

IPTABLES - NETFILTER

Sistemi molto comuni quando si vuole mascherare alle applicazioni il funzionamento della rete [sostanzialmente facendo un NAT in locale].

Il vantaggio è di avere un HOST LINUX nella cui parte kernel è implementato NETFILTER, che permette di utilizzare delle regole che vengono applicate ai pacchetti di rete che o attraversano il suo host, o sono creati da applicazioni che girano sul suo host.

↳ qualunque pacchetto che si trova sul quell' host può essere selezionato, e può subire modifiche.

IPTABLES: comando che può essere lanciato [\Rightarrow si trova a livello applicazione] e tramite esso indicare a Netfilter quali regole fare applicare e a quali pacchetti.



Presso un gateway avente un'interfaccia sulla rete privata, ed un'interfaccia sulla rete pubblica, è possibile trasportare un NAT tramite il controllo, ed eventualmente il delete, dei pacchetti.

Tramite iptables e netfilter è possibile selezionare un pacchetto, girarlo ad una applicazione locale che lo manipola e successivamente lo ripedisce nelle code del kernel \Rightarrow per es: potrei intercettare i pacchetti dell'applicazione SKYPE, passarli alla mia applicazione locale, modificarli in un qualche modo [o anche scartarli] per poi ripassarli a SKYPE come se nulla fosse.

NATURALMENTE PER FAR CIÒ SONO NECESSARI PRIVILEGI DI AMMINISTRATORE DI SISTEMA!

SCHEMA GESTIONE PACCHETTI DI UN HOST DA PARTE DEL SISTEMA NETFILTER:

FASE 1: Pre-routing

Il sistema riceve un pacchetto \Rightarrow bisogna capire a chi è indirizzato tale pacchetto, se ad un processo locale o ad un altro host [\Rightarrow la nostra macchina funge da relay];

[Se il pacchetto è diretto ad un processo locale all' host \Rightarrow viene inserito nella coda di INPUT del processo, avendo eventualmente la possibilità di modificarlo prima di passarlo al processo; una volta uscito dal processo, ovvero inserito nella coda di output del processo, il pacchetto può essere sempre modificato.

A questo punto il pacchetto può essere ripedito ad un altro processo locale, oppure indirizzato verso l'esterno della rete. *

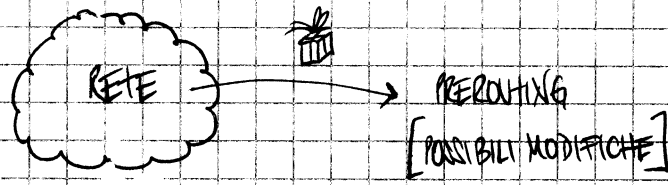
\rightarrow Se il pacchetto non è diretto ad un processo locale, ovvero è diretto all'esterno entra nella fase di FORWARDING, durante la quale può comunque essere manipolato. *



A questo (*) punto vi è un'alternativa fare localmente: loro aprire prima chi è il next hop + ai indirizzarlo, le politiche aprire qual'è l'interfaccia di rete attraverso la quale spedirlo
 ↳ una volta deciso tutto quanto si entra nella fase di ROUTING, dove posso sempre modificarlo prima di re-inserirlo nella rete.

N.B.

Giunte alla fase di ROUTING posso effettuare la modifica dell'indirizzo mittente [⇒ ATTAGE il pacchetto]



[il pacchetto è indirizzato ad un processo locale all'host?
 il pacchetto è indirizzato ad un altro host [⇒ l'attuale host svolge la relay]]

inserso il pacchetto nella coda di INPUT del processo
 [POSSIBILI MODIFICHE]

PROCESSO

inserso il pacchetto nella coda di OUTPUT del processo
 [POSSIBILI MODIFICHE]

inserso il pacchetto in uno stato appropriato alla fase FORWARD
 [POSSIBILI MODIFICHE]

A chi è indirizzato il pacchetto?
 con quale interfaccia spedire il pacchetto?

ROUTING
 [POSSIBILI MODIFICHE]

