honeyBox®

4 Port-Version-Generation 2

Attack Detection and Alarm

- reliable detection of attackers in the network
- rapid detection of worm outbreaks
- virtually no false alarms (false positives)
- simple integration into the network
- no changes required to the network infrastructure
- no effect on the (high) availability of the network
- very low operating costs

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

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 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.

secXTREME Information Security

Functions and Characteristics

FUNCTIONS

Honeypot
- Several hundred virtual honeypots are possible for each interface
- 4 interfaces
- 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 via SSHv2 and serial connection
- Alert system (e-mail, pager, syslog, database, log files)
- Backup / restore / recovery
- Watchdog
- Hardware

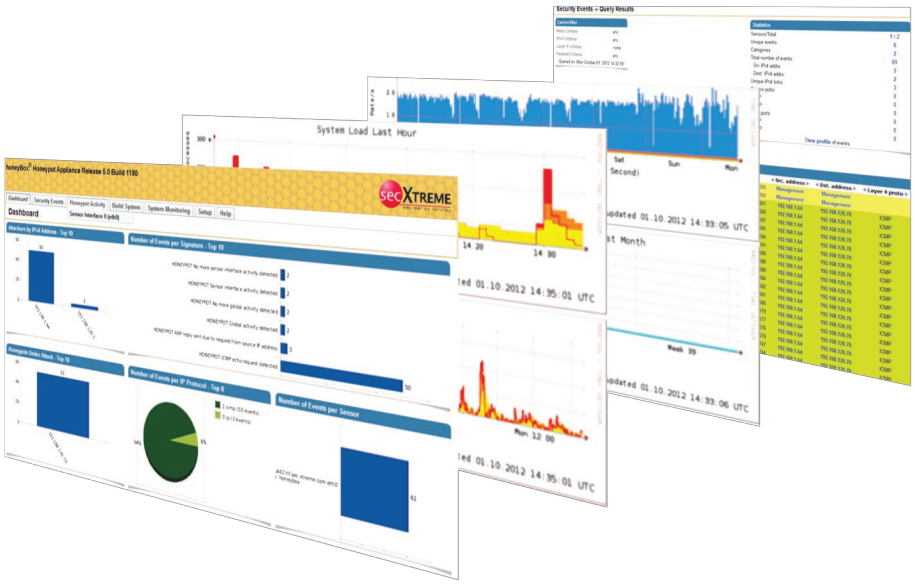
Installation
- CD-ROM (Software Appliance)
- USB stick (recovery of hardware appliance)

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 warrenty extension for up to 5 years
- Keep Your Hard Disk option

The Honeypot Appliance 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.
A variety of criteria can be used for evaluation, allowing investigation through selective drill-down.



Hardware	
CPU	Intel Celeron M 440, 2.0 GHz
RAM	1024 MB DDR2 SDRAM, non-ECC
Network	4 x 10/100/1000 copper
USB	2 x USB 2.0
Storage	250 GB, SATA-II, 7200 RPM
RS232	1x RJ45
Power Supply	110-240 VAC, 50-60 HZ, 4,2A
Power Consumption (typ.)	200 Watt
Operating Temp.	0 to + 40 °C
Humidity	5 % - 95 % , non condensing
Housing Size	426 mm x 44mm x 366 mm (BxHxT)
Certifications	CE, FCC, RoHS

Awards for the honeyBox® Appliance Family

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