AUTENTICAZIONE CENTRALIZZATA CON LINUX E SAMBA

Analizzeremo come creare - con un sistema linux slackware 11- e col pacchetto samba un sistema di autenticazione centralizzato per l'intera rete .
Premettiamo che:

1) l'articolo non ha alcuna pretesa di completezza. trattansi unicamente degli appunti dell'autore, scritti per evitare inutili ricerche (e fatiche) in futuro.

2) le utenze "reali" sono quelle del sistema linux, a cui samba si appoggia. In pratica ogni utente della rete deve avere un'equivalenza nel sistema linux. Non useremo quindi LDAP. Il metodo da noi seguito si rivela efficace fino al numero di poche centinaia di utenze. Oltrepassato questo limite ecco che diventa produttivo installare un server LDAP.

3) Non intendiamo creare un sostituto di active directory. Il pacchetto samba ancora non supporta tutte le raffinatezze e le possibilità (e tutte le complicazioni) di Active Directory.

4) Viene preso in considerazione unicamente il caso in cui il server e' linux ed i client sono windows xp professional. I sistemi windows xp home non possono essere uniti ad un dominio per precisa volonta' di microsoft.

5) Utilizzeremo la fantastica ed insuperata slackware 11 e samba 3.0.23c . Il tutto dovrebbe funzionare correttamente anche con altre ditribuzioni, a patto di utilizzare la medesima versione di samba.

6) Non analizzeremo le problematiche riferite alla sicurezza. L'amministratore dovra' trovare per conto suo la soluzione migliore in base al contesto spedifico.

PREPARAZIONE DEL SISTEMA

Occorre installare slackware 11, al termine della procedura di installazione si renda eseguibile il file /etc/rc.d/rc.samba tramite il comando

```
chmod +x /etc/rc.d/rc.samba
```

Dal prossimo riavvio del calcolatore, il sistema fara' partire i demoni samba, responsabili di tutto. Creiamo ora le directory occorrenti, e non presenti nell'installazione di "default" .
Creiamo la directory ove avverra' la registrazione delle operazioni, e togliamo alla directory tutte le restrizioni.

```
mkdir -p  /var/log/samba
chmod 777 /var/log/samba
```

Creiamo la directory ove posizioneremo gli script di netlogon. e togliamo alla directory tutte le restrizioni. In pratica quando un calcolatore windows accede al dominio , eseguira' uno o piu' script qui posizionati.

```
mkdir   /home/netlogon
chmod 777   /home/netlogon
```

creiamo una directory accessibile da chiunque, e togliamo a tale directory ogni restrizione.

```
mkdir   /home/public
chmod 777   /home/public
```

Creiamo la directory ove windows posizionera' il "profilo" dell'utente

corrente, e togliamo alla directory ogni restrizione. Per "profilo" si intende l'insieme delle impostazioni personali, quali sfondo del desktop, dimensione dei caratteri, cartella Documenti, ed ogni altra cosa riferita espressamente all'utente corrente.

```
mkdir   /home/profile
chmod 777     /home/profile
```

Creiamo ora una directory accessibile a chiunque. Il motivo e' preventivo: in futuro potrebbe servirci una zona di rete accessibile senza problemi. Inoltre togliamo a tale directory tutte le restrizioni.

```
mkdir   /home/dati
chmod 777     /home/dati
```

Ora editiamo il file /etc/samba/smb.conf. Tale file e' responsabile del comportamento di samba. All'interno di detto file dobbiamo inserire tutte le direttive occorrenti al servizio di autenticazione. Ecco qui sotto un ipotetico file smb.conf, coerente con le directory create poco fa.
Non spiegheremo ogni singola direttiva in maniera esaustiva. A fine documento il lettore potra' trovare tutte le fonti a cui l'autore si e' rifatto per la stesura del presente documento.

```
[ global ]

netbios name                    =           serversamba
workgroup                       =           veronese
server string                   =           samba server nt
log file                        =           /var/log/samba/%m.log
security                        =           user
encrypt passwords               =           yes
passdb backend                  =           smbpasswd
local master                    =           yes
preferred master                =           yes
os level                        =           66
domain master                   =           yes
domain logons                   =           yes
wins support                    =           yes
time server                     =           yes
log file                        =           /var/log/samba/log.%m
log level                       =           4
username map                    =           /etc/samba/smbusers
logon script                    =           logon.bat
logon path                      =           \\serversamba\profile\%U
enable privileges               =           yes
add user script                 =           /usr/sbin/useradd -m -s /bin/false %u
delete user script              =           /usr/sbin/userdel -r %u
add group script                =           /usr/sbin/groupadd %g
delete group script             =           /usr/sbin/groupdel %g
add user to group script        =           /usr/sbin/usermod -G %u %g
delete user from group script =             /usr/bin/gpasswd -d '%u' '%g'
set primary group script        =           /usr/sbin/usermod -g '%g' '%u'
add machine script              =           /usr/sbin/useradd -s /bin/false -d  \
  /dev/null -g dominio -M %u
# delete machine script         =           /usr/sbin/userdel -r %u
passwd program                  =           /usr/bin/passwd %u
passwd chat                     =           "*New password:*" %n\r "*New password
(again):*" %n\r \ "*Password changed*"
printcap name                   =           cups
printing                        =           cups
load printers                   =           yes
```

```
[ netlogon ]

comment                         =       directory degli script di
inizialiazzaione
path                            =       /home/netlogon
read only                       =       yes
guest ok                        =       yes
browseable                      =       no


[ home ]

comment                         =       dir utente
path                            =       /home/%U
browseable                      =       yes
writable                        =       yes


[ public ]


comment                         =       dir pubblica
path                            =       /home/public
browseable                      =       yes
writable                        =       yes
public                          =       yes
create mask                     =       0777


[ dati ]

comment                         =       cartella condivisa
path                            =       /home/dati
browseable                      =       yes
read only                       =       no
create mask                     =       0777
directory mask                  =       0777
public                          =       yes


[ profile ]

comment                         =       profili degli utenti
path                            =       /home/profile
browseable                      =       no
read only                       =       no
create mask                     =       0777
directory mask                  =       0777
public                          =       yes


[printers]

comment                         =       All Printers
path                            =       /var/spool/samba
printable                       =       yes
guest ok                        =       yes
browsable                       =       yes
# valid users                   =       claudio
public                          =       yes
printable                       =       yes
print ok                        =       yes
```

Il sistema non e' ancora completo. Occorre posizionare nella directory /home/netlogon uno script di logon. Il nome dello script e' logon.bat. Tale nome non e' obbligatorio, potrebbe anche chiamarsi pippo.bat, l'importante e' che tale
nome sia uguale a quanto indicato nel file /etc/samba/smb.conf. Inoltre e' obbligatoria l'estensione " .bat " . Ecco un ipotetico file logon.bat , coerente con l'esempio di cui sopra.

```
net use w:  \\serversamba\dati
net time    \\serversamba  /SET /YES
```

Lo script si compone di sole due righe, la prima riga connette una unita' di rete dal nome " w " , corrispondente alla sezione " dati " dichiarato nel file smb.conf . La seconda riga indica al calcolatore windows di sincronizzare il proprio orologio con quanto espressamente indicato dal server samba.
Lo script deve essere scritto obbligatoriamente con gli strumenti di windows quali blocco note e simili. Questo poiche' gli " a capo " non sono uguali tra sistemi unix, linux e windows. Editare lo script con la suite office e poi rinominare il tutto e' un errore, e porta al non funzionamento.

PREPARAZIONE DEGLI ACCOUNT

Questa parte e' un poco laboriosa.
Occorre rispettare alcuni vincoli:

a) ogni utenza "fisica" deve essere una utenza valida del sistema linux
b) dette utenze possono essere o non essere amministratori del pc windows ospite del dominio. Inoltre tali utenze potrebbero appartenere ad uno dei gruppi di lavoro di windows, coi rispettivi privilegi e limiti .
c) i gruppi di lavoro windows devono essere mappati correttamente coi rispettivi gruppi di linux. Per ottenere cio' utilizzaremo il comando " net " del pacchetto samba, che svolge compiti differenti rispetto al comando " net " di windows, malgrado il nome uguale possa trarre in inganno. Ecco una semplice ed incompleta tabella ove i gruppi dei due sistemi vengono mappati [1] . Questa parte non e' da sottovalutare. E' una buona idea documentarsi sul funzionamento dei sistemi windows uniti in un dominio, poiche' il loro comportamento e' differente rispetto ai sistemi windows non uniti in un dominio.
d) ogni nome netbios dei pc windows del dominio deve avere una utenza particolare sul pc linux. Tale utenza ha il medesimo nome netbios del pc windows, a cui viene aggiunto il simbolo del dollaro " $ " . Quindi se abbiamo un pc dal nome netbios " aristotele " , occorre creare sul pc linux adibito a PDC , una utenza dal nome " aristotele$ "

Iniziamo le operazioni creando (sul pc linux) due gruppi di lavoro. In uno di questi gruppi inseriremo gli utenti amministratori di dominio , nell'altro gruppo inseriremo gli utenti non privilegiati .

```
groupadd dadmin [sara' il gruppo amministratore]
groupadd dusers [sara' il gruppo non amministratore]
```

Ora creiamo l'utente " computer$ " . Il simbolo del dollaro lascia capire che nel dominio vi sara' un computer il cui nome e' " computer " .

```
useradd -d /dev/null -s /bin/false computer$
passwd -l computer$
smbpasswd -a computer$
```

Ora creimo l'utente di dominio " il_capo " . L'utente " il_capo "

potra' disporre del pc windows da lui utilizzato, al 100% , senza limitazioni di sorta. In pratica diventera' un amministratore del sistema da lui utilizzato e del dominio in oggetto .

```
useradd -s /bin/false -g dadmin il_capo
passwd -l  il_capo
smbpasswd -a  il_capo
net groupmap add unixgroup=dadmin ntgroup="Domain Admins" type=d rid=512
```

Ora creiamo l'utente kevin. Tale utente avra' privilegi ristretti, all'interno del pc windows dal quale operera' ed all'interno del dominio in oggetto .

```
useradd -s /bin/false -d dusers kevin
passwd -l kevin
smbpasswd -a kevin
net groupmap add unixgroup=dusers ntgroup="Domain Users"  type=d rid=513
```

Anche l'utente root deve avere una password valida per il sistema samba. Questo perche' solo gli utenti linux con UID=0 e gli utenti appartenenti al gruppo "Domain Admins" possono aggiungere macchine al dominio. Il comando e' il seguente:

```
smbpasswd -a root
```

Ricordiamo che le pass valide per il server samba possono essere differenti dalle pass valide per il sistema linux, anche se per comodita' esse vengono fatte coincidere, in totale inosservanza delle piu' elementari regole di sicurezza.
Potremmo inoltre creare un gruppo aggiuntivo, popolato dai nomi netbios degli elaboratori windows inseriti nel dominio. Lasciamo al lettore tale possibilita' .

[1]
segue una tabella contente i principali gruppi di lavoro presenti nei sistemi windows, ed una loro ipotetica mappatura con gruppi del mondo linux. I gruppi del gruppo linux nella tabella sottostante non sono presenti nelle installazioni standard di linux e devono venire creati appositamente. I nomi proposti non sono obbligatori e l'amministratore puo' scegliere tale nome come meglio preferisce, a patto di avere un'armonia di base con tutto il lavoro. Ricordiamo che il " rid " [relative identifier] nei sistemi windos e' la parte finale del " sid " [security identifier] , cioe' un dentificatore utilizzato in reti di computer windows per identificare univocamente un utente, oppure una macchina (una risorsa in reti windows) in un dominio.

GRUPPI WINDOWS	GRUPPI LINUX
Domain Admin	domadmins
Doamin Users	domusers
Domain Guests	domguests
Administrators	compadministrator
Users	compusers
Guests	compguests
System Operators	compsystoperators
Account Operators	compaccoperators
Backup Operators	compbckoperators
Print Operators	complpoperators
Replicators	compreplicators
Power Users	compusroperators

Per completezza riportiamo una tabella dei gruppi di lavoro del mondo windows e dei rispettivi RID .
Fonte: http://www.afp548.com/article.php?story=200608252114039

Inoltre gli svilppatori di samba trattano l'aspetto dei gruppi di lavoro windows <--> linux e la reciproca mappatura in modo molto esteso.
Maggiori informazioni a questo link:
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/groupmapping.html

GRUPPI	VALORE RID
Domain Administrator	500
Domain Guest	501
Domain KRBTGT	502
Domain Admins	512
Domain Users	513
Domain Guests	514
Domain Computers	515
Domain Controllers	516
Domain Certificate Admins	517
Domain Schema Admins	518
Domain Enterprise Admins	519
Domain Policy Admins	520
Builtin Admins	544
Builtin users	545
Builtin Guests	546
Builtin Power Users	547
Builtin Account Operators	548
Builtin System Operators	549
Builtin Print Operators	550
Builtin Backup Operators	551
Builtin Replicator	552
Builtin RAS Servers	553

PREPARAZIONE DEL SISTEMA WINDOWS

Potrebbe capitare che un sistema windows xp professional [ricordiamo ancora che i sistemi windows xp home non possono fare parte di un dominio, per precisa volonta' di microsoft] appena installato rifiuti di collegarsi al dominio. In termine tecnico si dice che tale pc " non fa' il join al dominio ". Un motivo potrebbe essere imputato a samba. Infatti nelle varie distribuzioni linux tale pacchetto viene compilato con opzioni differenti, ognuna delle quali rispecchia la specifica esigenza della distribuzione. Occorre documentarsi presso il sito della propria distribuzione e correggere eventualmente alcuni parametri nel file /etc/samba/smb.conf e/o nel computer windows. Nella distribuzione slackware 11 in accoppiata con samba 3.0.23c , nessuna modifica occorre. Tutto e' funzionante fin dal primo tentativo, a patto di eseguire i passaggi in maniera corretta.
Alcune volte il problema della difficolta' del join al dominio gestito da linux + samba , puo' essere risolto modificando sul pc windows i parametri seguenti. Tale rimedio non e' universale.

pannello di controllo ---> strumenti di amministrazione ---> criteri di protezione locale ---> criteri locali ---> opzioni di protezione

cercare le seguenti voci ed impostarle a " disattivato "

- membro di dominio, aggiunta crittografia o firma digitale ai dati del canale protetto (sempre)

- membro di dominio, aggiunta crittografia o firma digitale ai dati del canale protetto (quando possibile)

- membro di dominio, aggiunta firma digitale ai dati del canale protetto

(quando possibile)

Ora dobbiamo modificare la seguente voce di registro di windoes

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetLogon\Parameters

la voce

requiresignorseal

deve essere uguale a 0 (zero). Attenzione poiche' tale voce potrebbe essere gia' a zero. Occorre cancellarla ugualmente e re-impostarla a zero.
Ora il sistema windows e' pronto ad essere unito al dominio gestito dal PDC linux + samba. Eseguiamo un riavvio del sistema windows , per rendere effettive le modifiche eseguite. Poi ci rechiamo su " risorse del computer " , eseguiamo un clic destro e dove c'e' " nome computer " impostiamo i dati necessari per il join al dominio

- nome dominio
- nome di un utente abilitato ad inserire i pc al dominio (ci viene chiesto da una maschera che appare) , indichiamo root e la pass di root valida per samba
- infine indichiamo il nome utente valido per il dominio, nel caso in oggetto " kevin " , con la pass precedentemente creata.

VARIABILI POSSIBILI IN SMB.CONF

Riportiamo un elenco parziale delle variabili possibili in smb.conf, ed il loro significato. Un elenco completo e' ottenibile dalla pagina man di smb.conf

%S	Nome del servizio corrente
%h	Nome Internet del server Samba
%P	Directory radice del servizio
%m	Nome NetBios del client connesso
%u	Nome Utente (Linux)
%L	Nome NetBios del server SAMBA
%g	Gruppo cui appartiene l'utente %u (Linux)
%M	Nome Internet dell'host connesso
%U	Nome utente della sessione (Samba - non necessariamente uguale a %u)
%R	Livello di protocollo selezionato dopo la negoziazione
%G	Gruppo primario cui appartiene l'utente %U (Samba)
%d	Pid del processo server
%H	Home directory dell'utente %u
%a	Architettura del client; è riconosciuto Samba, Wfw, Win95 e WinNT
%v	Versione di Samba
%I	Indirizzo IP del client
%T	Data e pra correnti

Ringraziamenti: Un grazie al Dr. Pietro Reverso, responsabile tecnico della technonetsrl [http://www.technonetsrl.it] , il quale mi ha chiarito diversi dubbi.
Un ringraziamento particolare agli amici del newsgroup it.comp.os.linux.sys dai quali ho imparato davvero molto.

L'autore si e' rifatto alle seguenti fonti:
http://www.csltoscana.net/howtosamba.html
http://mercury.chem.pitt.edu/~sasha/LinuxFocus/Italiano/March2002/article177.shtml
http://www.ce.unipr.it/~stillo/
http://www.stenoit.com/modules/spxsection/item.php?itemid=5
http://www.finex.org/book/export/html/493
http://casa.kurgan.org/kb/Samba/NuovaInstallazione
http://linuxdidattica.org/docs/altre_scuole/planck/samba/samba1.html