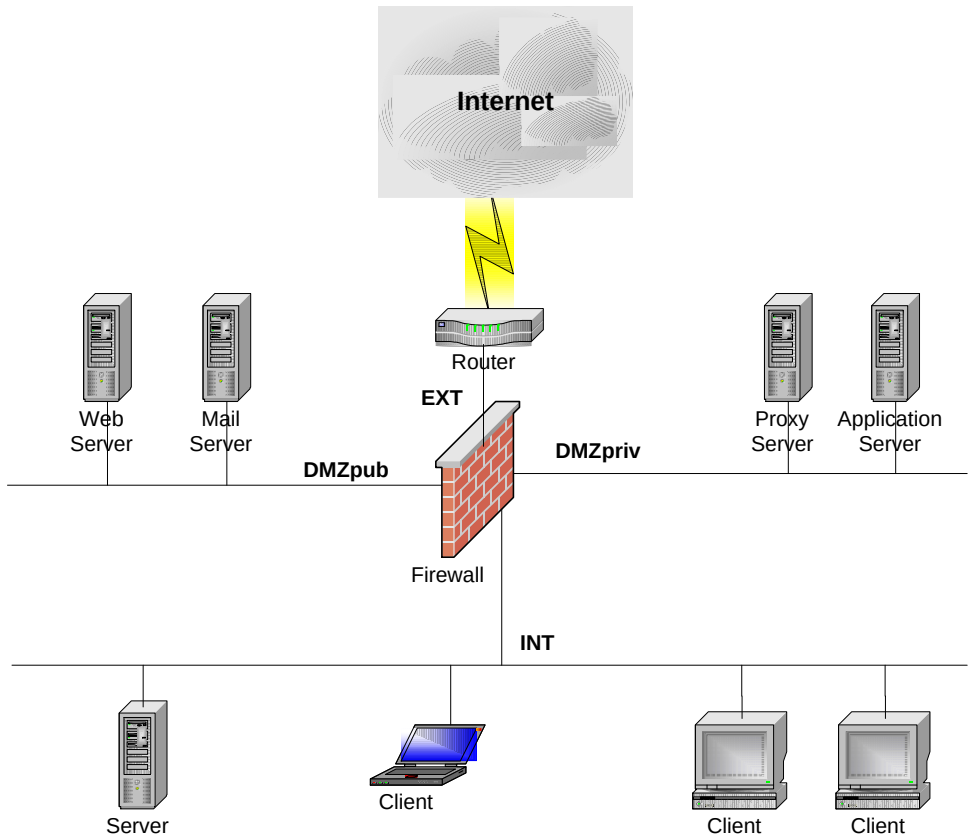
Articolo per ICT Security 2004/19 (Gennaio 2004).
Titolo:

L'uso di strumenti Open Source per il controllo della rete locale e del suo perimetro.

Summary : L'articolo prende in esame gli elementi classici di un sistema di sicurezza perimetrale di rete (firewall, intrusion detection system, sniffer, content filtering) ed evidenzia quali prodotti del mondo Open Source sono in grado di svolgere al meglio tali compiti e quali funzionalità avanzate possono mettere in azione sul campo.

Definiamo il territorio

Vedremo in questo articolo quali prodotti della sfera Open Source sono in grado di facilitare il nostro compito di tenere sotto controllo una rete locale ed il suo perimetro verso Internet svolgendo le funzionalità ormai classiche in information e network security di firewall, intrusion detection system, sniffer e content filtering.
Per poter visualizzare al meglio l'uso degli elementi che toccheremo definiamo un sempliche schema di rete perimetrale di sicurezza che ci accompagnerà in queste righe [figura 1] : tale schema comporta la suddivisione di un'ipotetica rete locale in una sottorete esterna affacciata direttamente verso Internet (*ext*), in una DMZ pubblica (*dmzpub*) dove posizionare i server che erogano servizi verso Internet, in una DMZ privata (*dmzpriv*) per i server che erogano servizi alla rete interna e nella rete interna stessa (*int*) dove vi sono i vari client aziendali e altri eventuali server interni.



[Figura 1]

Notiamo immediatamente che già questo semplice perimetro suddivide il traffico possibile della nostra rete locale in 12 differenti flussi informativi ognuno da guardare da un diverso punto di vista.

Definiamo i flussi informativi

I 12 flussi informativi che si vengono a creare con il loro punto di vista e le domande che tali punti ci portano sono i seguenti :

1. INT verso EXT : come si muovono i miei utenti su Internet, cosa fanno e dove navigano ?
2. INT verso DMZpriv : a quali servizi accedono i miei utenti sulla mia DMZ privata e come devono essere protetti da eventuale personale malevolo ?
3. INT verso DMZpub : i servizi erogati nella DMZ pubblica per l'esterno (Internet) saranno anche utilizzati dai miei utenti interni; devo proteggerli anche da loro ? In che modo ?
4. EXT verso INT : tale flusso di norma dovrebbe essere tutto bloccato.
5. EXT verso DMZpriv : tale flusso di norma dovrebbe essere tutto bloccato.
6. EXT verso DMZpub : l'anonimo utente di Internet come accede ai miei server che devono erogare servizio verso l'esterno ? Quali azioni deve poter fare e quali no ?
7. DMZpriv verso EXT : i server che erogano servizio alla rete interna devono uscire su Internet ? Per quali servizi ?
8. DMZpriv verso DMZpub : i server privati devono accedere in qualche modo ai server pubblici ?
9. DMZpriv verso INT : di norma tale flusso è bloccato, ma se qualche sviluppatore software della nostra azienda ha bisogno di far collegare un Web Server in DMZ privata verso un SQL server di sviluppo della rete Interna per provare un nuovo servizio della Intranet aziendale ?
10. DMZpub verso EXT : i server che erogano servizio verso l'esterno devono loro stessi poter uscire su Internet per qualche motivo ?
11. DMZpub verso DMZpriv : tale flusso di norma dovrebbe essere tutto bloccato.
12. DMZpub verso INT : tale flusso di norma dovrebbe essere tutto bloccato.

Gli strumenti

Come abbiamo appena visto le domande che ci poniamo sul nostro traffico di rete aziendale sono molteplici e ci portano immediatamente a sentire la necessità di mezzi per tenere sotto controllo la situazione.
Strumenti per poter applicare specifiche politiche di sicurezza al traffico (permettere, bloccare, effettuare log) ed ai flussi informativi in cui è suddivisibile, strumenti per individuare tempestivamente anomalie e per analizzare nel dettaglio situazioni particolari.
Genericamente gli strumenti principali, o forse solo i più usati, rientrano nelle categorie di Firewall (per l'applicazione di una policy sul traffico), di Intrusion Detection System (per la rilevazione di situazioni anomale e la generazione di allarmi), di Network Sniffer (per un'analisi dettagliata del traffico) e di Content Filtering (per l'analisi o l'applicazione di policy a livello applicativo).
Il mondo Open Source ci mette a disposizione prodotti specifici in ognuna di queste categorie con alcune funzionalità estremamente avanzate anche rispetto al mainstream commerciale.

Firewall : Linux Netfilter/Iptables

Netfilter/Iptables[1] è la componente di firewalling presente nei kernel di Linux 2.4 e 2.5 (Pkttables nei kernel 2.6). Essa risiede direttamente nella parte di networking IP interna al kernel e permette di creare tramite un'utility in user mode (iptables) svariate catene di policy da applicare al traffico di rete. E' un firewall stateful inspection (per cui è in grado di mantenere traccia delle connessioni e delle direzioni del traffico sia in TCP che in UDP e ICMP) ed è in grado di effettuare tutte le operazioni sui pacchetti che ci aspettiamo da un firewall moderno (NAT molti a uno o Mascheramento IP, NAT uno a uno o Statico, NAT uno a molti o Bilanciamento, PAT, redirezione del traffico, etc.). E' sufficientemente flessibile da permettere di definire la topologia dello schema di figura 1 e scrivere a quel punto le regole ragionando correttamente per flussi informativi [figura 2].

```
# Creazione nuove catene
/usr/sbin/iptables -N int-ext
/usr/sbin/iptables -N ext-int
/usr/sbin/iptables -N int-dmz1
...
# Definizione topologia
/usr/sbin/iptables -A FORWARD -i eth0 -o eth3 -j int-ext
/usr/sbin/iptables -A FORWARD -i eth3 -o eth0 -j ext-int
/usr/sbin/iptables -A FORWARD -i eth0 -o eth1 -j int-dmz1
...
# Regole suddivise per flussi
# Interno verso Esterno
# -------------------------
/usr/sbin/iptables -A int-ext -p tcp -d 0/0 --dport 80 -j ACCEPT
/usr/sbin/iptables -A int-ext -p tcp -d 0/0 --dport 6000:6010 -j LOG --log-prefix '#INT-EXT/DROP/XTERM## '
/usr/sbin/iptables -A int-ext -p tcp -d 0/0 --dport 6000:6010 -j DROP
…
```

[figura 2]

Senza dilungarsi oltre sulle funzionalità base di Netfilter/Iptables, che è al di fuori dello scopo di questo articolo, citiamo alcuni esempi di funzionalità avanzate di tale prodotto, forse meno note.
Netfilter presenta dei moduli aggiuntivi inseriti in una collezione definita Patch-o-Matic o altri moduli scritti da terze parti recuperabili sul web. Tra i più interessanti possiamo trovare :

- Base/Quota : permette di definire delle regole assegnando ad una specifica sorgente o destinazione un massimo di traffico consumabile in un determinato periodo di tempo;
- Base/Time : permette di definire delle regole valide solo in determinati periodi temporali;
- Extra/Ipmark : permette di marcare i pacchetti con combinazioni estremamente articolate (è un'evoluzione del modulo MARK) per prendere successive decisioni sul traffico così differenziato (precedenze su code, source routing, etc.);
- Extra/Tarpit : crea l'equivalente delle sabbie mobili per determinate connessioni, in modo da rallentare notevolmente diverse categorie di flooding o denial of service;
- Extra/String: è uno dei moduli aggiuntivi più potenti, permette di creare regole basate sul payload dei pacchetti con una sintassi simile all'IDS Snort. E' possibile creare regole per bloccare, ad esempio, specifici attacchi inserendone il pattern caratteristico o per bloccare anche e-mail o connessioni web contenenti parole chiave all'interno del testo;
- Out/Mirror : rinvia al mittente, come uno specchio, tutto i pacchetti che riceve e che corrispondono alla regola scritta contenente l'opzione di mirror;
- Out/Ipt_p2p[2] : riconosce tramite pattern definiti all'interno del modulo i principali software di peer to peer (Kazaa, Bittorrent, Gnutella, etc.).

Tra le funzionalità avanzate è interessante citare anche il progetto HIPAC[3] : High Performance Packet Classification for Netfilter, per chiunque abbia problemi di performance con un numero molto elevato di regole. Esso sostituisce l'algoritmo di scorrimento delle policy classico (dall'alto verso il basso) con alcuni algoritmi più efficienti permettendo un'ottima scalabilità di performance anche con molte centinaia di regole.

IDS : Snort

Snort[4] è un ottimo intrusion detection system free ed Open Source. Viene distribuito completo di un aggiornato set di signature per riconoscere attacchi noti o situazioni anomale. Ha un ottimo sistema di riassemblaggio dei pacchetti, operazione indispensabile per svolgere un'analisi efficace tramite signature del traffico transitato, evitando che l'attaccante divida semplicemente il suo attacco frammentando i pacchetti IP in modo opportuno per farli passare inosservati.

Intorno a Snort sono nate diverse suite di interfacce grafiche per la sua gestione o per l'analisi dei log o allarmi da esso generati, sia commerciali che free. Una delle migliori, nonché ovviamente per coerenza con il titolo dell'articolo Open Source, è Eagle X[5] di Engage Security, la quale si presenta come un pacchetto auto-installante con un semplice click di mouse su Windows 2000. E' composta da un motore Snort per l'analisi del traffico, da un database MySQL per lo stoccaggio dei dati, un'ottima interfaccia grafica WIN32 per l'installazione, configurazione e aggiornamenti automatici delle signature e da un server Apache con pagine PHP per il controllo dei log e lo stato runtime dell'IDS.

La facilità dell'installazione con una suite automatica non toglie comunque i due principali problemi nell'uso efficace di un Intrusion Detection System : il posizionamento ed il tuning.
Per ottenere un reale ritorno in termini di sicurezza dall'uso di questo tipo di strumento è necessario che il traffico visto dall'IDS sia quello che maggiormente ci interessa tenere sotto controllo per criticità delle informazioni gestite dai server indirizzati. Nel nostro schema di rete di esempio i punti dove si potrebbero posizionare le interfacce stealth degli IDS sono in DMZ pubblica e in DMZ privata (ovviamente su delle porte di monitor degli switch nelle due sottoreti, in modo che la macchina con il software di instrusion detection possa ricevere anche il traffico di tutte le altre).
Posizionati i sistemi è necessario effettuare un accurato e preciso tuning delle signature da attivare o meno o addirittura da modificare ad hoc, in modo da limitare i falsi allarmi e rendere efficaci quelli veri. Tuning che va rigorosamente rivisto ad ogni variazione delle reti interessate (nuovi server o nuovi servizi erogati da questi o variazioni sostanziali dell'utenza in numero o in abitudini).

Sniffer : Dsniff

Dsniff[6] è una suite completa di sniffer a basso livello : niente interfaccia grafica o software di analisi dei dati catturati, ma velocità e precisione nel mettere da parte quello che potrebbe interessarci catturare. Le utility che la compongono sono le seguenti :

- Dsniff : per l'intercettazione di password usate in vari protocolli di rete (telnet, posta, ftp, etc.);
- FileSnarf : per l'intecettazione di file con vari protocolli di file sharing;

- MailSnarf : per l'intercettazione della posta elettronica;
- MsgSnarf : per l'intercettazione dei contenuti dei protocolli di chat;
- UrlSnarf : per l'intercettazione degli indirizzi navigati dagli utenti;
- WebSpy : per replicare in tempo reale su un Netscape/Mozilla della macchina sniffer i siti visitati dagli utenti.

La suite è completata da alcune componenti per effettuare operazioni di arp spoofing verso gli switch in modo da poter effettuare sniffing del traffico anche se privi di porte di monitor.

Diciamo che i tutori della privacy potrebbero avere qualcosa da ridire sulle funzionalità dei vari moduli di Dsniff !

Solitamente questi strumenti (a meno che il vostro 'mestiere' non sia quello di hacker malevolo o black hat) sono attivati su una macchina sempre pronta per ogni evenienza solo in casi particolari. Questi possono essere o il sospetto/certezza dell'attività di un intruso esterno o il sospetto/certezza di attività illecite (per la legge o per le politiche aziendali) da parte di utenti interni.

I dati ottenuti tramite Dsniff e un buon prodotto office di spreadsheet (Excel di Microsoft Office o SpreadSheet di Open Office[7]) permettono di effettuare analisi forensi molto approfondite.

Content Filtering

Il Content Filtering è una categoria che racchiude in se stessa un intero mondo, cioè tutti i prodotti in grado di fare analisi o di applicare policy a livello applicativo (sulla navigazione, sulla posta elettronica, sul file transfer, etc.). Citerei in questa occasione solo un esempio di sistema per il controllo della posta elettronica compreso di antivirus e antispamming.
Il server di posta (o anche solo mail relay di perimetro verso il mail server interno) potrebbe essere uno dei vari e ottimi prodotti Open Source (sendmail, qmail o postfix). Il sistema di content filtering che si interfaccia all' MTA è MailScanner[8], il quale permette di effettuare archiviazione di tutta la posta in transito o svariati controlli sugli attachment ed in più è in grado di usare le funzionalità di un ottimo antispam come SpamAssassin[9] e di vari antivirus commerciali (preoccupandosi lui di decodificare gli attachment in MIME e passare i file all'antivirus per il controllo e di effettuare gli aggiornamenti delle signature dell'antivirus dai siti dei produttori).

Conclusione

Il vantaggio dei prodotti Open Source nell'ambito dell'Information and Communication Security è quello di avere a disposizione un sorgente aperto, controllabile in ogni sua parte e modificabile in caso di necessità. Questo permette un'estrema flessibilità sia nell'uso che nell'integrazione di strumenti o prodotti con funzionalità diverse, ma che solo nel loro complesso ci permettono di effettuare tutte quelle operazioni necessarie a mantenere la nostra rete sotto controllo e, speriamo, sicura.

Il fatto che buona parte dei prodotti Open Source visti agisca a basso livello non presentando comode interfacce precotte ha sì il lato negativo di dover disporre di un ottimo know-how interno in azienda (o se non interno comunque reperibile esternamente da partner fidati), ma anche quello positivo di comprendere veramente i processi che avvengono sulla nostra struttura di rete ed agire di

conseguenza senza la maschera di un'interpretazione visuale di un prodotto intelligente quanto si vuole, ma automatico e non umano.

Ing. Davide Casale
professore a contratto di Reti di Calcolatori,
Politecnico di Torino
e-mail: casale@davidecasale.com

Sitografia:

1- Linux IPTABLES : http://www.netfilter.org

2- Linux IPTABLES modulo Ipt_p2p per il peer to peer : http://mega.ist.utl.pt/~filipe/ipt_p2p/)

3- NF-HIPAC : http://www.hipac.org

4- SNORT : http://www.snort.org

5- EAGLE X : http://www.engagesecurity.com/products/eaglex/

6- DSNIFF : http://www.monkey.org/~dugsong/dsniff/

7- OpenOffice : http://www.openoffice.org

8- MailScanner : http://www.mailscanner.info

9- SpamAssassin : http://www.spamassasin.org