

So locken Sie Hacker in die Falle

Süß & klebrig

Angriffe auf das Firmennetzwerk werden immer dreister. Internet Professionell zeigt, wie Sie Hacker mit Hilfe eines Honeypots austricksen und selbst zum Gejagten machen. **Von Achim Wagenknecht**

» Wer die Verantwortung für die Sicherheit eines Netzwerks trägt, macht bei Angriffen sofort die Schotten dicht. Aber wäre es nicht schön, einem Angreifer einmal ungeniert bei seiner kriminellen Arbeit zusehen zu können? Statt Angriffe sofort abzublocken, können Sie Hacker im Honeypot wie im Aquarium beobachten. Den Köder in der Hacker-Falle bildet ein leicht zugänglicher PC mit offensichtlichen Schwachstellen. Mit Hilfe einer unsichtbaren Bridging-Firewall wird der Angreifer beobachtet. Desktop-PCs oder Server mit Schwachstellen findet man überall. Wenn Sie keinen vorrätig haben, setzen Sie einfach ein Windows-System oder eine ältere Linux-Distribution neu auf.

Damit daraus ein Honeypot wird, benutzen Sie zusätzlich Honeywall. Das ist eine Firewall, die sich entweder mit NAT oder als Bridge konfigurieren lässt. Letzteres hat den Vorteil, dass das Gerät im Netz unsichtbar wird. Es verbindet zwar zwei Netzsegmente mit Hilfe zweier Netzwerkkarten, aber keine davon hat eine IP. Und dass der Traffic zwischen diesen beiden Netzwerkkarten auch noch akribisch beobachtet wird, bemerkt der Angreifer überhaupt nicht.

Honeywall ist eine spezialisierte Linux-Distribution, die Sie auf der Heft-CD finden oder unter honeynet.org/tools/cdrom herunterladen können. Dann fehlt nur noch ein Pentium III mit drei Netzwerkkarten und 256 MByte

RAM, und Sie können Ihre Hackerfalle bauen. Wenn Sie Honeywall im Echtbetrieb einsetzen wollen, sollten Sie reichlich Platz für Log-Dateien vorsehen. Das Team von Honey.net.org empfiehlt mindestens 30 GByte. Für Tests reichen aber schon 2 GByte. Wer keine PCs übrig hat, kann den Honeypot alternativ auch unter Vmware auf einem einzelnen PC simulieren. Dieser braucht dann allerdings reichlich RAM: Den Testrechner für den Workshop muss Internet Professionell erst von 500 MByte auf 1 GByte aufrüsten, damit der Honeypot reibungslos läuft.

»Ein unwiderstehlicher Köder«

Vmware ist genau wie kleine Festplatten nur für den Testbetrieb zu empfehlen. Denn die Schwarzhüte da draußen sitzen nicht rum und häkeln Bildschirmschoner. Stattdessen erforschen sie zum Beispiel, wie sich ein simulierter PC unter Vmware von einem echten Rechner unterscheiden lässt. Im Ernstfall sollte also ein echter Computer den Köder spielen. Vergleichen Sie im Zweifel einfach nur die aktuellen Hardware-Preise mit dem Schadenspotenzial eines gehackten Netzwerks.


Um dem Hacker Futter zu geben, können Sie auf dem Köder-PC zum Beispiel ein Image von einem echten Datenbank-Server installieren. Damit der Hacker keinen Schaden anrichten kann, lassen Sie ein Skript über den kompletten Datenbestand laufen, das die Daten gezielt

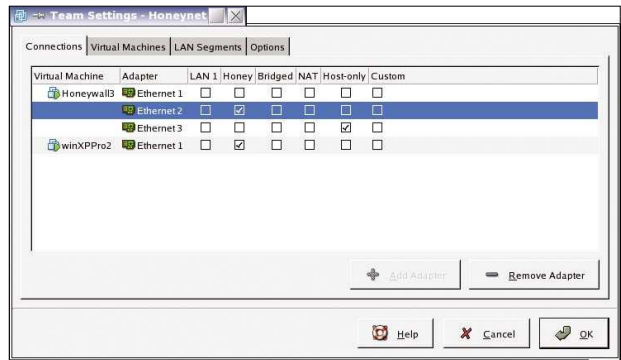
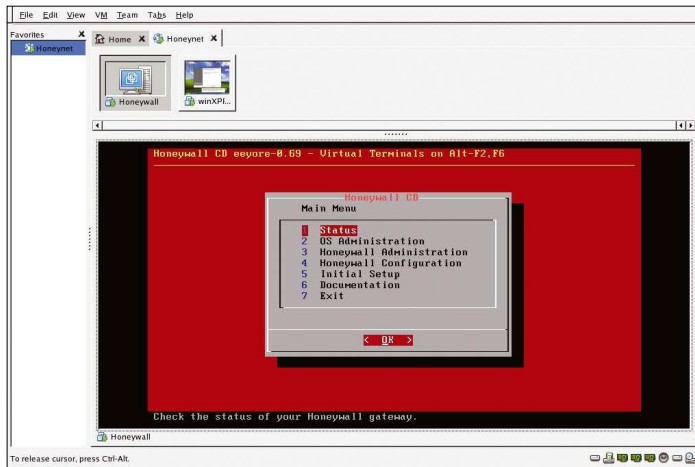
Info

Auf einen Blick

» Aus einem Köder-PC und einer unsichtbaren Bridging-Firewall bauen Sie Ihren eigenen Honeypot. Anschließend werten Sie Hacker-Zugriffe auf den ungeschützten PC detailliert aus.

Das brauchen Sie

- » Honeywall
- » Zwei zusätzliche PCs oder Vmware und einen PC mit 1 GByte RAM
- » Software auf CD 



Mit der Honeywall-CD ist ein hoch interaktiver Honeypot schnell installiert – mit echten PCs oder wie hier unter Vmware.

Vmware verbindet den virtuellen Köder-PC über ein simuliertes LAN mit Honeywall.

verfälscht. Ein ähnliches Verfahren gegen MySQL-Datendiebe können Sie in Internet Professionell, Ausgabe 5/2005, auf Seite 84 nachlesen.

Eine wichtige Frage bei Honeypots ist: Wo stelle ich die Falle auf? Wenn Sie viele Hacker anlocken wollen, um deren Angriffe zu studieren, schließen Sie den Honeypot außerhalb der Firewall direkt ans Internet an. In einem kleinen Netz ist die einfachste Möglichkeit, nach Feierabend den DSL-Stecker vom normalen Router abzuziehen und stattdessen den Honeypot ans Internet anzuschließen.

»Innere Abwehr«

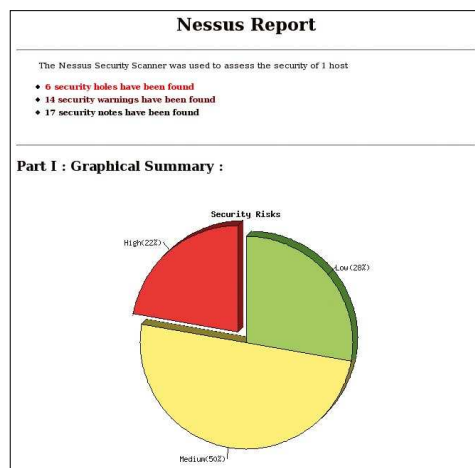
Im Inneren eines Netzwerks platziert, kann ein Honeypot als zusätzliches Intrusion-Detection-System dienen oder Angriffe aus den eigenen Reihen entlarven. Aber wer anfängt, sich mit Honeypots auseinander zu setzen, sollte den Honigtopf vor allem deshalb im lokalen Netz installieren, damit er ihn gründlich testen kann. Denn Honeypots sind nicht nur eine gute Möglichkeit, Hacker zu beobachten und vielleicht einmal einen Cracker dingfest zu machen. Ein Honeypot ist immer auch ein Risiko. Wer mit einem Honeypot absichtlich die Angriffsfläche seines Netzes erhöht, muss ganz genau wissen, was er tut. Apropos: Sie sollten das Aufstellen eines Honeypots unbedingt mit Ihrem Chef absprechen.

»Die Falle anstöpseln«

Für einen Hardware-Honeypot installieren Sie Honeywall auf einem normalen PC. Dann schließen Sie einen Köder-PC über die Honeywall-Bridge ans Netzwerk an. Einen virtuellen Honeypot können Sie komplett unter Vmware installieren. Unter www.vmware.com bekommen Sie eine 30-Tage-Testversion. Vmware kann ganze virtuelle Netzwerke auf einem einzelnen Windows-XP- oder Linux-Rechner simulieren. Dazu werden mehrere virtuelle PCs installiert und mit virtuellen Netzwerken verbunden.

Vmware kennt unterschiedliche Netzwerkverbindungen. Das Host-only-Netz verbindet den virtuellen PC über seine virtuelle Netzwerkkarte mit seinem Wirtssystem. In den Bridged- und NAT-Modi greift der simulierte Rechner auf die Netzwerkkarte seines Gastgebers zu. Sind mehrere simulierte PCs vorhanden, so können zwischen diesen wiederum virtuelle LAN-Segmente definiert werden. Es sind also reichlich Möglichkeiten vorhanden, Honeypots zu Testzwecken zu vernetzen.

Im Internet-Professionell-Testlabor fassen die Autoren Honeywall und einen Köder in einem virtuellen Netzwerk zusammen, das durch die überbrückte Netzwerkkarte des Gastrechners mit dem echten LAN verbunden ist. Von einem Linux-Rechner im echten Netz aus greifen die Tester das System mit Nessus an.



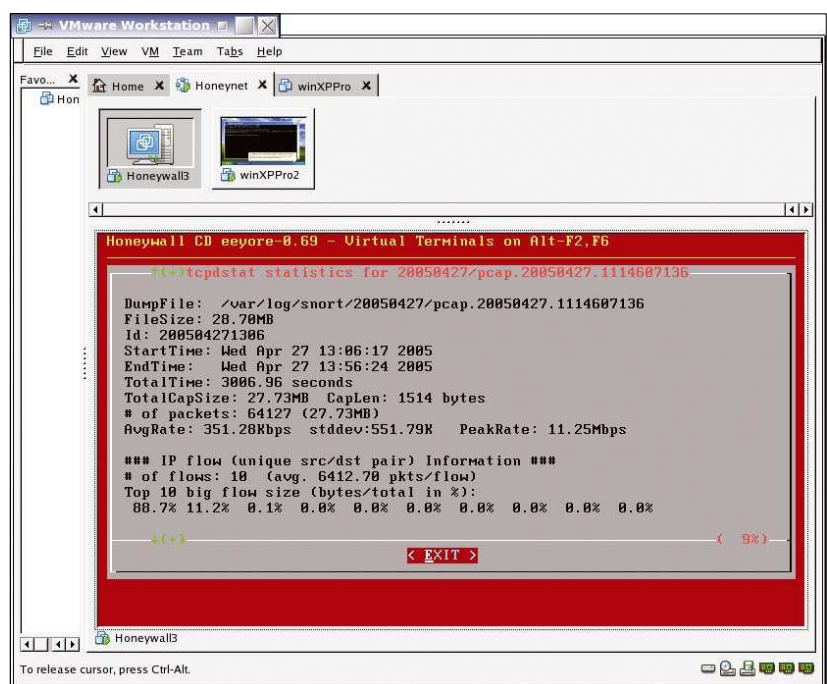
Info

Würmer angeln

Computerwürmer sind hochinteressante Studienobjekte für IT-Security-Experten. Aber die Biester mit einem Windows-PC einzufangen ist viel zu riskant. Studenten von der RWTH Aachen haben daher einen speziellen Honeypot entwickelt, der Windows-Würmer auf Linux-Systeme lockt und dort speichert.

► www.mwcollect.org

Der Security-Scan mit Nessus fördert ein halbes Dutzend Sicherheitslücken auf dem Köder-PC zutage.



Honeywall zeichnet genau auf, was ein Angreifer tut.

Info

High and Low

Honeyspots werden unterschieden nach dem Maß an Interaktion, das sie dem Angreifer bieten.

Der in diesem Workshop beschriebene Aufbau bietet dem Angreifer ausgesprochen viele Interaktionsmöglichkeiten (High Interaction). Solch ein Aufbau ist sehr aufwendig, bietet aber die besten Chancen, einen Hacker tatsächlich dingfest zu machen. High-Interaction-Honeyspots enthalten meist komplette Betriebssysteme inklusive Anwendungen und gefälschten Benutzerdaten. Low-Interaction-Honeyspots wie Honeyd können einem Angreifer dagegen leicht Tausende von IP-Adressen in einem Netzwerk vorgaukeln. Sie sind leichter zu installieren, aber auch leichter zu enttarnen. Schwach interaktive Honeyspots entfalten eine gewisse Schutzwirkung, indem sie Angreifer verwirren und ausbremsen.

»Honeywall aufstellen«

Legen Sie auf VMware einen virtuellen Rechner für Honeywall an. Honeywall ist eine Distribution, die stets von CD startet. Für einen Hardware-Honeywall müssen Sie das ISO-Image auf CD brennen und immer im Laufwerk lassen. Wenn Sie aber auf VMware installieren, weisen Sie der virtuellen Maschine statt eines realen CD-ROM-Laufwerks direkt das ISO-Image auf der Festplatte zu. Das können Sie direkt beim Einrichten der Maschine per Assistent erledigen oder später mit dem Menübefehl *VM, Settings*. Hier markieren Sie in der Hardware-Liste das CD-ROM-Laufwerk, kreuzen die Option *Use ISO image* an und tragen den Pfad zur ISO-Datei ein.

Neben Hardware spart das auch Nerven. Denn wenn Sie den Wirts-PC booten und die Honeywall-CD des virtuellen Rechners im Laufwerk vergessen haben, dann bootet der echte Computer mit der Honeywall-CD. Und die ist bei der Installation gnadenlos: Sie löscht und formatiert die komplette Festplatte. Zum Glück tut sie das aber erst, nachdem sie dreimal nachgefragt hat.

Apropos Festplatte: Honeywall funktioniert nur mit IDE-Laufwerken, nicht mit SCSI. Da VMware aber SCSI-Festplatten als Standard einsetzt, müssen Sie die Einstellung der virtuellen Festplatte in VMware erst auf IDE umstellen.

Honeywall versetzt die Netzwerkkarten in den Promiscuous Mode. Normalerweise nimmt eine Netzwerkkarte nur die Datenpakete an, die für sie bestimmt sind. Im Promiscuous Mode nimmt sie alles an. Das ist für Überwachungseinrichtungen wie Honeywall die bessere Einstellung. Auf einem echten PC ist das auch kein Problem, aber wer in VMware unter Linux eine virtuelle Netzwerkkarte im Promiscuous Mode betreiben will, muss erst die Rechte dafür freischalten. Das kann zum Beispiel mit folgendem Befehl geschehen, der mit Root-Rechten eingegeben werden muss:

```
chmod a+rw /dev/vmnet0
```

Wenn Sie Honeywall das erste Mal starten, wählen Sie aus dem Hauptmenü den Punkt 5: *Initial Setup*. Es erscheint ein Assistent, der Sie Schritt für Schritt durch die Einstellungen leitet. Leider kennt dieser Assistent keinen Zurück-

Knopf. Wer etwas falsch einstellt und voreilig auf *Return* drückt, muss von vorn anfangen. Auch Plausibilitätsprüfungen fehlen. So können Sie zum Beispiel problemlos Broadcast-Adressen vergeben, die nicht zu den IP-Adressen der Honeyspots passen. Das Honeywall muss also sorgfältig geplant werden. Damit das klappt, finden Sie unter www.honeywall.org/papers/cdrom/InitialSetup.pdf eine Kurzanleitung mit Checkliste.

Wenn Sie Honeywall nach der Ersteinrichtung erneut starten, müssen Sie sich als *root* am System anmelden. Dann können Sie das Menü mit dem Befehl *Menu* wieder aufrufen. Sie können die Einstellungen von Honeywall auf Diskette speichern – einfach zur Sicherheit, oder um mehrere gleichartige Honeywalls aufzusetzen.

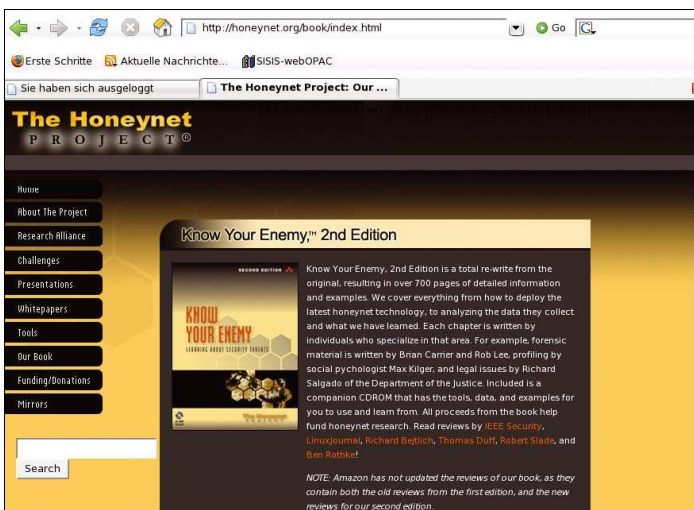
Wenn Ihr Honeywall fertig ist, testen Sie als Erstes mit einem einfachen Ping, ob er erreichbar ist. Der Köder-PC sollte das Ping ganz normal beantworten. Honeywall zeichnet parallel dazu den Kontaktversuch auf. Sie finden ihn unter *Status, Inbound Connections*.

Vor einem Testlauf können Sie die Log-Dateien von Honeywall mit *OS Administration, Clean out logging directories* leeren, damit die Daten übersichtlich bleiben. Danach müssen Sie das System mit *Honeywall Administration, Activate Honeywall* neu starten.

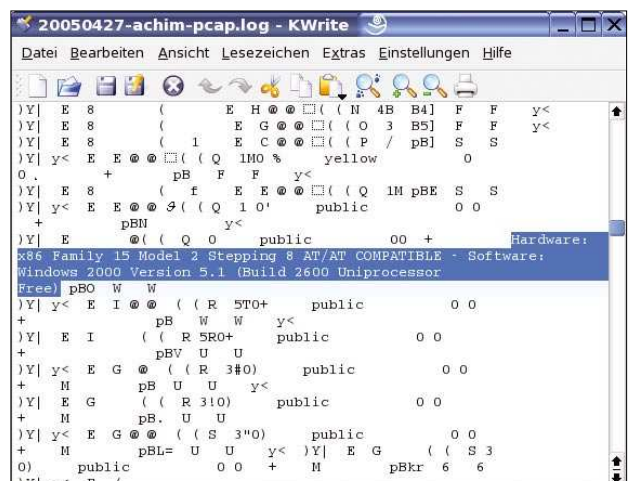
Wenn der Honeywall funktioniert, muss die Honeywall alle Angriffe auf den Köder-PC durchlassen, sie dabei aber protokollieren. Ob das klappt, können Sie mit einem Security Scanner oder einem Exploit für das Betriebssystem Ihres Köder-PCs ausprobieren.

»Testen mit Nessus«

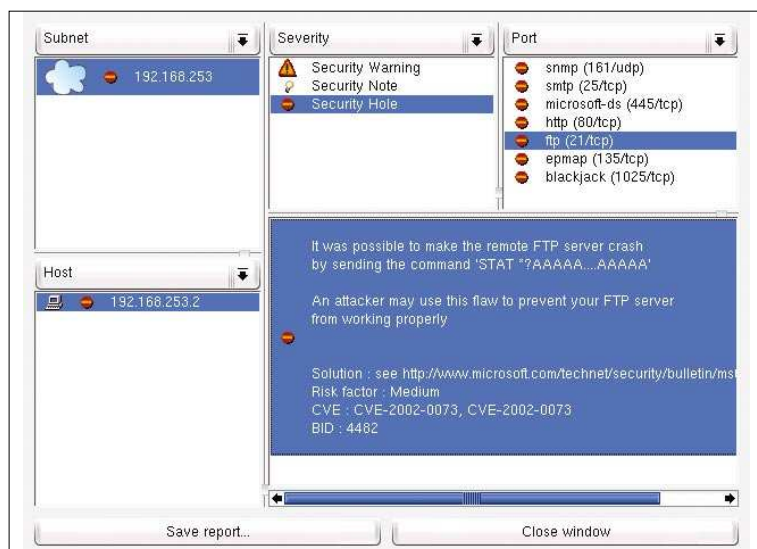
Als Security Scanner hat sich Nessus bewährt. Nachdem Sie Nessus unter Linux installiert haben, müssen Sie als *root* mit dem Befehl *nessus-adduser* einen Benutzer anlegen und mit *nessus-mkcert* ein Zertifikat erzeugen. Dann starten Sie den Nessus-Server mit *nessusd -D*. Den Client rufen Sie mit dem Befehl *nessus* auf. Nachdem Sie sich mit dem eben angelegten Benutzernamen angemeldet haben, können Sie die Scan-Optionen einstellen. Da auf dem Honeywall nicht produktiv gearbeitet wird, können Sie ihn hemmungslos hacken. Entfernen Sie also ruhig die Option *Safe Scan* unter der Registerlasche *Scan Options* im Nessus-Client. Nessus führt mit Hilfe von Plug-ins eine



Das Honeywall-Projekt erforscht Hacker mit Hilfe von Honeyspots.



Im Protokoll der Honeywall-Sitzung ist deutlich zu erkennen, wie der Angreifer das Betriebssystem ermittelt.



Der Test mit Nessus zeigt: Der Honeypot von Internet Professionell lässt sich gut hacken.

riesige Bandbreite an Tests durch. Unter *Plugins* finden Sie die Liste der installierten Module. Aktivieren Sie alle und stellen Sie unter *Target selection* das Ziel Ihres Angriffs ein.

Im Testlabor kann Internet Professionell mit Nessus auf dem Köder-PC unter Windows XP zuverlässig den *Generic Host Process for Win32 Services* zum Absturz bringen. Dieses Programm ist besser unter seinem Dateinamen *svchost.exe* bekannt und wird unter anderem vom MS-Blaster-Wurm ausgenutzt. Zudem löst Nessus einen Neustart aus und fördert jede Menge weitere Sicherheitslücken zutage.

»Gotcha!«

Parallel dazu zeichnet Honeywall zuverlässig auf, was der Hacker auf dem Honeypot macht. Die Ergebnisse eines Angriffs finden Sie unter *Status*. Der Punkt 13 in diesem Menü offenbart die Traffic-Statistik. Ein typischer Nessus-Scan erzeugt um die 30 MByte an Traffic. Mehr als die Hälfte der Scans beziehen sich auf HTTP. In den Protokoll-dateien von Snort ist jede einzelne Abfrage detailliert aufgezeichnet.

Um die Log-Dateien weiter zu analysieren, können Sie sie per SSH/SCP vom Honeywall-Rechner auf einen anderen PC laden. Die Optionen dazu finden Sie unter *Honeywall Configuration, Honeywall Upload*. Den Upload selbst starten Sie von der Kommandozeile, indem Sie das Skript *usr/local/bin/upload.sh* ausführen. Im Echtbetrieb kann Honeywall die Protokolle per *crontab* regelmäßig automatisch hochladen. Für die Analyse eignen sich Tools wie zum Beispiel Sawmill (www.thesawmill.co.uk) oder Snortalog (jeremy.chartier.free.fr/snortalog).

Honeywall bietet noch weit mehr Möglichkeiten, als in diesem kurzen Workshop gezeigt werden kann. So kann das Programm bei Angriffen per E-Mail automatisch Alarm schlagen. Die Option dazu finden Sie unter *Honeywall Configuration, Alerting*. Der E-Mail-Alarm funktioniert nur, wenn Sie in den Firewall-Regeln ausgehende Verbindungen auf Port 25 erlauben und einen SMTP-Server haben, der Verbindungen von Ihrem Honeywall-System akzeptiert.

Mit dem hier beschriebenen Aufbau können Sie einen Hacker bei seinem Werk beobachten. Wenn der Angreifer aber seine Kommunikation verschlüsselt, dann haben

Sie von Ihren Beobachtungen nichts: Alles, was Sie zu sehen bekommen, ist kryptischer Zeichensalat. Eine Lösung für dieses Problem ist Sebek.

»Verschlüsselte Hacks knacken«

Sebek ist ein Client-Server-System zur Überwachung verschlüsselter Kommunikation. Auf Köder-Rechnern mit Linux können Sie Sebek als Kernel-Modul installieren. Das ermöglicht es, verschlüsselte Kommunikation an ihrem Endpunkt abzufangen, nachdem sie dechiffriert wurde. Für Windows gibt es einen Sebek-Client, der Interaktionen mit der Kommandozeile abfängt.

Honeywall arbeitet nahtlos mit Sebek zusammen. Die Honeywall-Bridge nimmt die Sebek-Pakete von den Honey-pots in Empfang und leitet sie an einen Sebek-Server weiter. Unter *Honeywall Configuration, Sebek* können Sie dessen IP einstellen.

Um zu verhindern, dass Ihr Honeypot als Basis für weitere Angriffe missbraucht wird, sollten Sie unter *Honeywall Configuration, Connection Limiting* die ausgehenden Verbindungen des Honey-pots begrenzen. Zudem kann Honeywall Traffic nicht nur blockieren oder protokollieren, sondern auch verändern. Damit erlauben Sie Hackern, weitere Angriffe von Ihrem System zu starten, die anscheinend auch funktionieren. Aber da das System die Datenpakete manipuliert, läuft der Angriff schließlich ins Leere. Sie aktivieren diese Option, indem Sie unter *Honeywall Configuration, Snort_inline* das *Snort_inline ruleset* auf *Replace* schalten. Und sollte ein Angreifer trotzdem einmal über die Stränge schlagen, können Sie unter *Honeywall Administration, Emergency Lockdown* den Not-Ausschalter drücken.

»Fazit«

Mit der Honeywall-CD gelingt es Ihnen, in wenigen Stunden einen eigenen Honeypot als Hackerfalle aufzusetzen. Sie können beliebige Köder-Computer anschließen, wodurch die Honey-pots sehr individuell und hoch interaktiv werden. Zudem können Sie die Aktivitäten des Angreifers detailliert beobachten und wirksam einschränken. Bevor Sie jedoch Ihr lehrreiches Hackquarium ins Internet stellen, sollten Sie das System im eigenen LAN ausgiebig ausprobieren.

[jp]

Links

Marktübersicht Honey-pots

BOF

Ein einfacher Honeypot unter Windows

► www.nfr.com/resource/backOfficer.php

Honeyd

Der beste Low-Interaction-Honey-pot unter Linux

► www.honeyd.org

cmdexe.pl

Honeyd mit simulierter Windows-Kommandozeile und als Boot-CD

► www.honeynet.org.br/tools

Symantec Decoy Server

Der professionelle High-Interaction-Honey-pot simuliert komplette Server

► www.symantec.de

Specter

Der beste Honeypot im Internet-Professionell-Vergleichstest vom März 2004

► www.specter.com

KF Sensor

Low-Interaction-Honey-pot mit Schnittstelle für eigene Erweiterungen

► www.keyfocus.net/kfsensor

Fake AP

Simuliert zehntausende WLAN-Access-Points, um Angreifer in die Irre zu führen

► www.blackalchemy.to/project/fakeap

Jackpot Mailserver

Täuscht Spammern einen offenen Mail-Server vor

► jackpot.uk.net

Labrea Tarpit

Dieser Low-Interaction-Honey-pot bremsst Angreifer aus

► www.hackbusters.net

Google Hack Honey-pot

Gut für Webmaster: simuliert angreifbare Skripts auf Webseiten

► ghh.sourceforge.net