Esercitazione di riepilogo

Dopo aver configurato come di consueto una rete client (10.1.1.0/24) / router / server (10.9.9.0/24) realizzare il seguente sistema di comunicazione.

- Il primo script, **toctoc.sh**, gira sulle macchine client ed accetta come parametri due indirizzi IP (router e server) ed un numero di porta TCP (port).
  Usando ssh, deve depositare nella directory /tmp/ di router un file che abbia come nome l'IP address di client, che contenga in una singola riga i valori server e port separati da uno spazio, mantenendo poi la connessione ssh per almeno un minuto.

Esempio, sulla macchina 10.1.1.1 lancio
toctoc.sh 10.1.1.254 10.9.9.1 80 → viene creato sulla macchina 10.1.1.254 un file di nome /tmp/10.1.1.1 che contiene "10.9.9.1 80"

- Il secondo script **routerconf.sh** serve a configurare inizialmente il router, che deve agire da firewall, bloccando di default tutto il traffico tranne quello indispensabile per il funzionamento di toctoc.sh.

- Il terzo script **serverconf.sh** serve a configurare il firewall dei server per accettare traffico entrante solo dagli host della rete locale.

- Il quarto script **avanti.sh** è pensato per girare su router, e deve verificare senza mai fermarsi, ogni 5 secondi, se sono presenti connessioni ssh a router a cui corrispondano in /tmp file inviati da client "toctoc". Nel caso ne trovi deve:

1. verificare via SNMP se sul server richiesto nel file sia in esecuzione il processo rsyslogd, in tal caso inserire le regole nel packet filter che consentano al client di attraversare il router solo per connettersi al server sulla porta remotaspecificata nel file.
   NOTA1Porre attenzione alla direzione delle connessioni.
   NOTA2: Vista la limitazione di traffico sui server, è necessario mascherare i pacchetti che dai client attraversano router.
2. cancellare il file creato dal client e disconnettere forzatamente la connessione ssh attivata da toctoc.sh agendo sul server sshd

- Il quinto script **timeout.sh**, in esecuzione sul router anch'esso, deve osservare il transito dei pacchetti relativo alle connessioni abilitate da avanti.sh. Trascorsi 5 minuti circa (per comodità nel calcolo si possono trascurare i secondi) di assenza di traffico relativo ad una connessione, deve rimuovere dal packet filter la regola che la consente, inserita in precedenza da avanti.sh.
  All'atto della chiusura della connessione, aggiornare sulla directory LDAP ospitata dal router il conteggio delle connessioni osservate tra il client ed il server. A questo fine predisporre uno schema che consenta di costruire un sottoalbero del DIT formato da un primo livello di entry che rappresentino i client, ed un secondo livello di entry che rappresentino i server a cui il client si è connesso (e quante volte)

- Lo script **openclose.sh** può essere usato per concentrare le operazioni di apertura e chiusura del firewall in modo da garantirne la coerenza tra avanti.sh e timeout.sh.