Sicurezza nelle reti

Manipolazione indirizzi IP

Concetti – Reti

- Rete IP definita dalla maschera di rete
- Non necessariamente concetto geografico
  - Non è detto che macchine della stessa rete siano vicine

Concetti – Reti

- Non necessariamente concetto topologico
  - Non è detto che macchine della stessa rete non siano sparse
- Di fatto identifica un insieme di macchine quindi di luoghi

Concetti – Zone

- Definiscono concetti topologici
- Le zone identificano aree a differente criticità
  - Internet a bassa criticità, DMZ a media criticità, Locale ad alta criticità
- Le zone identificano aree con differenti pertinenze
  - Laboratori
  - Amministrazione

Concetti – DMZ

- De militarized zone ovvero terra di nessuno
- Indica il posto a media sicurezza in cui sono poste le apparecchiature che erogano servizi verso Internet

Concetti – DMZ

- Di solito le apparecchiature della DMZ erogano servizi che richiedono l'accettazione di connessioni in ingresso (Web, mail, name server)
- Le apparecchiature della DMZ di solito non iniziano connsssioni (eccezioni sono mail server e name server primari che allineano i secondari)

Routing

- Modo con cui i pacchetti sono instradati in reti differenti
- Normalmente per i client ci si limita ad un default gateway
- Anche le piccole reti operano così
- Reti più grosse operano associando gateway a differenti reti in modo da poter differenziare gli invii (ciò significa disporre di più schede di rete dedicate ai vari instradamenti)

Source routing

- Indirizzamento basato sulla provenienza
- Necessario quando vi sono più reti che arrivano ad una scheda multihomed (con più indirizzi IP)

Source routing

- I pacchetti in ingresso dalle reti arrivano alla stessa scheda ma con indirizzi di destinazione differenti
- I pacchetti di risposta che emergono dalla scheda debbono prendere una strada o l'altra a seconda dell' indirizzo sorgente in modo da tornare alla rete da cui provenivano le richieste

Masquerading

- Sostituisce l'indirizzo IP mittente dei pacchetti provenienti dalla LAN interna con l'indirizzo IP pubblico presente sulla scheda di rete.
- Risparmio di indirizzi IP perchè permette di usare sulla LAN indirizzi IP privati

Masquerading

- Scambio tra indirizzo IP e numero di porta dato che questo veicola l'informazione relativa al reale indirizzo IP
- Alle volte definito anche Network Address Translation (NAT) o Source NAT (SNAT)

DNAT

- Destination NAT
- Usato per tradurre un indirizzo IP di destinazione in un altro
- Utile per tradurre un IP pubblico di un pacchetto che entra da Internet in un Firewall in un IP privato corrispondente ad un server posto in una DMZ
- Si può fare anche il DNAT di una singola porta facendo puntare servizi differenti su macchine differenti

Mangling

- Mangling è qualunque attività di modifica di un pacchetto e quindi includerebbe tutti i tipi di NAT

Mangling

- Con mangling si indicano specificatamente le attività di:
  - Type of service (TOS) (minimizzare i ritardi, massimizzare il throughput, massimizzare l'efficenza, minimizzare i costi, operare normalmente)
  - Time to live (TTL) (per limitare il numero di hop)
  - Mark setting (MARK) (particolarità di routing)

Route

- Programma per gestire le tabelle di routing
  - *route add* inserisce righe nella tabella
    - `route add –net 0.0.0.0/0 gw 192.168.1.254 dev eth0`
  - *route del* toglie righe nella tabella
  - *route print* visualizza i dati della tabella

Ip

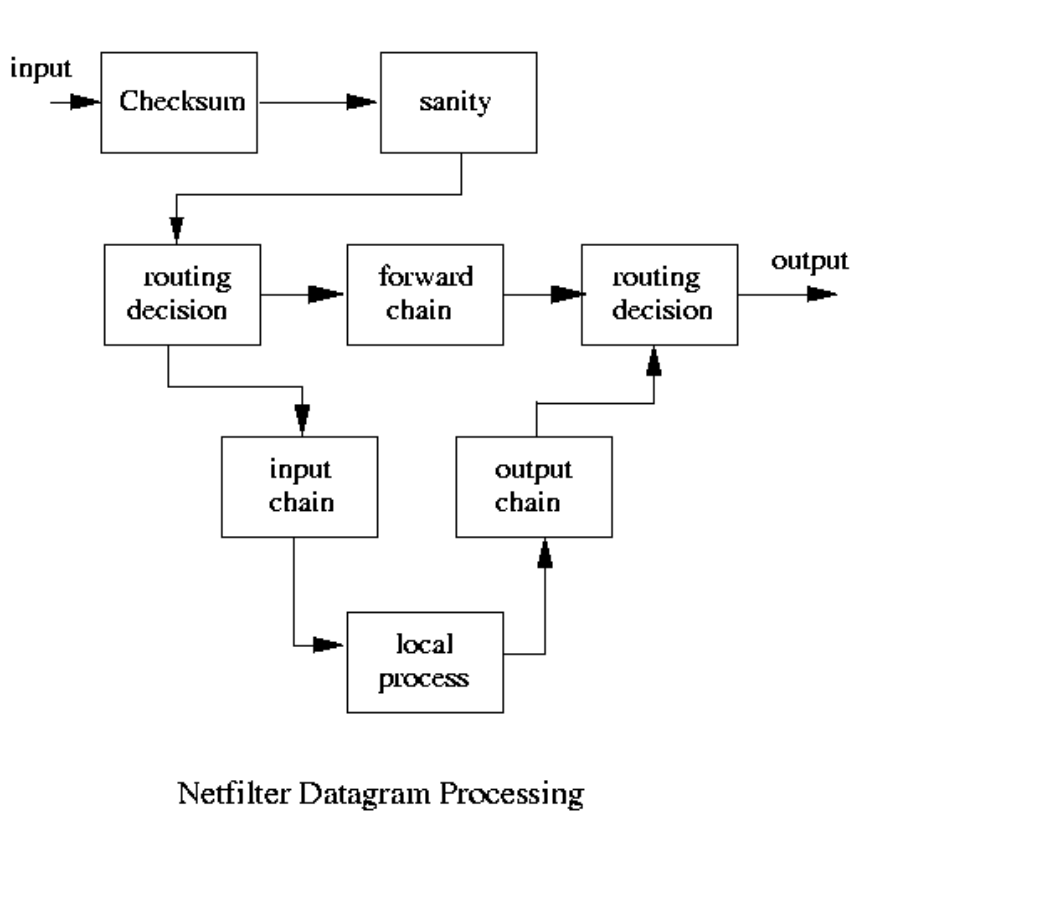
- Programma avanzato per la gestione delle tabelle di routing
- Indispensabile per il source routing
- Permette di creare delle tabelle di routing 'normali' (tabella main)
- Permette di creare delle tabelle di regole avanzate e di aggiungerle in modo da attivarle

Source routing con Ip

```
#Crea le tabelle con le source route
ip route add 192.168.1.0 dev eth0 src 192.168.1.1 table prov1
#Crea due route di default nelle tabelle
ip route add default via 192.168.1.254 table prov1
#Inserisci una tabella di default nella tabella main
ip route add default via 192.168.1.254
#Crea le tabelle di uscita (non indispensabile)
ip route add 192.168.1.0 dev eth0 src 192.168.1.1
#Crea le source route usando le tabelle
ip rule add from 192.168.1.1 table prov1
```

Iptables

- Pacchetto del kernel di linux usato per la gestione delle attività di conversione IP



Netfilter Datagram Processing

Iptables

- Iptables ha tre tabelle: filter, nat e mangle
- Ogni tabella ha un set predefinito di catene legata ad una particolare fase del processo di invio del pacchetto
- Normalmente viene utilizzata la tabella filter e le catene INPUT and OUTPUT per filtrare il traffico.
- La catena FORWARD è utilizzata per i compiti di filtraggio del routing.

Iptables

- Per la traduzione degli indirizzi IP si utilizza la tabella nat e le sue catene PREROUTING
- Si usa anche la tabella mangle e le sue catene PREROUTING e OUTPUT

Iptables

- Nella tabella nat la catena PREROUTING viene usata per modificare i pacchetti prima che vengano 'routati' e la catena POSTROUTING per farlo prima che lascino il sistema. La catena OUTPUT viene usata per i pacchetti generati nel sistema

Iptables

- La tabella mangle usa normalmente le catene PREROUTING e OUTPUT
- Nei kernel più nuovi la tabella mangle utilizza le catene INPUT, FORWARD e POSTROUTING in modo da poter effettuare delle operazioni di mangle in un qualunque fase del processo

Iptables

- Implementazione del masquerading:

```
iptables -t nat -A FORWARD -i eth1
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

- La prima regola indica che vengono forwardati i pacchetti che entrano da eth1
- La seconda regola indica di effettuare il masquerading dei pacchetti che lasciano l'interfaccia eth0

Iptables

- Implementazione del DNAT:

```
iptables -t nat -A PREROUTING -i eth0 -j DNAT -
  -to-destination 192.168.1.1

iptables -t nat -A PREROUTING -p tcp --dport 80
  -j DNAT --to-destination 192.168.1.2 -to-port
  8080
```

- La prima regola invia ogni pacchetto ricevuto da eth0 al server 192.168.1.1
- La seconda trasmette tutto il traffico web ad un differente host che risponde sulla porta 8080 e non sulla porta 80

Iptables

- Implementazione di mangling:

```
iptables -t mangle -A OUTPUT -p tcp --dport smtp
  -j TOS --set-tos 16
```

- La regola setta il TOS a 16 in modo da minimizzare i ritardi (TOS=16)
- Con queste regole si possono operare impostazioni sulla QoS (Quality of Services)