Real Security & Iptables

Giuseppe Augiero

Security

Sicurezza?

- In ambito informatico con la parola “Sicurezza” si intende la ***sicurezza dell’informazione***.

- La sicurezza informatica definisce *le regole per il controllo dell’accesso all’informazione e alle risorse*.

Principi di base

Occorre garantire:

- **Confidenzialità**: solo chi e' autorizzato conosce l'informazione.
- **Integrità**:l'informazione non può essere manomessa da chi non e' autorizzato.
- **Disponibilità**: l'informazione e' disponibile per chi ha l'autorizzazione ad usarla.

Sicurezza

- Esiste un conflitto tra sicurezza e facilità di utilizzo di un computer.
- La sicurezza è considerata un **costo** e non un beneficio.
- Non si comprende il valore dei dati da proteggere.

Dinamicità

- La sicurezza non ha uno sviluppo statico ma **è un processo iterativo.**

Analisi del rischio

- Comprensione delle insicurezze.
- Definizione di priorità.
- Implementazione di Sistemi Esperti.

- Occorre effettuare un Trade-Off !!!

Politiche di sicurezza

- Fornire linee guide.
- Soluzioni implementabili.
- Accettabile da parte di tutti.
- Controllare che siano rispettate (audit)
- Responsabilizzare.
- Scegliete gli obiettivi per valutare il trade-off.
- Facilità di utilizzo.
- Valutare i costi.

Progettazione della sicurezza

- Minimi privilegi.
- Prevedere diversi livelli.
- Prevedere diversi sistemi di sicurezza.
- Centralizzare la gestione.
- Concentrare l'attenzione sui punti deboli.
- Fail-over.
- Partecipazione di tutti gli utenti.

Audit

- Analisi dei log non e' una operazione banale.

- Le ragioni di analisi possono essere:
  - controllo delle operazioni effettuate
  - controllo del rispetto delle politiche di sicurezza
  - Ricerca di segni di intrusione

Da chi dobbiamo difenderci?

- Hackers.
- Crackers.
- Ricercatori di informazioni.
- Procutatori di Denial of Service.
- Virus e Cavalli di Troia.

Motivazioni

- Furto.
- Modifica delle informazioni.
- Odio.
- Motivazioni politiche/religiose.
- Sfida intellettuale.

Sicurezza in rete: Firewalls

Firewall

- E’ un sistema di protezione perimetrale tra due reti (p.es.lan e Internet).
- Tutto il traffico da e verso Internet deve passare da un unico nodo (il firewall).
- Il firewall non deve essere visibile.

I punti di forza:

- Centralizza le politiche di sicurezza.
- Centralizza i log e i messaggi di allarme.
- Previene il foot-printing.
- Permette di usare sistema di strong security.

Categorie di Firewalls

- Packet filters e screening routers.
- Application gateways e proxy servers.
- Stateful inspection.
- Soluzioni ibride.

Le regole

- Definizione di una lista in cui ogni elemento (regola) definisce se un particolare tipo di traffico deve passare o non passare.
- Possibilità di utilizzare operatori relazionali.

- E’ importante l’ordine delle regole !

“La Filosofia del gioco”

- Il design delle policy di un firewall può seguire uno dei seguenti approcci:

  - permetto, e nego tutto il resto

    (+ sicuro)

  - nego, e permetto tutto il resto

    (- sicuro)

Le regole d'oro

- Stealth rule:

  E' buona norma inserire come all'inizio della lista, una regola che rende il firewall invisibile.

- Clean Up rule:

  Alla fine della lista occorre inserire una regola che neghi tutto il traffico non permesso (drop su catch-all).

Antispoofing e Rfc 1918

Architettura di un firewall

- Il firewall può essere un prodotto hw o sw.
- Se il firewall è software occorre "*bastionizzare*" la macchina su cui gira.

- In generale la configurazione di un firewall e' una operazione complessa.

Iptables

IpTables

- Iptables e' parte integrante di netfilter.
- Netfilter e' il framework di manipolaggio pacchetti che mette a disposizione il kernel di Linux.
- Supporto kernel 2.4 e 2.6
- Successore di ipfwadm e ipchains.

Come installare IPT

- Iptables e' parte integrante del kernel 2.4 e 2.6
- Per usare le funzionalità di iptables occorre attivare il supporto dal Kernel
- Ricompilazione del Kernel.

L’architettura

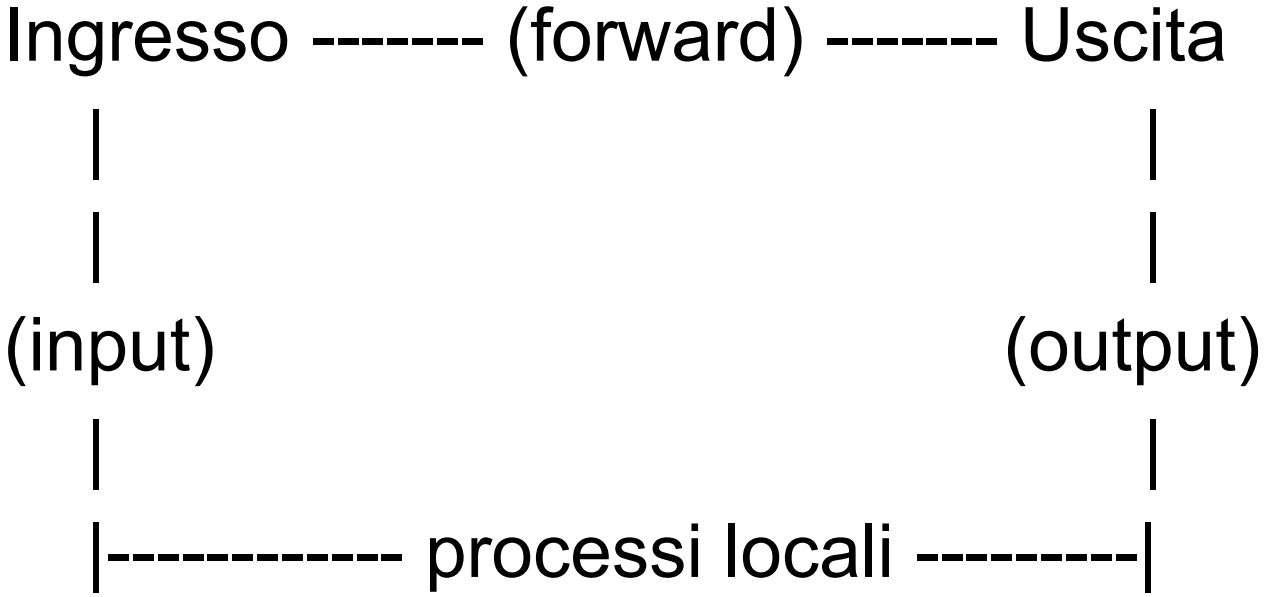
Di default iptable e’ composto da tre tabelle:

- **Filter**
- **Nat**
- **Mangle**

Ogni tabella contiene più catene.

Ogni catene e’ una lista di regole ordinate.

Filter



Le policy

- Di default esistono tre catene (Input/ Output/Forward).
- Una catena e’ un insieme di regole
- Ogni regola definisce cosa bisogna fare con il traffico identificato.
- Se non esiste una regola per il traffico viene applicata la policy generale della catena.

Azioni da intraprendere:

- **Accept**
- **Drop (timeout)**
- **Reject**

- Il traffico in drop o reject può essere monitorizzato e loggato.

Operazioni su catene (1)

- **Creare una nuova catena**
  Opzione `-N' oppure `--new-chain':
  iptables -N test

- **Cancellare una catena**
  Opzione `-X' o `--delete-chain'.
  iptables -X test
  Le catene devono essere vuote
  Le tre catene predefinite non possono essere cancellate.

Operazioni su catene (2)

- **Svuotare una catena**

  iptables -F forward

  Se non si specifica una catena, allora *tutte* le catene saranno svuotate.

- **Consultare una catena**

  E’ possibile ottenere una lista delle regole di una catena usando il comando `-L' (o `--list').

Operazioni su regole

Una regola può essere:

- **Aggiunta** a una catena (--append oppure -A).
- **Cancellata** da una catena (--delete oppure -D).
- **Rimpiazzata** in una catena (--eplace oppure -R).
- **Inserita** in una catena (--insert oppure -I).

Definizione di una regola

- **-p** *Procotollo*
- **-s** *source ip address*
- **-d** *destination ip source*
- **-i** *interfaccia di rete*
- **--sport** *porta sorgente*
- **--dport** *porta destinazione*
- **--tcp-flags** *(Syn/Ack/Fin/Rst)*
- **-j** *azione da intraprendere*

Network Address Traslation

- Il Nat permette di modificare l'indirizzo Ip dei pacchetti che transitano su un router.
- Perché utilizzare il nat ?
- Nat crea un falso senso di sicurezza.

Iptables e Nat

- La regola da utilizzare per nattare i pacchetti e' :

  iptables -t nat -A POSTROUTING -o [wan-int] -j MASQUERADE

E' necessario abilitare l'ip forwarding:

echo 1 > /proc/sys/net/ipv4/ip_forward

Mangle

- Mangle e’ un tabella particolare usata per manipolare i pacchetti.
- E’ possibile marcare i pacchetti (MARK).
- Modificare il TOS.
- Modificare il TTL.

Catene Mangle

- Le catene che troviamo nella tabella Mangle sono:

- Pre Routing
- Post Routing

Tracciamento

- Attraverso il modulo ip_conntrack e' possibile tenere traccia delle connessioni.
- Il tracciamento ci permettete di capire se un dato pacchetto fa parte di una determinata connessione.

Stato pacchetti

- NEW – Il pacchetto non e' correllato a nessuna connessione ed e' teso a creare una nuova connessione.
- ESTABLISHED – Il pacchetto appartiene a una connessione (p.es un pacchetto di risposta).
- RELATED – Il pacchetto e' correlato ma non appartiene a nessuna connessione esistente (p.es. icmp o ftp).
- INVALID - Non e' stato possibile ricavare lo stato del pacchetto.

Stato pacchetti (2)

- Le opzioni di iptables per controllare lo stato del pacchetto sono:

  iptables -m state –state NEW, ESTABLISHED, RELATED, INVALID

Esempi

Ripulire le catene

iptables –F INPUT

iptables –F FORWARD

iptables –F OUTPUT

Primo script

- Impostiamo una politica di default.

- *iptables –P INPUT DROP*
- *iptables –P FORWARD DROP*
- *iptables –P OUTPUT ACCEPT*

Accettiamo traffico web

- Vogliamo che il traffico web verso la nostra macchina sia consentito:

iptables –A INPUT –p tcp –d 4.4.4.4 –dport 80 –j ACCEPT

Subnet

- Per accettare il traffico in ingresso da una specificata subnet possiamo definire la regola:

  iptables –A INPUT –s 4.4.4.0/24 –j ACCEPT

Bloccare

- Per bloccare tutto il traffico provenienete da un determinato Ip possiamo definire la regola:

iptables –A INPUT –s 1.1.1.1 –j DROP

Bloccare traffico SSH

- Per bloccare il traffico ssh provenienete da un determinato Ip possiamo definire la regola:

iptables –A INPUT –s 1.1.1.1 –p tcp –dport 22 –j DROP

Utility

- Per salvare la regole definite in iptable:
- *iptables-save > file*

- Per ripristinare le regole salvate:
- *iptables-restore < file*

Domande?