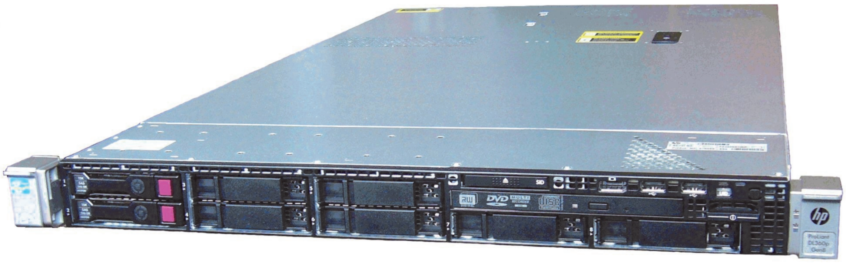
honeyBox®

enterprise

Attack Detection and Alarm



- reliable detection of attackers in the network
- rapid detection of worm outbreaks
- virtually no false alarms (false positives)
- each appliance can monitor up to 80 subnets
- simple integration into the network
- no changes required to the network infrastructure
- VLAN support (802.1q)
- no effect on the (high) availability of the network
- very low operating costs

Background

Companies need reliable data on the security status of their networks. IDS/IPS cannot provide network-wide coverage, but with honeypots, unauthorized access can be detected anywhere in the network. Attempted attacks are logged centrally and alerts can be transmitted.

Solution

secXtreme has developed the honeyBox® Honeypot Appliance specifically to deal with this threat, covering the requirement at low cost. When appropriately configured, the appliance delivers substantial benefits in terms of security, implementation time, investment and operating costs.

The honeyBox® Honeypot Appliance is based on the Generic Software Security Appliance from secXtreme and contains all the functions of that system, enabling secure out-of-the-box operation suitable for a computer centre.

OPERATIONAL SCENARIOS

Monitoring your LAN for attackers

Scenario: Your LAN is not monitored end-to-end, yet attacks on your internal systems could cause serious damage.
Implementation: As a solution dedicated to the detection of internal attacks, honeypot appliances can provide you with rapid protection without any need to change the network structure.
Result: The ability to detect and to record attacks keeps you constantly updated as to whether any attackers are at work in your network. You can then initiate any measures necessary to block and analyze the attack.

Additional monitoring of your DMZs

Scenario: You use IPS in your DMZs to protect your systems, but once an attacker has taken over one of the DMZ systems, the IPS can no longer detect and prevent the attack from spreading within the DMZ.
Implementation: You install a honeypot appliance and patch its sensor interfaces into the individual DMZ systems. As soon as the virtual honeypots are attacked, you can initiate countermeasures.
Result: substantial improvement in the security and availability of your DMZ systems

secXTREME
Information Security

FUNCTIONS

Honeypot

- 4 interfaces
- Up to 80 VLANs
- Up to 500 virtual honeypots for each VLAN possible
- 40+ honeypot templates
- 19+ special services
- Network data recorder

Security

- Hardened Debian Linux
- SSHv2
- HTTPS (local CA)
- File system integrity checks
- Security baselining
- Local firewall
- Digitally signed software

Management

- Web GUI monitoring
- Setup using KVM, SSHv2 or serial connection
- Alert system (e-mail, pager, syslog, database, log files)
- Backup/restore/recovery
- Watchdog
- Hardware monitoring

Installation

- USB stick (recovery of hardware appliance)

Integration

- Secure updates over the internet
- NTPv3 time synchronisation
- E-mail
- Syslog (CSV and CEF)

Support

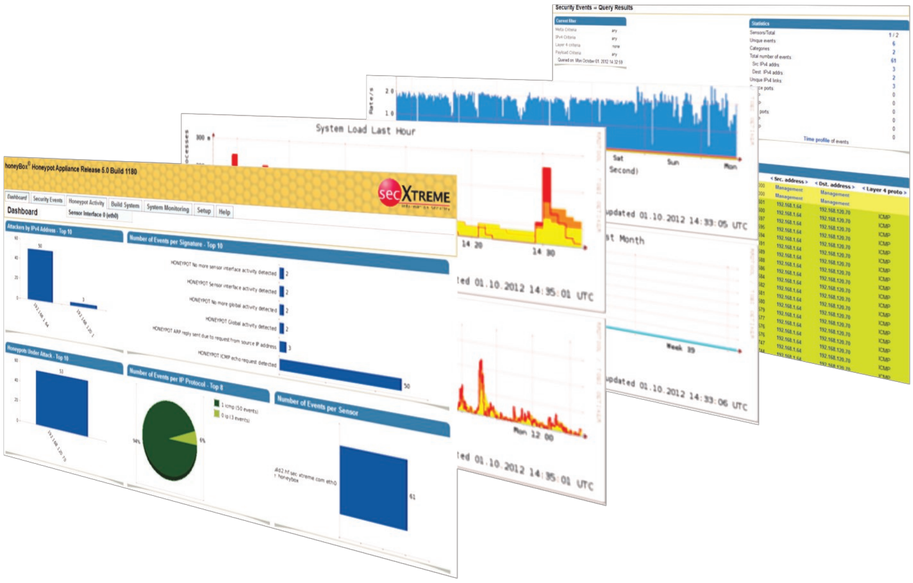
- 5x8 telephone and e-mail service

Hardware exchange

- NBD exchange or warranty extension for up to 5 years

Functions and Characteristics

The honeyBox® enterprise appliance can operate as a stand-alone solution. Alerts are collected in the central repository and analyzed via browser over a secure HTTPS connection. For larger installations, it is recommended that a dedicated high-performance server is used for the management server function. This one will work with the Appliances which take over the functions of a sensor. A variety of criteria can be used for evaluation, allowing investigation through selective drill-down.


honeyBox® Honeypot Appliance Release 5.0 Build 1180
secXTREME
Dashboard
System Load Last Hour
Security Events » Query Results
Statistics

Hardware	
CPU	Intel Xeon E5-2620 6-Core / 2,0 GHz
RAM	8 GB Registered DIMMs PC3-10600R
Network	4 x 1 Gbit copper (Fiber 1 Gbit or 10 Gbit opt.)
USB	7 x USB 2.0
Storage	2 x 146 GB, 6G SAS, 15 000 RPM (RAID 1)
RS232	1 x serial DB9
Power Supply	2 x 100-240 VAC, 50-60 HZ, 4,5 - 2,2 A
Power Consumption (typ.)	160 Watt typ., 750 Watt max.
Operating Temp.	+10 to +35 °C,
Humidity	10 % - 90 %, non condensing
Housing Size	434,7 mm x 43,2 mm x 698,5 mm (WxHxD)
Certifications	CISPR 22, EN55022, EN55024, FCC u. a.

Awards for the honeyBox® appliance family

2. Platz
INNOVATIONSPREIS-IT 2010 initiative mittelstand QUALIFIZIERT
INNOVATIONSPREIS-IT BEST OF 2013 initiative mittelstand IT-SECURITY
TOP 2011 IT-Lösung
ITBestenliste.de

QUALIFIZIERT initiative mittelstand 2009 INNOVATIONSPREIS-IT

secXTREME Information Security

About secXtreme GmbH: secXtreme GmbH is a company that specialises in information security. This includes audits, penetration testing, security analyses and training courses. In addition to these areas, secXtreme develops special solutions for the security environment. secXtreme is a member of the German CERT-Verbund and supports customers with incident management and forensic analysis.

All trademarks used are trademarks of the relevant proprietors; we reserve the right to make technical changes, errors excepted.

secXtreme GmbH
Kiefernstraße 38
D-85649 Brunnthal-Hofolding

Tel. +49(0)89-18 90 80 68-0
Fax.+49(0)89-18 90 80 68-77
E-mail: info@sec-xtreme.com
WWW: www.sec-xtreme.com