es 1 iptables

Ti spiegherò passo passo come inserire una regola di logging nella catena `FORWARD` di `iptables`, in modo da registrare i pacchetti destinati alla porta 22 (SSH) che non vengono accettati dalle regole iniziali. Queste regole di logging devono essere inserite immediatamente prima delle regole `DROP` esistenti, così da registrare i pacchetti che verrebbero altrimenti scartati.

Procedimento Dettagliato

1. **Visualizzazione delle Regole Attuali**: Per iniziare, visualizziamo le regole attuali della catena `FORWARD` con l'opzione `-line-numbers` per vedere l'ordine delle regole.

   ```
   iptables --line-numbers -vnL FORWARD
   ```

   Questo comando ti mostra qualcosa di simile:

   ```
   Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
   num   pkts bytes target     prot opt in     out     sour
   ce               destination
   1        0     0 ACCEPT     tcp  --  *      *       192.
   168.20.20        192.168.10.10        tcp spt:22 state E
   STABLISHED
   2        0     0 ACCEPT     tcp  --  *      *       192.
   168.10.10        192.168.20.20        tcp dpt:22
   3        0     0 DROP       tcp  --  *      *       0.0.
   0.0/0            0.0.0.0/0            tcp spt:22
   4        0     0 DROP       tcp  --  *      *       0.0.
   0.0/0            0.0.0.0/0            tcp dpt:22
   ```

   Qui puoi vedere che le regole `DROP` per i pacchetti SSH sono in posizione 3 e 4.

Descrizione delle Regole Esistenti

1. **Regola 1**: Accetta i pacchetti TCP dallo sport 22 di `192.168.20.20` a `192.168.10.10` se lo stato della connessione è `ESTABLISHED`.

2. **Regola 2**: Accetta i pacchetti TCP destinati alla porta 22 da `192.168.10.10` a `192.168.20.20`.
3. **Regola 3**: Scarta (DROP) tutti i pacchetti TCP provenienti dalla porta 22.
4. **Regola 4**: Scarta (DROP) tutti i pacchetti TCP destinati alla porta 22.

2. **Identificazione della Posizione Correttiva**: Abbiamo identificato che dobbiamo inserire la nostra regola di logging prima delle regole `DROP`, quindi alla posizione 3.
3. **Inserimento della Regola di Logging**: Ora inseriamo la regola di logging alla posizione corretta. Utilizziamo il comando `iptables -I` per inserire la nuova regola nella posizione desiderata.

   ```
   iptables -I FORWARD 3 -j LOG --log-prefix " ssh pre-drop
   "
   ```

   Questo comando inserisce una nuova regola nella posizione 3, spostando le precedenti regole 3 e 4 in giù di una posizione.

   - `I FORWARD 3`: Indica di inserire la nuova regola nella catena `FORWARD` alla posizione 3.
   - `j LOG`: Specifica che l'azione della regola è di loggare i pacchetti.
   - `-log-prefix " ssh pre-drop "`: Aggiunge un prefisso al messaggio di log per identificare facilmente i pacchetti loggati.
4. **Verifica dell'Inserimento**: Dopo aver inserito la regola, è una buona pratica verificare che sia stata effettivamente inserita nella posizione corretta.

   ```
   iptables --line-numbers -vnL FORWARD
   ```

   Dovresti vedere qualcosa del genere:

   ```
   Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
   num   pkts bytes target     prot opt in     out     sour
   ce               destination
   1        0     0 ACCEPT     tcp  --  *      *       192.
   168.20.20        192.168.10.10        tcp spt:22 state E
   STABLISHED
   2        0     0 ACCEPT     tcp  --  *      *       192.
   ```

```
168.10.10        192.168.20.20        tcp dpt:22
3        0     0 LOG        all  --  *      *       0.0.
0.0/0            0.0.0.0/0            LOG flags 0 level
4 prefix " ssh pre-drop "
4        0     0 DROP       tcp  --  *      *       0.0.
0.0/0            0.0.0.0/0            tcp spt:22
5        0     0 DROP       tcp  --  *      *       0.0.
0.0/0            0.0.0.0/0            tcp dpt:22
```

Ora, qualsiasi pacchetto che non venga accettato dalle prime due regole `ACCEPT` e che sia destinato alla porta 22 (o provenga dalla porta 22) verrà registrato dal log prima di essere scartato dalle regole `DROP`.

Considerazioni Finali

- **Log Prefix**: Il prefisso del log (`-log-prefix " ssh pre-drop "`) può essere personalizzato per rendere i log più comprensibili e facili da filtrare.
- **Persistenza delle Regole**: Ricorda che le modifiche apportate con `iptables` non persistono dopo un riavvio. Dovresti assicurarti di salvare le regole, ad esempio utilizzando `iptables-save` e `iptables-restore`, oppure configurando uno script di inizializzazione che viene eseguito al boot del sistema.

```
# Salvare le regole attuali in un file
iptables-save > /etc/iptables/rules.v4

# Ripristinare le regole da un file
iptables-restore < /etc/iptables/rules.v4
```

Con questo procedimento, puoi inserire con precisione una regola di logging nella catena `FORWARD` di `iptables`, garantendo che tutti i pacchetti SSH non accettati vengano registrati prima di essere scartati.