Rendere sicura una rete eterogenea con Software Free

by Georges Tarbouriech
<georges.t(at)linuxfocus.org>

About the author:

Georges è un utente Unix di vecchia data. Vuole ringraziare la comunità Free Software per la grande quantità di strumenti per la sicurezza che ci ha portato.

Translated to English by:
Georges Tarbouriech
<georges.t(at)linuxfocus.org>

Abstract:

Questo articolo fu pubblicato per la prima volta sul numero speciale sulla sicurezza di Linux Magazine edizione Francese. L'editore ha gentilmente concesso a LinuxFocus di pubblicare ogni articolo di questo speciale. Di conseguenza LinuxFocus vi darà la possibilità di leggerlo non appena questi articolo sono stati tradotti dal francese all'inglese. Ringraziamo tutte le persone che sono coinvolte i questo progetto. Questa breve nota editoriale sarà riprodotta ogni qualvolta troverete un articolo che ha la stessa origine.

Prefazione

La sicurezza nelle reti di computer è provabilmente una delle maggiori sfide del 21° secolo.
Tuttavia, come per molti argomenti che possono preoccupare, tutti ne parlano, ma coloro che dovrebbero esser più interessati all'argomento non sembrano avere realiazzato l'importanza della cosa ed il conseguente disastro. I "più coinvolti", ovviamente, sono i produttori di software o i system designer. Il più lampante esempio ci viene dato, per l'ennesima volta, da Redmond, dove la sicurezza sembra essere solo una parola, o almeno essa è molot meno seguita del marketing.
Fortunatamente, le ultime due decadi del 20° secolo, hanno visto nascere e crescere la filosofia del software gratuito. Se "desiderate" incrementare la sicurezza delle vostre macchine, dei vostri sistemi, delle vostre reti... questo è il posto dove cercare . La comunità del Free Software ha prodotto molto di più delle grandi aziende nel settore della sicurezza.
Detto questo, nono sono sufficienti i soli strumenti, e, per esempio, rendere sicura una rete è un lavoro a tempo piento: ci sono modifiche da fare in ogni momento!

Questo significa, in altre parole, che non potrete mai dire che la vostra rete sia sicura al 100%. Potete solo ridurne i rischi. Quello che andremo ad affrontare in questo articolo è solo una parte di quello che si dovrà fare per limitare i rischi. Dopo aver letto questo numero speciale (Nota dell' autore: vi ricordo che questo articolo fa parte di un numero speciale dell' edizione francese di Linux Magazine, completamente orientato alla sicurezza), avrete un poca di più conoscenza sulla sicurezza, ma non sarete ancora in nessun modo di dire che la vostra rete sarà sicura.
Come ultima nota, ma non meno importante: questo tipo di articolo non può essere completamente esaustivo. C'è una elevata quantità di documentazione su questo argomento ed a tutt'ora non si è ancora coperto il problema nella sua interezza. Di conseguenza non aspettatevi che in questo articolo si citi ogni strumento o prodotto, come pure sistemi operativi, configurazioni, utilizzi... e quello che vi gira attorno.
Per chiudere questa prefazione, lasciatemi aggiungere che alcune parti di questo articolo sono state ispirate dalla rivista LinuxFocus, ma non preoccupatevi, con il prermesso dell'autore: si scopre alla fine che si tratta in vero della stessa persona!

Presentazione

Prima parlremo di come sia la struttura di una rete molto eterogenea, che contenga svariati sistemi operativi. Più sistemi operativi sono presenti e più aumenta la complessità in quanto non tutti i sistemi operativi sono uguali. In aggiunta a questo si consideri che le macchine presenti in rete spesso hanno funzioni diverse: si avrà così una rete diversificata.
In un secondo momento valuteremo alcuni strumenti essenziali per incrementare la sicurezza. La scelta è arbitraria, in quanto ve ne sono fin troppi di strumenti adatti allo scopo rendendo impossibile elencarli tutti. Ovviamente vi spiegherò come rendere più sicure e le macchine e le reti per mezzo di questi strumenti.
La sezione seguente vi illustrerà le diverse funzionalità e metodi dei vari sistemi, da utilizzare durante la fase di messa in sicurezza dei medesimi.
La conclusione cercherà di spiegarvi la "relatività" del processo di messa in sicurezza, per farvi capire come mai esso sia un percorso arduo, tortuoso e senza fine, senza scadere nel "fantastico" o nel "futuribile".

Un caso di rete eterogenea

Dapprima consideriamo che ricorrere all'utilizzo del protocollo TCP/IP è un vantaggio, in quanto si tratta dell'unico protocollo che è "parlato" da quasi ogni sistema operativo sulla terra. Per mezzo di esso, molteplici sistemi soo in grado di scambiarsi dati l'un l'altro. Di conseguenza nel nostro esempio il protocollo TCP/IP sarà sempre presente. In altre parole: non andremmo ad analizzare protocolli proprietari, ne quelli poco diffusi od obsoleti. Non andremmo nemmeno a trattare della struttura fisica della rete, ovvero il tipo di connessione, la categoria della connessione e quant'altro.
In questa rete inseriremo un poco di tutto. Ovviamente troveremo Unix, sia esso proprietario o free: per esempio, una scelta di Solaris 2.6, o SunOS 5.6, se preferite, Irix 6.5, Liux (RH 6.5), MacOS X. Avremmo potuto anche aggiungere QNX o NeXTSTEP, o NetBSD o OpneBSD. Sul lato più "comune" avremmo l'unico e solo NT 4.0 (null'altro: il resto è peggio) *[nota del traduttore: Georges qui usa il termine Not Terminated 4.0, che letteralmente tradotto, verrebbe ad esser Non Terimanto, ovvero incompleto.]*. Qui avremmo potuto anche aggiungere OS2, che dopotutto è meglio di altri Sistemi Operativi. Per finire aggiungeremo un qualcosa di "poco convezionale", per esempio BeOS e AmigaOS (Sì esiste.... bhe non molto usato e diffuso!).
Ovviamente qualcuno di voi starà già lamentandosi: perchè non AIX o HP−UX? No! Se avessimo dovuto citare tutte le varianti di Unix, avremmo scritto un articolo lungo quanto dieci volumi di enciclopedia. Tuttavia i concetti fondamentali del tutto sono appliccabili ad ogni sistema operativo.

Bene, che faremo fare ai vari sistemi?
Facciamo un esempio: poniamo che Solaris sia l'application server. Irix si occuperà dei backup. NT sarà un altro application server. Linux sarà il gateway. Un'altra macchina Linux farà il server web o un database server. Tutto il resto saranno client. Considereremo la rete composta da circa 30 macchine e ricorreremo ad un password file per l'autentifica. Certo, avremmo potuto scegliere un sistema di autentifica più sofisticato: NIS (note anche come YP o pagine gialle), o LDAP, o Kerberos, ... Ma vediamo di renderci le cose semplici. Non ricorreremo nemmeno all'uso di NFS. Sebbene sia spessissimo utile, quandi si tratta di sicurezza è meglio dimenticarselo, a scapito di alcune prestazioni. In francia, i vecchi, dicono di non metter tutte le proprie uova nello stesso cesto. Con questo voglio dire che solo i protocolli necessari, ma "insicuri" saranno presenti una sola volta per macchina. Ovvero solo un server ftp, uno http, e preferibilmente su macchine Unix. Alcune macchine Unix saranno SSH server, e le altre ssh client. Ma torneremo su questo argomento in un secondo momento. Ricorreremo all'uso di IP statici: nessun server DHCP. In parole povere lavoriamo in una situazione semplificata. Tutto ciò può esser applicato a 50 macchine in rete: con più macchine potrebbe essere un incubo.

Gli strumenti e come usarli.

Come sempre c'è più di un modo per fare le cose. La situazione ideale è quella in cui si parte da zero, ovvero con le macchine da installare e la rete da configurare. Ma questa è una realtà che può esistere solo nei film! Di conseguenza consideriamo una rete in crescita nel tempo, con le macchine che si spostano da un luogo all'altro, da una funziona ad un'altra, e con nuove macchine che vengono aggiunte. A causa della corsa ai "MHz", per esempio, le attuale macchine con processore Intel non hanno una lunga vita. Dopo circa 3 anni diviene difficile trovare parti di ricambio. Di conseguenza queste macchine o vengono riutilizzate in altri ruoli o o vi troverete con montagne di queste: triste ma vero! Fortunatamente alcune hanno un ciclo vitale più lungoe permettono una certa flessibilità ed espandibilità. Non crediate che questa digressione sia fine a se stessa. Un buon amministratore deve avere un modo di lavorare con una certa flessibilità mentale.

Le basi

Definiremo come "generalità" i primi passi del nostro lavoro. Questa consiste nel tutto quello che non sia strettamente necessario sulle varie macchine: di certo non un semplice compito! Ogni sistema operativo, incluso Unix, installa una incredibile quantità di servizi, protocolli, che non utilizzerete mai. Il motto sarà: eliminate tutto! Nell'ambiente Unix, una maniera semplice ma brutale è quella di commentare tutte le voci nel file /etc/inetd.conf. Questo farà si che la macchina abbia meno servizi possibili. Certament questo modo è un poco esagerato, ma in molte macchine è una procedura più che accettabile. Dipende dalle vostre necessità. Nell'ambiente Linux alcuni possono ricorrere al comando *chkconfig* per disattivare alcuni servizi.
Fate anche un controllo dei file con flag SUID/SGID e non esitate a rimuovere il bit in questione, o considerate l'opzione di disattivare il programma in questione. Un riga di comando del tipo: *find / −user root −a \(−perm −4000 −o −perm −2000 \) −print* vi mostrerà la lista di questi file incriminati. Per rimuovere il bit potete usare questo comando: *chmod a−s nome_e_percorso_del_programma* (nota: questo ovviamente ridurrà alcune funzionalità del programma in oggetto. Quel bit, di solito, ha una giustificazione per esser presente).
Rimuovete programmi "pericolosi" o quelli noti come "rischiosi": i comandi remoti come, per esempio, rsh, rlogin, rcp,... SSH li rimpiazzerà appieno.
Controllate anche i permessi delle cartelle, per esempio /etc, /var, ... Più sono restrittivi e più sicureo sarà il tutto. Per esempio digitare il comando *chmod −R 700* sulla cartella che contiene i files di avvio (/etc/rc.d/init.d nella maggior parte dei sistemi Unix) è un'idea ottima! La stessa regola si può applicare a tutti i sistemi che siano parte di una rete: rimuovete quello che non usate o, almeno, disattivatelo. Per quel che concerne WinNT fermate tutti i servizi che volete dal pannello di controllo. Ci sono molte cose "basilari" da sistemare e moltissima documentazione in merito.

Gli strumenti

Iniziamo dall'ambiente Unix, in quanto è l'unico sistema da prendere seriamete per quanto concerne problemi di sicurezza inerenti gli account. Per fortuna ci sono moltissimi strumenti free di questo tipo e la maggior parte di essi funziona praticamente su qualsiasi versione di Unix (o quasi).

Da questo momento in poi si andrà a lavorare sulla singola macchina, in quanto, rendere sicura un rete significa rendere sicuri i singoli elementi della rete stessa. Installare questi strumenti è alquanto semplice, ecco prechè non useremo molto tempo su questo argomento. Alcuni loro parametri dipendono dall'ambiente operativo, come anche alcuni requisiti... A voi il compito di studiare caso per caso. Il primo strumento che verrà utilizzato è noto come *shadow utils*. La sua funzione è quella di crittare le password. Per fortuna questo strumento è già parte integrante di molte distribuzioni. Il file /etc/shadow viene "creato" da questo strumento partendo dal file /etc/passwd.

Ancora meglio sarebbe il sistema *PAM* (Pluggable Authentication Modules: sistema di autentificazione a moduli) vi permette di restringere gli accessi anche a livello di servizio. Tutto viene controllato dalla cartella contente i file di configurazione inerenti ogni singolo servizio. Questa cartella di solito è /etc/pam.d. Molti servizi possono esser "controllati" dal sistema PAM, per esempio ftp, login, xdm, ed altri, permettendo all'amministratore di decidere chi ha il permesso di fare cosa.

Il prossimo strumento è un qualcosa di cui non si possa fare a meno: *TCPWrapper*. Anche questo funziona su praticamente ogni variante Unix. Per esser concisi esso permette di restringere gli accessi ai servizi ad alcuni host. Gli host sono abiliti o interdetti al servizio per mezzo di due soli file: /etc/host.allow e /etc/host.deny. TCPWrapper può essere configurato in due modi: o cambiando i servizi o modificando il file /etc/inetd.conf. In un secondo momento vedremo come TCPWrapper operi in perfetta sintonia con altri strumenti. Potete trovare TCPWrapper presso ftp://ftp.porcupine.org/pub/security

Un altro strumento interssante è xinetd. Anche qui, per farla breve, vi dirò solamente che xinetd è un sostituto di inetd con molteplici funzioni. Se siete interessati a questo strumento lo potete trovare presso http://www.xinetd.org.

Nell'ambiente Linux esiste uno strumento senza cui non potrete mai sopravvivere: il suo bome è Bastille−Linux, e lo potete trovare presso http://www.bastille−linux.org. Questo strumento, scritto in Perl, non è solamente didattico ma anche molto efficiente. Dopo aver eseguito lo script, dovrete rispondere a molte domande ed, in accordo alle vostre risposte, Bastille−Linux agirà di conseguenza. Ogni domanda è sufficientemente spiegata e vi verrà pure proposta una risposta predefinita. Potrete cambiare il responso ad una risposta, iniziare con una nuova configurazione, verificare cosa sia stato fatto,... Avrete tutto a portata di mano! Bastille−Linux offre anche la possibilità di configurazione di firewall; torneremo su questo argomento in un secondo momento. Nel momento in cui sto scrivendo questo articolo, Bastille−Linux ha come versione la 1.1.1 ma già la 1.2.0 è in stato di release candidate. È stata molto migliorata e dispone di una interfaccia gtafica basta su Tk e Perl. (Nota dell'autore: questo articolo fù scritto molti mesi fa. La attuale versione di Bastille−Linux è la 1.3.0).

Anche i sistemi di rilevamento intrusione sono essenziali. Due "mastini" di questo tipo sono noti come snort e portsentry. Il primo può esser scaricato presso http://www.snort.org ed il secondo dal sito web dell'Abacus,http://www.psionic.com. Queti due strumenti non debbono essere raffrontati: il primo fa parte dei NIDS (Network Intrusion Detection System: sistemi di rilevamento intrusioni di rete) e verte su questo genere di informazioni, il secondo è invece imperniato sulla macchina in se ed è più reattivo. snort ha molteplici opzioni per monitorare il traffico di rete. Potete "ascoltare" il traffico che volete: quello in ingresso, in uscita, all'interno del firewall o all' esterno di quest'ultimo. Ovviamente questo strumento può creare e gestire dei log di sistema che possono esser molto grandi, e quindi è essenziale che sappiate che cosa vlete! Ne esiste anche una versione per ambiente Win32, ed è da considerarsi importante ogni versione che esista per questo tipo di

piattaforma, vista la scaristà di strumenti di tipo free.

portsentry ha una funzionalità assai interessante: può bloccare le porte sottoposte scansione secondo le vostre scelte. Potere reindirizzare l' attaccante verso un indirizzo inesistente o verso il firewall. Ovviamente potete scegliere chi bloccare e chi no. Ora possiamo tornare al TCPWrapper: portsentry è in grado di modificare il contenuto di /etc/hosts.deny, se lo volete. Di conseguenza portsentry diviene uno strumento abbastanza efficiente. Non mi addentrerò nella filofia utilizzata da portsentryche ricorre al binding delle porte. Dipende essenzialmente da voi: fate la vostra scelta solo dopo che avrete vagliato bene l'argomento. Vi ricordo che portsentry può anche rendere una macchina "invisibile", il che, a volte, non è affatto male! In aggiunta debbo anche dire che portsentry può comportarsi in maniera differente a seconda dell'ambiente su cui gira; la modalità più evoluto è, attualmente, "riservata" a Linux (o almeno per ora).

Non si può in ogni caso parlare di sicurezza senza menzionare la crittografia. Tuttavia le legi su questo argomento variano da paese a paese, ed in alcuni l' uso della medesima è vietato.
Nota dell'autore: la sezione dell'articolo che segue è stata rimossa dalle traduzioni, in quanto era inerente la sola legislazione francese.
Per concludere la sezione inerente la crittografia, si potrebbe dire: installate ssh (sia come client che come server) sulle vostre macchine Unix, ovviamente secondo le vostre necessità e controllando che la legge del paese in cui vi trovate lo permetta.

Per completare la carrellata sugli strumenti per Unix, ve ne citerò alcuni di tipo proprietario. Sotto Solaris abbiamo ndd; sotto Irix ipfiltered. MacOS X vi permette l'utilizzo di alcunoi strumenti free qualis ssh, ipfwadmin, ...
Torneremo su questi più tardi.

Andiamo ora ad affrontare l'unico e solo (per fortuna!) NT4.0. In questo caso non possiamo parlare di strumenti free... tuttavia gli uomini di Redmond ci hanno fornito strumenti "gratuiti" per implementre le funzionalità del sistema (ovviamente queste implementazioni non hanno nulla a che fare con correzioni e bug, in quanto il sistema non alcun big!). Per quel che rigurda la sicurezza, NT 4.0 è un modello... d'assurdità! Dire che è similie ad un colabrodo! Non fateci caso. Secondo questa filosofia dovete solamente scarivarvi l'ultimo service pack (il 6 in questo attuale momento) e gli HotFix... che altro non sono che delle patch di sicurezza. Dopo di ciò potrete ricorrere alla serie di strumenti gratuti che vi vengono offerti (gratuiti nel senso che che sono liberametne utilizzabili ma non sono free in quanto potete avere solo l'eseguibile e non il sorgente). E per questo sistema è tutto.

Per quanto concerne altri sistemi dovrete voi cercare. Per AmigaOS, il team di sviluppo non sembra moltocoinvolto nell'implementazione del TCP/IP, difatto quello disponibile è un poco datato. Tuttavia il doftware di pubblico domini vi può tenere ben occupati nelle ricerche. Per quel che riguarda BeOS, puretopo le cose non sono molto migliori: questo grandioso sistema operativo sembra avere un futuro alquanto compromesso, e lo sviluppo dell supporto di rete, il cui nome è Bone, è ancora in fase di completamento.
(Nota dell'autore: Sfortunatamente BeOS oggi come oggi è un prodotto non più vivo. Un piccolo gruppo di sviluppatori stanno cercando di tenerlo in vita come software free... e debbo dire che stanno facendo un lavoro grandioso!)
Per quest'ultimo, in ogni caso, troverete degli strumenti sviluppati per Unix che possono aiutarvi a migliorare le cose.

Rendere gli host sicuri

Ora dovrete configurare tutto e questi strumenti! Nuovamente, consideriamo che ogni macchina Unix abbia le shadow−utils, PAM, TCPWrapper, e che ogni servizio strettamente necessario non sia attivo, che le cartelle ed i file a rischio siano stati controllati e messi in grado di non nuocere, ecc...

Sulle macchine Linux è il momento di eseguire Bastille−Linux. (Questo strumento dovrebbe funzionare sulla maggior parte delle distribuzioni anche se nacque per RedHat e Mandrake). Rispondete liberamente al fine di creare una macchina con elevate restrizioni.
Sulla macchina Linux utilizzata come gateway, il sistema deve essere del tipo minimalistico. Potete liberamente rimuovere la maggior parte dei servizi: http, ftp, ... Rimuovete anche X: non vi serve a nulla! Rimuovete tutto il software non strettamente necessario,... ovvero la maggior parte delle cose. Fermate i serivi inutili. Dovreste ottenere, alla fine, un sistema in cui il comando *ps ax* non riempirà completamente lo schermo. Se utilizzare l'IP Maquerading, il comando *lsof −i* dovrebbe farvi vedere una sola riga: quella inerente il server in ascolto (in tale caso sto supponendo che la connessione non sia di tipo permanente).
In maniera arbitraria installeremo portsentry sulle macchine Linux e questo strumento sarà avviato al boot della macchina, ricorrendo alla modalità " avanzata" (che è solamente riservata a Linux, per mezzo delle opzioni −atcp e −audp). Questo presuppone che TCPWrapper sia installato e che vi sia un firewall. Torneremo poi su quest'ultimo.

Per quel che riguarda Solaris, ricorreremo all'uso di *aset* e di *ndd*. Torneremo nel dettagio di questi più avanti. Anche portsntry dovrà essere installato. Potremmo anche aggiungere IP Filter e sostituire la versione standard di RCPbind con la versione 2.1 disponibile presso porcupine.org. Per Irix sceglieremo ipfilterd, che come il nome suggerisce, useremo per filtrare i pacchetti. Questo strumento è incluso nella distribuzione di Irix, ma non viene installato nella configurazione standard.

Per quel che concerne NT lo cose si rendono alquanto complicate... La soluzione despotica consiste nel bloccare le porte 137 e 139, che altro non sono che le famose porte su cui il protocollo NetBIOS risponde (o ancor meglio, rimuovete questo protocollo)... ma in tal caso andremmo a perdere la rete di Windows, il che può divenire un piccolo porblema se riguarda un application server! Potete anche installare snort, ma non farà si che le macchine non rimangano come dei colabrodi. Di conseguenza dovrete gestire in maniera molto restrittiva i gli accessi a cartelle e partizioni dei dischi... ovviamente se utilizzate NTFS, che in tale caso sono necessarie. Esiste un piccolo programma gratuito che vi permette di risolvere le problematiche degli account guest, ma purtroppo il codice sorgente di questo programma non è disponibile. Installate tutte le patch ed i fix inerenti la sicurezza che riuscite a trovare! Come ultima cosa... tiratevi sù le maniche della camicia e cercate di rendere il tutto il meno vulnerabile possibile. Sarà un poco come andare allo sbaraglio in una battaglia, ma non potete evitare questa ultima parte!

Per quel che riguarda i sistemi meno diffusi dovrete darvi da fare in ricerche e fare la vostra scelta. Come sempre, ed ovviamente come prima cosa da fare, la regola basirlare dovrà esser applicata il più possibile: meno servizi e server sono attivi e più sicuri sarete!

Proteggere la rete

Se le macchine che partecipano alla rete sono state correttamente "preparate", sarete già a metà dell'opera. Avrete però bisogno di andare oltre. Dato che stiamo parlando di software free, sceglieremo un firewall free per il gateway: bhe in fondo si tratta solo di una macchina che vi permetterà di accedere al "selvaggio" mnondo esterno. Arbitrariamente (sì ancora arbitrariamente) utilizzeremo per questo scopo una macchina Linux: in questo modo potremmo ricorrere al filrewall bastato su Bastille−Linux. Questo funziona sia con ipchans, sia con ipfwadm a seconda del kernel che state utlizzando. Se state utilizzando un kernel della seri 2.4.x Bastille−Linux ricorrerà a iptables.

Una piccola digressione: non è una buona idea avere tutti i problemi legati alle nuove funzioni, specialmente quando la sicurezza diviene un elemento essenziale. La "sfrenata corsa" all'ultima release del kernel può portare a situazioni assai negative. Questo non vuole dire che il lavorare su di nuovi kernel sia una pessima idea, ma a volte l'unione tra strumenti già esistenti e queste ultime versioni di kernel potrebbe dimostrarsi non

stabile, il che alla fine, comporterebbe un grosso errore e molti grattacapi, nonchè compromettere la sicurezza. Un piccolo consiglio: abbiate pazienza! La nuova funzionalità di firewall integrata nel kernel 2.4 è una cosa che promette assai bene.... ma forse ancora troppo giovane. Detto questo a voi la scelta finale...

Alla fine, Bastille−Linux è un firewall semplice ma efficace. Tuttavia esistono strumenti assai più elaboarti, come per esempio T.REX. Lo si può trovare presso il sito http://www.opensourcefirewall.com. Se stat cercando uno strumento free e sofisticato, allora T.REX fà per voi.

Esistono altre soluzioni, come per esempio i proxy, tuttavia questi non sono sempre la migliore scelta. Un'altra digressione: i proxy vengono spesso chiamati firewall. Tuttavia si tratta di due cose assai diverse. I firewall di cui stiamo parlando ricorrono a sistemi di filtraggio dei pacchetti e non hanno alcun metodo di autentificazione. Vi sono due tipi di proxy server: applicazioni o socks. In parole povere un proxy applicativo svolge per voi prendendosi cura dell'intera comunicazione e permette anche le autentificazioni dell'utente. Questo è anche il motivo per un proxy ha delle richieste di risorse più elevate rispetto ad un firewall. Ma, e qui mi ripeto, questo tipo di strumento vi protegge per brevi periodi. Un firewall può esser crackato in circa 15 minuti. Interessante vero? Ecco perchè vi è la necessità di rendere sicure le macchine nella vostra rete: basare la sicurezza di una rete solo ed esclusivamente o su di un firewall o di un prozy è una pura pazzia!!

Un ulteriore metodo per ridurre i rischi in una rete è di ricorrere alla crittografia. Per esempio ricorrere all'uso di telnet è come stendere un tappetto rosso ai cracker. È un poco come dare loro le chiavi di casa nostra. Non solo sarebbero in gradi di vedere i dati che vi circolano, ma, e la cosa è ancora più grave, possono vedere le nostre password in chiaro: simpatico no? Di conseguenza sentititevi liberi di ricorrere ad ssh con quei protocolli " poco sicuri". se proprio _DOVETE_ (??) ricorrere all'uso di telnet, inviate i dati per mezzo di una connessione sicura: in altri parole reindirizzate la sessione telnet su di una porta sicura. Potrete trovare qualcosa di più su questo argomento su questo articolo intitolato "Nel tunnel" (LinuxFocus, May2001, article 202). (Pubblicità gratuita!)

Ok, abbiamo provato ad incrementare la sicurezza, ma ora dovremmo controllare il nostro operato. Per farlo, ovviamente, dovremmo divenire dei cracker, o almeno un qualcosa di simile: ricorreremo ai loro strumenti. Strano no? Anche in questo settore abbiamo una buona scelta di programmi, e quindi, di nuovo arbitrariamente, ne sceglieremo due tra i tanti: nmap e nessus. Non sono ridondanti, in quanto il secondo ha come requisito il primo. Questi due strumenti sono essenzialmente dei portscanner, anche se nessus è ben di più di un semplice portscanner. Nessus vi informa di possibili vulnerabilità del sistema, raffrontando il responso del portscanner con il proprio database di vulnerabilità note. Utilizzare questi strumenti su di una rete vi permetterà di trovare i punti deboli dei vai host, indipendentemente dal loro sitema operativo. I risultati sono strablianti, tanto da rendere questi strumenti un elemento essenziale per la vostra rete. Potete trovare nmap presso http://www.insecure.org e nessus presso http://www.nessus.org.

Dall'inizio dell'articolo stiamo discutendo della sicurezza di macchine che costituiscono una rete locale ed alcune di queste sono anche esposte al mondo esterno. Nel caso di un ISP (Internet Service Provider: Fornitore di Servizi Internet) il discorso, ovviamente, sarà alquanto diverso, quindi non andremo molto nei dettagli di questo caso. In ogni caso possiamo dire che il discoro succitato rimane valido, ma vi sarà la necessità di ricorre a soluzioni più elaborate, come, per esempio, le VPN (Vitual Private Network: Reti PRivate Virtuali), o autentificazione attraverso LDAP, ecc. Si tratta in ogni caso di un qualcosa di assai diverso, essenzialmente dovuto alle limitazioni e restizioni che variano di caso in caso. E per non parlare di e−business, dove le cose divengo assai complicate. Li chiamano siti sicuri! Non mi venite a raccontare cose del genere... Inviate il numero della vostra carta di credito in internet? Se lo fate siete molto coraggiosi! Un piccolo suggerimeto: se siete in grado di comprendere il francese date un'occhiata a questo sito: http://www.kitetoa.com, ne varrà la pena.

Particolarità dei sistemi

Come avevo precendentemente citato, i vari sistemi non sono uguali nemmeno se visti dal punto di vista del nemico. Alcuni sono molto robusti, mentre altri son dei veri colabrodo. Paradossalmente (bhe non così tanto, dopotutto), i sistemi operativi gratuiti risultano essere tra i pi robusti. I vari BSD (OpenBSD, NetBSD, FreeBSD,...), le svariate distibuzioni di Linux sono molto avanti per quel che riguarda la sicurezza. Ed anche questa volta si tratta di lavoro svolto dalla comunità del software free. Gli altri, anche gli Unix più blasonati, sono un poco meno evoluti. Se poi si tratta di sistemi non Unix... bhe le cose peggiorano!

Tutti gli strumenti che ho citato in questo articolo sono stati sviluppati per sistemi operativi free. La maggior parte dei sistemi operativi Unix proprietari possono trarne beneficio. Tuttavia questi sistemi operativi proprietari spesso hanno i propri strumenti. Per esempio, per quel che riguarda Solaris, avevamo citato *ndd* ed *aset*. Al contrario del pensiero comune, i sistemi di Sun Microsystem non sono affatto uno standard di sicurezza. Uno strumento ceom aset permette di migliorare lo stato delle cose per quel che riguarda i diritti di accesso. aset offre tre livelli di protezione: basso (low), medio (med), ed elevato (high). Potete eseguirlo in una shell o richiamarlo dalla crontab. In un ambiente di rete le cose cambiano rapidamente: quello che era vero ale 17.00 potrebbe non più esser vero alle 17.30. Ecco che risulta importante ed interessante la possilità di esegure una serie di comandi in maniera periodica per avere un certo livello di omogeneità. Ecco il motivo pre cui aset ha la possibiltà di essere eseguito per mezzo della crontab. Esso, quindi, controllerà ogni 30 minuti, o quando preferite, i permessi delle directory, dei file,...
nnd permette di variare i parametri dello stack IP. Per esempio può essere utilizzato per nasconder il fingerprint del sistema. Un sistema identificato con certezza è più vulnerabile, in quanto i cracker sanno come attaccarlo propriamente. Con nnd, per esempio, potete cambiare il paramentro TCP Maximum Segment Size (MSS). Normalmente questo valore è pari a 536 in un sistema Solaris 2.6. Il comando *ndd −set /dev/tcp tcp_mss_def 546* lo modificherà in 546. Normalmente, più è elevato il valore di MSS e migliore è la situazione (attenzione però che nemmeno troppo elevato va bene!). Nmap, per esempio, è in gradi tro identificare questo punto debole. Per mezzo di ndd siete quindi in grado di modificare il comportamento e confondere nmap. Se avete macchine che utilizzano Solaris come sistma operativo, sentitevi liberi di utilizzare ndd. ndd ha molteplici opzioni, date pure un'occhiata alle pagine del manuale (man ndd).
Potete anche utilizzare IP Filter, uno strumento atto al filtraggio dei pacchetti. Lo potete trovare pressoftp://coombs.anu.edu/pub/net/ip−filter.

Per quel che riguarda Irix, la situazione è, anche in questo caso, differente. SGI (nota come Silicon Graphics), come il nome stesso suggerisce, ha studiato i suoi sitemi per uso strettamente grafico.. La sicurezza non era di certo il loro scopo principale. Dato che la necessità porta alla soluzione, divenne obbligatorio trovare una soluzione per ridurre i rischi. Di conseguenza venne fornito ipfiterd nella distribuzione di Irix, ma questo strumento non viene normalmente installato. Lo dovrete cercare voi! Essendo ipfilterd uno strumento atto a filtrare i pacchetti, esso riuscirà a negare o permettere le connessioni con la macchina. Questo strumento basa la sua configurazione sul file ipfiltered.conf, e qui le cose di complicano. La sintassi di questo file è assai peculiare e non gradisce per nulla spazi inaspettati o righe vuote. Per esempio, per permettere alla macchina "mars" di parlare con la macchina "jupiter" (che nel nostro esempio è la nostra workstation Irix), dovrete digitare una riga del tipo:
accept −i ec0 between jupiter mars
La macchine non elencate in questo file non saranno in grado di collegarsi a jupiter. La cosa può pure peggiorare: se non cambierete con *systune* il parametro *ipfilterd_inactive_behavior*, nessuno sarà più in grado di accedere alla macchina! Efficiente vero?? Questo parametro normalmente ha come valore 1, ma voi dovrete cambiarlo in 0 per mezzo del comando *systune −i ipfilterd_inactive_behavior 0*.
Un'altra cosa importante da tenere a mente è che Irix è possiede una grossa vulnerabilità nota come fam (File Alteration Monitor: Supervisore dell' alterazione dei file). Questo programma ha il compito di una funzione assai interessante: la comunicazione tra i vari servizi. Per esempio, se un utente abbia o meno il permesso di avere delle bellissime icone nel file manager o meno. In ogni caso esiste solo una cosa da fare riguardo questo sistema: disattivarlo! Lo so che la cosa suona come un qualcosa di assai triste, ma è necessario farlo.

Per terminare il dicorso sui sistemi Unix, lasciate che vi dica che QNX è molto vunerabile, ma anch'esso può trarre beneficio da questi strumenti. Per quel che riguarda MacOS X posso dirvi che ha in sè molti di questi strumenti che ho precedentemente citato.

Dobbiamo ora parlare del sistema che è divenuto di riferimentro tra le reti: il solo ed unico Windows NT4.0. Rendere sicura questa macchina è un qualcosa di utopistico, cntrariamente a quanto dica il Re di Redmond (e molte altre persone). Se si simula un attacco con nessus, per esempio, cadremo nell'incubo. Fintatochè NetBIOS è attivo, nessus vi fornirà i nomi di ogni macchina nel dominio e dei corrispettivi utenti, incusli gli amministratori. LA risposta potrebbe essere: eliminate NetBIOS! Certamente, eliminando questo protocollo, però non avremmo più la rete (quella nota come Rete Microsoft)... Dovete sceglier che cosa fare e da che parte stare.
nessun vi infoemerà cortesemente che potere anche effettuare l'accesso come utente guest con una sessione nulla (il che implica password nulla e username nullo). Rimuovete quell'utente! Ok, ma come? Sarà mica tutto così?
Ora riducete l'accesso alle partizioni (NTFS), alle directory. Per le partizioni in FAT non vi sono soluzioni. Tuttavia, a seconda del software che andate ad utilizzare, potreste avere bisogno della FAT: non tutti i software lavora correttamente su partizioni NTFS. Per terminare, evitate in maniera assoluta IIS, specialmente come ftp server. In vero... non installatelo. Infatti, se oggi molti ISP sono tanto pazzi da ricorrere ad IIS, n oi no possiamo fare altro che suggerire loro di ricorrere ad Apache, ma ora non andremo a perdere altro tempo su IIS, dato che esite molta documentazione in merito.
Per dovere di cronaca devo dirvi che esiste un modo per trasformare questo colabrodo in un flitro (avremmo quindi piccoli buchi!). Il problema nle fare questo è che non basterebbe un'intera rivista per guidarvi nell'operato. Lasciate che citi solo le cose più importanti. Il punto è che no nsi potrà ricorrere al software free per render sicuro questo sistima: vi ricordo che stiamo parlando di Microsoft! Il primo suggerimento è di ricorrere a MCSE (Microsoft Security Configuration Editor: Edito Microsoft per la Configurazione della Sicurezza) disponibile sul ServicePack 4 assieme ad MMC (Microsoft Management Console). Tuttavia siate molto cauti! Se fate un errore siete fritti! Ovviamente questo strumento esiste nella sola lingua inglese. Se utilizzate una versione nazionalizzata (ovvero non inglese) del vostro sistema potrebbe portare a non ottenere mai il risultato voluto. Vi ricordo che mescolare varie lingue con il sistema operativo di casa Redmond non produce mai buoni risultati... A seguire, tra le cose essenziali, dovrete rendere sicuro l'account di Administrator, o, ancr meglio, disabilitarlo. Date un occhio a *passprop* disponibile con il SP 3. Potete anche rendere le password più restittive per mezzo della dll *passfilt* con l'interazione del registro (ho sempre pensato che chi ha inventato quest'oggetto doveve esser sotto l'effetto dell' LSD...). Disabilita il famosissimo guest account. Non è di molta utilità (leggete sopra), ma almeno rende le cose meno danno di quanto non lo siano. Potete anche restingere gli accessi ai log di sistema. Nella chiave "HKEY_LOCAL_MACHINE" create le chiavi *System\CurrentControlSet\Services\EventLog\Application*, *System\CurrentControlSet\Services\EventLog\Security* e *System\CurrentControlSet\Services\EventLog\System*. Aggiungete la voce "RestrictGuestAccess" che debbono avere come tipo REG_SZ e con valore 1. Potete anche crittare le password con *syskey*. Siate però cauti in quanto si tratta di un'operazione NON reversibile! Alla fine una buona nuova: potete restringere l'acesso di guest. Ancora dovremmo cimentarci con il registro, con il tree "HKEY_LOCAL_MACHINE". La chiave in question è *System\CurrentControlSet\Control\Lsa*. Dovremmo aggiungere la voce "RestrictAnonymous", il cui tipo sarà "REG_DWORD" ed il valore 1. Ma siccome siamo nel mondo Microsoft.... sappiate che questo potrebbe influire sui servizi di rete alterandone alcuni... Tra le altre cose importanti, potete restringere gli accessi ad alcune porte per mezzo dell'icona di Rete nel Pannello di Controllo. Nelle Proprietà del TCP/IP, scegliete "Avanzate" ed attivate la voce "Sicurezza" (Penso che i nomi siano questi, ma no posso controllare in quanto non ho questo genere di cose in casa). Nella finestra della Sicurezza scegliete Permetti solo, e scegliete solo le porte che volete attivare. Anche qui siate cauti. Dovrete essere coscienti di quanto fate o alcuni servizi potrebbero non funzionare più.
i potrebbe dire molto di più, ma qui abbiamo trattato solo l'essenziale. Per saperne di più potete visitare sans.org: Vi sono tonnellate di documentazione disponibile.

L'insopportabile chiarezza delle cose

Bene, ora avete fatto tutto quello che vi ho suggerito. Bhe se controllerete di nuovo la vostra rete con nessus, scoprirete che avrete ancora problemi di sicurezza. Non vi dirò da dove scaturiscono... noi già lo sappiamo! Tentare di eludere questi problemi non li risolve. Certamente questo operare riduce i problemi legati a NetBIOS, ma di certo non limita i danni. Create dei sottodomini. Evitate di collegarvi come amministratore. Installate tutte le possibili correzioni. Come ultima risorsa provate a mascherare queste macchine dietro delle macchine Unix, da usarsi come gateway. Sfortunatamente il concetto di sicurezza relativa non è proprio della sola casa di Redmond. Una rete è un oggetto vivo: c'è sempre qualcosa che si muove, che si evolve, che nasce. Un buon amministratore è un tipo "paranoico", e, di conseguenza, costantemente controlla la lista delle correzioni. Scrive delle serie di comandi per automatizzare i processi. Per esempio controlla regolarmente il cambio dei bit di SUID e SGID nel file e nelle cartelle, i file critici, i log di sistema,... Al costo di qualche amico in meno, bloccate il floppy ed il CDROM. Non permette agli utenti di scaricare programmi senza il vostro consenso, specialmente se si tratta di software eseguibile, come spesso capita nel mondo Microsoft. Evitate di lasciare che i vostri utenti aprano liberamente allegati di office nelle mail senza che queste vengano correttamente filtrate. Lo so, potrei sembrare un despota, ma che potete fare contro i macro−virus? Evitat di ricorrere a prodotti come Outlook. Ancora una volta, dovete ben sapere che cosa volete! Lo so che quello che vi dico è inutile, ma potete parlare realmente di sicurezza con questo tipo di prodotti? Forse che il famosissimo "I love you" non vi ha insegnato ancora nulla?.
Per quel che riguarda il mondo Unix, anche in questo caso dovete controllare che cosa venga scaricato. I programmi per la verifica del checksum non sono stati inventati senza alcuno scopo.

Abiutatevi a monitorare la vostra rete su base regolare con log, script, scansioni,... Noterete che le cose mutano rapidamente, e non sempre per nel verso giusto.
Come ultima nota, non si è parato dei backup, ma mi raccomando di non dimenticarvene! Le strategia non mutano: backup quotidiani, settimanali e mensili. Anche una macchina Unix può avere dei problemi, anche se la cosa non è abituale. A volte gli stessi utenti commettono degli errori,... ma fortunatamente non così spesso. tutti pensano che i problemi provengano o dalle macchine o da chi ne ha cura,... mai (o quasi) dall'utente :−(

Ed eccoci giunti alla fine!

Se avete letto fino a qui siete coraggiosi. Il problema è che abbiamo solo affrontato lo strato superficiale del problema! La sicurezza è un argomento infinito e che non riguarda la sola rete. Applicazioni vulnerabili possono compromettere la rete. Per esempio un firewall mal configurato rende la situazione assai più preicolosa che non avere affatto un firewall. Una macchina Unix, di solito contiene migliaia di file. Chi può essere sicuro che nessuno di questi sia vulnerabile? Chi mai potrebbe pensare che un cracker cerchi di forzare una chiave a 128 bit? Non siate stupidi: cercherà di trovare anche l'ingresso di servizio. Mi ripeto, lo sò, ma cercate di installare tutti gli sturmenti atti alla sicurezza che potete, anche una piccola crepa nella nostra diga può essere dannosa, e di certo i cattivi la sfrutteranno.

La sicurezza è anche un modo di vita: fate attenzione a tutto ciò che accade. Per esempio, visitate regolarmente i siti web sulla sicurezza, del produttore del vostro sistema operativo,... Per esempio Sun pubblica le correzioni raccomandate per ogni sistema una volta al mese. SGI pubblica una nuova release di Irix ogni 3 mesi. Microsofto spesso fornisce ServicePack o HotFix. I distributori di Linux pubblicano una errata corridge ogni qual volta viene scoperta una nuova vulnerabilità. Lo stesso accade per la famiglia BSD. Se non utilizzate un prodottodo che bisogna di correzioni, rimuovetelo dal vostro disco fisso. E così via: la lista di cose da fare è immensa. In parole povere, questo è un lavoro che no si può accantonare!

Lasciate che mi ripeta: questo aiuta solamente a rendere la vostra rete meno vulnerabile. Non aspettatevi di poter ottenere una rete sicura al 100%, nemmeno ad una certa ora del giorno (bhe forse tranne quando tutte le macchine che vi partecipano sono spente). Si potrebbe dire che essere paranoici non è obbligatorio per fare questo tipo di lavoro, ma di certo aiuta! Ma per carità di Dio, non siate così rigidi ogni giorno della vostra vita, anche perchè il non esserlo vi renderà più accettabili da chi vi sta attorno...

Bibliografia e riferimenti

- http://www.linuxsecurity.com
- http://www.sans.org
- http://www.infosyssec.org
- http://www.securityfocus.com
- http://www.cs.purdue.edu/coast/hotlist/

La vita è dura: prendiamoci un poco di svago

Un altro modo di fare il proprio lavoro ;−)

2005−01−10, generated by lfparser_pdf version 2.51