SECHS HONEYPOT-PRODUKTE IM TEST

Hackerfallen

Mit Honeypots lassen sich Hacker fangen, Würmer ausbremsen und nervige Spammer leimen. *Internet Professionell* testet sechs führende Honeypot-Produkte.

VON ACHIM WAGENKNECHT

Wer über gut gepflegte Security Policys, Firewalls und IDS-Systeme hinaus noch mehr für die Sicherheit tun will, kann einen Honeypot installieren. Das ist ein System, das von außen aus dem Internet betrachtet aussieht wie ein produktiver Rechner, den zu knacken, auszuspionieren und zu missbrauchen sich lohnt. In Wahrheit werden die Ports und Dienste, die potenzielle Cracker zu sehen bekommen, nur simuliert.

Das Verfahren ergänzt und erweitert herkömmliche Intrusion-Detection-Systeme. So vermeidet ein gut aufgebauter Honeypot Fehlalarme. Er ist so eingerichtet, dass keine produktive Aktivität darauf stattfindet. Jede Aktivität auf dem Honeypot ist daher eindeutig ein Angriff. Schlägt im umgekehrten Fall das IDS nicht an, obwohl der Honeypot Aktivität zeigt, so ist dem IDS offensichtlich etwas entgangen: Es muss nachgebessert werden. Um das IDS so anhand des Honeypots kalibrieren zu können, müssen beide Systeme unabhängig voneinander arbeiten.

Cracker fangen

Ein anderes Konzept sieht vor, dass das IDS dem Honeypot vorgeschaltet ist und jeden erkannten Angriff auf die süße Falle umlenkt. Statt den Angreifer einfach abzuweisen, hält man ihn möglichst lange bei der Stange und beobachtet ihn. Jeder Tastendruck des Crackers wird aufgezeichnet. Im Idealfall kann man den Angreifer schließlich identifizieren und dingfest machen.

Das Honeypot-System Specter geht sogar noch weiter und markiert die Rechner unvorsichtiger Angreifer mit eindeutigen Signaturen, die gegebenenfalls vor Gericht als Beweis dienen können. Das funktioniert allerdings nur, wenn der Angreifer eine ausführbare Datei vom Honeypot herunterlädt und auf seinem PC startet. Specter bietet mehrere solcher Köder an.

Die Kandidaten

Im Testfeld finden sich Kandidaten aus der Open-Source-Gemeinde und kommerzielle Produkte wie der Symantec Decoy Server, der über 9000 Euro kostet. Letzterer bietet allerdings auch Luxus pur. Er stellt bis zu vier virtuelle Server auf einem Rechner zur Verfügung, auf denen beliebige Anwendungen installiert werden können. So lassen sich individuelle Crackerfallen aufbauen, die den echten Servern zum Verwechseln ähnlich sehen. Das geht ansonsten nur mit sehr viel Handarbeit mit VMware oder User Mode Linux. Solchen selbst gestrickten Honeypots hat der Decoy Server zudem ausgefeilte Überwachungs-Optionen voraus.

Die anderen Kandidaten sind nicht so luxuriös. Zudem ist auch kein anderer Honeypot derart interaktiv, dass ein Angreifer sich tatsächlich root-Rechte verschaffen und schalten und walten kann, wie er will. Dass Symantec trotzdem den Testsieg knapp verfehlt, liegt neben dem hohen Preis am einzigen echten Nachteil des Decoy Servers: er läuft ausschließlich unter Solaris und kann auch nach außen hin nur Solaris darstellen.

Nicht getestet wurden Selbstbau-Honeypots, wie sie auf der Basis von VMware oder User Mode Linux konstruiert werden können. Das heißt aber nicht, dass diese Lösungen nichts taugen. Im Gegenteil: Ein sorgfältig von Grund auf selbst aufgebauter Honeypot bietet größtmögliche Flexibilität gegen ernsthafte professionelle Angreifer, setzt aber auch einiges an Know-how voraus. [JP]

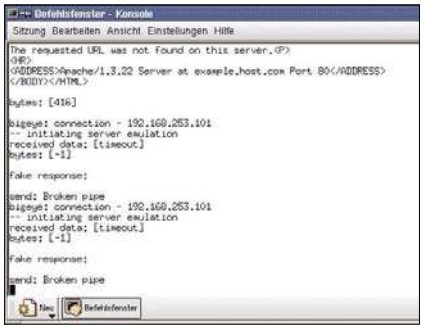
Specter

INTERNET PROFESSIONELL EMPFEHLUNG DER REDAKTION

Specter lässt sich unter Windows im Handumdrehen installieren und konfigurieren. Es ist gut geeignet, um kleine bis mittlere Netzwerke über Firewall und IDS hinaus noch einen Tick sicherer zu machen. Das System kann 14 Betriebssystem-Varianten inklusive Mac OS simulieren und lässt sich bequem mit Profilen konfigurieren. Für die Auswertung der Cracker-Aktivitäten stehen E-Mail-Alarm sowie Protokolle im klassischen Log-Format wie auch als Datenbank zur Verfügung.

An Funktionalität und Bedienkomfort lässt Symantecs Decoy Server keine Wünsche offen. Da das Produkt jedoch nur Solaris-Rechner simulieren kann, muss es Specter den Vortritt lassen.

ILLUSTRATION: BODO MERTOGLU



Bigeye

Ganz gleich was der Angreifer unternimmt: Er bekommt von Bigeye eine Antwort, die ihm zu denken gibt.

Bigeye kann neben seiner Funktion als Honeypot auch als Sniffer oder Logger eingesetzt werden. Als Honeypot kann das Programm FTP oder HTTP simulieren, Letzteres als Apache oder Microsoft Internet Information Server (IIS). Das Programm wird im Quelltext vertrieben und lässt sich im Test unter Suse Linux 8.0 problemlos kompilieren und starten. Die mitgelieferte Anleitung ist trotz des bemüht coolen Stils des Autors sehr nützlich.

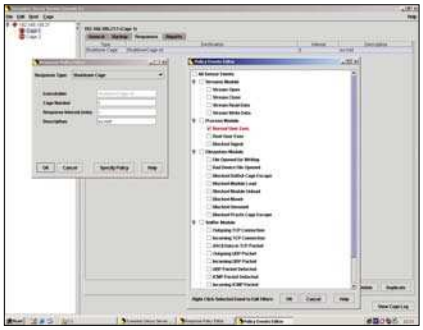
Die Standard-Antworten, die der Angreifer zu sehen bekommt, sind im Klartext in den Verzeichnissen HTTP und FTP abgelegt, wo sie mit einem einfachen Text-Editor angepasst werden können. Im Sicherheitstest meldet Nessus 48 Sicherheitslücken – in diesem Fall ein sehr guter Wert, denn das ist ein optimaler Köder für den Angreifer. Das Programm kann nur einen einzelnen Server simulieren, der seine IP-Adresse vom Host-System übernimmt.

Der simulierte Webserver sendet zufällig entweder die Statusmeldung 200 (ok) oder 404 (Seite nicht gefunden) aus. Wer immer nur eine der beiden Meldungen senden will, muss die Zufallsfunktion im Quelltext entfernen.

Im FTP-Modus kommt der Angreifer bis zu einem gefälschten Inhaltsverzeichnis, an dem er sich dann die Zähne ausbeißen kann. Leider fehlen Bigeye Funktionen, um sinnvoll auf Angriffe reagieren zu können. Weder E-Mail-Alarm noch spezielle Event-Logs sind vorhanden.

Fazit. Bigeye eignet sich für experimentelle Honeypots in abgesicherten Umgebungen wie zum Beispiel einer DMZ. In der Nähe von produktiven Servern sollte man das System nicht installieren.

Ranking	38 %
Internet	violating.us/projects/bigeye
Preis	kostenlos
Plattform	Linux



Decoy Server

Im Decoy Server können bis zu vier virtuelle Server präpariert werden – überwacht bis zum letzten Bit.

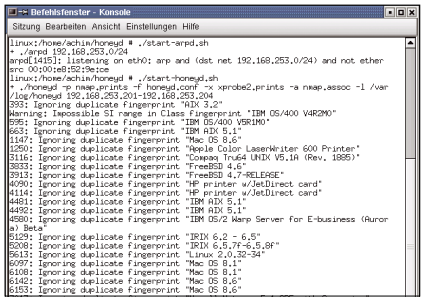
Wer gegen ernsthafte, hoch motivierte Angreifer zu kämpfen hat, dem bleibt kaum etwas anderes übrig als der Decoy Server. Das Programm stellt virtuelle gekapselte Server zur Verfügung, auf denen vorhandene Server eins zu eins gespiegelt werden können. Am besten nimmt der Admin noch ein paar subtile Änderungen vor, damit der Cracker keine echten Daten erbeuten kann. Ein Angreifer kann so sehr lange in dem Glauben gehalten werden, einen echten Produktivserver geknackt zu haben.

Bis zu vier dieser Server können auf einem Rechner installiert werden. Gesteuert und überwacht wird das System von einer Fernsteuerungs-Oberfläche von Windows aus. Abgesehen vom hohen Preis ist der einzige Haken an der Sache die Systemplattform: Der Decoy Server läuft ausschließlich unter Sun Solaris und erscheint auch dem Angreifer immer als Sun Solaris. Wer einen ähnlich flexiblen Honeypot unter Linux braucht, muss mit User Mode Linux oder VMware und zusätzlichen Tools jede Menge Klimmzüge machen. Microsoft-Anwendern bleibt nur VMware. Bis so eine Lösung läuft, können Tage oder Wochen ins Land gehen – der Decoy Server kann dagegen an einem Tag installiert werden.

Das Programm kann sogar mit Hilfe von Templates E-Mail-Verkehr simulieren. Die umfangreichen Auswertungs-, Alarm- und Statistik-Funktionen spendieren dem Sicherheits-Admin zusätzlichen Komfort.

Fazit. Wer Solaris anwendet, saftige Schäden über 20 000 Euro befürchten muss und schnell und einfach einen schlagkräftigen Honeypot aufsetzen will, ist mit dem Decoy Server von Symantec optimal bedient.

Ranking	75 %
Internet	www.symantec.de
Preis	ab 9217 Euro
Plattform	Solaris



Honeyd

Honeyd ist das ausgereifteste Honeypot-Projekt der Open-Source-Szene, das Windows und Linux-Systeme simuliert.

Das Tool kann gegen Cracker, Würmer und Spammer eingesetzt werden. Der Honeyd-Server lässt sich mit Hilfe von Start-Skripts einfach hochfahren. Um die Installation zu vereinfachen, steht ein Linux-Toolkit zur Verfügung *(www.tracking-hackers.com/solutions/honeyd)*. In der Standard-Distribution kann das Programm Windows- und Linux-Server sowie Cisco-Router simulieren. Da Honeyd außerdem skriptgesteuert eine Vielzahl von Servern gleichzeitig simuliert, kann auf diese Weise ein komplettes Subnetz täuschend echt nachgeahmt werden.

Honeyd kann beliebig viele freie IP-Adressen in einem Netz übernehmen und mit simulierten Servern versehen. Auf der Projekt-Website stehen außerdem Konfigurationsdateien für den Betrieb als Wireless-Honeypot sowie Solaris, Macintosh und Cray zur Verfügung.

Das Programm wird mit Perl-Skripts gesteuert. Simuliert werden sechs verschiedene Dienste: SMTP, POP3, RPC, Telnet, Apache und IIS. Um verschiedene Betriebssysteme simulieren zu können, antwortet Honeyd auf entsprechende Scans mit den passenden Fingerprints. Honeyd wird in der Open-Source-Szene aktiv weiterentwickelt. So sind in der Standard-Distribution schon Erweiterungen von mehreren Programmautoren enthalten. Andere Entwickler erforschen, wie sich Honeyd als Spamfalle und Wurmkur einsetzen lässt *(www.honeyd.org/spam.php* und *www.honeyd.org/worms.php)*.

Fazit. Honeyd ist das Programm der Wahl für alle, die sich intensiv mit der Honeypot-Technik auseinander setzen wollen, ohne gleich viel zu investieren.

Ranking	63 %
Internet	www.honeyd.org
Preis	kostenlos
Plattform	Linux, BSD, Solaris

Honeyweb

Honeyweb ist darauf spezialisiert, angreifbare Webserver zu simulieren – gern auch zusammen mit Honeyd.

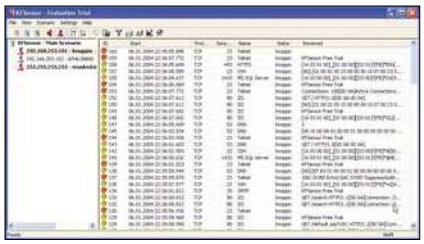
Honeyweb präsentiert im Sicherheitstest mit Nessus die meisten simulierten Sicherheitslöcher: 55 Schwachstellen meldet der Sicherheits-Scanner. Das sollte jeden Cracker ködern.

Wird Honeyweb mit einem unbekannten Request konfrontiert, so speichert es diesen in einer speziellen Log-Datei. Die Chancen stehen gut, dass neue Exploits in dieser Datei landen – zur Freude des Security-Admins, der den Exploit dann analysieren kann. Das Programm kann sich IP-Adressen von Angreifern merken, um auf wiederholte Anfragen von der gleichen Adresse immer gleich zu reagieren. Um sich gegen Angriffe mit fehlgeformten URLs zu schützen, untersucht das Programm die eingehenden Requests mit Hilfe von regulären Ausdrücken und präsentiert dem Angreifer die erwartete Antwort.

Um dem Angreifer Erfolgserlebnisse zu vermitteln, kann Honeyweb gefälschte gesperrte Inhaltsverzeichnisse übermitteln oder dem Angreifer eine *.htaccess*-Datei schicken. An den verschlüsselten Passwörtern in *.htaccess* kann der Angreifer dann seine Brute-Force-Programme arbeiten lassen. Das Programm läuft unter Linux und Windows, sofern Python installiert ist. Es simuliert sowohl Apache als auch den Microsoft Internet Information Server. Zusammen mit Honeyd kann Honeyweb eine Vielzahl von Webservern im Adressraum des Subnetzes simulieren. Im Standalone-Modus erzeugt es nur einen einzelnen Server.

Fazit. Honeyweb ist vor allem als Ergänzung zu Honeyd interessant. Allein kann es zu wenig.

Ranking	56 %
Internet	www.var-log.com
Preis	kostenlos
Plattform	Unix, Mac OS, MS-DOS, Windows 95/98/Me/NT/2000/XP, OS/2



KF-Sensor

KF-Sensor ist spielend leicht installiert und kann mit Hilfe von Szenarios flexibel konfiguriert werden.

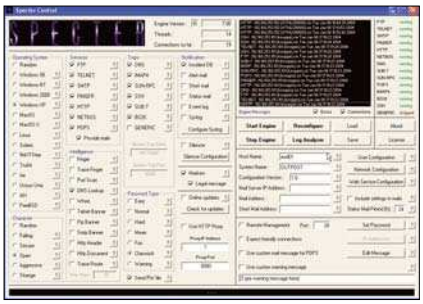
KF-Sensor kann viele Dienste sogar in mehreren Varianten simulieren: So werden POP3, SMTP und Telnet in einer allgemeinen, einer Microsoft- und einer Linux-Variante angeboten. Aus den vorhandenen Diensten kann sich der Benutzer Szenarien zusammenstellen. Damit diese konsistent bleiben, sollte man darauf achten, nicht Windows- und Linux-Dienste in einem Szenario zu mischen.

Jeder verfügbare Dienst kann detailliert konfiguriert werden. So kann neben Name, Port und Timeout auch definiert werden, wie ernst ein Zugriff auf diesen Dienst zu nehmen ist. Ernsthaftere Zugriffe lösen schneller Alarm aus. Apropos Alarm: KF-Sensor ist das einzige Produkt im Testfeld, das tatsächlich Sirenen heulen lässt. Damit nicht genug, kann der Benutzer bei Alarm außerdem eine beliebige Anwendung mit Parametern starten. So lässt sich der Admin zum Beispiel per SMS warnen.

Auf ganz ähnliche Weise können über eine Standard-Konsolenschnittstelle beliebige Server eingebunden werden. Wer »Kuckucksei« – den Klassiker unter den Hackerjagd-Geschichten – gelesen hat, weiß, dass Clifford Stoll bei seiner Hackerjagd oft improvisieren musste. Es kann im Ernstfall hilfreich sein, einem Angreifer einen selbst geschriebenen Server als Sahnestück vorzusetzen. Man könnte ihn zum Beispiel »Top Secret Custom SAP Connector« nennen. Wer das ausprobieren möchte, kann eine auf 14 Tage limitierte Testversion aus dem Netz laden.

Fazit. KF-Sensor bietet viele spannende Möglichkeiten, ist aber auch etwas schwerer zu bedienen als Specter.

Ranking	69 %
Internet	www.keyfocus.net/kf-sensor
Preis	970,68 Euro
Plattform	Windows NT/2000/XP/2003 Server



Specter

Specter bietet ausgeklügelte Funktionen, um Angreifer anzulocken, zu verwirren und zu identifizieren.

Die Bedienoberfläche von Specter verwirrt anfänglich, weil alle Optionen in einem einzigen Fenster präsentiert werden. Hat man sich daran gewöhnt, ist das System sehr komfortabel. Es simuliert 14 Betriebssysteme inklusive Windows, Mac OS und Linux. Der simulierte POP3-Server kann noch realistischer präsentiert werden, indem man vorgefertigte oder selbst geschriebene Mails einbindet.

Ob dem Cracker ein sorgfältig oder schlampig gepflegtes System präsentiert wird, lässt sich in Charakteren einstellen. Neben »offen« und »sicher« stehen auch ein »schwer gestörtes« und ein »seltsames« System zur Verfügung. Letzteres verhält sich unvorhersehbar. Die Variante »agressiv« dagegen gibt sich dem Angreifer zu erkennen, sobald genug Informationen über ihn gesammelt wurden.

Ein Silencer filtert sich wiederholende Meldungen aus den Logs aus, um eine Überflutung von Mail-Accounts oder Log-Servern zu vermeiden. Raffiniert sind die Marker: Das sind ausführbare Dateien, die der Angreifer herunterladen kann und die eindeutige Markierungen auf seinem PC hinterlassen, wenn er sie startet. Ist der Hacker identifiziert, kann sein PC beschlagnahmt und die Markierungen ausgewertet werden. Die Marken können als Beweismaterial vor Gericht verwendet werden. Specter light für 599 Dollar simuliert nur Windows NT, 2000 und XP. Die Komplettversion, die auch Linux, Mac und diverse Unix-Betriebssysteme darstellen kann, kostet 899 Dollar.

Fazit. Specter bietet den durchdachtesten Ansatz, wenn es darum geht, einen Cracker mit möglichst einfachen Mitteln tatsächlich dingfest zu machen.

Ranking	76 %
Internet	**www.specter.com**
Preis	**ab 599 Dollar**
Plattform	**Windows NT/2000/XP, Linux, Mac OS, Unix**

Zusatznutzen

Netzwerk-Administratoren jagen mit Honeypots nicht nur Hacker, sondern nutzen die Funktionen der Programme auch, um Spammer zu stoppen und die Aktionen von Angreifern auszubremsen.

Eine weitere Anwendung neben der Hackerhatz besteht für Honeypots darin, sie neben produktiven Systemen aufzustellen, um von diesen abzulenken. In dem Fall sollten die echten Server hohe IP-Adressen bekommen und die Honeypots niedrige. Da die meisten Schwachstellen-Scanner die niedrigen IPs zuerst untersuchen, werden die Ressourcen des Angreifers auf diese Weise für eine ganze Weile gebunden. Jedenfalls so lange, bis dieser Trick sich bei den Schwarzhüten herumgesprochen hat.

Um den Angreifer noch weiter zu behindern, lassen sich manche Töpfe auch mit besonders klebrigem Honig füllen. Sobald ein Angreifer Verbindung zu einem solchen Honeypot aufnimmt, verlangsamt dieser gezielt die Kommunikation.

Neben Schwachstellen-Scannern lassen sich auch Würmer auf diese Weise ausbremsen – eine Technik, die angesichts der anhaltenden Wurmplage im Internet noch viel zu wenig eingesetzt wird. Es gibt sogar einen Honeypot, der auf diese Bremswirkung spezialisiert ist: Labrea Tarpit *(labrea.sourceforge.net).* Auf ganz ähnliche Weise lassen sich auch Spammer ausbremsen (siehe *www.tracking-hackers.com/solutions/sendmail.html).* Dieser Honeypot ist besonders simpel: Auf einem Linux-Server, der nichts mit E-Mail zu tun hat, wird Sendmail mit der Option *–bd* gestartet, so dass es Mails annimmt, aber nicht ausliefert. Ergebnis: Jede Menge Spam in */dev/nul,* also genau da, wo er hingehört.

So bewertet *Internet Professionell*

Im Internet-Pro-Labor setzen die Tester praxisnahe Szenarios ein, um die Fähigkeiten und Bedienbarkeit der Honeypot-Produkte zu überprüfen.

Installation & Konfiguration

Hier benoten die Tester, welche Plattform benötigt wird und wie einfach sich das Programm installieren lässt. Eine grafische Bedienoberfläche für die Konfiguration bedeutet ebenso einen Vorteil. Müssen allerdings Quelltexte geändert werden, gehen Punkte verloren.

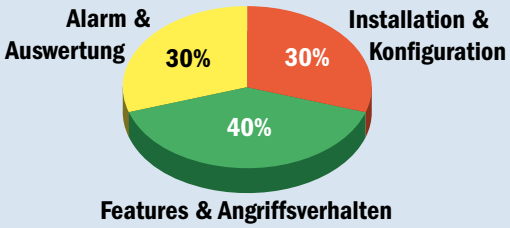
Features & Angriffsverhalten

Die Anzahl und Art der Dienste, die der Honeypot simulieren kann, gehen in dieser Rubrik in die Bewertung ein. Auch die Menge der simulierbaren Server und die verfügbaren Betriebssysteme spielen hier eine Rolle. Kann der Honeypot Würmer, automatisierte Scans und Spammer ausbremsen, gibt es noch zusätzliche Punkte.

Auswertung & Reaktion

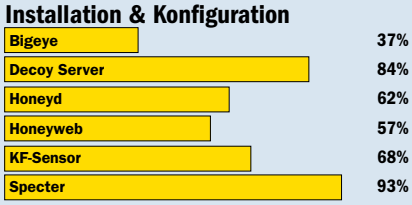
Wenn der Honeypot einen Gegenangriff starten kann, wird dies positiv bewertet. Auch die Alarmierung des Admins über verschiedene Kommunikationswege ist ein wichtiger Faktor. Außerdem werden die Auswertungsoptionen bewertet. Steht eine Datenbank statt eines Textprotokolls zur Verfügung, wird dies honoriert.

Gewichtung

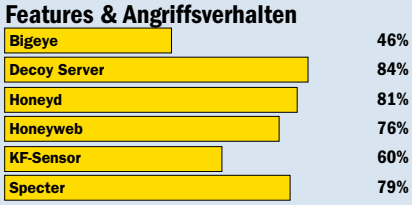


Testergebnisse

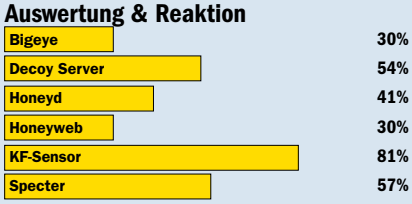
Installation & Konfiguration



Features & Angriffsverhalten



Auswertung & Reaktion



Überblick: Honeypot-Produkte

INTERNET PROFESSIONELL EMPFEHLUNG DER REDAKTION

Produkt	Bigeye 0.3	Decoy Server 3.1	Honeyd 0.7	Honeyweb 0.4	KF-Sensor 2.0.2	Specter 7.0
Hersteller	Violating Networks	Symantec	Niels Provos	Kevin Timm	Keyfocus	Netsec
Internet	violating.us/projects/bigeye	www.symantec.de	www.honeyd.org	www.var-log.com	www.keyfocus.net/kfsensor	www.specter.com
Preis	kostenlos	ab 9217 Euro	kostenlos	kostenlos	970,68 Euro	ab 599 Dollar
Plattform	Linux	Solaris	Linux, BSD, Solaris	Unix, MacOS, MS-DOS, Windows 95/98/Me/NT/2000/XP, OS/2	Windows NT/2000/XP/2003 Server	Windows NT/2000/XP
Gesamtwertung	**38 %**	**75 %**	**63 %**	**56 %**	**69 %**	**76 %**
Ausstattung						
simulierte Dienste	FTP, HTTP (Apache, IIS)	alle unter Solaris möglichen	SMTP, HTTP (Apache, IIS), SMTP, POP3, RPC, Telnet	HTTP (Apache, IIS)	FTP, HTTP (Apache, IIS), Sendmail, Telnet, mySQL, POP3, SMTP, MS SQL-Server etc.	FTP, Telnet, SMTP, HTTP, Netbus, POP3, DNS, IMAP4, Sun-RPC, SSH und andere
simulierte Betriebssysteme	Windows, Linux	Solaris	Windows, Linux, Cisco Router	Windows, Linux	Windows, Linux, Unix	Windows, MacOS, Linux, Unix und andere
Anzahl simulierbarer Maschinen	1	4	Tausende	Tausende	1	1
gefundene Sicherheitslücken	48	12	8	55	8	8
Gegenangriff	nein	ja	nein	nein	nein	ja
E-Mail-Alarm	nein	ja	ja	nein	ja	ja
frei definierbare Alarm-Schnittstelle	ja	nein	ja	ja	ja	nein
Protokolldatenbank	nein	ja	nein	nein	ja, ODBC	ja
Protokoll Syslog/Event-Log	ja/ja	ja/ja	ja/ja	ja/ja	ja/ja	ja/ja
integrierte DoS-Abwehr	nein	nein	nein	nein	ja	nein
Bedienung & Support						
Installation	manuell	Solaris-Installer	manuell	manuell	Windows-Installer	Windows-Installer
Konfiguration	im Quelltext	grafische Oberfläche	Konfigurationsdateien editieren	im Quelltext	grafische Oberfläche, Baukastensystem	grafische Oberfläche
Support	per E-Mail	individuelle Kundenbetreuung	per E-Mail	per E-Mail	per E-Mail	per E-Mail
Dokumentation	englischsprachige Readme-Datei	englischsprachiges Handbuch	englischsprachige Readme-Datei, Website, Beispielkonfigurationen	englischsprachige Readme-Datei	englischsprachiges Handbuch	englischsprachiges Handbuch
Verhaltensprofile	manuell	manuell	manuell	manuell	manuell	fünf Charaktere
vorgefertigte Mails	nein	ja	nein	nein	nein	ja
individuelle Mails	nein	ja, Assistent	nein	nein	nein	ja
Online-Update	nein	nein	nein	nein	nein	ja
Fernwartung	nein	ja	nein	nein	ja	ja
IP-Adresse	Host	frei definierbar	übernimmt alle freien Adressen im Subnetz	übernimmt alle freien Adressen im Subnetz	Host	vom Host übernommen
Testversion	frei, da Open Source	auf Anfrage, 30 Tage	frei, da Open Source	frei, da Open Source	Download, 14 Tage	nein