Inquiry

onward SECURITY

HERCULES SecDevice

Automated Vulnerability Assessment Tool

HERCULES SecDevice is an automated security assessment tool designed for connected products. It is equipped with functions such as vulnerability testing, fuzz testing, and web security testing. Adopting our patented AI machine learning technology, it accelerates the time and accuracy of vulnerability discovery. The assessments cover IEC 62443, OWASP TOP 10, CWE / SANS TOP 25, and more.

Features

- **Designed for IoT product security:**
  It is designed for the security testing of connected products. It can automatically analyze and test the security of the targeted equipment through the internet or wireless network connections. Simultaneously, it supports automatic continuous testing and reduces labor processing time.
- **Diversified vulnerability testing techniques:**
  Utilizing fuzz testing, network vulnerability scanning, web vulnerability scanning, and DOS testing techniques, it can discover known and unknown vulnerabilities, including operating systems, network applications, network protocols, web pages, wireless security vulnerabilities, and more.
- **TCF intelligent discovery technology:**
  AI technology is used to learn network packets to assist testers to discover the vulnerabilities of various proprietary network protocols, and improve the coverage and integrity of the discovery.
- **Comprehensive test records:**
  The attack packets and test methods in the discovery process can be recorded. SecDevice provides clear reasons for the vulnerabilities and relevant supporting data to help the user quickly review the product security issues.

Easier	Integrated	Higher Coverage
Start a scan within three steps	Support major security testing in one tool	120+ test items and patented methods

Step1. **Select test item** Step2. **Choose test target** Step3. **Start testing**	• Automatic port identification • Known vulnerability testing • Web security testing • Fuzzing • Wireless network testing • Exploit	• System layer vulnerability • Network layer vulnerabilities • Protocol layer vulnerability • Web layer vulnerabilities • Wireless layer vulnerability

Benefits

- **Reduce labor and tool costs:**
  It can save the training time of security personnel and reduce the costs of purchasing multiple sets of tools.
- **Reduce professional dependence:**
  Simple operation design makes testers easily to use, and through detailed test records, effectively help developers solve problems.
- **Improve the integrity of product security testing:**
  Patented AI machine learning technology can support the discovery of customized protocol security and make up for the shortcomings of traditional security testing methods.

Awards

Facebook Linkedin Twitter Contact us

Specifications

SecDevice uses known and unknown vulnerability discovery technology to test connected devices for as follows:

Network Security	Based on the addressing technology of IPv4 or IPv6, the security test packet is sent to the target through the network. The test scope covers the operating systems and application programs of the tested devices.
Web Security	Based on the test target defined by the URL, aim at the web-based operating interfaces provided by most connected devices, and check the security of web applications.
Wireless Security	Based on the service set identifier (SSID) to define the test target, aim at wireless connection services provided by the equipment to analyze if any vulnerabilities existing.

Supported Protocols

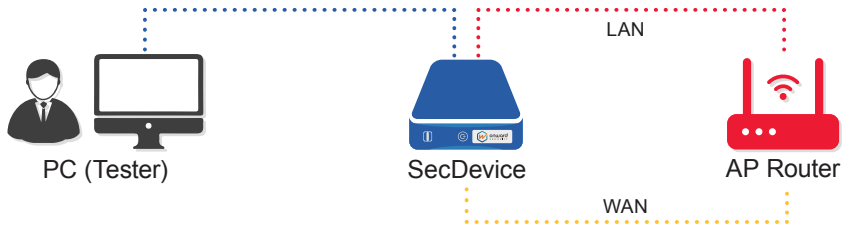
Core Network	ARP, ETHERNET, ICMP(v4/v6), IGMPv3, IP(v4/v6), TCP(v4/v6), UDP(v4/v6)
IIoT	BACnet, CoAP, DNP3, EtherNet / IP, FINS, S7omm, IEC 60870-5-104, IEC 61850(Goose/MMS/Sampled Value), Modbus, OPC UA, ProfitNet
Network Management	CWMP, DHCP(v4/v6), DNS, LDAPv3, NTP, OCSP, PPTP, SIP, SNMP(v1/v2/v3/trap), SSHv2, TFTP, Telnet, TLS 1.2, UPnP, IPsec, RADIUS, IKEv2, IPMI, NFSv4, VLAN, FTP, BGP, BFD

File System	CIFS/SMB
Web Application	HTTP, WEB Fuzz(Including XML and JSON format)
VoIP/IMS	RTP, RTCP, RTSP
Wireless	802.11 WLAN Client / AP 802.11 WPA Client / AP

Applications

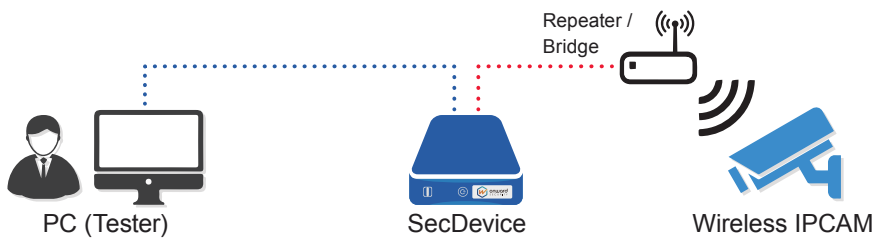
The connected devices with a single network connection interface

e.g. IIoT equipment or medical devices



The connected devices with 2 network connection interfaces

e.g. network devices



The connected devices with wireless networks

e.g. surveillance systems