

Freier Analytiker fürs Netzwerk

Das Paketgeneratoren- und Analysetool Hping gehört in die Werkzeugkiste jedes Security Auditors. Die dritte Generation des Tools ist zwar offiziell erst im Alpha-Stadium. Sie bietet aber zahlreiche neue Möglichkeiten und lässt sich recht einfach erweitern, weshalb sich ein Blick darauf lohnt. VON SIMON WEPFER

Auf dem Gebiet der Netzwerkanalyse tummeln sich zahlreiche Werkzeuge unterschiedlicher Prägung. Bei Hping3 handelt es sich um einen Vertreter, der vom Benutzer die Bereitschaft abverlangt, in die Tiefe der Linux- oder Unix-Shell hinabzusteigen. Dann aber wird er mit einem mächtigen Funktionsumfang belohnt. Die Steuerung kann wie bei der Vorgängerversion über Befehlszeilen-Parameter erfolgen. Doch die Stärke der dritten Ausgabe und gleichzeitig wichtigste Neue-

rung zeigt sich erst in der interaktiven Shell. Dorthin gelangt der Anwender, wenn er Hping3 ohne Argumente aufruft. Diese Befehlsumgebung ist nämlich Skriptfähig und bietet dadurch mehr Möglichkeiten als das übergeordnete Ansteuern durch Perl- oder Shellscripsts. Der flexible Paketgenerator ist zum eigentlichen Security-Testing-Framework pubertiert: Hping3 integriert neben der eigenen Syntax die grafikfähige Skriptsprache Tcl/Tk (Tool Command Language/Toolkit).

Aller Anfang ist ping

Die grundlegende Arbeitsweise des Netzwerk-Tools lässt sich anhand der «ping»-Funktion veranschaulichen. Um eine ICMP-Meldung (Internet Control Message Protocol) abzusetzen, dient in der interaktiven Shell von Hping3 der folgende Befehl:

```
hping send "ip(daddr=192.168.1.1)+icmp".
```

Das interne Kommando «hping send» verschickt das Paket, welches in der APD-Form (Ars Packet Description) vorliegt. Diese ist besonders für erfahrene Hping2-Benutzer einfach zu verstehen. Wenn man in einem anderen Fenster etwa mit «tcpdump» den Verkehr beobachtet, sieht man, dass der Ping-Befehl erfolgreich war und der angesprochene Router eine Antwort lieferte:

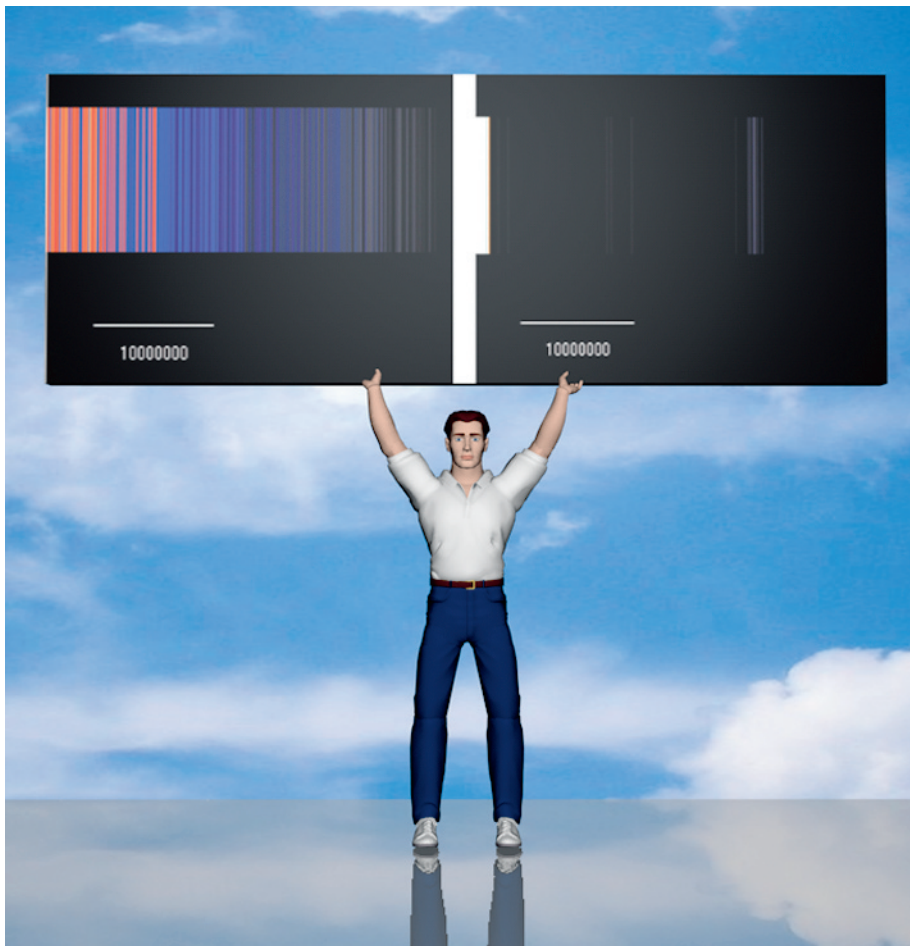
```
IP 192.168.1.34 > 192.168.1.1:
ICMP echo request, id 0, seq 0,
length 8
IP 192.168.1.1 > 192.168.1.34:
ICMP echo reply, id 0, seq 0,
length 8
```

Um ein Paket zu empfangen, dient das Kommando «hping recv <interface> [timeout] [packets-count]». Das Argument «timeout» ist optional und gibt die Zeit in Millisekunden an. Der Standardwert liegt bei -1 (unendlich). Wird «packets-count» weggelassen, wartet Hping3 nur ein einziges Paket ab. Die empfangenen Pakete werden anschliessend als Liste dargestellt.

Scripten eines Portscanners

Die obigen Beispiele lassen bereits erahnen, was in Hping3 steckt. Die wahren Stärken

Simon Wepfer ist CTO bei der Sicherheitsberaterin Oneconsult in Thalwil.



Eine gleichmässige Verteilung von Sequenznummern im Spektrogramm steht für höhere Sicherheit.

tauchen aber erst in Verbindung mit Tcl/Tk auf. Scripts können in einer externen Datei gespeichert werden und über folgende Syntax ausgeführt werden:

```
hping3 exec [script] [argumente...]
```

Als Beispiel wurde im Test ein einfacher Portscanner implementiert, der einen Rechner auf offene Ports untersucht. Hierzu dient das hier abgebildete Listing. Zuerst werden einige Variablen mit Standardwerten abgefüllt. Die Variable «ports» ist ein Array und definiert die zu testenden TCP-Ports. In diesem Beispiel kamen lediglich http (80) und https (443) zum Einsatz. Der Spass startet in Zeile 13, in der die Kommandozeilen-Argumente, also die zu testenden Hosts, in einer Schleife entgegen genommen werden. Mit der Funktion «puts» (Zeile 14) wird ein String ausgegeben. Danach legt das Skript die Absenderadresse für den Zielhost in «myaddr» ab und startet eine neue Schleife für jeden Port, den es zu scannen gilt.

Zeile 19 generiert nun ein Syn-Paket («flags=s») an den aktuellen Host und Port. Die Antwort nimmt in Zeile 21 die Variable «packets» entgegen. Die so eingefangenen Pakete werden nun ausgewertet, indem überprüft wird, ob ein Paket vom aktuell getesteten Host kommt (Zeile 24).

In den nächsten Zeilen überprüft der Scanner die gesetzten TCP-Flags. Erhält er ein «Syn-Ack», ist der Port gewillt, die Verbindung anzunehmen: Er ist also offen (Zeilen 26 bis 28). Hier setzt das Skript auch gleich für weitere Tests die «openport»-Variable. Bei einem Paket mit gesetztem Reset-Flag ist der Port geschlossen (Zeilen 30 bis 31). Erhält der Scanner keine Antwort, ist der Host entweder nicht erreichbar oder durch eine Firewall gefiltert. Zeile 38 überprüft, ob ein offener Port gefunden wurde. Hier könnte der Sicherheitspezialist nun weitere Systemtests einfügen, die einen offenen Port benötigen, wie etwa die Abfrage von TCP-Timestamps.

FAKTEN & BEWERTUNG

Hping3

Entwickler: Salvatore Sanfilippo und andere

Preis: Open-Source

Vorteile Schneller Zugriff auf Netzwerkbefehle, mit Skripten vielseitig erweiterbar.

Nachteile Recht hohe Einarbeitungszeit für Neueinsteiger.

www.hping.org

Sehr gut

5,5

Bewertungsschlüssel: 6 = Ausgezeichnet; 5,5 = Sehr gut; 5 = Gut; 4 = Genügend; 3 = Ungenügend; 2 = Mangelhaft; 1 = Schlecht

```

1 # hping3 scripting example
2 # (c) 2007 OneConsult GmbH
3
4 # set default values
5 set timeout 1000
6 set ports {80 443}
7 set ttl 30
8 set sport 80
9 set interface eth1
10 set maxpack 100
11
12 # scan hosts
13 foreach host $argv {
14   puts "host: $host"
15   set myaddr [hping outifa $host]
16   set openport {}
17   foreach {port} $ports {
18     # send syn-packets
19     hping send "ip(saddr=$myaddr,daddr=$host,ttl=$ttl)+tcp(sport=$sport,dport=$port,flags=s)"
20     # receive answer
21     set packets [hping rcv $interface $timeout $maxpack]
22     # process answer
23     foreach p $packets {
24       if {[string match "$saddr=$host*" $p]} {
25         switch -regexp $p {
26           flags=sa {
27             puts " $port: open"
28             set openport $port
29           }
30           flags=r {
31             puts " $port: closed"
32           }
33         }
34       }
35     }
36   }
37   # do other things with open ports
38   if {$openport != {}} {
39     # insert additional tests here
40   }
41 }

```

Vielseitig erweiterbares Tool: Mit einem einfachen Skript wird Hping3 zum Port-Scanner.

Natürlich besteht in diesem Script noch Optimierungbedarf, aber wer genug Zeit hat, kann sich mit Hping3 seinen eigenen Portscanner programmieren, ohne sich intensiv mit Netzwerkstacks herumschlagen zu müssen. Das Werkzeug stellt auch zahlreiche Standardfunktionen zur Verfügung, welche über das Statement «source hpingstdlib.htcl» eingebunden werden. Die referenzierte Datei wird mit dem Sourcecode mitgeliefert und residiert dort im Unterverzeichnis «lib».

ISN-Spektrogramm mit Tk

Mittels Tk können gar grafische Elemente oder grafische Oberflächen implementiert werden. Das komplexe Beispiel auf <http://wiki.hping.org/94> zeigt die Verwendung von Tcl/Tk für eine Spektralanalyse von initialen Sequenznummern (ISN). Die Flusskontrolle unter TCP verwendet Sequenznummern. Um unter anderem die Gefahr von Spoofing zu minimieren, verwirft ein Host Pakete mit ungültigen Sequenznummern. Gelingt es einem Angreifer jedoch, die Sequenznummer der nächsten Verbindung zu bestimmen (oder einzukreisen), kann er eine solche beenden, übernehmen oder den Host als Brückenkopf für Portscans auf andere Systeme missbrauchen (so genannte idle scans).

Das Skript schickt Syn-Pakete an einen offenen Port und analysiert die Sequenznummer des Syn-Ack-Paketes. Die Differenz zur vorherigen Sequenznummer trägt es im Spektrogramm ein. Kollidieren Werte, werden sie heller dargestellt. Dadurch lässt sich die Entropie der Sequenznummern optisch einschätzen. Im Idealfall zeigt die Spektralanalyse eine gleichmässige Verteilung.

Fazit: Komplex aber sehr nützlich

Hping3, das derzeit für Linux- und Unix-Systeme vorliegt, bietet mit seinen neuen Scripting-Funktionen enorme Möglichkeiten zur Erstellung und Automatisierung von Netzwerktests. Die zwei hier vorgestellten Anwendungen können beliebig erweitert und kombiniert werden. Die Unterstützung von Tcl/Tk ermöglicht die Visualisierung des Netzwerkverkehrs und die Einbindung weiterer grafischer Elemente und Benutzerinterfaces. Hping3 ist ein Tool, das ein Security-Tester – hat er es erst einmal näher kennen gelernt – freiwillig nicht mehr so schnell her gibt. ■

Die hier besprochenen Skripts, der Test sowie sämtliche Links sind auch auf der Computerworld-Website zu finden.

Alle Informationen auf:
www.computerworld.ch/testcenter