Sicurezza

39

ninux.org

Contents

1 Sicurezza

In una rete wired tradizionale, il controllo dell'accesso è molto semplice: Se una persona ha accesso fisico ad un calcolatore o hub della rete, allora può usare (o abusase) le risorse della rete. Mentre i meccanismi del software sono una componente importante di sicurezza della rete, limitare l'accesso fisico ai dispositivi della rete è l'ultimo meccanismo di controllo di accesso. Semplicemente, se tutti i terminali e i componenti della rete sono soltanto accessibili agli individui fidati, allora la rete può probabilmente considerarsi fidata.

Le cose cambiano significativamente con le reti wireless. Mentre l'apparente portata del vostro access point può sembrare influire giusto per alcune centinaia di metri, un utente con un' antenna di alto guadagno può potere usare la rete a partire da parecchi isolati di distanza. Se un utente non autorizzato è rilevato, è impossibile semplicemente *tracciare il cavo* indietro fino alla locazione dell'utente. Senza trasmettere un singolo pacchetto, un utente malintenzionato può persino scaricare il log di tutti i dati della rete sul disco. Questi dati possono più successivamente essere usati per lanciare un attacco più sofisticato contro la rete. Non assumere mai che le onde radio si *arrestino* semplicemente al limite della vostra proprietà.

Naturalmente, anche nelle reti wired, non è mai sufficientemente possibile fidarsi completamente di tutti gli utenti della rete. Impiegati scontenti, utenti della rete maleducati e semplici errori da parte di utenti onesti possono causare danni significativi al funzionamento della rete. Come progettista di rete, il vostro obiettivo dovrebbe essere di facilitare la comunicazione privata fra gli utenti legittimi della rete. Mentre una determinata quantità di controllo e di autenticazione di accesso è necessaria in tutta la rete, siete venuti a mancare nel vostro compito se gli utenti legittimi trovano difficile usare la rete per comunicare.

Un vecchio detto dice che l'unico modo di proteggere completamente un calcolatore è di disconnetterlo, chiuderlo in una cassaforte, distruggere la chiave e seppellire il tutto con calcestruzzo. Mentre un tal sistema potrebbe essere completamente *sicuro*, è inutile per la comunicazione. Ricordarsi soprattutto di ciò più che di altro quando prendete decisioni per la sicurezza della vostra rete, la rete esiste proprio per dare la possibilità ai suoi utenti di comunicare fra di loro. Le considerazioni di sicurezza sono importanti, ma non dovrebbero essere intese contro gli utenti della rete.

1.1 Sicurezza fisica

Nell'installare una rete, state costruendo un'infrastruttura dalla quale la gente dipenderà. E così, la rete deve essere affidabile. Per molte installazioni, i guasti che si presentano spesso sono dovuti alle manipolazioni umane, accidentali o no. Le reti hanno componenti fisiche, fili e contenitori, cose che possono essere disturbate facilmente. In molte installazioni, la gente non conoscerà le apparecchiature che avete installato, o, la curiosità le condurrà a sperimentare. Non si renderanno conto dell'importanza di un cavo collegato ad una porta. La gente potrebbe spostare un cavo Ethernet in modo da poter collegare il proprio portatile per 5 minuti, o spostare un interruttore per usufruirne. Una spina potrebbe essere rimossa da una sorgente di alimentazione perché qualcuno ha bisogno di quella presa a parete. Assicurare la sicurezza fisica di un'installazione è preminente. Segni ed etichette saranno soltanto utili ai pochi, che possono leggere, o parlare la vostra lingua. Mettere le cose lontane e limitare l'accesso sono il modo migliore per assicurare che gli incidenti, o le riparazioni siano evitate.

In economie meno sviluppate le giuste viti, connessioni elettriche, o contenitori non sono facili da trovare. Dovreste poter trovare rifornimenti elettrici alternativi che funzionano nello stesso modo. Le recinzioni personalizzate sono inoltre facili da produrre e dovrebbero essere considerate essenziali in tutta l'installazione. È spesso economico pagare un muratore per fare i fori ed installare un condotto, dove questa sarebbe un'operazione costosa nel mondo sviluppato, questo tipo di attività a forte utilizzo di mano d'opera può essere acquistabile nei paesi del sud. Il PVC può essere incorporato in pareti di cemento per far passare il cavo da una stanza ad un'altra, evitando fori profondi ogni volta che un cavo deve essere passato. Per isolare, sacchetti di plastica possono essere inseriti nel condotto intorno ai cavi.

Le piccole apparecchiature dovrebbero essere montate sulla parete e le più grandi dovrebbero essere messe in un armadio o in un armadietto.

1.1.1 Interruttori

Gli interruttori, gli hubs o gli access points interni con una presa a parete possono essere avvitati direttamente su una parete. Mettere questa apparecchiatura più alta possibile ridurrà la probabilità che qualcuno tocchi il dispositivo o i suoi cavi.

1.1.2 Cavi

I cavi dovrebbero essere nascosti e fissati. Meglio seppellire i cavi, che lasciarli liberi per una distanza lunga yard, durante le quali potrebbero essere usati per appendere vestiti ad asciugare, o semplicemente annodati ad una scala ecc. Per evitare i parassiti e gli insetti utilizzare un condotto elettrico di plastica. La spesa marginale val bene la pena. Il condotto dovrebbe essere sepolto a circa 30cm di profondità (sotto il gelo nei climi freddi). È inoltre consigliato comprare il più grande condotto disponibile al momento, in modo da poter utilizzare la stessa tubazione anche per i cavi futuri. È anche possibile trovare il condotto di plastica del cavo tra quelli che sono utilizzati per le costruzioni. In caso contrario, si può semplicemente fissare il cavo, inchiodandolo alla parete ed assicurandosi che esso non penda dove può essere annodato, intrappolato o tagliato.

1.1.3 Alimentazione

Tenere le sorgenti di alimentazione chiuse in un armadietto. Se ciò non è possibile, montare la sorgente di alimentazione sotto uno scrittorio, o sulla parete e usare doct tape (gaffer tape, un nastro adesivo forte) per fissare la spina nella presa a parete. Sull'UPS e sulla sorgente di alimentazione, non lasciare le prese a parete vuote, sigillarle se necessario. La gente ha la tendenza ad usare la presa a parete più facilmente raggiungibile, così è necessario rendere queste prese difficili da usare. Se non lo fate, potreste trovare un ventilatore o una luce inserita nella vostra UPS; benchè sia piacevole avere luce, è più piacevole mantenere il funzionamento del vostro server!

1.1.4 Acqua

Proteggere la vostra apparecchiatura da acqua e da umidità. In tutti i casi assicuratevi che la vostra apparecchiatura, compreso la vostra UPS è almeno a 30cm da terra, per evitare un allagamento. Inoltre provare a coprire con un tetto la vostra apparecchiatura, di modo che l'acqua e l'umidità non cadranno su di essa. Nei climi umidi, è importante che l'apparecchiatura abbia una ventilazione adeguata in modo da assicurare che l'umidità si esaurisca. Gli armadietti devono essere ventilati, o l'umidità ed il calore degraderanno o distruggeranno il vostro equipaggiamento.

1.1.5 Tralicci

L'apparecchiatura installata su un traliccio è spesso al sicuro dai ladri. Ciò nonostante, per dissuadere i ladri e mantenere la vostra apparecchiatura al sicuro dal vento è buona regola per un tecnico prendere le massime precauzioni. L'apparecchiatura dovrebbe essere verniciata con un colore opaco, bianco o grigio per riflettere il sole e per renderlo piatto e non interessante allo sguardo. Dovrebbero essere preferite le antenne del pannello che sono molto più sottili e meno interessanti dei dischi. Tutta l'installazione sulle pareti, dovrebbe richiedere una scaletta per raggiungerla. Nella scelta dei posti dove mettere l'apparecchiatura, trovarne di ben illuminati ma non in vista. Inoltre evitare le antenne che assomigliano alle antenne della televisione, perché sono articoli che attrarranno l'interesse dai ladri, dove invece un'antenna di wifi sarà inutile al ladro medio.

1.2 Minacce contro la rete

Una differenza sostanziale fra Ethernet e wireless è che le reti wireless sono costruite su un ***mezzo condiviso***. Assomigliano molto di più ai vecchi hubs della rete che ai commutatori moderni, in quanto ogni calcolatore connesso alla rete può *vedere* il traffico di ogni altro utente. Per controllare tutto il traffico della rete su un punto di accesso, ci si può sintonizzare semplicemente al canale che si sta usando, mettere la scheda della rete nella modalità per monitorare ed eseguire il log di ogni dato. Questi dati potrebbero essere direttamente utili ad un intercettatore (inclusi dati come email, dati voce, o logs di chat online). Possono anche contenere passwords ed altri dati sensibili, contribuendo a compromettere ancora ulteriormente la rete. Come vedremo più avanti in questo capitolo, questo problema può diminuire mediante l'uso della crittografia.

Un altro problema serio con le reti wireless è che i suoi utenti sono relativamente ***anonimi***. Mentre è vero che ogni dispositivo wireless include un indirizzo MAC univoco che è dato dal fornitore, questi indirizzi possono essere cambiati spesso con un software. Anche con l'indirizzo MAC, può essere molto difficile stabilire dove un utente wireless sia localizzato fisicamente. l'influenza in più direzioni, le antenne di alto guadagno e le ampie variazioni delle caratteristiche della radiotrasmittente possono rendere impossibile determinare se un utente wireless malintenzionato sia seduto nella stanza accanto o è in un appartamento di un palazzo lontano un miglio.

Mentre lo spettro non autorizzato fornisce un enorme riduzione dei costi dell'utente, esso ha lo sfavorevole effetto secondario degli attacchi ***denial of service*** (***DoS***) che sono banalmente semplici. Semplicemente girando su un access point ad alta potenza, un telefono cordless, un trasmettitore video, o altro dispositivo 2.4GHz, una persona malintenzionata potrebbe causare problemi significativi sulla rete. Molti dispositivi della rete sono vulnerabili ad altre forme di attacchi denial of service, di tipo per esempio disassociation flooding e overflows della tabella ARP.

Vi sono parecchie categorie di individui che possono causare i problemi su una rete wireless:

- ***Utente involontario***. Poichè la maggior parte delle reti wireless sono installate nelle zone densamente popolate, è comune per gli utenti di un portatile collegarsi casualmente alla rete errata. La maggior parte dei client wireless sceglieranno semplicemente ogni rete wireless disponibile quando la loro rete preferita non è disponibile. L'utente può allora usare questa rete come di consueto, completamente ignaro di trasmettere dati sensibili a qualcun'altro della rete. La gente malintenzionata può persino approfittare di questo installando gli access points in posizioni strategiche, per provare ad attrarre utenti inconsapevoli e per catturare i loro dati. Il primo punto per evitare questo problema sta nell'istruire i vostri utenti e sta nel sollecitare l'importanza di collegamento soltanto alle reti conosciute e fidate. Molti clients wireless possono essere configurati per collegarsi soltanto alle reti fidate, o per chiedere il permesso prima di collegarsi ad una nuova rete. Come vedremo più avanti in questo capitolo, gli utenti possono collegarsi in maniera sicura a reti aperte pubbliche usando la crittografia forte.
- ***War drivers***. Il fenomeno "war driving" deve il suo nome al popolare film hacker del 1983, "War Games". I war drivers sono interessati all'individuazione dell'ubicazione fisica delle reti wireless. Tipicamente girano in automobile con un portatile, un GPS e un'antenna omnidirezionale, annotando nome e posizione geografica di tutte le reti che trovano. Questi dati sono poi uniti ad altri dati di altri war drivers e sono trasformati in mappe grafiche che descrivono "l'impronta" wireless di una particolare città. La maggior parte dei war drivers probabilmente non propone minaccia diretta alle reti, ma i dati che raccolgono potrebbero essere di interesse a cracker della rete. Per esempio, potrebbe essere evidente che un access point non protetto rilevato da un war driver sia situato all'interno di un palazzo riservato, quali un governo o un ufficio corporativo. Una persona malintenzionata potrebbe usare queste informazioni per accedere illegalmente alla rete. Senza dubbio, in primo luogo un tale AP non dovrebbe essere mai installato, ma il war driving rende il problema ancora più grave. Come vedremo più avanti in questo capitolo, i war drivers che usano il popolare programma NetStumbler possono essere rilevati con i programmi quale Kismet. Per più informazioni sui war driving, vedere link come http://www.wifimaps.com/, http://www.nodedb.com/, o http://www.netstumbler.com/ .

- ***Rogue access points***. There are two general classes of rogue access points: those incorrectly installed by legitimate users, and those installed by malicious people who intend to collect data or do harm to the network. In the simplest case, a legitimate network user may want better wireless coverage in their office, or they might find security restrictions on the corporate wireless network too difficult to comply with. By installing an inexpensive consumer access point without permission, the user opens the entire network up to potential attacks from the inside. While it is possible to scan for unauthorized access points on your wired network, setting a clear policy that prohibits them is very important. The second class of rogue access point can be very difficult to deal with. By installing a high powered AP that uses the same ESSID as an existing network, a malicious person can trick people into using their equipment, and log or even manipulate all data that passes through it. Again, if your users are trained to use strong encryption, this problem is significantly reduced.
- ***Intercettatore***. Come accennato prima, l'intercettazione sulle reti wireless è un problema molto difficile da risolvere. Usando uno strumento di monitoraggio passivo (come Kismet), un intercettatore può scaricare tutti i dati della rete da una distanza grande, senza mai far rilevare la sua presenza. I dati con una debole cifratura possono essere scaricati e decifrati semplicemente più tardi, mentre i dati non cifrati possono essere letti facilmente in tempo reale. Se avete difficoltà a convincere gi altri di questo problema, potreste mostrare loro strumenti come Etherpeg (http://www.etherpeg.org/) o Driftnet (http://www.ex-parrot.com/~chris/driftnet/). Questi strumenti rappresentano una rete wireless con dati grafici, mediante file JPEG e GIF. Mentre gli altri utenti stanno navigando in Internet, questi stumenti visualizzano semplicemente tutti i grafici trovati in un unico collage grafico. L'utilizzo frequente di strumenti come questo sono la dimostrazione di quanto si dice sulla sicurezza wireless. Mentre potete dire ad un utente che la loro email è vulnerabile senza crittografia, niente raggiunge lo scopo meglio di mostrare loro le immagini di ciò che stanno guardando quando navigano con il loro web browser. Di nuovo, anche se non può completamente essere evitata, un'adeguata applicazione della crittografia forte scoraggerà l'intercettatore.

Questa introduzione vuole darti un'idea dei problemi a cui state andando incontro quando progettate una rete wireless. Più avanti in questo capitolo, parleremo degli strumenti e delle tecniche che vi aiuteranno a diminuire questi problemi.

1.3 Autenticazione

Prima dell'assegnazione dell'accesso alle risorse della rete, gli utenti dovrebbero in primo luogo essere ***autenticati***. In un mondo ideale, ogni utente wireless avrebbe un identificativo che è unico, non cambiabile e non può usabile da altri utenti. Questo è un problema molto difficile da risolvere nel mondo reale.

La prima utilità che abbiamo come unico identificativo è l'indirizzo MAC. Questo è un numero a 48 bit assegnato dal fornitore ad ogni dispositivo wireless e Ethernet. Impiegando il ***filtro mac*** sui nostri access points, possiamo autenticare gli utenti in base al loro indirizzo MAC. Con questa caratteristica, l'access point mantiene una tabella interna di indirizzi MAC autorizzati. Quando un utente wireless prova ad associarsi ad un access point, l'indirizzo MAC del client deve essere sulla lista autorizzata, o l'associazione sarà negata. Alternativamente, l'AP può mantenere una tabella di indirizzi MAC *dannosi* conosciuti, e consentire tutti i dispositivi che non sono sulla lista.

Purtroppo, questo non è il meccanismo ideale di sicurezza. Mantenere tabelle MAC su ogni dispositivo può essere scomodo, richiedendo che tutti i dispositivi client abbiano i loro indirizzi MAC registrati ed aggiornati sugli APs. Ancora peggio, spessogli indirizzi MAC possono essere cambiati con un software. Osservando gli indirizzi MAC in uso su una rete wireless, un aggressore risoluto può eseguire uno *spoofing* di un indirizzo MAC approvato e connettersi con successo all'AP. Mentre il filtro MAC eviterà gli utenti involontari e perfino la maggior parte dei individui curiosi dall'accesso alla rete, il filtro MAC da solo non può impedire gli attacchi degli aggressori risoluti.

I filtri MAC sono utili per limitare temporaneamente l'accesso dei client maleducati. Per esempio, se un portatile ha un virus che trasmette grandi quantità di spam o altro traffico, il suo indirizzo MAC può essere

aggiunto alla tabella del filtro per arrestare immediatamente il traffico. Questo vi darà tempo di rintracciare l'utente e di risolvere il problema.

Un'altra popolare utilità di autenticazione wireless è quella chiamata ***rete chiusa***. In una rete tipica, gli APs trasmetteranno in browcast il loro ESSID molte volte al secondo, permettendo che i client wireless (così come gli strumenti come NetStumbler) trovino la rete e visualizzino la sua presenza all'utente. In una rete chiusa, l'AP non segnala l'ESSID e gli utenti devono conoscere il nome completo della rete prima che l'AP permetta l'associazione. Ciò impedisce agli utenti casuali di scoprire la rete e di selezionarla nel loro client wireless.

Ci sono un certo numero di svantaggi in questa utilità. Forzare gli utenti a digitare il completo ESSID prima del collegamento alla rete induce all'errore e spesso conduce a sostenere chiamate e reclami. Poiché la rete non è ovviamente rilevabile da strumenti di indagine come NetStumbler, questo può impedire che la vostra rete sia mostrata sulle mappe dei war drivers. Ma significa anche che altri installatori di rete non possano trovarla facilmente e specificamente non sapranno che voi già state utilizzando una dato canale. Un vicino coscienzioso può effettuare un'indagine del luogo, non vedere reti vicine ed installare la sua propria rete sullo stesso canale che state utilizzando. Ciò causerà problemi di interferenza ad entrambi voi ed il vostro vicino.

Per concludere, usare le reti chiuse alla fine aggiunge poco alla vostra sicurezza generale delle reti. Usando strumenti di monitoraggio passivi (quale Kismet), un utente esperto può rilevare i pacchetti trasmessi dai vostri client leciti all'AP. Questi pacchetti necessariamente contengono il nome della rete. Un utente malintenzionato può allora usare questo nome per associarsi all'access point, proprio come un utente normale.

La crittografia è probabilmente il miglior strumento che abbiamo per autenticare gli utenti wireless. Con la crittografia forte, possiamo identificare univocamente un utente in modo che è molto difficile ingannarlo e usare quell'identità per determinare un ulteriore accesso alla rete. La crittografia inoltre ha il beneficio di aggiungere uno strato di privacy impedendo agli intercettatori di accedere facilmente al traffico di rete.

Il metodo di crittografia più ampiamente impiegato sulle reti wireless è la ***crittografia WEP***. WEP corrisponde a ***wired equivalent privacy*** ed è supportato virtualmente da tutta le apparecchiature 802.11a/b/g. Il WEP usa una chiave condivisa di 40 bit per cifrare i dati fra l'access point e il client. La chiave deve essere inserita sull'APs così come su ciascuno dei clients. Con il WEP abiliato, i clients wireless non possono collegarsi con l'AP fino a che non useranno la chiave corretta. Un intercettatore che ascolta una rete abilitata WEP vedrà ancora il traffico e gli indirizzi del MAC, ma il contenuto dei dati di ogni pacchetto è cifrato. Ciò fornisce un meccanismo ragionevolmente buono di autenticazione aggiungendo inoltre un po' di privacy alla rete.

Il WEP non è definitivamente la migliore soluzione di crittografia forte disponibile. Per prima cosa, la chiave di WEP è condivisa fra tutti gli utenti. Se la chiave v scoperta (diciamo, se un utente dice ad un amico qual'è la password, o un impiegato se ne va) allora cambiare la password può essere proibitivamente difficile, poiché deve essere cambiata in tutti gli APs e i dispositivi client. Ciò inoltre significa che gli utenti leciti della rete possono tranquillamente intercettare il traffico di tutti gli altri, poiché tutti conoscono la chiave condivisa.

La chiave stessa spesso è scelta male, rendendo fattibili i tentativi offline di crack. Ancora peggio, l'implementazione del WEP stesso non è funzionante in molte implementazioni, rendendo ancora più facile eseguire il crack su alcune reti. Mentre i fornitori hanno implementato un certo numero di estensioni a WEP (come quelle con le chiavi più lunghe e gli schemi veloci di rotazione), queste estensioni non fanno parte degli standard e non c'è interoperabilità fra apparecchiature di fornitori differenti. Aggiornando tutti i vostri dispositivi wireless con i firmware più recenti, potete impedire alcuni degli attacchi iniziali trovati in WEP.

Il WEP può ancora essere uno strumento utile di autenticazione. Assumendo che i vostri utenti siano fidati e non diano ad altri la password, voi potete essere ragionevolmente certi che i vostri client wireless siano al sicuro. Anche se il craking del WEP è possibile, è al di là dell'abilità della maggior parte dei utenti. Il WEP è estremamente utile per la sicurezza dei collegamenti interurbani Punto-a-Punto, anche sulle reti generalmente aperte. Usando il WEP su un tale collegamento, scoraggerete altri all'associazione e al collegamento, molto

probabilmente useranno altri APs disponibili. Il WEP è definitivamente un pratico modo per far *stare alla larga* gli utenti dalla vostra rete. Chiunque rilevi la rete vedrà che è richiesta una chiave, indicando chiaramente che non sono benvenuti ad usarla.

La forza più grande del WEP è l'interoperabilità. Per aderire agli standard, tutti i dispositivi wireless supportano di base il WEP. Anche se non è il metodo più sicuro disponibile, è certamente l'utilità più comunemente implementata. Analizzeremo più avanti altre tecniche più avanzate di crittografia in questo capitolo.

Per maggiori particolari circa lo stato della crittografia di WEP, vedere questi contenuti:

- http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- http://www.cs.umd.edu/~waa/wireless.pdf
- http://www.crypto.com/papers/others/rc4_ksaproc.ps

Un altro protocollo di autenticazione di strato di data link è il ***Wi-Fi Protected Access***, o ***WPA***. WPA è stato creato specificamente per occuparsi dei problemi WEP conosciuti accennati precedentemente. Fornisce uno schema significativamente più forte di crittografia e può usare una chiave privata condivisa, chiavi uniche assegnate ad ogni utente, o persino certificati SSL per autenticare sia il client che il suo access point. Le credenziali di autenticazione sono controllate usando il protocollo 802.1X, che può consultare una base dati di terze parti come RADIUS. Con l'uso del Temporal Key Integrity Protocol (TKIP), le chiavi possono essere ruotate rapidamente col tempo, riducendo ulteriormente la probabilità che una sessione particolare possa essere sottoposta a crack. In generale, WPA fornisce autenticazione e privacy significativamente migliori dello standardWEP.

La difficoltà con WPA è che, come in questo scritto, l'interoperabilità fra fornitori è ancora molto bassa. WPA richiede hardware dell'access point piuttosto recenti e firmware aggiornati su tutti i client wireless, così come un lavoro notevole di configurazione. Se state installando una rete in un'ambiente in cui controllate l'intera piattaforma hardware, WPA può essere ideale. Autenticare sia client che APs, risolve il problema dell'access point del rogue e fornisce molti vantaggi significativi rispetto al WEP. Ma nella maggior parte degli ambienti della rete in cui l'hardware è piuttosto vecchio e la conoscenza degli utenti wireless è limitata, l'installazione di un WPA può essere un incubo. È per questo motivo che se la crittografia non è usata affatto, la maggior parte dei siti continuano ad usare WEP.

1.3.1 Captive portals

Uno dei più comuni strumenti di autenticazione utilizzati sulle reti wireless è il ***captive portal***. Un captive portal usa un web browser standard per dare ad un utente wireless l'occasione di presentare le credenziali al momento del login. Può anche essere usato per presentare le informazioni (come un Acceptable Use Policy) all'utente prima di concedere l'accesso remoto. Usando un web browser anziché un programma personalizzato per l'autenticazione, i captive portals funzionano virtualmente con tutti i portatili e sistemi operativi. I captive portals sono usati tipicamente sulle reti aperte senza altri metodi di autenticazione (quali i filtri WEP o MAC).

Per cominciare, un utente wireless apre il suo portatile e seleziona la rete. Il suo computer chiede un DHCP lease, che è assegnato. Dopo di che può usare il suo web browser per andare in tutti i siti su Internet.

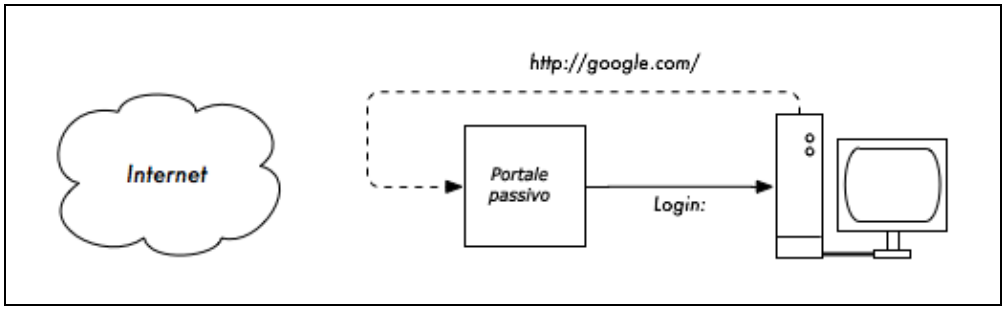

Figura 6.1: L'utente richiede una pagina web ed è reindirizzato.

Invece di ricevere la pagina richiesta, all'utente è presentata una videata di login. Questa pagina può richiedere all'utente di digitare un nome e una password, di cliccare semplicemente su un bottone di *login*, di digitare i numeri di un ticket prepagato, o di immettere tutte le altre credenziali che gli amministratori della rete richiedono. L'utente allora immette le sue credenziali, che sono controllate dall'access point o da un altro server sulla rete. Ogni accesso alla rete è bloccato fino a quando non si verificano queste credenziali.

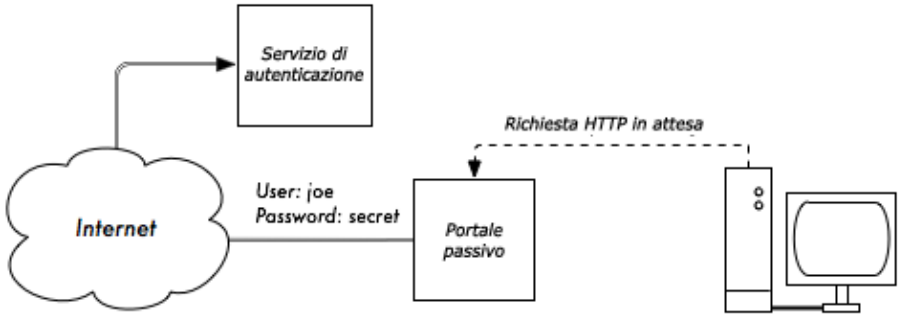

Figura 6.2: Le credenziali dell'utente sono verificate prima che accesso di rete remoto sia assegnato. Il server di autenticazione può essere l'accesss point stesso, un'altra macchina sulla rete locale, o un server dovunque su Internet.

Una volta autenticato, all'utente è permesso di accedere alle risorse della rete e tipicamente è reindirizzato al sito originalmente richiesto.

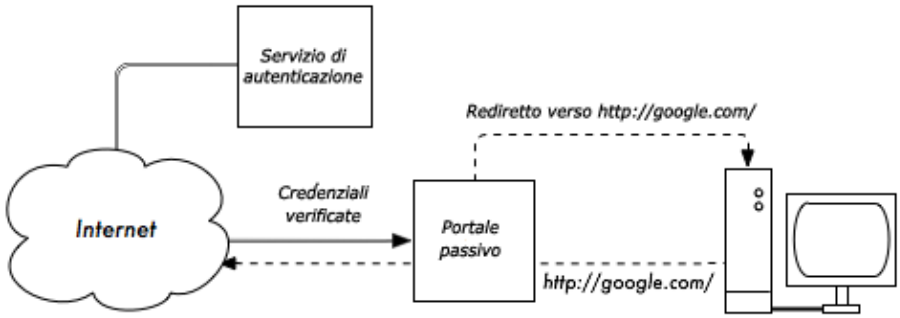

Figura 6.3: Dopo l'autenticazone, all'utente è consentito di accedere al resto della rete.

I captive portals non forniscono crittografia agli utenti wireless, ma invece si può contare sugli indirizzi MAC e IP del client come unico identificatore. Poiché questo non è necessariamente molto sicuro, molte implementazioni richiederanno all'utente di autenticarsi nuovamente periodicamente. Ciò può essere fatto spesso automaticamente minimizzando una finestra speciale di pop-up nel browser quando l'utente entra la prima volta.

Poiché non forniscono crittografia forte, i captive portals non sono una scelta molto buona per le reti che hanno bisogno di essere bloccate per permettere soltanto l'accesso agli utenti fidati. Sono molto più adatti ai caffè, agli hotel e ad altre posizioni pubbliche di accesso dove sono previsti solo utenti casuali nella rete.

Negli ambiente pubblici o semi-pubblici di rete , le tecniche di crittografia quale WEP e WPA sono del tutto inutili. Non c'è un modo semplice di distribuire le chiavi pubbliche o condivise a membri di un grande pubblico senza compromettere la sicurezza di quelle chiavi. In questi ambienti, un'applicazione semplice come un captive portal fornisce un livello intermedio di servizio fra il completamente aperto e il

completamente chiuso.

Due popolari implementazioni di captive portal open source sono NoCatSplash e Chillispot.

1.3.1.1 NoCatSplash

Se dovete fornire semplicemente agli utenti una rete aperta con informazioni e un accettabile uso della policy, date un'occhiata a NoCatSplash. È accessibile online al link http://nocat.net/download/NoCatSplash/ .

NoCatSplash fornisce ai vostri utenti una schermata personalizzabile di caricamento, richiedendo loro di cliccare un bottone *login* prima di usare la rete. Ciò è utile per identificare gli operatori della rete e visualizzare le regole per l'accesso di rete.

NoCatSplash è scritto in C e funzionerà su quasi ogni sistema operativo Unix compreso Linux, BSD e perfino piattaforme embedded come OpenWRT. Ha un semplice file di configurazione e può fornire ogni file HTML personalizzato come schermata di caricamento. Tipicamente funziona direttamente sull'access point, ma può anche lavorare su un router o su un proxy server. Per più informazioni, vedere http://nocat.net/ .

1.3.1.2 Altri popolari progetti hotspot

NoCatSplash is just one simple captive portal implementation. Many other free implementations exist that support a diverse range of functionality. Some of these include:

- Chillispot (http://www.chillispot.org/). Chillispot is a captive portal designed to authenticate against an existing user credentials database, such as RADUIS. Combined with the application phpMyPrePaid, pre-paid ticket based authentication can be implemented very easily You can download phpMyPrePaid from http://sourceforge.net/projects/phpmyprepaid/.
- WiFi Dog (http://www.wifidog.org/). WiFi Dog provides a very complete captive portal authentication package in very little space (typically under 30kb). From a user's perspective, it requires no pop-up or javascript support, allowing it to work on a wider variety of wireless devices.
- m0n0wall (http://m0n0.ch/wall/). As mentioned in chapter five, m0n0wall is a complete embedded operating system based on FreeBSD. It includes a captive portal with RADIUS support, as well as a PHP web server.

1.4 Privacy

La maggior parte dei utenti sono beatamente ignari del fatto che le loro email, conversazioni di chat e perfino password riservate siano trasmessi spesso *in chiaro* in dozzine di reti non protette prima di arrivare alla loro ultima destinazione su Internet. Non ci può essere niente di più errato, tipicamente gli utenti ancora hanno una certa aspettativa di privacy quando usando le reti di computer.

La privacy può essere realizzata, anche su reti non protette come access points pubblici ed Internet. L'unico metodo efficace provato per la protezione della privacy è l'uso di una forte ***crittografia end-to-end***.

Le tecniche di crittografia come WEP e WPA tentano di indirizzare il problema della privacy al secondo strato, lo strato data-link. Mentre questo protegge dagli intercettatori che ascoltano sul collegamento wireless, la protezione finisce all'access points. Se il client wireless usa protocolli insicuri (come POP o semplice SMTP per la ricezione e la trasmissione delle email), allora gli utenti dietro l'AP possono ancora scaricare i dati di sessione e vedere dati sensibili. Come accennato precedentemente, WEP inoltre soffre del fatto di usare una chiave privata condivisa. Questo significa che gli utenti wireless legittimi possono ascoltarsi di nascosto a vicenda, poiché tutti conoscono la chiave privata.

Usando la crittografia alla fine remota del collegamento, gli utenti possono evitare con cura l'intero problema. Queste tecniche funzionano bene anche su reti pubbliche non protette, in cui gli intercettatori stanno

ascoltando e possibilmente persino stanno maneggiando i dati che vengono dall'access point.

Per accertare la privacy dei dati, una buona crittografia end-to-end dovrebbe fornire le seguenti caratteristiche:

- ***Autenticazione verificata alla fine remota***. L'utente dovrebbe sapere senza dubbio che alla fine del collegamento remoto c'è chi sostiene di essere. Senza autenticazione, un utente potrebbe dare dati sensibili a chiunque sostenga essere il servizio legittimo.
- ***Metodi di crittografia forte***. L'algoritmo di crittografia dovrebbe resistere all'esame accurato pubblico e non dovrebbe essere decifrato facilmente da terzi. Non c'è privacy nell'oscurità e la crittografia forte è ancora più forte quando l'algoritmo è ampiamente conosciuto e conforme alla revisione paritaria. Un buon algoritmo con una chiave adeguatamente grande e protetta può fornire una crittografia difficile da decifrare con qualunque sforzo nel corso della nostra vita usando la tecnologia corrente.
- ***Crittografia a chiave pubblica***. Sebbene non sia un requisito assoluto della crittografia end-to-end, l'uso della crittografia a chiave pubblica anziché di una chiave condivisa può assicurare che i dati dell'utente specifico rimangano privati, anche se la chiave di un altro utente del servizio viene compromessa. Inoltre risolve determinati problemi con la distribuzione delle chiavi agli utenti sulle reti non protette.
- ***Incapsulamento dei dati***. Un buon meccanismo end-to-end di crittografia protegge tanti dati quanti ne sia possibile. Ciò può variare dalla cifratura della singola email in una transazione all'incapsulamento di tutto il traffico IP, compreso i lookups DNS ed di altri protocolli supportati. Alcuni strumenti di crittografia forniscono semplicemente un canale sicuro che altre applicazioni possono utilizzare. Ciò permette ad ogni utente di far girare il programma desiderato ed ancora avere la protezione della crittografia forte, anche se i programmi stessi non la supportano.

Siate consci che le leggi che riguardano l'uso della crittografia variano ampiamente da un posto ad un altro. Alcuni paesi trattano la crittografia come un'arma e possono richiedere un permesso, il deposito delle chiavi private, o persino la proibizione del suo uso del tutto. Prima di implementare qualsiasi soluzione che coinvolga la crittografia, verificate che l'uso di questa tecnologia sia consentito nella vostra zona locale.

Nelle seguenti sezioni, daremo un'occhiata ad alcuni strumenti specifici che possono assicurare una buona protezione ai dati dei vostri utenti.

1.4.1 SSL

La tecnologia di crittografia end-to-end più ampiamente disponibile è il ***Secure Sockets Layer***, conosciuto semplicemente come ***SSL***. Supportato virtualmente in tutti i web browsers, l'SSL usa la crittografica a chiave pubblica e una ***public key infrastructure*** (***PKI***) fidata per assicurare la comunicazione di dati sui siti web. Ogni volta che visitate un URL del web che comincia con https, state usando SSL.

L'implementazione dell'SSL sviluppata nei web browsers include una collezione di certificati di fonti affidabili, denominata ***certificate authorities*** (***CA***). Questi certificati sono chiavi crittografiche usate per verificare l'autenticità dei siti web. Quando visualizzate un sito web che usa SSL, prima di tutto il browser e il server si scambiano i certificati. Il browser allora verifica che il certificato fornito dal server corrisponda al suo nome del DNS host, che non sia scaduto e che sia firmato da un Certificate Authority di fiducia. Il server opzionalmente verifica l'identità del certificato del browser. Se i certificati sono approvati, il browser e il server allora negoziano una chiave master di sessione usando i certificati precedentemente scambiati per proteggerla. Quella chiave poi è usata per cifrare tutte le comunicazioni fino a quando il browser non si disconnette. Questo genere di incapsulamento di dati è conosciuto come ***tunnel***.

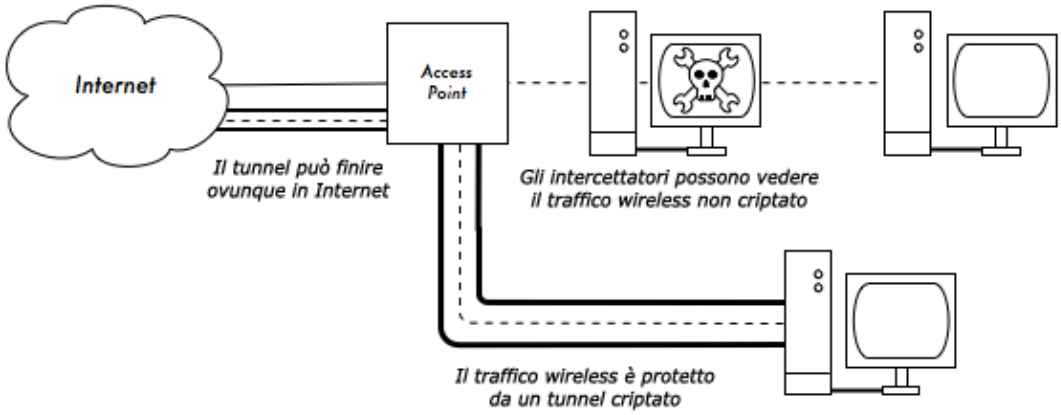

Figura 6.4: Gli intercettatori devono decifrare la crittografia forte per monitorare il traffico nel tunnel cifrato. La conversazione all'interno del tunnel è identica a qualunque altra conversazione non cifrata.

L'uso dei certificati con PKI non solo protegge la comunicazione dagli intercettatori, ma impedisce gli attacchi ***man-in-the-middle*** (***MITM***). In un attacco man-in-the-middle, un utente malintenzionato intercetta tutta la comunicazione fra il browser e il server. Presentando certificati falsi sia al browser che al server, l'utente malintenzionato potrebbe mantenere due sessioni cifrate simultanee. Poiché l'utente malintenzionato conosce il segreto su entrambi i collegamenti, è inutile osservare e maneggiare i dati che passano fra l'assistente ed il browser.

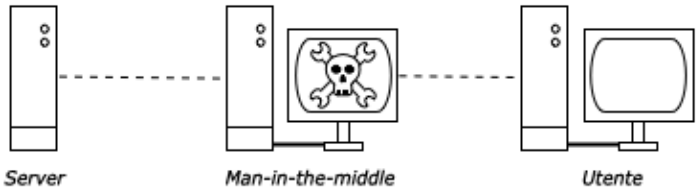

Figura 6.5: L'attacco man-in-the-middle controlla efficacemente tutto quello che l'utente vede e può registrare e maneggiare tutto il traffico. Senza un'infrastruttura a chiave pubblica per verificare l'autenticità delle chiavi, la crittografia forte da sola non può proteggere da questo genere di attacco.

L'uso di una buona PKI impedisce questo genere di attacco. Per riuscire, l'utente malintenzionato dovrebbe presentare un certificato al cliente che è firmato da un Certificate Authority di fiducia. A meno che un CA non si comprometta (molto improbabile) o l'utente sia ingannato nell'accettare il certificato falso, allora un tale attacco non è possibile. Ecco perché è estremamente importante che gli utenti capiscano che ignorare gli avvertimenti circa i certificati scaduti o falsi è molto pericoloso, particolarmente quando si usano le reti wireless. Cliccando sul tasto *ignora* presentato dal loro browser, gli utenti si aprono ad attacchi estremamente potenziali.

L'SSL non solo è usato per il web browsing. Un protocollo email non sicuro come IMAP, POP e SMTP può essere reso sicuro spostandolo in un tunnel SSL. La maggior parte dei clients di email moderni supportano IMAPS e POPS (IMAP e POP sicuri) come pure SMTP protetto da SSL/TLS. Se il vostro email server non fornisce il supporto SSL, potete ancora renderlo sicuro con SSL usando un pacchetto come Stunnel (http://www.stunnel.org/). L'SSL può essere usato per rendere sicuro efficacemente ogni servizio che gira su TCP.

1.4.2 SSH

La maggior parte della gente pensa a SSH come sostituto sicuro del **`telnet`**, esattamente come **`scp`** e **`sftp`** sono le controparti sicure di **`rcp`** e **`ftp`**. Ma SSH è molto di più di una shell remota cifrata. Come l'SSL, usa la crittografia forte a chiave pubblica per verificare il server remoto e per cifrare i dati. Anziché una PKI, usa una cache con l'impronta digitale della chiave che è controllata prima di consentire un collegamento. Può usare passwords, chiavi pubbliche, o altri metodi per l'autenticazione dell'utente.

Molta gente non sa che SSH può anche fungere da tunnel di cifratura per tutti gli usi, o persino da web proxy cifrato. Prima di ogni cosa protocolli insicuri possono essere protetti dalle intercettazioni e dagli attacchi stabilendo un collegamento SSH ad una posizione affidabile vicina (o persino sopra) ad un server remoto.

Mentre questa tecnica può essere una po' troppo avanzata per molti utenti, gli architetti della rete possono usare SSH per cifrare il traffico attraverso collegamenti non affidabili, come i punti Punto-a-Punto wireless. Poiché gli strumenti sono liberamente disponibili e girano sotto lo standard TCP, ogni utente preparato può implementare collegamenti SSH per se, fornendo la propria crittografia end-to-end senza l'intervento dell'amministratore.

OpenSSH (http://openssh.org/) è probabilmente l'implementazione più popolare sulle piattaforme UNIX-like. Implementazioni free come Putty (http://www.putty.nl/) e WinSCP (http://winscp.net/) sono disponibili per Windows. OpenSSH inoltre funzionerà su Windows sotto il pacchetto di Cygwin (http://www.cygwin.com/). In questi esempi si assume che stiate usando una versione recente di OpenSSH.

Per realizzare un tunnel cifrato da una porta sulla macchina locale ad una porta sulla parte remota, usare l'opzione **-L**. Per esempio, supponiamo di voler dirottare il traffico del web proxy su un collegamento cifrato dello squid server a squid.example.net. Dirottare alla porta 3128 (la porta di default del proxy) usando questo comando:

```
ssh -fN -g -L3128:squid.example.net:3128 squid.example.net
```

L'opzione **-fN** del comando ssh esegue un fork in background dopo il collegamento. L'opzione **-g** permette ad altri utenti di collegarsi sul vostro segmento locale alla macchina locale ed usarla per la crittografia sul collegamento non affidabile. OpenSSH userà una chiave pubblica per l'autenticazione se ne avete installata una, o chiederà la vostra parola d'accesso dalla parte remota. Potete allora configurare il vostro web browser per collegarvi alla porta 3128 di localhost come suo servizio web proxy. Tutto il traffico web allora sarà cifrato prima della trasmissione verso la parte remota.

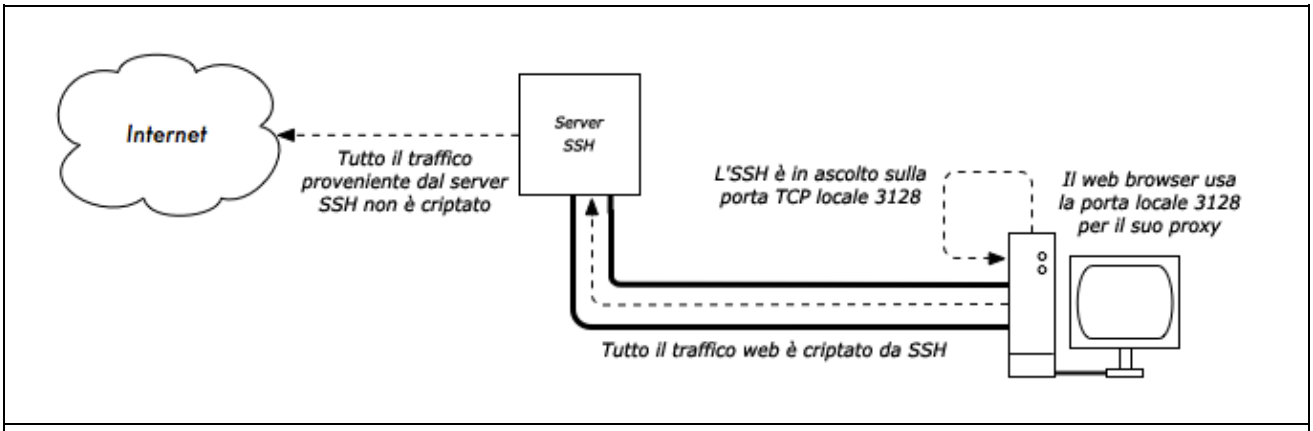

Figura 6.6: l tunnel SSH protegge il traffico web traffic fino al server SSH stesso.

SSH può anche fungere da proxy dinamico SOCKS4 o SOCKS5. Ciò permette di creare un web proxy cifrato,

senza la necessità di installare uno squid. Notare che questa non è un caching proxy; semplicemente si limita a cifrare tutto il traffico.

```
ssh -fN -D 8080 remote.example.net
```

Configurate il vostro web browser per usare SOCKS4 o SOCKS5 sulla porta locale 8080 e dimenticatevene.

SSH può cifrare i dati su ogni porta TCP, comprese le porte usate per le email. Può persino comprimere i dati lungo il percorso, che può far diminuire la latenza sui collegamenti a bassa capacità.

```
ssh -fNCg -L110:localhost:110 -L25:localhost:25 mailhost.example.net
```

L'opzione **-C** attiva la compressione. Potete aggiungere quante regole volete di inoltro nella porta specificando tante volte l'opzione **-L**. Notare che per collegarvi ad una porta locale minore di 1024, dovete avere permessi di root sulla macchina locale.

Questi sono giusto alcuni esempi della flessibilità di SSH. Implementando chiavi pubbliche ed usando l'agente di inoltro ssh, potete automatizzare la creazione di tunnel cifrati durante la vostra rete wireless e proteggere le vostre comunicazioni con la crittografia e l'autenticazione forti.

1.4.3 OpenVPN

OpenVPN è un'implementazione open source e free costruita sulla cifratura SSL. Ci sono implementazioni del client OpenVPN per una vasta gamma dei sistemi operativi, compreso Linux, Windows 2000 /XP e versioni maggiori, OpenBSD, FreeBSD, NetBSD, Mac OS X e Solaris. Essendo un VPN, esso incapsula tutto il traffico (compresi DNS e tutti i altri protocolli) in un tunnel cifrato, non solo in una singola porta TCP. La maggior parte della gente lo trova considerevolmente più facile da capire e configurare di IPSEC.

OpenVPN presenta anche alcuni svantaggi, come una latenza piuttosto alta. Una certa quantità di latenza è inevitabile in tutti i sistemi di cifratura/decifratura fatti nello spazio utente, ma si può minimizzare usando calcolatori di ultima generazione su entrambe le estremità del tunnel. OpenVPN può usare chiavi condivise tradizionali, ma realmente brilla quando è usato con i certificati SSL e un certificate authority. OpenVPN presenta molti vantaggi che garantiscono una buona affidabilità nel fornire la sicurezza end-to-end.

- È basato su un protocollo cifrato testato e robusto (SSL e RSA)
- È abbastanza facile da configurare
- Funziona su molte piattaforme differenti
- È ben documentato
- È free ed open source.

Come SSH e SSL, OpenVPN deve collegarsi ad una singola porta TCP dal lato remoto. Una volta collegato, può incapsulare tutti i dati attraverso lo strato di rete, o persino attraverso lo strato di Data-Link, se la vostra soluzione lo richiede. Potete usarli per creare collegamenti VPN robusti fra diverse macchine, o usarlo semplicemente per collegare routers di rete su reti wireless non protette.

La tecnologia VPN è un campo complesso ed è ben oltre la portata di questa sezione. È importante capire come i VPNs trovino posto nella struttura della vostra rete per assicurare la migliore protezione possibile senza aprire la vostra organizzazione a problemi involontari. Ci sono molte buone risorse online che si occupano dell'installazione di OpenVPN su un server e su un client, Io raccomando questo articolo del giornale Linux: http://www.linuxjournal.com/article/7949 così come l'ufficiale HOWTO: http://openvpn.net/howto.html

1.4.4 Tor & Anonymizers

Internet è principalmente una rete aperta basata sulla fiducia. Quando vi collegate ad un web server attraverso Internet, il vostro traffico attraversa molti routers differenti, gestiti da una grande varietà di istituzioni, di società e di individui. In linea di principio, uno qualunque di questi routers ha la capacità di osservare molto attentamente i vostri dati, vedendo come minimo la sorgente e gli indirizzi di destinazione ed abbastanza spesso anche il contenuto reale dei dati. Anche se i vostri dati sono cifrati usando un protocollo sicuro, per il vostro fornitore Internet è possibile controllare la quantità di dati della sorgente e la destinazione di quei dati. Questo è spesso abbastanza per avere un'immagine ragionevolmente completa delle vostre attività in linea.

La privacy e l'anonimato sono importanti e collegati molto strettamente l'uno all'altro. Ci sono molti validi motivi per considerare la possibilità di proteggere la vostra privacy e il vostro traffico di rete con un ***anonimizzante***. Supponete di voler offrire la connettività di Internet alla vostra Comunità locale installando un certo numero di access point affinché la gente ci si colleghi. Indipendentemente dal fatto che vi facciate pagare gli accessi o no, c'è sempre il rischio che nell'uso della rete ci sia qualcosa che non sia legale nel vostro paese o regione. Potreste spiegare al sistema legislativo che questa particolare azione illegale non è stata realizzata da voi, e che potrebbe essere stata effettuata da chiunque si sia connesso alla vostra rete. Il problema è evitato nettamente se fosse tecnicamente non fattibile determinare dove realmente è partito il vostro traffico. E cosa dire circa la censura online? Pubblicare pagine web anonimamente può anche essere necessario per evitare la censura del governo.

Ci sono strumenti che vi permettono di rendere anonimo il vostro traffico in modo relativamente facile. La combinazione del ***Tor*** (http://tor.eff.org/) e del ***Privoxy*** (http://www.privoxy.org/) è un modo potente di far girare un proxy server locale che passerà il vostro traffico Internet tramite un certo numero di servers attraverso tutta la rete, rendendo molto difficile seguire la traccia delle informazioni. Il tor può girare su un pc locale, sotto Microsoft Windows, Mac OSX, Linux e una varietà di BSD, dove esso rende anonimo il traffico dal browser su quella macchina particolare. Tor e Privoxy possono anche essere installati su un server gateway, o persino su un piccolo access point embedded (come un Linksys WRT54G) dove si fornisce automaticamente l'anonimato a tutti gli utenti della rete.

Il Tor lavora rimbalzando ripetutamente i vostri collegamenti TCP attraverso un certo numero di servers dispiegati sotto Internet e spostando le informazioni di percorso in un certo numero di strati cifrati (da qui il termine ***onion routing***), che spuntano fuori mentre il pacchetto si muove attraverso la rete. Ciò significa che, dato un qualsiasi punto nella rete, la sorgente e gli indirizzi di destinazione non possono essere collegati insieme. Ciò rende l'analisi di traffico estremamente difficile.

L'esigenza di privacy del proxy Privoxy in relazione al Tor nasce dal fatto che le ricerche del nome del server (ricerca DNS) nella maggior parte dei casi non passano attraverso il proxy server e qualcuno che analizza il vostro traffico potrebbe facilmente vedere che stavate provando a raggiungere un luogo specifico (diciamo *google.com*) dal fatto che avete trasmesso una ricerca DNS per convertire google.com nel suo specifico indirizzo IP. Privoxy si collega al Tor come SOCKS4a proxy, che usa gli hostnames (non indirizzi IP) per indirizzare i vostri pacchetti alla destinazione progettata.

In altre parole usare Privoxy con il Tor è un modo semplice ed efficace per impedire l'analisi del traffico tramite il collegamento del vostro indirizzo IP ai servizi che usate online. Unito con i sicuri, protocolli cifrati (come quelli che abbiamo visto in questo capitolo), Tor e Privoxy forniscono un alto livello di anonimato su Internet.

1.5 Monitoraggio

Le reti di computers (e in particolare le reti wireless) sono invenzioni incredibilmente utili e divertenti. Tranne, naturalmente, quando non funzionano. I vostri utenti possono protestare che la rete è *lenta* o *sconnessa* ma che cosa realmente significa questo? Senza visione di che cosa realmente sta accadendo, amministrare una rete può essere molto frustrante.

Per essere un coordinatore della rete efficace, avete bisogno dell'accesso agli strumenti che mostrano esattamente che cosa sta accadendo sulla vostra rete. Ci sono varie classi di strumenti di monitoraggio. Ciascuno mostra un differente aspetto di che cosa *sta andando*, dall'interazione radiofonica fisica in tutto il percorso a come le applicazioni dell'utente interagiscono a vicenda. Guardando come la rete cambia col tempo, potete farvi un'idea di che cosa è *normale* per la vostra rete e perfino ricevere una notifica automaticamente quando le cose sembrano essere fuori dall'ordinario. Gli strumenti elencati in questa sezione sono tutti abbastanza potenti e sono liberamente disponibili al download dalle sorgenti elencate.

1.5.1 Rilevamento reti

I più semplici strumenti di monitoraggio wireless forniscono semplicemente una lista di reti disponibili, con le informazioni di base (come l'intensità e il canale del segnale). Essi rilevano rapidamente le reti vicine e determinano se sono nella gamma o stanno causando interferenza.

- **Il client incluso**. Tutti i moderni sistemi operativi forniscono incluso il supporto per le reti wireless. Ciò include tipicamente la possibilità di esplorare le reti disponibili, permettendo che l'utente scelga una rete da una lista. Mentre virtualmente è garantito che tutti i dispositivi wireless abbiano un semplice programma di utilità di scansione, la funzionalità può variare ampiamente fra le diverse implementazioni. Questi strumenti sono in genere soltanto utili per la configurazione del computer in una installazione a casa o in ufficio. Forniscono poche informazioni in più oltre ai nomi della rete ed alla disponibilità del segnale all'access point correntemente in uso.
- **Netstumbler** (http://www.netstumbler.com/). Questo è lo strumento più popolare per il rilevamento delle reti wireless sotto Microsoft Windows. Supporta una varietà di schede wireless ed è molto facile da usare. Esso rileva le reti aperte e cifrate, ma non può rilevare le reti wireless *chiuse*. Inoltre esso fornisce anche uno strumento di misura segnale/rumore che traccia al passare del tempo i dati dell'apparecchio radioricevente in un grafico. Inoltre integra una varietà di dispositivi GPS, per fare il log delle precise informazioni sulla locazione e sull'intensità del segnale. Ciò rende Netstumbler uno strumento pratico per avere per un'indagine informale del sito.
- **Ministumbler** (http://www.netstumbler.com/). Dai creatori di Netstumbler, Ministumbler fornisce gran parte delle stesse funzionalità della versione di Windows, ma lavora sulla piattaforma Pocket PC. Ministumbler è pratico da far funzionare su un PDA tenuto in mano con una scheda wireless per la rilevazione degli access point nel campo d'azione.
- **Macstumbler** (http://www.macstumbler.com/). Mentre non è direttamente in relazione con il Netstumbler, Macstumbler fornisce gran parte delle stesse funzionalità ma per piattaforma Mac OS X. Funziona con tutte le schede Apple Airport.
- **Wellenreiter** (http://www.wellenreiter.net/). Wellenreiter è un piacevole rivelatore wireless grafico delle reti su Linux. Richiede Perl e GTK e supporta schede wireless Prism2, Lucent e Cisco.

1.5.2 Analizzatori di protocollo

Gli analizzatori di protocollo di rete forniscono un grande dettaglio delle informazioni che attraversano una rete, permettendo che controlliate i diversi pacchetti. Per le reti wired, potete controllare i pacchetti dello strato data-link o più sopra. Per le reti wireless, potete controllare le informazioni lungo tutto il percorso fino ai singoli frames 802.11. Di seguito trovate parecchi popolari analizzatori di protocollo di rete (e free):

- **Ethereal** (http://www.ethereal.com/). Ethereal è probabilmente l'analizzatore di protocollo più popolare disponibile. Lavora con Linux, Windows, Mac OS X e vari sistemi BSD. Ethereal cattura i pacchetti direttamente *dal filo* e li visualizza in un'intuitiva interfaccia grafica. Può decodificare oltre 750 protocolli differenti, ogni cosa da frames 802.11 a pacchetti HTTP. Esso assemblerà i pacchetti frammentati e seguirà facilmente intere sessioni TCP, anche quando altri dati interrompono il modello. Ethereal è molto utile per il troubleshooting dei complicati problemi della rete e per sapere esattamente che cosa sta accadendo quando due computers colloquiano *sul filo*.
- **Kismet** (http://www.kismetwireless.net/). Kismet è un potente analizzatore di protocollo wireless per ogni Linux , Mac OS X, e perfino la distribuzione embedded OpenWRT Linux. Esso lavora con tutte

la schede wireless che supportano la modalità passiva del monitoraggio. Oltre che rilevazione di base della rete, Kismet eseguirà il log passivamente di tutti i frames 802.11 sul disco o nella rete nel formato standard PCAP, per un'analisi successiva con strumenti come Ethereal. Kismet inoltre contiene l'impronta di alcune informazioni del client associato, l'impronta digitale hardware AP, la rilevazione di Netstumbler e l'integrazione GPS. Poiché è un monitor della rete passivo, può persino rilevare reti wireless *chiuse* analizzando il traffico trasmesso dai clients wireless. Potete far girare Kismet su parecchie macchine subito e avere il rapporto completo sulla rete indietro fino ad ad un interfaccia centrale di utenti. Ciò permette il controllo wireless sopra una zona grande, come un'università o un campus corporativo. Poiché usa il monitor in modalità passiva, fa tutto senza trasmettere alcun dato.

- **KisMAC** (http://kismac.binaervarianz.de/). Esclusivamente per la piattaforma di Mac OS X, KisMAC fa molto di più di quello che Kismet può fare, ma con un'eccellente interfaccia grafica. È un dispositivo di scansione passivo che esegue il log dei dati sul disco in formato PCAP compatibile con Ethereal. Non supporta la scansione passiva con le schede AirportExtreme (a causa delle limitazioni nel driver wireless), ma supporta la modalità passiva con una varietà di schede USB wireless.
- **Driftnet** e**Etherpeg**. Questi strumenti decodificano i dati grafici (come i files GIF e JPEG) e li visualizzano come in un collage. Come accennato precedentemente, gli strumenti come questi sono utili nei problemi di troubleshooting, ma sono anche molto utili nella dimostrazione dell'insicurezza dei protocolli non cifrati. Etherpeg è disponibile a http://www.etherpeg.org/, e Driftnet può essere scaricato da http://www.ex-parrot.com/~chris/driftnet/.

1.5.3 Monitoraggio della larghezza di banda

La rete è lenta. Chi sta monopolizzando tutta la larghezza di banda? Usando una buon strumento di monitoraggio della larghezza di banda, potete determinare facilmente la fonte dei problemi di assalto dei virus e dello spam. Tali strumenti possono anche aiutarti a progettare una capacità futura quando il numero degli utenti della rete diventerà troppo grande per i canali disponibili. Questi strumenti vi daranno una rappresentazione visiva di come il traffico stia fluendo attraverso la vostra rete, compreso il traffico che viene da una macchina o da un servizio particolare.

- **MRTG** (http://people.ee.ethz.ch/~oetiker/webtools/mrtg/). La maggior parte degli amministratori della rete ad un certo punto del loro girovagare incontra MRTG. Originalmente scritto nel 1995, MRTG è possibilmente l'applicazione di monitoraggio della larghezza di banda più ampiamente usata. Usando Perl e C, essa genera una pagina Web piena di grafici che dettagliano il traffico inbound ed outbound che passa su un particolare dispositivo della rete. Con MRTG è semplice eseguire ricerche su switchs di rete, access points, servers ed altri dispositivi e visualizzare i risultati in grafici che cambiano nel tempo.
- **RRDtool** (http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/). Sviluppato dalle stesse persone che hanno scritto mrtg, rrdtool è un'applicazione di monitoraggio generica più potente. RRD è la sigla di "round-robin database". È un formato di dati generico che permette di rintracciare facilmente qualsiasi particolare data point ottenuto da una media di dati in un intervallo di tempo. Mentre rrdtool non monitorizza direttamente le interfacce o i dispositivi, molti pacchetti di controllo dipendono da esso per memorizzare e visualizzare i dati che raccolgono. Con pochi semplici scripts di shell, potete facilmente monitorare i vostri switchs di rete e access points e tracciare la larghezza di banda usata in un grafico su una pagina Web.
- **ntop** (http://www.ntop.org/). Per l'analisi storiche e l'uso di traffico, potete studiare ntop. Questo programma genera una dettagliata stampa in tempo reale del traffico della rete osservato, visualizzandola nel vostro web browser. Si integra con rrdtool e restituisce grafici e tabelle che descrivono visivamente come si sta usando la rete. Sulle reti molto occupate, ntop può usare molta CPU e spazio su disco, ma vi capire approfonditamente di come si sta usando la vostra rete. Funziona su Linux, su BSD, su Mac OS X e su Windows.
- **iptraf** (http://iptraf.seul.org/). Se avete bisogno di fare una fotografia istantanea dell'attività della rete su un sistema Linux, provate iptraf. È un programma di utilità a linea di comando che vi permette di dare uno sguardo immediato ai collegamenti ed ai flussi in rete, comprese le porte ed i protocolli. Può

essere molto pratico per la determinazione di chi sta usando un particolare collegamento wireless e quanto pesante sia il suo carico. Per esempio, visualizzando un dettagliato breakdown statistico per un'interfaccia, potete immediatamente trovare gli utenti del client peer-to-peer e determinare esattamente quanta larghezza di banda attualmente stanno usando.

1.5.4 Troubleshooting

Che cosa fate quando la rete si sconnette? Se non potete accedere ad una pagina Web o all'email server e cliccare sul tasto di ricarica non risolve il problema, allora dovrete provare ad isolare il punto esatto del problema. Questi strumenti vi aiuteranno a determinare proprio dove esiste un problema del collegamento.

- **ping**. Quasi ogni sistema operativo (compresi Windows , Mac OS X e naturalmente Linux e BSD) include una versione del programma di utilità ping. Usa i pacchetti ICMP per tentare di contattare uno specifico host, e vi dice quanto tempo è necessario per ottenere una risposta. Sapere su cosa eseguire un ping è importante altrettanto quanto come eseguire un ping. Se trovate che non potete connettervi ad un particolare servizio nel vostro web browser (diciamo, http://yahoo.com/), potreste provare a eseguire un ping su di esso:

```
$ ping yahoo.com¶
PING yahoo.com (66.94.234.13): 56 data bytes¶
64 bytes from 66.94.234.13: icmp_seq=0 ttl=57 time=29.375 ms¶
64 bytes from 66.94.234.13: icmp_seq=1 ttl=56 time=35.467 ms¶
64 bytes from 66.94.234.13: icmp_seq=2 ttl=56 time=34.158 ms¶
^C¶
--- yahoo.com ping statistics ---¶
3 packets transmitted, 3 packets received, 0% packet loss¶
round-trip min/avg/max/stddev = 29.375/33.000/35.467/2.618 ms¶
```

- Quando avete finito di raccogliete i dati digitate control-C. Se ai pacchetti occorre molto tempo per tornare, ci può essere una congestione di rete. Se i pacchetti di ritorno del ping hanno una TTL insolitamente bassa, potete avere problemi di percorso fra la vostra macchina e l'estremità remota. Ma cosa dire se il ping non restituisce alcun dato? Se state eseguendo un ping su un nome anziché su un inidirizzo IP, potete avere problemi di DNS. Provate ad eseguire il ping su un indirizzo IP di Internet. Se non potete raggiungerlo, è una buona idea vedere se potete eseguire il ping sul vostro router di default:

```
$ ping 216.231.38.1¶
PING 216.231.38.1 (216.231.38.1): 56 data bytes¶
64 bytes from 216.231.38.1: icmp_seq=0 ttl=126 time=12.991 ms¶
64 bytes from 216.231.38.1: icmp_seq=1 ttl=126 time=14.869 ms¶
64 bytes from 216.231.38.1: icmp_seq=2 ttl=126 time=13.897 ms¶
^C¶
--- 216.231.38.1 ping statistics ---¶
3 packets transmitted, 3 packets received, 0% packet loss¶
round-trip min/avg/max/stddev = 12.991/13.919/14.869/0.767 ms¶
```

- Se non potete eseguire il ping sulvostro router di default, allora probabilmente non potrete neanche raggiungere Internet. Se non potete neppure eseguire un ping su altri indirizzi IP sulla vostra lan locale, allora è meglio controllare il vostro collegamento. Se state usando Ethernet, è collegata? Se state utilizzando wireless, siete collegati alla giusta rete wireless ed è nella gamma? Il debugging della rete con il ping è un po' un'arte, ma è utile da imparare. Poiché probabilmente troverete il comando

ping su ogni macchina dove lavorerete, è una buona idea imparare ad usarlo bene.

- **traceroute** e **mtr** (http://www.bitwizard.nl/mtr/). Come con il ping, il traceroute si trova sulla maggior parte dei sistemi operativi (chiamato **tracert** in alcune versioni del Microsoft Windows). Lanciando il traceroute, potete trovare la locazione del problema fra il vostro calcolatore e qualsiasi punto su Internet:

```
$ traceroute -n google.com¶
traceroute to google.com (72.14.207.99), 64 hops max, 40 byte packets¶
1· 10.15.6.1· 4.322 ms· 1.763 ms· 1.731 ms¶
2· 216.231.38.1· 36.187 ms· 14.648 ms· 13.561 ms¶
3· 69.17.83.233· 14.197 ms· 13.256 ms· 13.267 ms¶
4· 69.17.83.150· 32.478 ms· 29.545 ms· 27.494 ms¶
5· 198.32.176.31· 40.788 ms· 28.160 ms· 28.115 ms¶
6· 66.249.94.14· 28.601 ms· 29.913 ms· 28.811 ms¶
7· 172.16.236.8· 2328.809 ms· 2528.944 ms· 2428.719 ms¶
8· * * *¶
```

- L'opzione **-n** dice al traceroute di non preoccuparsi di risolvere i nomi del DNS ed esegue la traccia più rapidamente. Potete vedere che al passo sette, il round trip time cresce fino a più di due secondi, mentre i pacchetti sembrano sparire al passo otto. Ciò indica un problema in quel punto nella rete. Se questa parte della rete è sotto il vostro controllo, potrebbe valere la pena di concentrare i vostri sforzi per un troubleshooting là. My TraceRoute (mtr) è un programma pratico che unisce il ping e il traceroute in un singolo comando. lanciando mtr, potete ottenere una media continua di latenza e di perdita di pacchetti ad un singolo host, invece della fotografia istantanea che il ping e il traceroute forniscono al momento.

```
·····························  My traceroute·  [v0.69]¶
tesla.rob.swn (0.0.0.0)·····  (tos=0x0 psize=64 bitpatSun Jan·  8
20:01:26 2006¶
Keys:·  Help··  Display mode··  Restart statistics··  Order of fields··
quit¶
·····································  Packets·····  Pings¶
Host·····························  Loss%··  Snt··  Last··  Avg·  Best·  Wrst
StDev¶
1. gremlin.rob.swn·····  0.0%····  4···  1.9··  2.0··  1.7··
2.6··  0.4¶
2. er1.sea1.speakeasy.net·····  0.0%····  4··  15.5·  14.0·  12.7·
15.5··  1.3¶
3. 220.ge-0-1-0.cr2.sea1.speakeasy.·  0.0%····  4··  11.0·  11.7·  10.7·
14.0··  1.6¶
4. fe-0-3-0.cr2.sfo1.speakeasy.net··  0.0%····  4··  36.0·  34.7·  28.7·
38.1··  4.1¶
5. bas1-m.pao.yahoo.com·····  0.0%····  4··  27.9·  29.6·  27.9·
33.0··  2.4¶
6. so-1-1-0.pat1.dce.yahoo.com·····  0.0%····  4··  89.7·  91.0·  89.7·
93.0··  1.4¶
7. ae1.p400.msr1.dcn.yahoo.com·····  0.0%····  4··  91.2·  93.1·  90.8·
99.2··  4.1¶
8. ge5-2.bas1-m.dcn.yahoo.com·····  0.0%····  4··  89.3·  91.0·  89.3·
93.4··  1.9¶
9. w2.rc.vip.dcn.yahoo.com·····  0.0%····  3··  91.2·  93.1·  90.8·
99.2··  4.1¶
```

- I dati saranno continuamente aggiornati e sarà eseguita una media su di essi in ogni momento. Come con il ping, dovreste digitare control-C quando avete finito di guardare i dati. Notare che dovete avere privilegi di root per lanciare il comando mtr. Mentre questi comandi non indicheranno precisamente cosa è successo nella rete, possono fornire abbastanza informazioni per sapere dove continuare ad effettuare un troubleshooting.

1.5.5 Test del throughput

Quanto può andare veloce la rete? Qual'è la capienza utilizzabile reale di un collegamento particolare della rete? Potete ottenere una stima molto buona della vostra capienza di throughput inviando una grande quantità di pacchetti sul collegamento e misurando quanto tempo è necessario al trasferimento dei dati. Mentre vi sono pagine web disponibili che effettueranno un *test di velocità* nel vostro browser (come http://www.dslreports.com/stest), questi test sono maggiormente inesatti quanto più lontana sarà la sorgente soggetta a test. Ancora peggio, essi non vi permetteranno di verificare la velocità di un particolare collegamento, ma soltanto la velocità del vostro collegamento a Internet. Qui vi sono due strumenti che vi permetteranno di effettuare il test del throughput sulle vostre reti.

- **ttcp** (http://ftp.arl.mil/ftp/pub/ttcp/). Ora per una parte standard dei più diffusi sistemi UNIX-like, ttcp è uno strumento semplice per testare le prestazioni della rete. Un'istanza può essere lanciata da qualsiasi lato collegamento che desiderate esaminare. Il primo nodo funziona in modalità ricezione e l'altra in modalità trasmissione:

```
node_a$ ttcp -r -s¶
¶
node_b$ ttcp -t -s node_a¶
ttcp-t: buflen=8192, nbuf=2048, align=16384/0, port=5001· tcp -> node_a¶
ttcp-t: socket¶
ttcp-t: connect¶
ttcp-t: 16777216 bytes in 249.14 real seconds = 65.76 KB/sec +++¶
ttcp-t: 2048 I/O calls, msec/call = 124.57, calls/sec = 8.22¶
ttcp-t: 0.0user 0.2sys 4:09real 0% 0i+0d 0maxrss 0+0pf 7533+0csw¶
```

- Dopo la raccolta dei dati in una direzione, dovreste invertire la trasmissione e eseguire la ricezione dal vostro partner per testare il collegamento nell'altra direzione. Lo strumento può testare sia i flussi UDP che i flussi TCP e può modificare vari parametri TCP e lunghezza del buffer in modo da permettere alla rete un buon funzionamento. Può persino usare il flusso di dati suggerito dagli utenti invece di trasmettere dati casuali. Ricordare che la lettura della velocità è in kilobytes, non in kilobit. Moltiplicare il risultato per 8 per trovare la velocità in kilobit al secondo. L'unico svantaggio reale di ttcp è che non ci sono sono voluti anni per svilupparlo. Fortunatamente, il codice è stato reso di pubblico dominio ed è liberamente disponibile. Come il ping e il traceroute, il ttcp è disponibile come comando standard su molti sistemi.
- **iperf** (http://dast.nlanr.net/Projects/Iperf/). Tanto quanto ttcp, iperf è uno strumento a linea di comando per la valutazione del throughput di un collegamento di rete. Supporta molte delle caratteristiche di ttcp, ma usa un modello *client* e *server* anziché della coppia *receive* e *transmit*. Per far girare iperf, lanciare un server da un lato e un client dall'altro:

```
node_a$ iperf -s¶
¶
node_b$ iperf -c node_a¶
------------------------------------------------------------¶
```

```
Client connecting to node_a, TCP port 5001¶
TCP window size: 16.0 KByte (default)¶
------------------------------------------------------------¶
[· 5] local 10.15.6.1 port 1212 connected with 10.15.6.23 port 5001¶
[ ID] Interval····· Transfer···· Bandwidth¶
[· 5]· 0.0-11.3 sec·· 768 KBytes·· 558 Kbits/sec¶
```

- Il lato del server continuerà ad ascoltare ed ad accettare i collegamenti del client sulla porta 5001 fino a che non digitiate control-C per ucciderlo. Ciò può essere estremamente pratico quando si effettuano più elaborazioni di test da varie locazioni. La differenza più grande fra ttcp e iperf è che iperf è in fase di sviluppo attivo ed ha molte nuove caratteristiche (compreso il supporto IPv6). Questo lo fa diventare una buona scelta come strumento di valutazione prestazioni quando si progettano nuove reti.

1.5.6 Salute della rete

Dalle informazioni fornite momento per momento, potete farvi un'idea generale della salute generale della rete e dei relativi servizi. Questi strumenti vi mostreranno le tendenze della rete e quando i problemi si presenteranno informeranno perfino un essere umano. Spesso, i sistemi notificheranno il problema prima che una persona abbia la possibilità di chiamare il supporto tecnico.

- **cactus** (http://www.cacti.net/). Come accennato precedentemente, molti strumenti usano RRDtool come back-end per generare i grafici sui dati raccolti. Cactus è un tale strumento. È uno strumento di amministrazione della rete basato su PHP che semplifica la raccolta dei dati e la generazione del grafico. Immagazzina la sua configurazione in una base di dati MySQL, ed è integrato con SNMP. Ciò lo rende molto semplice per pianificare tutti i dispositivi della vostra rete e controllare ogni cosa dai flussi della rete al carico della CPU. Cactus ha uno schema estendibile della raccolta di dati che vi permette di raccogliere quasi qualunque genere di dati a cui potete pensare (come il segnale radiofonico, il rumore, o gli utenti collegati) e di tracciarli su un grafico in funzione del tempo. Le minifoto dei vostri grafici possono essere unite in una singola pagina web. Ciò vi permette di osservare in un'occhiata il totale stato della vostra rete.
- **SmokePing** (http://people.ee.ethz.ch/~oetiker/webtools/smokeping/). SmokePing, anch'esso di Tobias Oetiker, è uno strumento scritto in Perl che visualizza la perdita dei pacchetti e la latenza su un singolo grafico. È molto utile far girare SmokePing su un host con una buona connettività alla vostra intera rete. Col tempo, si è trovato che possono essere indicati tutti i tipi di problemi della rete. Insieme con MRTG o Cactus, potete osservare l'effetto che la congestione di rete ha sulla perdita dei pacchetti e sulla latenza. SmokePing può facoltativamente spedire allarmi quando avvengono determinate circostanze, come quando si osserva una perdita eccessiva di pacchetti su un collegamento per un periodo di tempo esteso.
- **Nagios** (http://www.nagios.org/). Nagios è uno strumento di servizio di monitoraggio. Oltre che alle prestazioni fornite dai semplici ping (come con SmokePing), Nagios può osservare le prestazioni dei servizi reali di ogni numero di macchine. Per esempio, può interrogare periodicamente il vostro web server ed state sicuri che vi restituirà una pagina Web valida. Se un controllo viene a mancare, Nagios può informare una persona o un gruppo via email, SMS, o IM. Mentre Nagios certamente aiuterà un singolo admin per monitorare una grande rete, esso è usato al meglio quando avete una squadra per il troubleshooting con responsabilità divise fra i vari membri. Gli eventi con problemi possono essere configurati per ignorare problemi transitori, e poi intensificare le notifiche soltanto alle persone che sono responsabili della loro risoluzione. Se il problema è aperto per un periodo di tempo predefinito senza essere risolto, la persona può essere notificata ulteriormente. Ciò permette ai problemi provvisori di essere semplicemente annotati senza importunare la gente affinché i problemi reali siano portati all'attenzione della squadra.