iptables e logging

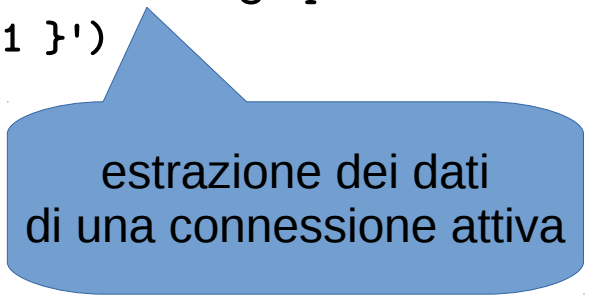
- Configurare iptables e rsyslog su client e server in modo che
  - tutti i pacchetti ricevuti dal server sulla porta 22/TCP
  - vengano loggati sul client, nel file `/var/log/pacchetti`
- Sul client,
  - esaminare continuamente il file `/var/log/pacchetti`,
  - per il primo pacchetto di una connessione mai vista prima,
    - se la connessione origina dal client stesso stampare su stdout il nome dell'utente che ne è responsabile,
    - se proviene da altre macchine stamparne l'ip

iptables e logging – sul server

```
#!/bin/bash

# configurazione di syslog: sfrutto la possibilità di usare file separati per la configurazione, che mi garantisce di non duplicare le direttive se eseguo più volte lo script

echo -e 'kern.=debug\t\t@192.168.56.201' > /etc/rsyslog.d/ese24apr.conf

systemctl restart rsyslog

# inserimento della regola iptables che produce i messaggi di log

iptables -I INPUT -p tcp --dport 22 -j LOG --log-level debug --log-prefix " ese24apr "
```

iptables e logging – sul client / 1

```
#!/bin/bash
# devo accertarmi che siano decommentate le direttive per la ricezione UDP
# posso farlo da script?
echo -e 'kern.=debug\t\t/var/log/pacchetti' > /etc/rsyslog.d/ese24apr.conf
systemctl restart rsyslog

function printuser() {
    # parametri: $SOURCEIP $DESTIP $SOURCEPORT $DESTPORT
    getent passwd $(ss -nte | egrep "$1:$3.*$2:$4" | awk -F 'uid:' '{ print $2 }'\
    | awk '{ print $1 }')
}
```



iptables e logging – sul client / 2

```
# elaborazione del file di log / esempio di riga:
# May 25 18:50:53 deis118 kernel: [ 2570.866572] IN=wlan0 OUT=
MAC=80:86:f2:47:00:54:9c:97:26:d0:46:2e:08:00 SRC=74.125.206.189 DST=192.168.1.71
LEN=64 TOS=0x00 PREC=0x00 TTL=40 ID=50758 PROTO=UDP SPT=443 DPT=53358 LEN=44

tail -f /var/log/pacchetti | grep --line-buffered " esercizio-las " | while read riga ;
do
    SOURCEIP=$(echo $riga | awk -F 'SRC=' '{ print $2 }' | awk '{ print $1 }')
    DESTIP=$(echo $riga | awk -F 'DST=' '{ print $2 }' | awk '{ print $1 }')
    SOURCEPORT=$(echo $riga | awk -F 'SPT=' '{ print $2 }' | awk '{ print $1 }')
    DESTPORT=$(echo $riga | awk -F 'DPT=' '{ print $2 }' | awk '{ print $1 }')

    # nota: DESTPORT qui dovrebbe essere sempre 22, ma per generalità  lo estraggo
```

iptables e logging – sul client / 3

```
    CONN="$SOURCEIP $DESTIP $SOURCEPORT $DESTPORT"
    if ! grep -q "$CONN" /tmp/known-connections ; then
        echo "$CONN" >> /tmp/known-connections
        if ip a | grep -q "inet $SOURCEIP/" ; then
            printuser $CONN # notare l'espansione senza apici!
        else
            echo "Pacchetto da $SOURCEIP"
        fi
    fi
done
```

netmon

- Monitorare il traffico ssh tra la VM Client e la VM Server sulla VM Router:
  - loggando attraverso syslog sul file /var/log/newconn l'inizio e la fine di ogni connessione diretta da Client a Server
  - (connection-monitor.sh) al verificarsi di questi eventi, avviare/fermare il monitoraggio della connessione per poter poi controllare il relativo traffico
  - (traffic-monitor.sh) durante la "vita" di ogni connessione, al superamento di una certa soglia espressa in numero di pacchetti per minuto:
    - (log-user.sh) connettersi alla sorgente del traffico eccessivo ed individuare l'utente responsabile e loggare lo username nel file /var/log/excess;
  - provvedere alla realizzazione di uno script di controllo (netmon.sh) che avvii ed arresti il monitoraggio, eseguendo tutte le operazioni di configurazione in modo automatico.
  - curare tramite signal handling la pulizia automatica di processi e catene in caso di terminazione volontaria o involontaria del procedimento di monitoraggio
- Realizzare una variante con tcpdump al posto di iptables