IDmachines

Eidola Tester Toolset and the EiDiagnostics

EiTester™

The ***EiTester™*** is, typically, an ARM or x86 device, currently, running Devuan Linux that supports the testing of networked devices and physical security infrastructure. The EiTester provides a wide range of device and system testing and infrastructure support capabilities. In addition to scanning, tracing, device configuration, device authentication, and public key infrastructure (PKI) tools. The EiTester also includes a number of infrastructure services, when in infrastructure mode, such as DNS, NTP, DHCP. The EiTester has all of the functionality of the Eidola ***EiWrench***™ included, with full support of the Open Supervised Device Protocol (OSDP) including conformance, configuration, integration, maintenance, testing, support and development of OSDP devices throughout their lifecycle. EiTester customers include end-users, system integrators and solution vendors[1]. The Eidola team remains involved in the further evolution and support of global standards for logical and physical security. In the case of OSDP, we run in partnership with the Security Industry Association, the OSDP Boot Camp for hands on training. This document refers to the user interface based functionality of an EiTester, for interacting directly with our application programming interface (API) please request API documentation and support from eidola@idmachines.com .

[1] The EiTester includes all the functional provided in the Eidola EiWrench plus the additional EiTester features.

IDmachines

EiTester Diagnostics and Tools

The EiTester consists of different tools and capabilities. These include:

Network and Infrastructure Diagnostics

Scan

The scan tool allows an NMAP scan of a network. The scan tool does not look to replace the scanning technology typically used in modern IT departments. It is targeted at physical security deployments and the ability to scan the physical security subnets that are of interest. The scan typically provides information on ports and services, their status, as well as the MAC address of the device and the company that registered the network interface. Preconfigured scan options exist as well as an ability to input customer commands. Scans, as well as any of the Eidola tools can also be drive via the Eidola Application Programming Interface (API).

SNMP

The Simple Network Monitoring Protocol diagnostic is used to gather detailed information about devices on the network. The information gathered is dependent upon the Management Information Base (MIB) structure and format of the manufacturer. The SNMP diagnostic gathers device information that can include manufacturer, make, model, firmware, last update, location, maintenance contact and other information.

TLS

The Transport Layer Security diagnostic performs an analysis of the whether devices that are using HTTPS are doing so in conformance with the standard for TLS 1.2. It checks the complete cipher suite that is used in the TLS protocol and captures the certificate used. The diagnostic provides an alarm if it does not find that TLS is being properly used and identifies the reasons.

Power Scanner

The Power Scanner diagnostic uses the SNMP to monitor and analyze the power consumption on the network monitored. The functionality is dependent on whether a network power supply is in use and conforms to the SNMP standard.

PKI

The EiTester PKI functionality comprises a set of tools to support the use of public key infrastructure (PKI) and digital certificates and their use with physical security systems. It includes the ability to stand up a test certificate authority (CA), to issue certificate revocation lists (CRLs), to generate key pairs on request, and to support PKCS-10 PEM Certificate requests, PKCS-12 certificate and key pair bundle, root certificates in PEM and DER formats. Additional PKI functionality can be crafted and IDmachines provides professional services and subject matter expertise for customers that require support beyond these tools.

IDmachines

One Button

The One Button diagnostic automates the analysis of a physical security network. It combines the Scan, SNMP and TLS functionality with a single click. After the Scan takes place the devices found on the network are then automatically used as devices under test (DUTs) for the SNMP and TLS diagnostics. The results are then generated in a variety of formats (txt, XML, JSON, CSV) and then available for further processing. The results include all data generated in the Scan, SNMP and TLS diagnostics.

Network Trace

The Network Trace diagnostic, as the name implies, performs a network trace, the default trace if for 2 minutes of the traffic on the network interface on the Eidola device. The diagnostic can be configured for other time periods and can be manually started and stops. This allows a field technician who may not have extensive network experience to gather a sample that could be sent to another location where a network engineer can perform an analysis.

Infrastructure Support

Eidola devices can run in either stand alone mode, where it is primarily a diagnostic tool as well as in infrastructure mode, where it provides network infrastructure capabilities. For example, a technician may arrive on a job site where the network supporting the physical security system is down and as a result it is not possible to perform network-based diagnostics. The infrastructure mode supports a wide range of network capabilities including DNS, NTP, DHCP, SNMP (Server), Wireless (SSID and Access Point and tunnel to Internet connections) in addition to the PKI capabilities. These capabilities can be selectively toggled as required via the user interface as well as through the API.

Physical Security Infrastructure

OSDP Monitor Dashboard acts as a monitor in the middle of an OSDP Access Control Unit (ACU) and a Peripheral Device (PD). As a diagnostic you and start and stop recording this communication, a display of the last 100 log lines is provided for the most recent snapshot of activity and well as the full captured results.

OSDP ACU starts an OSDP ACU server on the EiWrench that can then be used to exercise OSPD PDs. ACU start, stop, status, logging (including verbose), report, addressing and communication settings are available in the UI. The diagnostic includes a rich (more than two dozen) OPSD command set for interaction with PDs covering the protocol, commands and responses for PD conformance testing.

OSDP PD emulates a PD and much like the ACU tool it provides start, stop, status, logging, and CP conformance testing across protocol, commands and responses.

IDmachines

OSDP Inventory Checker provides the current build and configuration of OSDP devices, this is used to update documentation on current build and any (e.g. firmware) other updates. It provides a single way to gather configuration information across a wide range of manufacturers and devices.

OSDP File Transfer as the name implies allows the bidirectional communications and file transfer between the EiWrench and OSDP devices. It provides a means to perform firmware updates, maintenance access to OSDP devices and file management.

OSDP LED Exerciser allows testing of device LEDs with conforming OSPD commands. Green, Red, Blue, Amber supported. Set Green and Red and blink all.

OSDP Dashboard and Settings sets device configuration for address, poll timeout, timeout, com speed, verbosity, FQDN, network address. Transfers settings to Conformance Checking in OSDP ACU and OSDP PD.

Digital I/O Dashboard allows toggling of input and output bits based on OSDP commands. Supports 8 bits of I/O. Has a plug-in for I/O modules.

Infrastructure Health Check performs a check of the local network for further evaluation.

Power Scanner provides an SNMP (Simple Network Monitoring Protocol) query of a power supply management information base. Stores, measures, monitors and reports on supplies that are part of the physical security system that support SNMP.

EiWrench customers have access to Eidola support including knowledge base, discounts on training and other IDmachines services. If you have any questions or needs, please contact us through eidola@idmachines.com