ACTIVE DIRECTORY 2000, SQUID AND SAMBA
Author - Nic Maurel

I wrote this paper mainly because there isn't much documentation of integrating squid proxy into Microsoft Active Directory 2000, but with the help of samba 3 and winbind this can be done, and seemingly integrates very well. Squid does have "basic" auth but this requires a user prompt, which can be quite irritating for anal users. The main aim is to pass the authentication to the AD box so that authentication is transparent. This is what I am going to show you here.

Ok! What do we need?
- Fedora or Redhat box (I am currently running Fedora Core 2)
- Samba 3 or above (I used samba-3.0.21b) - which you can get from here
- Latest squid (I used squid-2.5.STABLE12 and not squid3 which is beta) - you can get it from here

Configuring samba
Unpack samba and compile from source. Now configure it..

```
# ./configure --prefix=/usr
 --localstatedir=/var
 --with-configdir=/etc/samba
 --with-privatedir=/etc/samba
 --with-fhs
 --with-quotas
 --with-msdfs
 --with-smbmount
 --with-ads
 --with-pam
 --with-pam_smbpass
 --with-syslog
 --with-utmp
 --with-sambabook=/usr/share/swat/using_samba
 --with-swatdir=/usr/share/swat
 --with-libsmbclient
 --with-winbind
 --with-winbind-auth-challenge
# make
# make install
```

The four main important ones are..

```
--with-pam
--with-pam_smbpass
--with-winbind
--with-winbind-auth-challenge
```

..these are not enabled by default and are required for this configuration to work. Once it's installed we can add a startup scripts for enabling during boot time, we can do that with..

```
Copy packaging/RedHat/smb.init  to  /etc/init.d/smb
Copy packaging/RedHat/winbind.init   to /etc/init.d/winbind
Add to your run levels so they will start at boot time
```

Now we edit the */etc/samba/smb.conf* to include:

```
security = ads                    <---------- Pass authentication to Active directory
password server = YourDomainC [AnotherPDC]
```

```
encrypt passwords = yes
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes

winbind separator =
realm = EXAMPLE.CO.ZA
winbind use default domain = yes
template shell = /bin/bash
template homedir = /home/%D/%U
```

Setup Kerberos
Kerberos is used to encrypt the sessions between the Proxy Server and Domain Controller, setup your file to look exactly like this and it will work. Edit your */etc/krb5.conf* as follows (make a backup of your current one just in case)..

```
#cp /etc/krb5.conf /etc/krb5.conf.orig
#vi /etc/krb5.conf
[libdefaults]
ticket_lifetime = 24000
default_realm = EXAMPLE.CO.ZA
dns_lookup_realm = yes
dns_lookup_kdc = yes

[realms]
EXAMPLE.CO.ZA = {
kdc = yourdomaincontroller.example.co.za
}
```

Setup your Server to use files as well as winbind to authenticate
Edit your */etc/nsswitch.conf*

```
Passwd: files winbind
group: files winbind
hosts: files winbind dns
```

Check winbind NSS and PAM files are installed
You will need to check if these files have today's date, if not copy them from your samba *source/nsswitch* directory. */lib* should contain the library file *libnss_winbind.so* and */lib/security* should contain the library file *pam_winbind.so*. If this file (*libnss_winbind.so.2*) does not exist you may need to do..

```
ln -s /lib/libnss_winbind.so /lib/libnss_winbind.so.2
```

Run this to recognize the changes..

```
#ldconfig
```

Then you need to check the permissions of the winbind pipe. *ntlm_auth* which is the helper Squid makes use of needs access to winbinds pipe which will be located in */var/lib/samba/winbindd_privileged/* and change accordingly as below or winbind will not start,because your squid user needs to read permissions

```
# chmod 750 /var/lib/samba/winbind_privileged
# chgrp squid /var/lib/samba/winbind_privileged
```

You change the pipe file to these permissions so that everyone can read it. So you should be able to see this..

```
# ls -al /var/lib/samba/winbind_privileged
srwxrwxrwx 1 root root 0 Jan 14 21:15 pipe
```

Now you join the the active directory domain..

```
# net ads join -U administrator
 - administrator is the administrator account of your windows 2000 domain
```

Setup PAM
Create these three files, if they already exist then go onto the next step..

```
#vi /etc/pam.d/system-auth-winbind
   #%PAM-1.0
   auth required /lib/security/pam_env.so
   auth required /lib/security/pam_securetty.so
   auth required /lib/security/pam_nologin.so
   auth sufficient /lib/security/pam_winbind.so
   auth sufficient /lib/security/pam_unix.so likeauth nullok use_first_pass shadow
   auth required /lib/security/pam_deny.so
   account sufficient /lib/security/pam_unix.so
   account required /lib/secuirty/pam_winbind.so
   password required /lib/security/pam_cracklib.so retry=3 type=
   password sufficient /lib/security/pam_unix.so nullok use_authtok md5 shadow
   password required /lib/security/pam_deny.so
   session required /lib/security/pam_limits.so
   session required /lib/security/pam_unix.so
```

```
#vi /etc/pam.d/samba
   #%PAM-1.0
   auth required pam_nologin.so
   auth required pam_stack.so service=system-auth-winbind
   account required pam_stack.so service=system-auth-winbind
   session required pam_stack.so service=system-auth-winbind
   password required pam_stack.so service=system-auth-winbind
```

```
#vi /etc/pam.d/squid
    #%PAM-1.0
    auth required /lib/security/pam_stack.so service=system-auth-winbind
    account required /lib/security/pam_stack.so service=system-auth-winbind
```

Compiling Squid
This is basically the last step, phew! But you need to configure Squid to use the Winbind NTLM helper. Do the following..

```
#./configure
--prefix=/usr
--datadir=/usr/share
--localstatedir=/var
--sysconfdir=/etc/squid
--infodir=/usr/share/info
--mandir=/usr/share/man
--enable-snmp
--enable-ssl
--enable-auth=ntlm,basic            <---- this is the one that's important
```

```
--enable-external-acl-helpers=wbinfo_group
#make
#make install
```

Edit your *squid.conf* to enable the ntlm helper as follows..

```
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children 5
auth_param ntlm max_challenge_reuses 0
auth_param ntlm max_challenge_lifetime 20 minutes
auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours

#Add your ACL:
acl yourdomain proxy_auth REQUIRED

#Modify your http_access lines to include “yourdomain”
http_access allow yourdomain
http_access deny all
```

You can set the acl to whatever you want, I just use domain because it's easy to spot in a config file. Now start squid

```
# squid -f /etc/squid/squid.conf
```

..and your should see 10 additional processes - for Basic and ntlm like this:

```
root     31715     1  0 Mar08 ?        00:00:00 squid -f /etc/squid/squid.conf
nobody   31717 31715  0 Mar08 ?        00:06:15 (squid) -f /etc/squid/squid.conf
nobody   31726 31717  0 Jan08 ?        00:00:10 (ntlm_auth) --helper-protocol=sq
nobody   31727 31717  0 Jan08 ?        00:00:01 (ntlm_auth) --helper-protocol=sq
nobody   31728 31717  0 Jan08 ?        00:00:00 (ntlm_auth) --helper-protocol=sq
nobody   31729 31717  0 Jan08 ?        00:00:00 (ntlm_auth) --helper-protocol=sq
nobody   31730 31717  0 Jan08 ?        00:00:00 (ntlm_auth) --helper-protocol=sq
nobody   31731 31717  0 Jan08 ?        00:00:00 (ntlm_auth) --helper-protocol=sq
nobody   31732 31717  0 Jan08 ?        00:00:00 (ntlm_auth) --helper-protocol=sq
nobody   31733 31717  0 Jan08 ?        00:00:00 (ntlm_auth) --helper-protocol=sq
nobody   31734 31717  0 Jan08 ?        00:00:00 (ntlm_auth) --helper-protocol=sq
nobody   31735 31717  0 Jan08 ?        00:00:00 (ntlm_auth) --helper-protocol=sq
```

Now you can go ahead and test your authentication. Since it is transparent authentication then you must log out of your domain and log onto your local administrator account to see if prompts for a username and password. If it does then enter your domain username and password and voila! Authenticated browsing - long and tedious but worth it!

Conclusion
And that's it, you will have to start your services in a specific order, due to dependencies, I start them as follows:
1. Samba
2. winbind
3. squid
You should also take close note of your log files, they help when troubleshooting a service that fails to start. Just to help you a bit, I have had issues with the winbind service when a Domain controller reboots, so all that needs to be done is the winbind service has to restart when the domain controller comes back up. Another issue I came

up with was that when I compiled squid it compiled as the user "nobody" instead of squid, which is fine because this is also an unprivileged user, I just made nobody own all of squid's files. Apart from that I also added SquidGuard for filtering and sarg for logging purposes. Well that's about it, I really hope this has been useful! Good luck and good night.