Quantalytics

Q-ConPot®

The **Q-ConPot**® (Control System Honeypot) network appliance is an ICS and SCADA honeypot. Network honeypots provide network obfuscation (hiding in plain sight) and denies the hacker easy network reconnaissance, while greatly increasing the likelihood of detecting a network breach. The **Q-ConPot** uses **Conpot**, an open source software package that has a wide range of built-in industrial protocols so that administrators can create attack surfaces that mimic their actual environment, or portray a very complex and fictional infrastructure. This enables administrators to create network obfuscation and deception, thereby denying hackers an accurate map of the network and its machines, as well as increasing the likelihood of the network breach being caught by an Intrusion Detection System (IDS) such as the **Q-Box**® or by the **Q-ConPot** itself. **The number of deployed decoy attack surfaces is limited only by the number of available LAN IP addresses.**

In order to increase the deception capabilities of **Conpot**, the administrator can create in the **Q-Conpot** custom Human-Machine Interfaces (HMIs), thereby increasing the number and type of attack surfaces. The response time of the attack surfaces can also be tweaked for various delay times so as to mimic the behavior of an industrial system under constant load. **Conpot** can be accessed using production Human-Machine Interfaces (HMIs) or via a web interface.

Also included are **Xplico**, an open source, enterprise class full packet capture, indexing, and database system so that in the event of an alert, administrators can immediately capture packets for forensic analysis, and **HoneyBadger**, which gives administrators using the **Q-ConPot**, unlike other honeypot systems, the ability to fight back by identifying the attacker's location via geolocating the attacker's IP address(es), as well as prevent TCP injection attacks, including 0-day (Zero Day) attacks.

Contact: Richard Avery
646-449-7810
Q-ConPot@quantalytics.com

Quantalytics. In-depth network defenses.

Quantalytics

Q-ConPot®

Q-ConPot 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)

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

- **Conpot - Conpot** is an open source, host-based, honeypot system designed to provide network obfuscation and deception on ICS and SCADA machine networks. **Conpot** allows the administrator to create attack surfaces that mirror the actual production environment, as well as additional attack surfaces to as to create a maze of faux equipment ("attack surfaces") that the hacker must navigate. This takes time and greatly increase the risk of the hacker being discovered before industrial equipment is compromised.

- **Xplico – Xplico** is a leading open source package for real time network packet capture and forensic analysis. In the event of suspicious activity, network administrators can capture and examine in depth real-time traffic for deeper analysis of suspicious network traffic. In addition to packet inspection, Xplico allows for reconstruction of the actual traffic. E.G. Data, e-mails, texts, IM's, pictures, etc.

- **HoneyBadger – HoneyBadger** is an open source, comprehensive TCP stream analysis tool for detecting and recording TCP attacks. **HoneyBadger** combines a variety of TCP stream injection attacks to help insure that the TCP attack identification is reliable, and not a false positive. **HoneyBadger** includes geolocation to pinpoint the attacker(s) physical location.

- **Webmin - Webmin** is used for network appliance housekeeping and network configuration. **Webmin** also allows for the linkage of multiple **Q-Conpot** appliances for simplified administration.

Contact: Richard Avery
646-449-7810
Q-ConPot@quantalytics.com

Quantalytics. In-depth network defenses.

- **HA Proxy – HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-Conpot** network appliances may be linked for automatic failover or load balancing for coverage of extremely large networks. Administration is done through a web gui. **The number of deployed attack surfaces is limited only the number of available LAN IP addresses.**
- **ModSecurity® – ModSecurity®** (**ModSec**) is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. We have hardened the **Q-ConPot's** built-in Apache web server to prevent conceivable attacks.
- **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-ConPot** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.).

The **Q-ConPot** network appliance is also available as a Virtual Machine (VM).

The **Q-ConPot** network appliance is completely administered through a Web GUI. All package usage is via Web interface, thereby opening up sophisticated intrusion detection, network forensic analysis, and network monitoring to even novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

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-ConPot** network appliance can be integrated with **Nagios®** on the **Q-Box®** as another notification route. SMS notification is available as an option. The **Q-ConPot** network appliance can also be integrated with the **Q-Log®** network appliance or any other Syslog or SIEM (Security Information and Event Management) solution.

Q-ConPot® and all registered trademarks above are property of their respective owner(s).