Q-Vul®

The **Q-Vul**® is a vulnerability testing and reporting network appliance built using **OpenVAS** (Open Vulnerability Assessment System). **OpenVAS**, previously called GNessUs, began as a fork from the Nessus® vulnerability scanning tool after Tenable Security removed its Nessus® open source version in 2004.

OpenVAS has evolved since then both with respect to its scanning engine, and the vulnerabilities it can find and identify. Currently, it can find and identify more than 47,000 security vulnerabilities in a variety of operating systems, including Windows, IOS, and Linux. The **Q-Vul** also can identify vulnerabilities in various network appliances, including routers, smart switches, and IoT devices.

The **Q-VUL** network appliance automatically updates **OpenVAS**'s **Network Vulnerability Tests** (**NVT**s) using the **OpenVAS** NVT Feed. The **OpenVAS** NVT Feed is updated at least weekly as fresh vulnerabilities are found. In addition to using the public NVT feed, users can add private NVTs.

The **Q-VUL** network appliance is intended to be placed on a network and run scans either after the release of new NVTs or upon the introduction of new hardware or software. Scans can be scheduled as frequently as desired. We recommend automated nightly scans in addition to scanning after **NVT** updates.

Q-VUL Hardware Specifications:

- 108 mm x 64 mm x 26 mm – 170 grams
  (4.25" x 2.50" x 1.125" – 6 oz)
- Power consumption under full load:
  8 watts, 120v-240v
- No fan or any moving parts. Must be installed in a well-ventilated space.
- Operates 0°C–70°C (32°F–158°F)

LED indicators:

- Power
- Link (physical connection to network)
- Activity (network traffic)
- 1000 mbps (gigabit) NIC connection
- Dual Band WiFi. (2.4 GHz & 5 GHz)

Contact: Richard Avery
646-449-7820
q-vul@quantalytics.com

Quantalytics. In-depth network defenses.

Quantalytics

Q-Vul®

The **Q-VUL** network appliance includes:

- **OpenVAS – OpenVAS** is the leading open source enterprise-class vulnerability testing and reporting package for software and hardware, including IoT devices. **OpenVAS** includes automated updating of the Network Vulnerability Tests (NVTs) as well as the ability to schedule scans. **OpenVAS** also includes comprehensive reports.

- **ModSecurity® – ModSecurity®** ("**ModSec"**) is is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. We have hardened the **Q-Vul's** built-in Apache web server to prevent conceivable attacks.

- **Webmin – Webmin** is leading open source Web GUI package for server configuration and maintenance. **Webmin** also allows for the linkage of multiple **Q-Vul** appliances for simplified administration.

- **HA Proxy** – **HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-VUL** network appliances may be linked for automatic failover or load balancing for coverage of extremely large networks. Administration is done through a web gui.

- **Tiny Honeypot (THP). THP** fools attackers by making it appear that the attack is working, while meanwhile logging the attack info. **THP** wastes an attacker's time, and creates an opportunity to detect the network intrusion by offering to the attacker what appears to be thousands of services.

- **ClamAV®** – **ClamAV®** is the leading open source anti-virus package.

The **Q-VUL** network appliance is completely administered through a Web GUI. This makes all features easily available even to novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

The **Q-VUL** network appliance has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.) Vulnerability scanning can be set up on either network interface.

Contact: Richard Avery
646-449-7820
q-vul@quantalytics.com

Quantalytics. In-depth network defenses.

The **Q-Vul** is also available as a Virtual Machine (VM).

Using the provided **Webmin** module, two-factor authentication can be added using **Google Authenticator** or **Authy**, a commercial service with its own app. **Google Authenticator** runs on Android, IOS, and Blackberry devices, and uses the standard TOTP protocol.

Notifications are provided by e-mail using **SendMail**, which is configured with a module in **Webmin**, and syslog entries. The **Q-Vul** network appliance can be integrated with **Nagios®** on the **Q-Box®** as another notification route. SMS notification is available as an option. The **Q-Vul** network appliance can also be integrated with the **Q-Log®** network appliance or any other Syslog or SIEM (Security Information and Event Management) solution.

Contact: Richard Avery
646-449-7820
q-vul@quantalytics.com