Netfilter

Introdución

- Netfilter é un firewall de estado presente no Kernel Linux
- Netfilter é xestionado mediante utilidades como iptables ou a máis moderna nftables
- Netfilter proporciona:
  - Filtrado nas capas TCP/IP 2 (Internet) e 3 (Transporte)
  - Seguimento de conexións
  - NAT e NAPT
  - Posibilidade de manipular das cabeceiras dos paquetes
- Con Netfilter é posible facer entre outras cousas:
  - Firewalls de filtrado con ou sen seguemento de conexións
  - Firewalls de host e de rede
  - Routers-firewall con NAT
  - Obrigar ao uso dun proxy usando NAT (proxy trasparente)
  - Sistemas de QoS

Conceptos Xerais

- **Regras** (rules): Unha regra é unha especificación que indica qué paquetes se seleccionan e qué acción se realiza con eles. Para que se seleccione un paquete debe cumprir todas as condicións especificadas na regra. As accións poden ser:
  - ACCEPT, DROP, REJECT, LOG, DNAT, SNAT, REDIRECT, MARK
- **Cadeas** (chains): Unha cadea é unha lista ordeada de regras. Para cada paquete de datos:
  - Se comproba si a regra se aplica, se non e así se pasa a seguinte regra da cadea
  - Se a regra se aplica, se executa a acción e se remata o procesamento
  - As chains teñen políticas (**policy**) que indican qué acción se debe levar a cabo para os paquetes aos que non se aplica ningunha regra. As políticas so poden ser ACCEPT ou DROP
  - Os usuarios poden definir as súas propias *chains*, pero existen sempre as seguintes cadeas predefinidas: PREROUTING, INPUT, FORWARD, OUTPUT e POSTROUTING

Conceptos Xerais

  - O usuario pode crear as súas propias *chains* para crear firewalls complexos e organizar de xeito convinte as distintas regras. A política por defecto das chains de usuario sempre é RETURN, que retorna o control a chain anterior.

- Táboas (tables): Unha táboa contén un conxunto de cadeas, tanto predefinidas como de usuario relativas ao tipo de procesamento. Netfilter define as seguintes táboas:
  - **filter**: é a táboa por defecto e contén regras de filtraxe dos paquetes (firewall)
  - **nat**: esta táboa almacena regras de traslación de direccións NAT e NATP
  - **mangle**: esta táboa almacena regras de modificación de campos do paquete IP (TTL, ToS...) además de poñer marcas para que se podan recoñecer e elaborar sistemas de QoS ou de rutado.
  - **raw**: permite procesar os paquetes antes de ser rexistrado na táboa de seguimento de conexións. O seu obxectivo e poder marcar con NOTRACK os paquetes que desexamos excluír do seguimento.

Procesamento de paquetes en Netfilter