HELPDESK

# Geheime Klopfzeichen

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.


ILLUSTRATION: CW/THÜ

**Frage: Was ist «Port knocking» und inwiefern erhöht dies die Sicherheit?**

Port knocking kann exponierte Dienste beziehungsweise Ports verstecken. Wenn aus operativen Gründen zum Beispiel ssh, ftp oder vpn zur Verfügung stehen, dauert es nicht lange, bis erste Portscans und Verbindungsversuche aus aller Welt eintreffen und die gut sortierten Logfiles verschmutzen.

Durch Port knocking manipuliert der Benutzer die Regeln einer Firewall: Schickt er eine geheime Sequenz aus Netzwerkpaketen, wird der gewünschte Port für seine IP-Adresse auf der Firewall dynamisch geöffnet; der gewünschte Dienst steht ihm nun zur Verfügung.

Port knocking ist Entwicklern von Rootkits und Trojanern bereits länger bekannt und wird nun auch zum Schutz von Systemen in Betracht gezogen. Doch einige Probleme erschweren die erfolgreiche Implementierung: Die manuelle Erzeugung einer sicheren Klopfsequenz ist keinem Normalsterblichen zumutbar und muss somit auf dem Client automatisiert werden. Zudem unterstützen die Firewalls aus der Fabrik noch kein Port knocking. Ein weiteres Hindernis taucht auf, wenn die Klopfsequenzen das Zielsystem nicht erreichen: Eine vorgeschaltete Firewall mit Stateful inspection wird TCP-Pakete mit seltsamen Flag-Kombinationen (hoffentlich) verwerfen. Nur naive Firewall-Administratoren würden solche nicht-konforme Pakete durchschleusen.

Bei der Prüfung einer Portknocking-Lösung ist auch zu beachten, wie sich das System verhält, wenn die Verbindung unerwartet abgebrochen wird. Bleibt der Port offen oder wird er nach einem Timeout geschlossen? Eine wachsende Zahl von Leichen im Firewall-Ruleset ist der Albtraum jedes Sicherheitsverantwortlichen.

> «Port knocking wird nun auch zum Schutz von Systemen in Betracht gezogen.»

Es dauert nicht lange, bis nach dem Stichwort «Port knocking» das geflügelte «Security through obscurity» fällt. Jedoch: Port knocking ist kein Authentifizierungsmechanismus! Ein durch diese Technik verborgener Dienst muss genau so sicher sein, wie ein ungeschützter. Ein Dienst mit Sicherheitslücken, durch Port knocking «geschützt»: Das ist tatsächlich «obscurity».

Die «advanced port knocking suite», http://www.iv2-technologies.com/~rbidou/ bietet einen guten Einstieg für angehende Port knocker. Das Perl-Script apks.pl lauscht auf die in der Datei apks.conf definierten Sequenzen. Sobald eine Sequenz abgearbeitet ist, wird ein Kommando auf dem System ausgeführt. Um zum Beispiel die Verbindung auf einen ssh Daemon zu erlauben, könnte im Falle einer iptables-Firewall das Kommando «iptables –I input_ext –p tcp –s %SOURCE –dport 22 –j ACCEPT» ausgeführt werden.

Unsere Tests deckten in der Datei apks.pl noch zwei Bugs auf: Das chop-Kommando in Zeile 382 sollte auskommentiert werden. Damit auch die Übergabe der Variable %SOURCE funktioniert, muss nach Zeile 368 folgender Befehl eingefügt werden:

«$cmd =~ s/%SOURCE/$prints[1]/;».

Als umfangreiche Ressource für Port knocking sei noch die Website portknocking.org erwähnt, hier finden sich weitere Implementierungen und Beispiele.

Derzeit ist Port knocking eher für Shell-Freaks und Systeme mit ausserordentlich hohem Schutzbedarf in Betracht zu ziehen. Dennoch wird eifrig weiter geklopft: Der aktuelle Trend geht nun in Richtung Onetime-Klopfsequenzen und hat damit bereits einen Fuss in der Kryptologie. Ob sich die Technik schlussendlich durchsetzt, liegt vermutlich in der Hand der Appliance-Hersteller. Zu Zeiten der Prohibition haben sich geheime Klopfzeichen jedenfalls als nützlich erwiesen, auch wenn sie keinen Schutz vor Razzien bieten konnten. ■

**Der Autor**
Simon Wepfer ist CTO und Consultant bei Oneconsult, Thalwil, www.oneconsult.com

**Unsere Experten beantworten Ihre Fragen.** Schreiben Sie uns: it-security@computerworld.ch

**Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch**