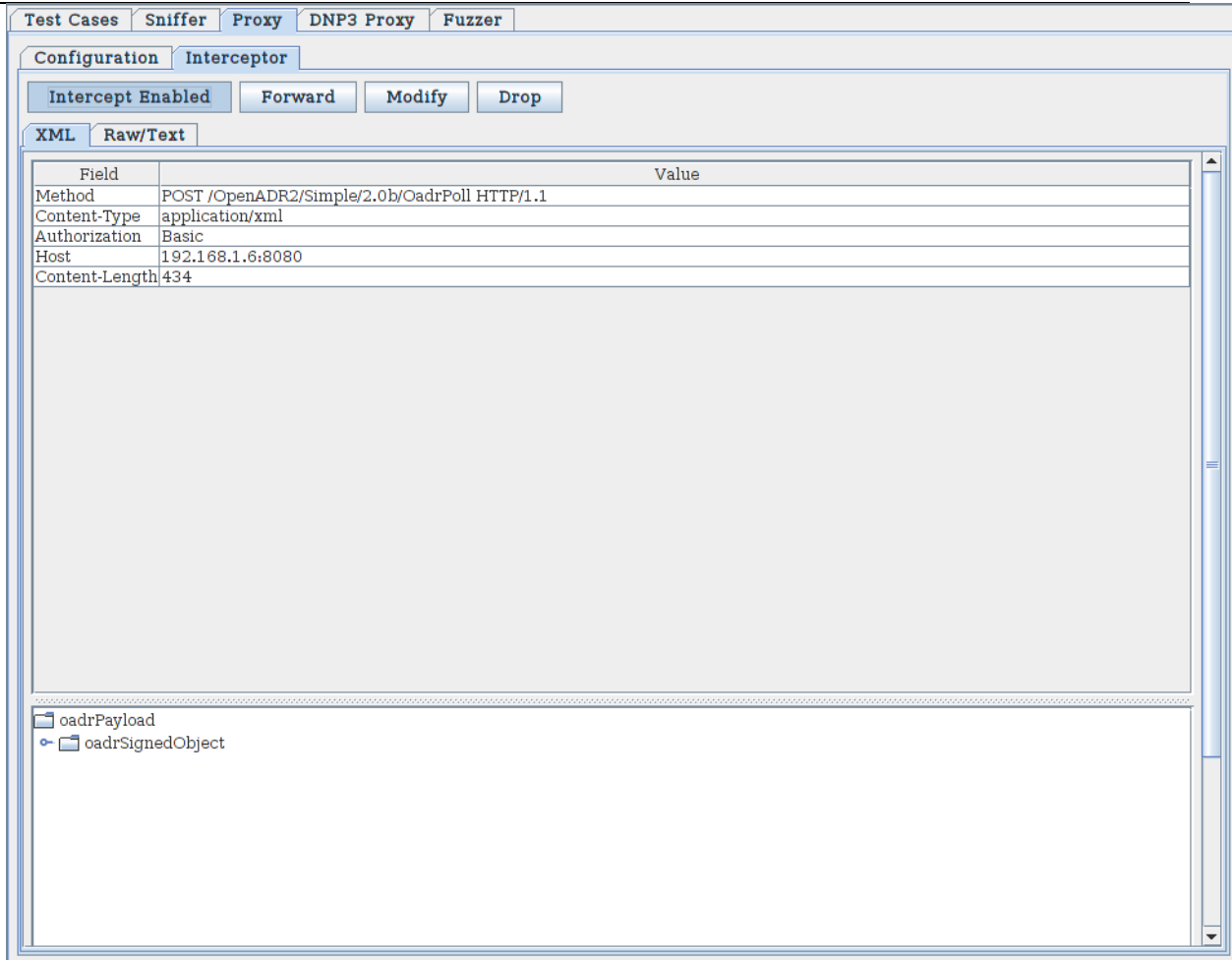


Figure 14 - Proxy Interceptor Panel

4. Once a packet arrives the user can edit the packet by double-clicking on the xml view and changing values or editing the packet in the raw/text view.
5. The user clicks modify to send the modified packet on.
 - 5.1. Optionally the user may click forward to forward the packet unmodified or drop to suppress the request or response.

Scenario 6: Using the Fuzzer

This section assumes that the user has successfully performed “Scenario 3: ARP Poisoning” and “Scenario 5: Using the Proxy”, and now wishes to fuzz packet requests and responses. Please note the tool does not support sending fuzz cases while the sniffer is still running. A third party tool such as Wireshark can be used externally to capture responses to fuzz cases.

1. The user begins in the Sniffer tab.
2. The user selects a packet to fuzz.
3. The user right-clicks on the packet and selects the “Send to Fuzzer” button.

Time	Type	SrcIP	DstIP	SrcMac	DstMac	Payload	
Sun Oct 1...	Request	/10.211.5...	/216.185...	00:1C:42:...	00:1C:42:...	GET /eios...	▲
Sun Oct 1...	Response	/10.211.5...	/216.185...	00:1C:42:...	00:1C:42:...	HTTP/1.1 ...	▼
Sun Oct 1...	Request	/10.211.5...	/216.185...	00:1C:42:...	00:1C:42:...	POST /eio...	▲
Sun Oct 1...	Response	/10.211.5...	/216.185...	00:1C:42:...	00:1C:42:...	HTTP/1.1 ...	▼
Sun Oct 1...	Request	/10.211.5...	/216.185...	00:1C:42:...	00:1C:42:...	POST /eio...	▲

Filter Expression:

Figure 15 - Sending Packet to Fuzzer

4. If the sniffer is still running the user must turn off the sniffer by clicking the Enable Sniffer button.
5. The user clicks on the Fuzzer tab.
6. If the packet the user selected is a “Request” type it will show up in the requests tab, otherwise it will show up in the response tab.

Requests

Responses

Time	Type	SrcIP	DstIP	SrcMac	DstMac	Payload	
Wed Oct ...	Request	10.211.5...	216.185....	00:1C:42:...	00:1C:42:...	POST /eios/OpenADR2/Simple/...	⬆

Remove

ID	Content	TestName	FuzzValue	DataType	Errors	
----	---------	----------	-----------	----------	--------	--

Select All

View Diff

Remove

Run Fuzzer

Figure 16 - Fuzzer Panel

7. The user selects and right-clicks on the packet and selects the “Fuzz Data” option.

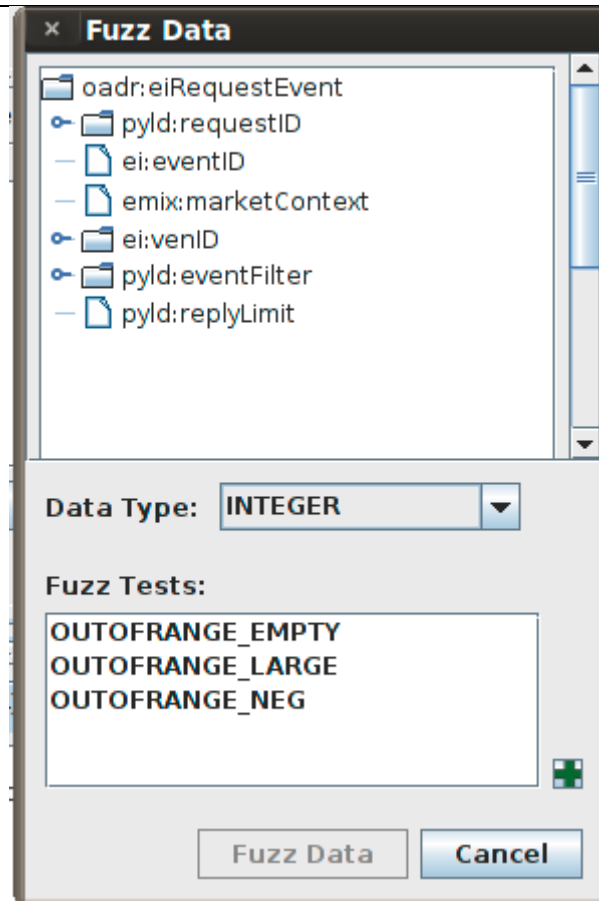


Figure 17 - Fuzzer Options Panel

8. The user expands the XML tree and selects one of the fields to fuzz.

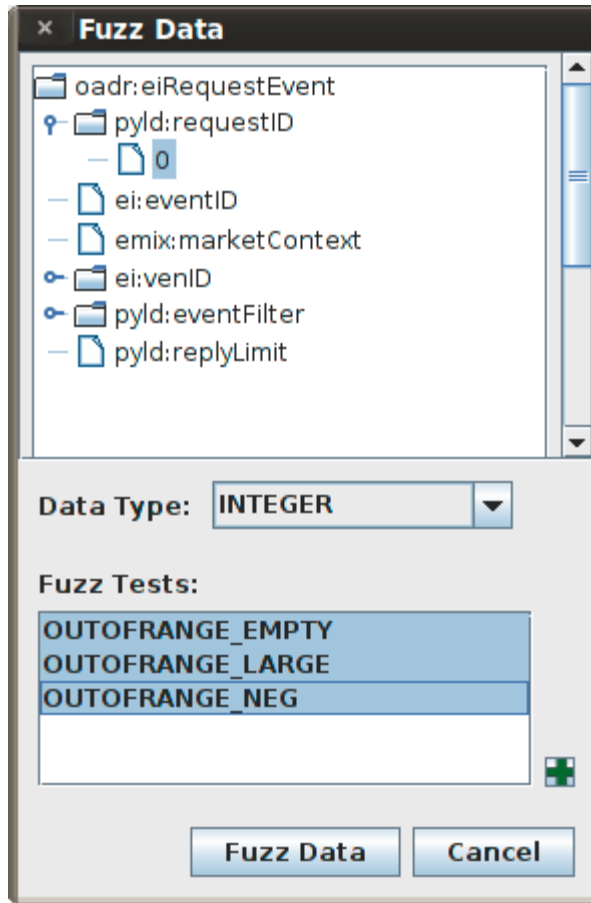


Figure 18 - Fuzzer Test Case Selection

9. The user selects one or more fuzz tests to run by holding CTRL and clicking multiple tests.
10. The user selects the “Fuzz Data” option.
11. The fuzzed packets now appear in the “Fuzz Packets” list.

Fuzz Packets:					
ID	Content	TestName	FuzzValue	DataType	Result
63	0	OUTOFRANGE_...		INTEGER	
63		OUTOFRANGE_...	777777777...	INTEGER	
63	77777777...	OUTOFRANGE_...	-1	INTEGER	
<div> <div>Select All</div> <div>View Diff</div> <div>Remove</div> <div>Run Fuzzer</div> </div>					

Figure 19 - Fuzz Packet Display

12. The user selects one or more fuzz packets to run.
13. The user clicks on the “Run Fuzzer” button to run the fuzz test.
14. The result is populated for the test.
 - 14.1. Please note that the proxy must be enabled and intercepting packets in order for the response packets to be fuzzed. The response fuzzing works by intercepting responses from the server to the client and modifying them before they are sent to the client.

Adding New Fuzz Test Cases

New fuzz test cases can be added in two ways:

1. In the fuzz dialog box click on the green “plus” arrow.

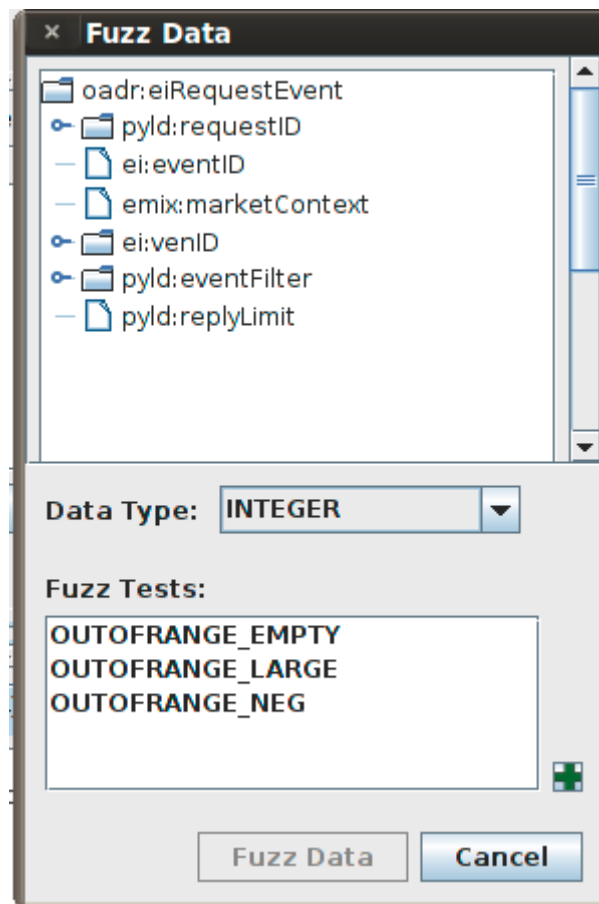
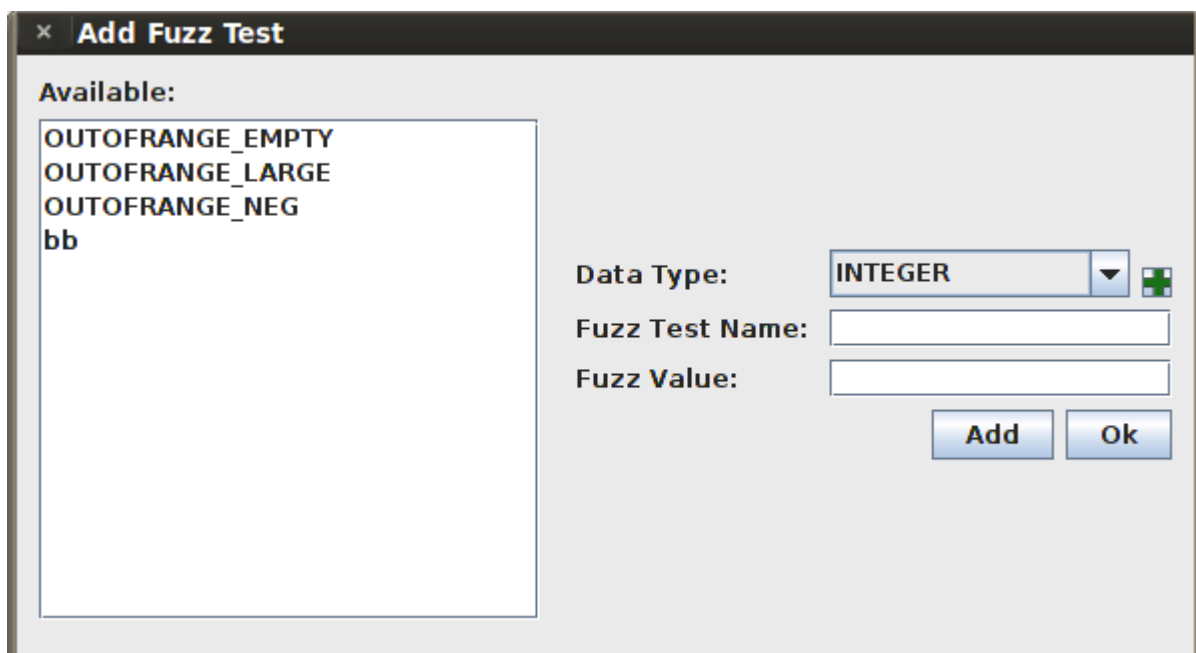


Figure 20 - Fuzzer Options Panel

2. From the file menu select add fuzz test.



The image shows a software dialog box titled "Add Fuzz Test". On the left, under the heading "Available:", there is a list box containing the text "OUTOFRANGE_EMPTY", "OUTOFRANGE_LARGE", "OUTOFRANGE_NEG", and "bb". To the right of the list box, there are three input fields: "Data Type:" with a dropdown menu currently showing "INTEGER" and a small green plus icon to its right; "Fuzz Test Name:" with an empty text box; and "Fuzz Value:" with an empty text box. At the bottom right of the dialog are two buttons labeled "Add" and "Ok".

Figure 21 - Add Fuzz Test Panel

3. The user can create new tests by specifying a data type, a test name, and a fuzz value.
4. These tests will be available to the user when they are running a new fuzz test.

5 TEST CASES FOR DNP3

In this section we will review some of the advanced features of the “Penetration Testing Toolkit” not covered in the previous sections. In general, highlighting over an item in the user interface should present the user with a description on how to use the item.

Scenario 1: Creating a Workspace and a Project

1. Launch the software.
2. You will be presented with the following screen:

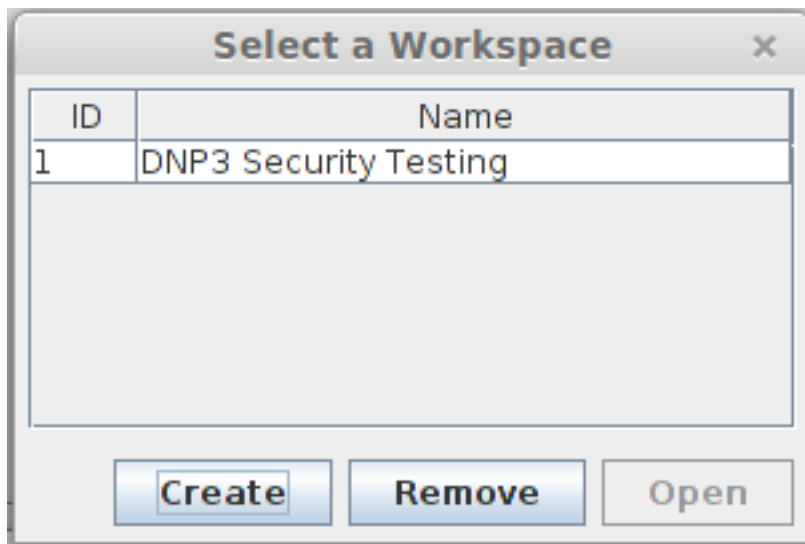


Figure 22 - Workspace Wizard

3. If this is the first time you are launching the software, the workspace list will be empty.
 - 3.1. Click the “Create” button to create a new workspace.
 - 3.2. You will be presented with a dialog to give a name to your workspace.
 - 3.3. Please give a meaningful name to your workspace that you will remember.
4. A workspace encompasses a set of projects which may be used to test different devices.
 - 4.1. An example of a name is “DNP3 Security Testing”.
5. Upon clicking OK, the workspace will appear in the list.
6. Select the workspace and click the “Open” button to open the workspace.
7. Upon opening the workspace you will be presented with the following screen.

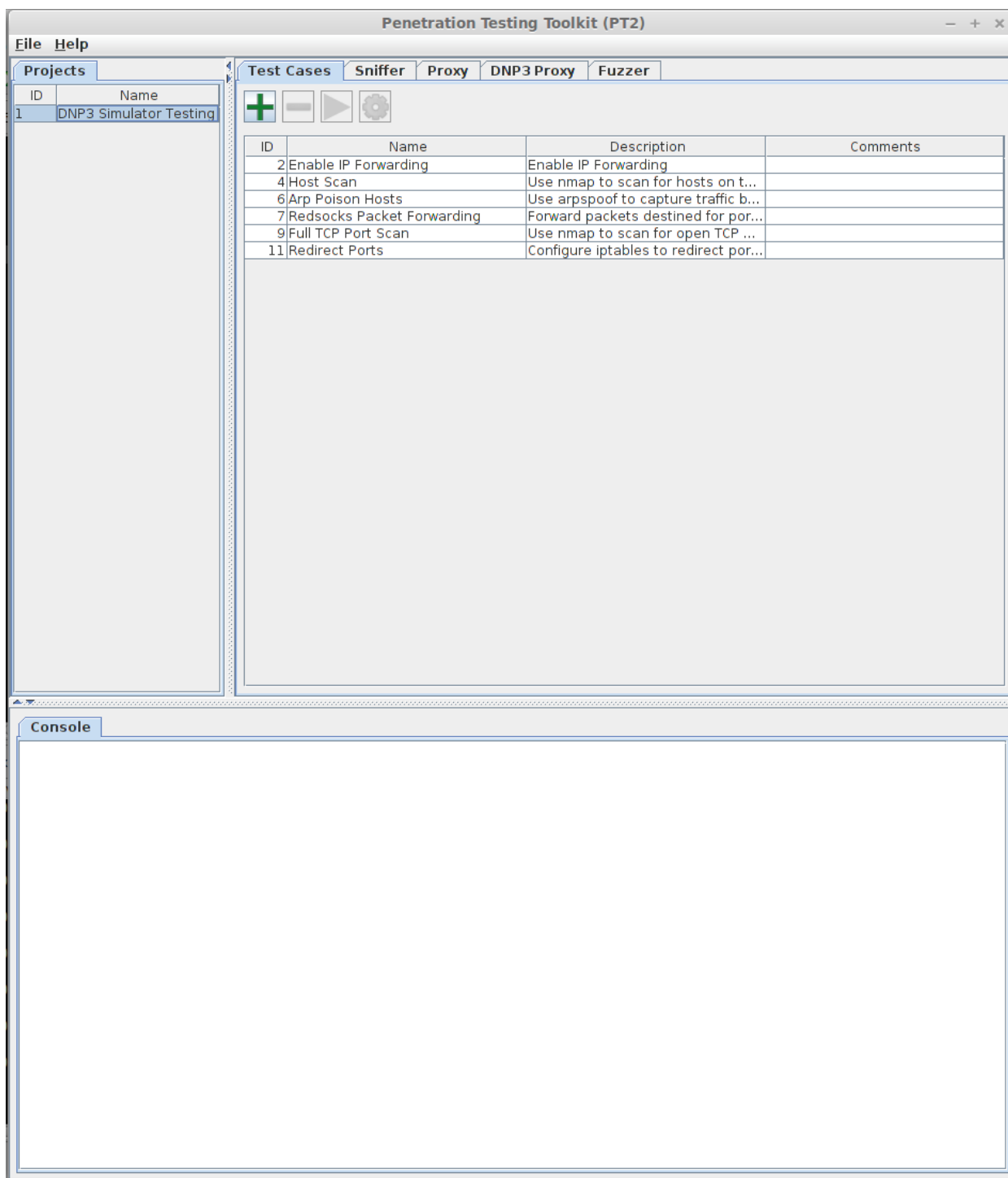
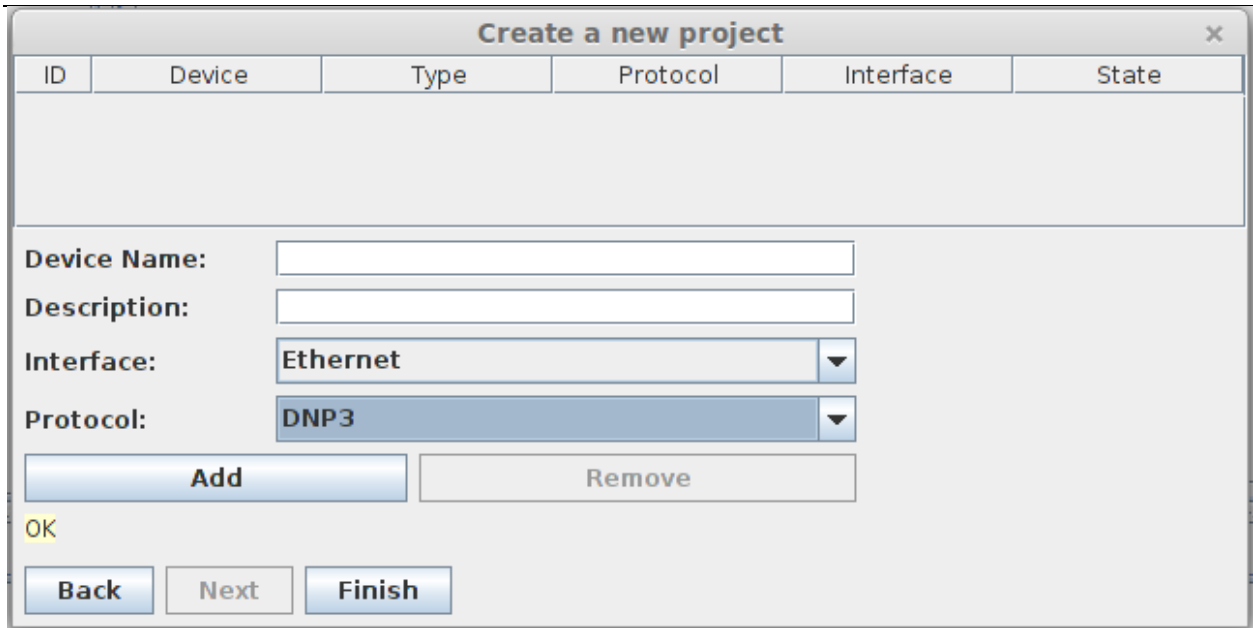


Figure 23 - Project Workspace View

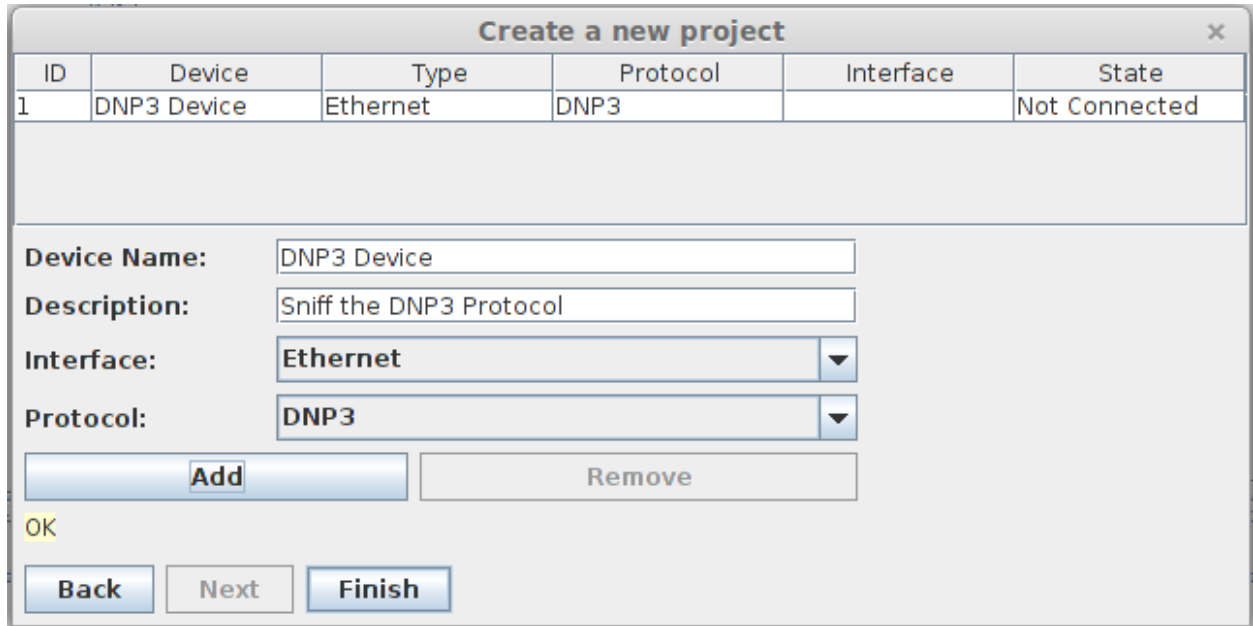
8. If this is the first time you are running the software, this screen may be empty.
9. To add a project to the workspace, from the “File” menu selected the “New Project” option.
10. You will be presented with the following dialog:



The dialog box titled "Create a new project" contains a table with the following headers: ID, Device, Type, Protocol, Interface, and State. Below the table are input fields for "Device Name:", "Description:", "Interface:" (with a dropdown menu showing "Ethernet"), and "Protocol:" (with a dropdown menu showing "DNP3"). There are "Add" and "Remove" buttons. At the bottom are "Back", "Next", and "Finish" buttons, along with an "OK" label.

Figure 24 - Create New Project Dialog

11. Please provide a meaningful name and description for your project and click next.
12. Upon clicking next, a new project will be added to the workspace.
13. The next step is to add a device, interface, and protocol to the project.



The dialog box titled "Add New Device" contains a table with the following headers: ID, Device, Type, Protocol, Interface, and State. The table has one row with the following values: 1, DNP3 Device, Ethernet, DNP3, Interface, and Not Connected. Below the table are input fields for "Device Name:" (containing "DNP3 Device"), "Description:" (containing "Sniff the DNP3 Protocol"), "Interface:" (with a dropdown menu showing "Ethernet"), and "Protocol:" (with a dropdown menu showing "DNP3"). There are "Add" and "Remove" buttons. At the bottom are "Back", "Next", and "Finish" buttons, along with an "OK" label.

Figure 25 - Add New Device Dialog

14. Please provide a device name and description, and the select the desired interface and protocol.
15. Click Add to add the device to your project.

16. Click Finish to exit the dialog.
17. If you now select the project, you will notice that the project has been populated with a list of default test cases.
18. The test cases are added based on the protocol that you selected.

Scenario 2: Host Discovery

This section assumes that the user has followed “Scenario 1” to create a new workspace and project. This section also assumes that the user is running a “Linux” operating system with the PT2 software started under a root user, and also that the user has network access to the device(s) they are evaluating.

1. Select the project from the project list panel on the left.
2. A set of default test cases will be populated in the GUI.
3. Select the test with the name “Host Scan” from the list of test cases.
4. Click the settings button “indicated by the gear symbol” above the list of test cases.

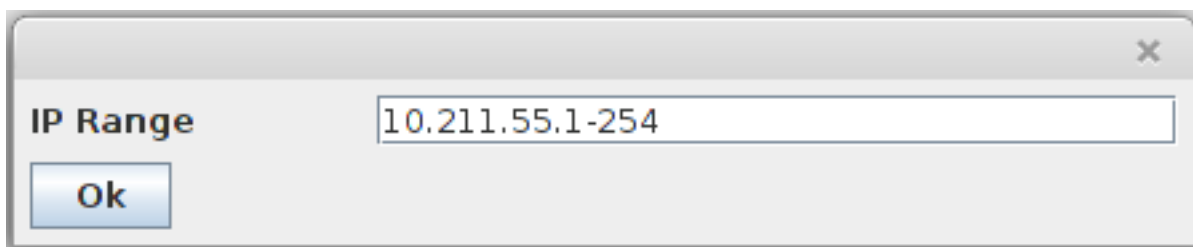


Figure 26 - Test Case Properties

5. Enter the IP range that is desired to be scanned.
6. Click the OK button.
7. Make sure the test case is selected and click the green run triangle.
8. The script will execute in a new window next to the console at the lower portion of the screen.

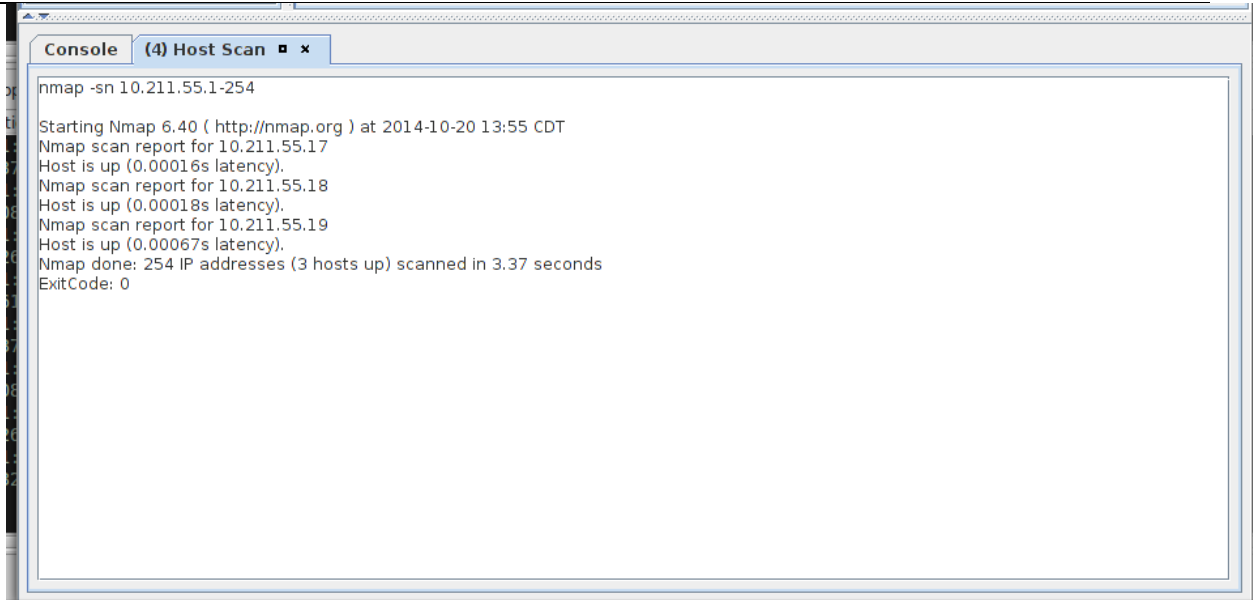


Figure 27 - Test Script Console

9. Please note that the console window displays the current test case ID in the tab, and the test script command and output in the text area below the tab.
10. Please take note of the hosts that have been detected.
11. Of particular interest are the IPs of the targeted device and the IP of the gateway device.
12. These can be found by correlating the MAC address to the discovered IP.

Locating the MAC address is out of scope for this manual. However, the device MAC address can typically be found on the device's label.

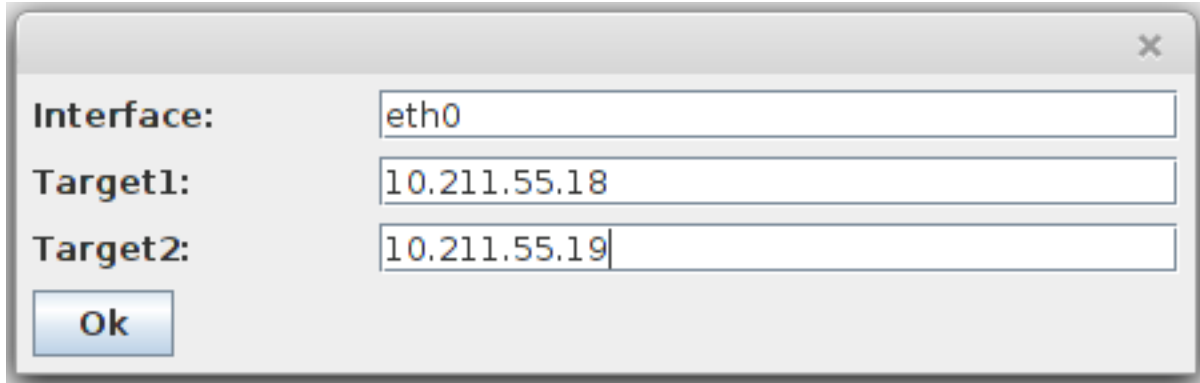
Scenario 3: ARP Poisoning

This section assumes that the user has followed Scenario 1 and Scenario 2 and has the following information available:

- IP Address of the Gateway or DNP3 Master
- IP Address of the Device

The user performs the following:

1. Select the test named "Arp Poison Hosts" from the test case list
2. Click on the gear icon to configure the test



A dialog box titled "Arp Poison Properties" with a close button (X) in the top right corner. It contains three input fields: "Interface:" with the value "eth0", "Target1:" with the value "10.211.55.18", and "Target2:" with the value "10.211.55.19". Below the input fields is an "Ok" button.

Figure 28 - Arp Poison Properties

3. If the Device and DNP3 Master are connected to the same physical network switch enter the IP address of the DNP3 Master in Target1 otherwise enter the IP address of the network gateway in Target1.
4. In Target 2 enter the IP address of the device.
5. Click OK to save the settings.
6. Click on the green run triangle to execute the test.
7. Please note that the test is now running and is available in the tab below the list of tests.

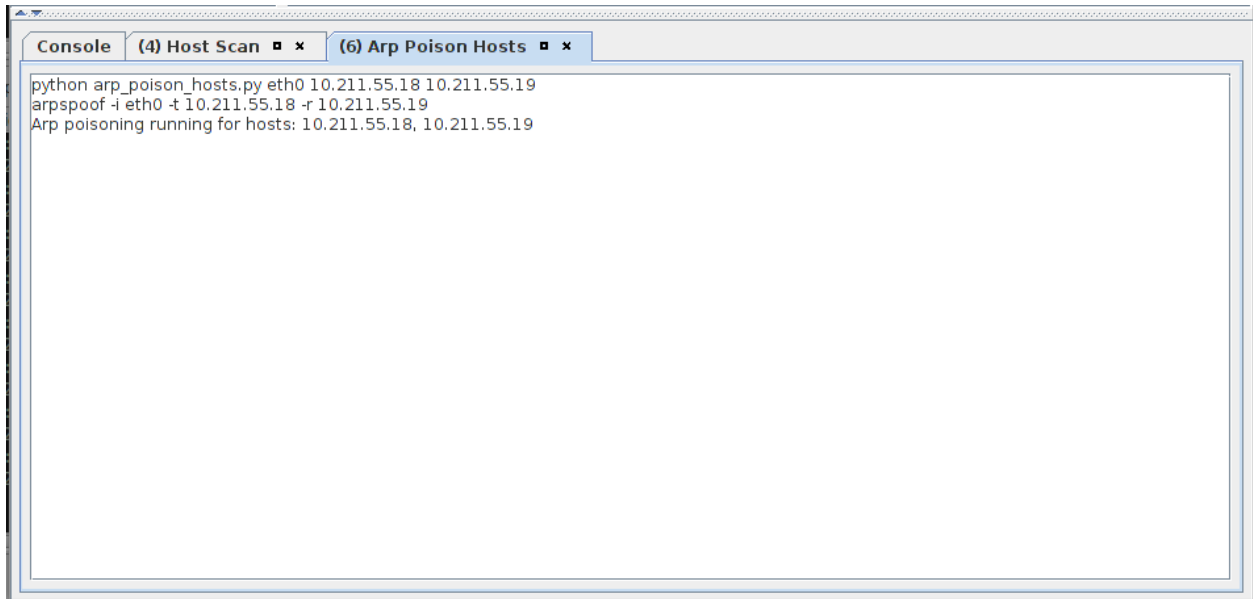


Figure 29 - Arp Poison Console

8. Since the ARP poisoning attack is an active test, the test will continue to run until the user stops the script. This can be accomplished by clicking on the square-shaped symbol next to the "X" in the tab, or exits the program.
 - 8.1. Please note that an Exit Code 0 or Exit Code 143 indicates that the script has successfully stopped.

9. The user must now enable IP forwarding to allow the packets to be forwarded to the remote host.
10. Select the test named “Enable IP Forwarding”.
11. Click on the green run arrow to execute the test.

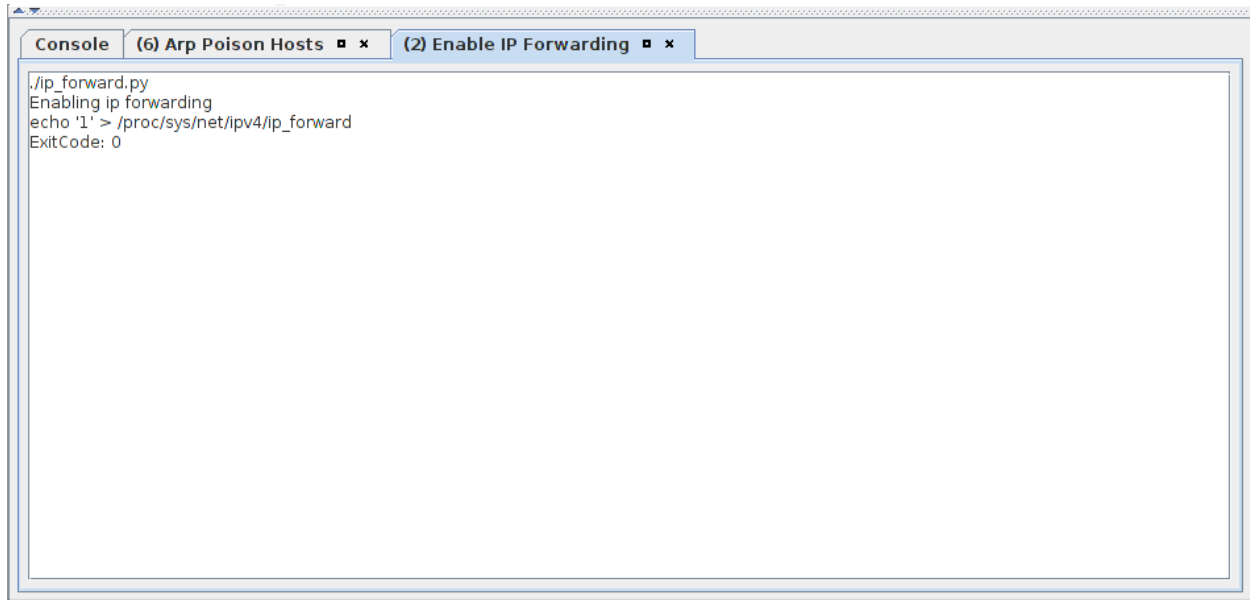


Figure 30 – IP Forwarding Console

Scenario 4: Traffic Sniffing

This section assumes that the user has successfully performed Scenario 3, ARP poisoning, and now wishes to view the sniffed packets.

The user performs the following:

1. Select the project from the project list.
2. Select the Sniffer Tab.
3. Click on the Options Panel.

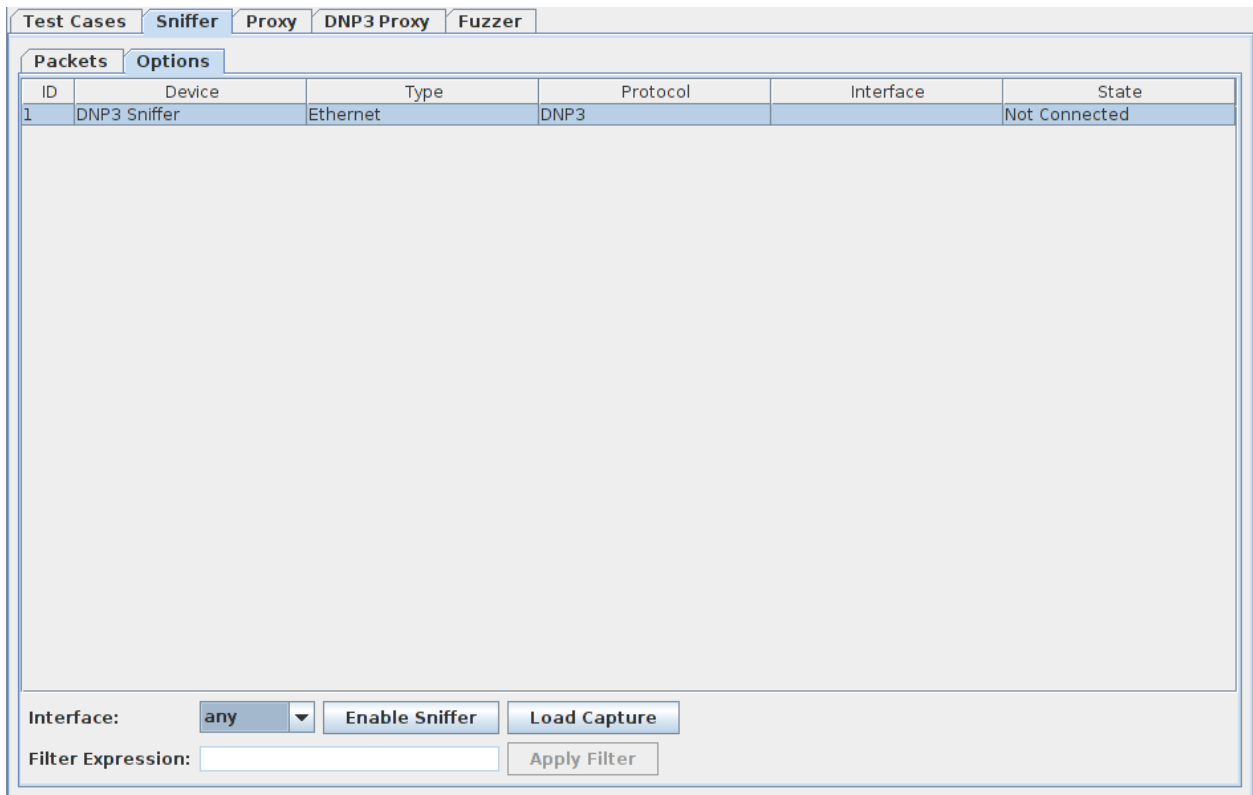


Figure 31 - Sniffer Options Panel

4. Select the physical interface from the dropdown list.
 - 4.1. Please note that this feature is supported only if you are running as an administrator or root user.
 - 4.1.1. On a Linux machine the Ethernet interface should be selected (e.g., eth0). Please note that using any interface aside from eth0 may cause the packet sniffer to not work correctly until the program is restarted.
5. Click the Enable Sniffer button.
6. Click on the Packets tab.
7. As packets are sent between the DNP3 Client and the Server, they will be captured in the Packets tab.

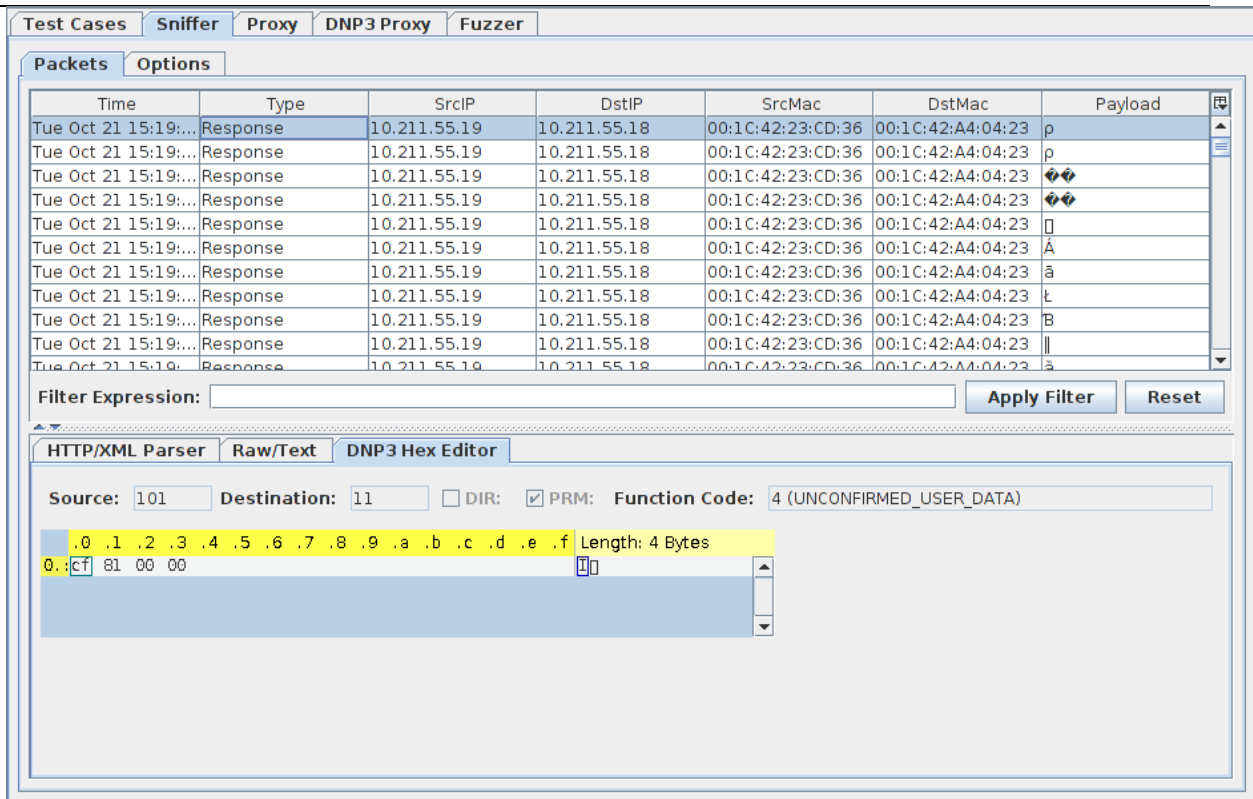


Figure 32 - Sniffer Packets

8. When you select a packet, the contents will be displayed in the analyzer panel.
9. The DNP3 Hex Editor view allows you to browse the DNP3 application packet content in a hex editor view.

Scenario 5: Using the DNP3 Proxy

This section assumes that the user has successfully performed Scenario 3, ARP poisoning, and now wishes to modify the intercepted packets. Please note, if the DNP3 Proxy does not immediately receive packets the tester can remedy the situation by disconnecting and reconnecting to the DNP3 client. If the DNP3 Proxy continues to not work correctly then this can be fixed by restarting the operating system.

The user performs the following:

1. Select the project from the project list.
2. Select the test cases tab.
3. Select the test named "Start Redsocks Packet Forwarding – DNP3".
4. Click the Run button to forward the packets from enable a socks proxy forwarder on port 12345 and forward packets from DNP3 port 20000 to the internal port 12345.
 - 4.1. The socks proxy forwarder encapsulates packets sent to it with a socks proxy header. It then forwards the packet to socks proxy on port 8081.

5. Click on the DNP3 Proxy Tab.

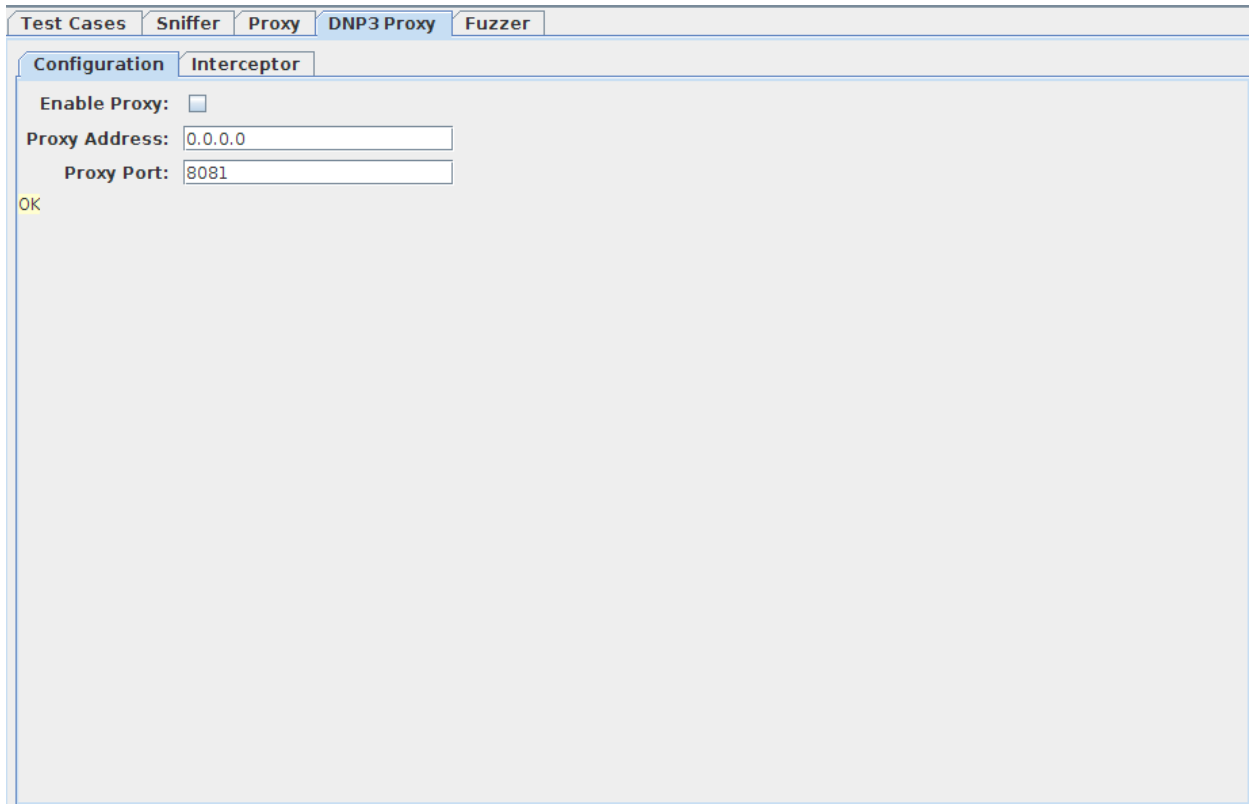


Figure 33 – DNP3 Proxy Options

6. Check Enable Proxy to enable the DNP3 proxy.
 - 6.1. If an error occurs, ensure that you have entered a valid IP address and that no other programs are utilizing the specified proxy port.

Using the Interceptor

The interceptor can be used to selectively modify individual requests or responses, drop, or pass through packets through unmodified.

In order to use the Interceptors the user performs the following:

6. Click on the interceptor tab within the DNP3 Proxy tab.
7. Click on “Intercept Enabled” to turn on the interceptor.
8. Wait for a packet to arrive.

6 ADVANCED USAGE

In this section we will review some of the advanced features of the “Penetration Testing Toolkit” not covered in the previous sections. In general, highlighting over an item in the user interface should present the user with a descriptive interface on how to use the item.

Removing the Database

The following data is automatically persisted in the database:

- Test Case Settings
- Captured Packets
- Created Test Cases
- Fuzz Test Cases
- Fuzz Test Results

To start from scratch and complete remove all information from the database, the database file must be deleted. The database file is located in the root directory of the software installation and is named “database.h2.db”. Delete this file to remove the database.

Removing Projects

Projects can be removed from the project list by right-clicking on a project and selecting the remove project button. Please note that this option is irreversible and that all test cases will be removed from the database.

Adding Test Cases

Test cases can be added to the graphical user interface in two ways, manually creating files and using the graphical user interface.

Manual Editing Files

Test cases added by manually creating files in the “scripts” directory of the software installation. If you look at the existing files you will notice that there are two types of files, XML and .py files.

The XML file describes the structure of a test case:

- Protocol
 - This field associates the test script with a particular protocol in the database. Projects, which are created with an interface supporting one of the protocols, will automatically be populated with the test script.
- Name
 - This field is a short describing of what the test script does.

- Description
 - This field describes in detail what the test script does.
- Parameters
 - Each test script contains 0 or more of these fields. Each of these fields has a set of parameters describing what the parameter is, any associated program flags, default values, and a tooltip hint.
- Command
 - This field points to the file to execute when the user runs this script.

The .PY file is the actual file that is executed. In general the .PY performs the tasks of launching third-party programs and reporting the results to the user.

In order to create a new script it is recommended that you copy these existing files and customize them to your particular need. This document does not go into detail on how to customize these scripts as the files are self-explanatory.

In order to load these new scripts, you will need to remove the database. Please see the advanced instructions for how to do this.

Adding and Removing Test Cases Using the GUI

Once a workspace and a project have been created and selected, the user can use the GUI to add and optionally remove a test case. To add a test case the user can click on the green plus arrow above the list of test cases. This adds a new line to the table. To edit the test case, the user will need to double-click on the line item they wish to change. To remove a test case, the user should click on the green minus arrow.

Please note that adding new scripts to a test case is not supported by the GUI method.

Removing all Packets from the Sniffer

Once in the sniffer pane, a user can remove the packets captured here. To do this, the user should right-click on a packet and then select “Clear all Packets”. This will remove all captured packets from the sniffer panel view.

Filtering Packets in the Sniffer Window

The user can apply regular expressions to the packets listed in the sniffer window in order to aid with testing. In order to do this, the user should enter the regular expression in the Filter Expression text field. For example the user may enter “Response” to show all response packets. Once the expression has been entered, the user should click the “Apply” button in order to apply the filter to the view. In order to remove any filters, the user should click the “Reset” button.

Customizing Columns in the Sniffer Window/Fuzzing Window

The user can customize the displayed columns by clicking the button in the upper right of the table.

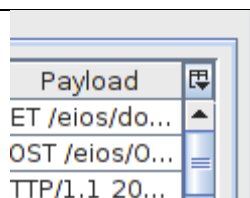


Figure 35 - Customize Columns

The user can choose the column to be displayed by checking or unchecking the respective radio button.

Controlling the Packets Captured by the Sniffer

Specifying a libpcap filter expression can control the packets captured by the sniffer. In order to do this, select the sniffer interface from the list in the Sniffer Options tab. Please note that the sniffer must be enabled in order to edit the filter. A default expression should appear in the filter expression textfield. This is the expression that is currently being used by the program. Enter a filter expression and click “Apply Filter” to apply the filter expression.

Please reference the following website on different filter expressions that can be applied:

<http://www.manpagez.com/man/7/pcap-filter/>

Loading a PCAP capture

Packet captures captured from a tool external to the Penetration Testing Toolkit can be loaded into the program. In order to do this it is recommended that the file be saved in a “libpcap” format. Please note that the default format provided by the “Wireshark” tool is not a compatible libpcap format.

Select the interface from the Sniffer Options tab. Click the “Load Capture” button to open a “browse for file” dialog. Select the capture file and click OK. Upon clicking OK, the packets will be loaded into the Sniffer Packets tab.

Enabling SSL Support in the Proxy

The proxy experimentally supports SSL. In order to enable SSL support the user should check the “Enable SSL” button in the Proxy tab. Please note that SSL support is currently experimental and has not been thoroughly tested as there were no SSL supported OpenADR clients at the time of development.

Uninstalling the Software

This software does not install any registry keys on the system and the only changes made are to the software installation directory.

The software persists data in a file named “database.h2.db” located in the root of the installation directory. In order to delete the persisted data (e.g., workspaces, projects, packets), the user would need to delete this directory.

Installation of EPRI Software at Client Site

EPRI develops software using a number of third party software products and tools that run on various operating systems and server platforms. Reports from the software industry suggest there are known security issues with some products and systems. EPRI recommends that, if you are using EPRI software, you review its use with your Information Technology (IT) department and their overall strategy to ensure that all recommended security updates and patches are installed as needed in your corporation. If you have any concerns please call the EPRI Customer Assistance Center (CAC) at 1-800-313-3774 (or email askepri@epri.com).

If you experience difficulties accessing the application

If you experience difficulties accessing the application after standard installation on Windows, please consult your IT department personnel to have proper access permissions setup for your use. If the problem can not be resolved, please call the EPRI Customer Assistance Center (CAC) at 1-800-313-3774 (or email askepri@epri.com).

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute Inc., (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent more than 90 percent of the electricity generated and delivered in the United States, and international participation extends to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together...Shaping the Future of Electricity