Laboratorio di Amministrazione di Sistemi LA

Prova pratica del 16 febbraio 2009

Descrizione generale del problema

Un internet cafè consente alle workstation collocate sulla rete privata 10.1.1.0/24 di accedere ad Internet tramite un router/firewall Linux (10.1.1.254). Gli utenti sono registrati in una directory LDAP ospitata dallo stesso router, in entry che tengono traccia del tempo e della banda consumate da ciascuno. Sulle workstation vengono eseguiti script che, segnalando su LDAP l'accesso e la disconnessione degli utenti, permettono ad un processo di monitoraggio in esecuzione sul router di configurare dinamicamente le regole di transito del traffico e di aggiornare il conteggio delle risorse utilizzate dagli utenti. Nel caso un utente esaurisca le risorse a sua disposizione, il router provvede a disconnetterlo.
Inoltre, anzichè usare un filesystem condiviso, i dati posti da un utente sulla propria home nella workstation vengono salvati sul server al termine della sessione di lavoro, e quando lo stesso utente ritorna ed apre una nuova sessione, vengono riportati sulla workstation (eventualmente diversa) su cui si logga.

Componenti da progettare

File da consegnare: **utenti.schema** - Schema da inserire nella configurazione della directory LDAP, che definendo gli opportuni attributi e classi permetta l'inserimento di entry strutturate come nell'esempio seguente:

```
dn: user=marco,dc=lab4,dc=ingbo
objectClass: utenti
user: marco
Stato: connesso
IP: 10.1.1.45
TempoResiduoMinuti: 10
TrafficoResiduoKB: 100
```

File da consegnare: **login.sh** - Si suppone che questo script venga automaticamente eseguito sulla workstation quando un utente esegue il login, a suo nome.

- Se trova una entry in LDAP corrispondente all'utente, che abbia Stato=disconnesso, TempoResiduoMinuti>0, TrafficoResiduoKB>0
  - aggiorna la entry con Stato=connesso ed IP=indirizzo della workstation
  - recupera dal router l'archivio corrispondente al più recente salvataggio della home, estraendolo nella home dell'utente
  - esce con codice 0
- Se anche solo una delle tre condizioni non è verificata, invoca logout.sh ed esce con codice 1.
- Se non trova una entry in LDAP corrispondente all'utente, esce con codice 2.

File da consegnare: **logout.sh** - Può essere invocato da login.sh o automaticamente al logout di un utente, ed è comunque eseguito a suo nome.

- Termina tutti i processi attivi dell'utente, possibilmente in modo "gentile" ma all'occorrenza in modo forzato
- Archivia il contenuto della home dell'utente sul router, con un nome di file che consenta di mantenere tutte le copie fatte in momenti diversi
- Aggiorna l'entry LDAP dell'utente con Stato=disconnesso.

File da consegnare: **fw.sh** - Viene invocato sul router con due parametri, il primo deve essere un IP address, il secondo una stringa che può assumere i valori "open" o "close". Si ipotizzi che le policy del firewall siano settate tutte a DROP con l'eccezione delle regole necessarie al traffico di loopback locale ed al traffico LDAP e SSH con le workstation. Nel caso sia invocato con "open", lo script configura il firewall per consentire l'accesso ad Internet da parte dell'indirizzo (privato) specificato come primo parametro, mentre nel caso sia invocato con "close" rimuove le regole inserite in precedenza per tale IP.
L'accesso ad internet deve essere limitato alle porte e protocolli specificati nel file /etc/allowed_ports, il cui contenuto ha una struttura come nell'esempio seguente:

```
tcp 80
udp 53
tcp 443
```

Suggerimento utile anche ai fini del punto successivo: si faccia un uso opportuno delle catene custom di iptables.

File da consegnare: **decrementa.sh** - Viene invocato sul router ogni minuto (indicare nei commenti quali operazioni di configurazione del sistema sono necessarie per ottenere tale esecuzione periodica automatica). Trova tutte le entry LDAP di classe "utenti" che hanno Stato=connesso, e per ciascuna

- calcola quanto traffico (in KB) tale utente ha generato dall'ultima esecuzione
- aggiorna TrafficoResiduoKB diminuendolo di tale quantità
- aggiorna TempoResiduoMinuti decrementandolo di 1
- se uno dei due valori diventa nullo o negativo invoca logout.sh sulla workstation su cui è loggato tale utente, a suo nome.

File da consegnare: **openclose.sh** - Trova tutte le entry che dall'ultima invocazione del medesimo script hanno cambiato stato ed invoca fw.sh nel modo opportuno per abilitare/disabilitare l'accesso ad internet della corrispondente workstation.