Quantalytics

Q-GridPot®

The **Q-GridPot**® (Grid System Honeypot) network appliance is a specialized, low impact honeypot appliance specifically for electric power grids using ICS and SCADA. 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-GridPot** uses **GridPot**, an open source software package that has built-in IEC 61850 protocols for imitating large scale electric power grids. This allows administrators to create attack surfaces that mimic their actual power grid environment, or portray a very complex and fictional power grid infrastructure. This, in turn, 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-GridPot** 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 **GridPot**, the administrator can create in the **Q-GridPot** 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 electric power grid under variable load. **GridPot** can be accessed using production Human-Machine Interfaces (HMIs) or via a web interface.

Also included is **ntop-ng**, an open source, enterprise class full packet capture, indexing, and forensics package. In the event of an alert, administrators can immediately capture packets for forensic analysis; plus **HoneyBadger**, which gives administrators using the **Q-GridPot**, 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.

Q-GridPot 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: 12 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
+1 646-449-7810
Q-GridPot@quantalytics.com

Quantalytics. In-depth network defenses.

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

GridPot - GridPot is an open source, host-based, low impact honeypot system designed to provide network obfuscation and deception for electric power grid ICS and SCADA machine networks. **GridPot** uses **ConPot** as its underlying framework, and deploys IEC 61850 additions to emulate real-world electric power grids.

- **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 so 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.

- **mtop-ng – ntop-ng** ("**ntop next generation**") is the latest iteration of ntop, which is used to probe all network traffic. Some of its features include showing realtime network traffic and hosts; create long term reports for network throughput, application and application protocols; monitor and report live throughput, network and application latencies, RTT, and full TCP stats; discover application protocols (e.g. Facebook, BitTorrent, etc.) by leveraging nDPI (ntop Deep Packet Inspection); characterize HTTP traffic using characterization services provided by Google and HPPT Blacklist; provide geolocation mapping of hosts; sort all network traffic via criteria including IP address, port, L7 protocol, throughput, Autonomous Systems (ASs); analyze IP traffic and sort by source and destination; IPv6 support; full Layer 2 support, including ARP stats; and an alerts engine to capture anomalous and suspicious hosts.

- **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-GridPot** appliances for simplified administration.

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

- **ModSecurity® – ModSecurity®** (**ModSec**) is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. We have hardened the **Q-GridPot**'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-GridPot** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.).

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

The **Q-GridPot** 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-GridPot** network appliance can be integrated with **Nagios®** on the **Q-Box®** as another notification route. SMS notification is available as an option. The **Q-GridPot** 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-GridPot® and all registered trademarks above are property of their respective owner(s).