Global Information Assurance Certification Paper

Samba as a domain member Windows 2000 and RedHat 9.0

The Practical Assignment for GSEC
Version 1.4
Option 2

By
Sidney Henry

March 2004

Table of contents

1. Summary

Now a day, people usually have a heterogeneous network. Many security issues come with that. As we all know, security is the most important aspect of a network. Without security, the network is deficient.

Samba has been so successful over the years that I've decided to demonstrate how it can seamlessly become a member of a Windows domain, showing it's capabilities in a heterogeneous network (Windows/Linux) and using Kerberos as a network authentication protocol. With the right configuration, we can let the Kerberos process know how to handle the Active Directory server. With the help of Pluggable Authentication Modules also know has PAM, we will be able to implement a particular policy for authorization.

We will test the connection to see if everything was done the right way. In each section, you must perform the suggested tests if you want to ensure that what you installed and configured is working properly.

2. Background

An information technologies company with several departments, which is: a services department, an accounting department and a research and development department. The accounting department and the services department contain approximately 50 workstations that use Windows 2000 Professional, 6 Windows 2000 servers and 3 Unix/Linux servers. All of the users in the company have an authentication account on the Windows 2000 domain controller in Active Directory. The research and development department contains 10 Linux workstations. For those Linux workstations, the system administrator had created a single account, every programmer have the same user and password account to authenticate to the Linux workstations. One day the system administrator noticed that somebody logged into the Linux machine when they where not supposed to, installed several applications and compromised the company security policies. The problem is that the system administrator can't investigate who did the damage, because everybody can log in with the same account. Using a single account, oblige the system administrator to change the password every time an employee quit or get fired, for precaution to not compromise the network security.

A solution for this problem is that we can duplicate the active directory accounts to the 10 Linux workstations but if we need to create a user account we will need to create this user account for each Linux workstation. An alternative is to centralize user's access and permissions. By using Samba as a member of the domain, the company will be able to control the amount of sessions opened by a user. They will be able to limit their access since they only want a user to be connected to one pc at a time. Users will be able to access to share resources, such as files and printers and centralized authentication management.

In order to meet the company's objective, I tested it in the laboratory before implementing it in the production environment. All information has been sanitized to avoid information package.

OBJECTIVES

- Authentication of Active Directory users on the Linux workstation.
- Users can connect with the use of certain services like SSH (Secure Shell) using their Active Directory account.
- Active Directory accounts are not duplicated on the Linux workstation.

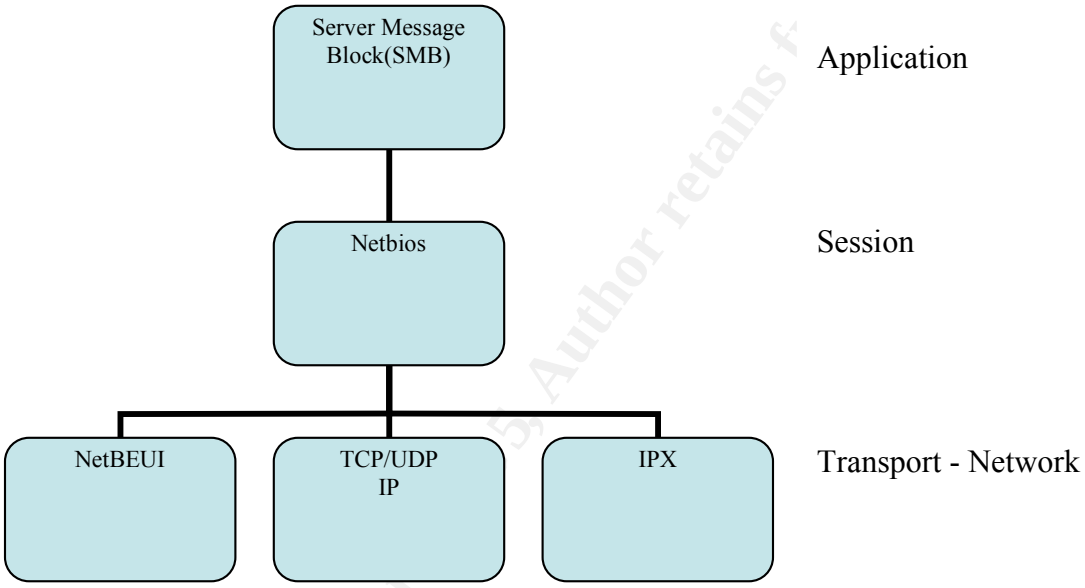
MATERIAL

Name	**Operating System**	**Role**
Moka	Windows 2000 server (active directory)	Domain controller
Arabica	Linux Redhat 9	Samba server
Expresso	Windows 2000 Professional	Workstation

3. Installation of Samba

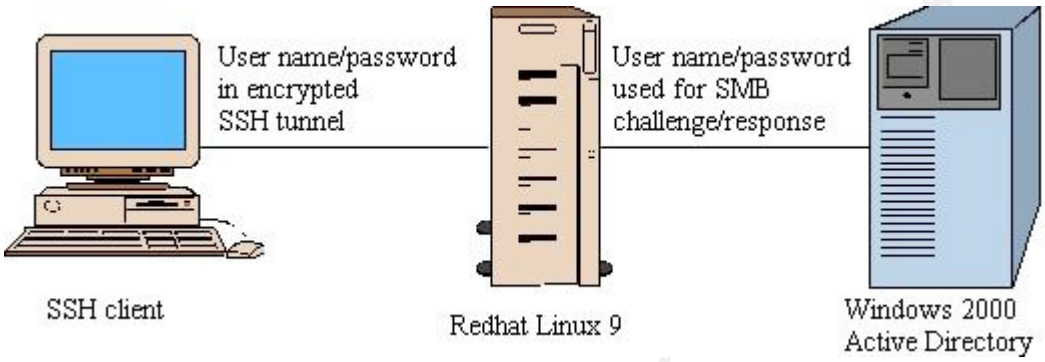
What is Samba?

Samba permits your Unix/Linux server to share resources, such as files and printers, with your Windows machines. Samba uses the connection-oriented protocol SMB [5]. Data packets travel in a virtual circuit and are sent, in order, between the client and the server. The Samba server's role is to act as a member of the domain.



Samba 3

Currently, Samba version 3 includes support for authentication with Kerberos 5 and LDAP, which enables Samba to become a member of a domain under Windows 2000 Active Directory or windows NT4-style domain as native member server. Samba 3.0 can act like a Windows 2000 domain controller and uses classic Windows administrative tools. [1]



Here is an example of a connection from a client who wants access to a resource on the Samba server.

How to install Samba

To begin, verify if Samba is already installed and then type:
] # rpm -qa | grep -i samba

Results

samba-common-2.2.7a-8.9.0
redhat-config-samba-1.0.4-1
samba-2.2.7a-8.9.0
samba-client-2.2.7a-8.9.0

You should uninstall the following packages:
]#rpm -e redhat-config-samba-1.0.4-1
]#rpm -e samba-2.2.7a-8.9.0
]#rpm -e samba-client-2.2.7a-8.9.0
]#rpm -e samba-common-2.2.7a-8.9.0

To install Samba, I use the rpm package on the samba website http://www.samba.org. It's the version 3.0.1-2. To install the package you should use the following root command:

]#rpm -ivh samba-3.0.1-2_rh9.i386.rpm
To verify which files were installed, you should use the following command:
] # rpm -ql samba | more

[2]

Samba configuration

To configure Samba, you need to edit the smb.conf file, which is found in the /etc/smb.conf directory. The file structure is: global, homes, printers.

Here is an example of a smb.conf file:

[global]

Workgroup = COLBERT
Netbios name = arabica
Server string = Samba Server
printcap name = /etc/printcap
load printers = yes
log file = /var/log/samba/log.%m
max log size = 50
#niveau de securité samba agit comme membre de domaine
Security = DOMAIN
Realm = COLBERT.CA

 # Winbind configuration
idmap uid = 10000-20000 # winbinb uid
idmap gid = 10000-20000
winbind separator = +
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes
 # répertoire des usagers du domaine
template homedir = /home/ads/%U
template shell = /bin/bash
#
obey pam restrictions = yes
password server = moka
encrypt passwords = yes

unix password sync = Yes
passwd program = /usr/bin/passwd %u
*passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n *passwd:*all*authentication*tokens*updated*successfully**

local master = no
os level = 33
domain master = no
preferred master = no

```
#============================ Share Definitions ===============
[homes]
   comment = Home Directories
   browseable = no
   writable = yes


# NOTE: If you have a BSD-style print system there is no need to
# specifically define each individual printer

[printers]
   comment = All Printers
   path = /var/spool/samba
   browseable = no
# Set public = yes to allow user 'guest account' to print
   guest ok = no
   writable = no
   printable = yes

[public]
   path = /var/public
   public = yes
   writeable = yes
   browseable = yes
   create mask = 0770
   valid users = @10000
```

The *Workgroup* parameter is the name of the Netbios workgroup or domain and the *Netbios* name is the computer name. The line *security = DOMAIN* indicates the type of security that the Samba server uses. *realm = COLBERT.CA* specifies the authentication domain.

In the file, there is a section for Winbind. It unifies names between Active Directory and UNIX. W*inbind uid* and *gid* allows Samba to use Windows user and group ID's and uses a UNIX implementation of Microsoft RPC calls. Winbind maintains a database called Winbind idmap.tdb in which it stores mappings between UNIX UIDs / GIDs and Active Directory SIDs. Users and groups who do not have local UID and GID used this mapping.

T*emplate homedir* is the user connection directory. For example, in /home/ads/%U, the variable %U refers to the user's name. There is no need to create the directory manually; it is created automatically by configuring the pam directory when a user connects for the first time. Continuing with other parameters, *obey pam restrictions* are used so that Samba refers to pam and *password server* indicates the server name that is in charge of authenticating the users. [4]

Once the file has been configured, it is possible to test the configuration by typing the following command:

]#tetstparm

Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[public]"
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions

Now samba is setup

4. Installation of the Kerberos client

What is Kerberos?

Kerberos is a network authentication protocol. It is used because the authentication is secure in that the passwords are not transmitted over the network. It uses a clock to limit the usage of keys and to detect replay attacks. Here the Windows 2000 serves also as the KDC (Key Distribution Center). Kerberos is responsible for keeping the approval secure between Windows and Linux within the domain. [6]

The Key Distribution Center accepts requests for tickets from Kerberos clients, validates their identity and grants tickets to them. The protocol is an IETF standard (RFC-1510)

Why we need to setup Kerberos client, because all authentication takes place between clients and servers. A Kerberos client is any entity that gets a service ticket for a Kerberos service. In this case we can talk about interoperability in my example I'm using a Microsoft Windows 2000 Domain, which by definition include a Kerberos realm.

Kerberos clients in a Windows 2000 domain

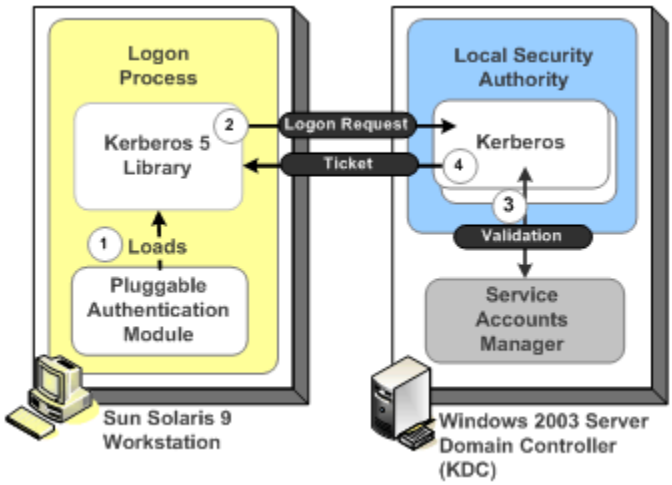
	Access to Windows 2000 Resources	**Access to non-Windows 2000 Resources**
Non-Windows Client Authentication to Windows KDC	Client Configuration	One-way Trust or Service Account

How does it work's

We need to configure a Kerberos client to use active directory as their default Key Distribution Center. The basic postulate of authentication Kerberos is as follows: if two entities share a secrecy which they are alone to know, they can check their respective identity by proving that they know the secrecy

- When you log in, your client contacts the Kerberos server to request a ticket
- You receive a special "ticket granting ticket" (TGT) encrypted using the client's password as the key
- The client then attempts to decrypt the TGT, using its password
- Allows the connection

Example



[9]

"UNIX workstation user can log on to the UNIX workstation shell using their Active Directory username and credentials. The logon request is passed from the shell to the Pluggable Authentication Module (PAM), and eventually to the Kerberos library, which begins an exchange of messages between the workstation and the Windows KDC" [9]

How to install Kerberos? First let's check to see if Kerberos is installed.

]#rpm -qa | grep -i krb

krbafs-1.1.1-9
pam_krb5-1.60-1
krb5-libs-1.2.7-14
krbafs-devel-1.1.1-9

krb5-devel-1.2.7-14

Then, you can find the krb5-workstation-1.2.7-14.i386.rpm on the redhat CD and then install the package on the Samba server.

]# rpm –ivh krb5-workstation-1.2.7-14.i386.rpm

Once installed, type the following command to verify that Kerberos is installed correctly

]#klist

If this command doesn't work, then try rebooting the computer. Next, configure the krb5.conf file which is usually found in the /etc directory. Here is an example of a krb5.conf file:

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 ticket_lifetime = 24000
 default_realm = COLBERT.CA
 dns_lookup_realm = false
 dns_lookup_kdc = false

[realms]
 COLBERT.CA = {
  kdc = moka.colbert.ca:88
  admin_server = moka.colbert.ca:749
  default_domain = colbert.ca
 }

[domain_realm]
 .colbert.ca = COLBERT.CA
 colbert.ca = COLBERT.CA

[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

Next, verify if there is a timeserver on the network. If not, then the clocks will have to be synchronized because Kerberos is using time synchronization to limit the use of the keys and help in detecting replay attacks; the clock of the Samba server will have to be synchronized with the KDC, which, in this case, is the domain controller as well. In order to request authentication tickets, a workstation is required to maintain its clock When the ticket his created they was an expiration time for the ticket the Kerberos client/server use this timestamp for the authentication that why it's important that their clocks has to be synchronized.

If there is a DNS server, verify that it is configured properly. The name resolution to the Samba server must function properly. Otherwise, you will have to configure the /etc/hosts file. We need to have a mechanism for resolving IP addresses for the KDC. Active Directory has built-in DNS services, and through the use of SRV resource records, Kerberos clients can locate the domain controllers and KDCs.

5. Configuration of Windows 2000 KDC

We need to set up Windows 2000 to act as the Kerberos Key Distribution Center (KDC). We create a user account on windows active directory, for example sidney. A key will have to be generated for the Samba machine from the Windows server and then the key will have to be imported to the Samba machine. To generate that keytab you will need ktpass.exe. The installation program is located on the CD-ROM in the \support\tools folder and the setup file (suptools.msi) must be opened manually to initiate the installation wizard.

To generate that keytab type:

C:\> ktpass -princ host/Arabica.colbert.ca@COLBERT.CA -mapuser sidney -pass password -out sidney.keytab

In Windows, the DNS server will have to be configured to include the Samba machine. If there isn't a DNS server, edit the c:\winnt\system32\drivers\etc\hosts file to include the Samba machine. [8]

6. Joining Samba to the domain

This command prompts users for their Kerberos principal name and password, and attempts to get an initial "ticket granting ticket" for that principal.

]# kinit sidney

To show the Kerberos tickets:

] # klist

Join the domain:

] #net ads join –U administrator

Start Samba and windbind services:

]# /etc/init.d/windbind start
]# /etc/init.d/smb start

Test the configuration:

]# smbclient '\\moka\data' -U administrator -k

]#wbinfo –g

To get information about the groups in your active directory

]#wbinfo –u

To get information about the users in your active directory

]#wbinfo –m
]#getent passwd

[7]

7. Pam configuration

The next step is getting all applications that request authorization to use Kerberos. The best way is to use PAM but we still allows UNIX authentication to keep a local account on the UNIX host.

What is PAM

"Pluggable Authentication Modules, also known as PAM, is a system for abstracting authentication and authorization technologies. With a PAM module it is possible to specify different authentication methods for different system applications without having to recompile these applications. PAM is also useful for implementing a particular policy for authorization" [1]. Since the beginnings of UNIX, user authentication has been accomplished by the user entering a password to be checked against the one stored in /etc/passwd. Remember in the smb.conf we configured samba to enable PAM support "*obey pam restrictions = yes"*. We can configured PAM to only allows console logins for local users but allows users from a NIS database to log in a SSH session.

Edit the /etc/nsswitch.conf to allow users and groups to be visible from windbind and modify the following parameters:

passwd: files winbind
shadow: files winbind
group: files winbind

in the /etc/pam.d/ directory contains the security files for authentication make a backup all files in that directory so if there any problem we can be able to log in .

Configuration of the samba file

```
#%PAM-1.0

auth       required     pam_nologin.so
auth       required     pam_stack.so service=system-auth
auth       required     /lib/security/pam_winbind.so
account    required     /lib/security/pam_winbind.so
account    required     pam_stack.so service=system-auth
session    required     /lib/security/pam_mkhomedir.so skel=/etc/samba/skel umask=0022
session    required     pam_stack.so service=system-auth
password   required     pam_stack.so service=system-auth
```

The line *session required /lib/security/pam_mkhomedir.so skel=/etc/samba/skel umask=0022* automatically creates a connection directory.

configuration of the login file

#%PAM-1.0

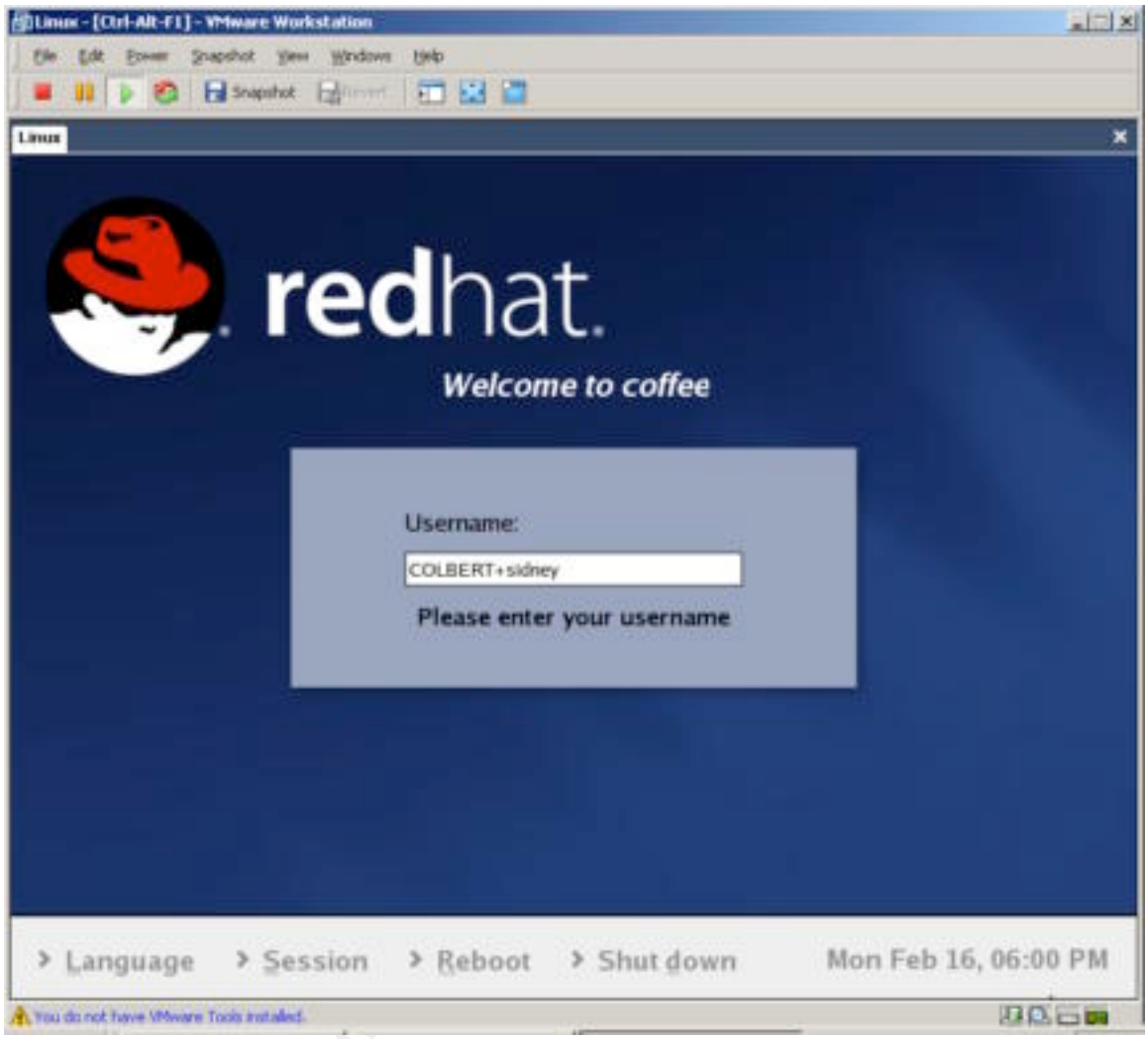
#%PAM-1.0
auth required /lib/security/pam_securetty.so
auth sufficient /lib/security/pam_winbind.so
auth sufficient /lib/security/pam_unix.so use_first_pass
auth required /lib/security/pam_stack.so service=system-auth
auth required /lib/security/pam_nologin.so
account required /lib/security/pam_stack.so service=system-auth
account sufficient /lib/security/pam_winbind.so
password required /lib/security/pam_stack.so service=system-auth
session required /lib/security/pam_stack.so service=system-auth
session optional /lib/security/pam_console.so

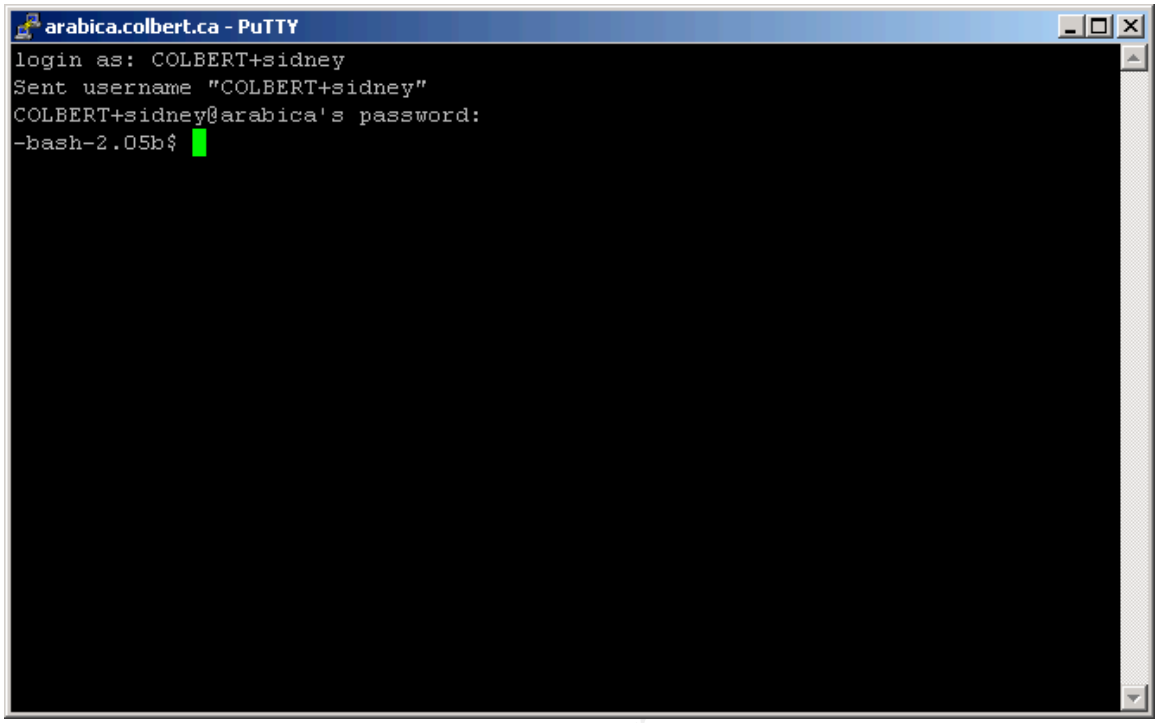
Configuration of the authconfig file

#%PAM-1.0

auth required /lib/security/pam_securetty.so
auth required /lib/security/pam_nologin.so
auth sufficient /lib/security/pam_winbind.so
auth required /lib/security/pam_pwdb.so use_first_pass shadow nullok
account required /lib/security/pam_winbind.so

8. Testing the connection





9. Troubleshooting

kinit(v5): Cannot find KDC for requested realm while getting initial credentials

libads/kerberos.c:ads_kinit_password(133)kerberos_kinit_password Administrator@COLBERT.CA failed: Preauthentication failed

- Change the administrator's password on the Windows 2000 PDC

smbd/sesssetup.c:reply_spnego_kerberos(172)Failed to verify incoming ticket

- Modify the smb.conf file security = DOMAIN

10. Conclusion

By using Samba as a member of the domain with Kerberos for authentication, the company will be able to control the amount of sessions opened by a user. There is no longer a single account for the Linux workstations every user can log in with their active directory account. If somebody installed an application the system administrator will be able to investigate. The authentication process has been reinforced, we don't need to create account entries in /etc/passwd and /etc/group. The domain security policies can be apply for the Linux Station.

A good way to increase security is to ensure that the system administrator is able to monitor every access to the network, no matter on what platform or on how many machines the users are logged in." Domain user access rights and file ownership/access controls can be set from the single Domain Security Account Manager (SAM) database (works with Domain Member servers as well as with MS Windows workstations that are Domain Members)" [1]. On a Windows network, the ability to make Linux workstations and servers work with Active Directory will provide a better control over the network's users and the workstations they use. This network configuration also ensures that the Active directory accounts are not duplicated on the Linux workstations. Users can access to the Linux workstation with protocols like SSH using their Active Directory account.

I realized that the knowledge of Kerberos is an asset to any system administrator or consultant trying to improve a company's network security. Samba should be used when a company wants to improve the network security. Also, as secure as Samba is, it's an Open-Source product that doesn't need any licenses. Meaning that you can scale the number of users connecting without purchasing any additional licences. Samba provide greater speed at less cost, it can provide a more stable long-term solution.

Before samba	After samba
The users accounts were duplicated	All users accounts will be created in Active Directory
The company wasn't able to manage all the network connections properly	Security policies in domain is managed via group policy
The Windows/Unix files couldn't be shared	Samba is used as a file server

Reference

[1] Samba Team "samba" URL http://www.samba.org (January 10, 2004)

[2] Linux-lea "lea-linux " URL http://lea-linux.org/admin/samba_nt_auth.php3?v=t (December 15, 2003)

[3] The UNIX and Windows 2000 Handbook: Planning, Integration and Administration "Lonnie Harvel, Steven Flynn ..(2002)

[4] Using Samba, 2nd Edition "By Jay Ts, Robert Eckstein, and David Collier-Brown " (February 2003)

[5] Samba "Gerald Carter , Richard Sharpe" (October 1999)

[6] Kerberos en environnement ISP UNIX/Win2k "Nicolas Fischbach" URL http://www.securite.org (January 10,2004)

[7] Redhat Linux Customization guide "Redhat " URL http://www.redhat.com (February 5, 2004)

[8] Active Directory pour Windows 2000 Server "M.Craft" (September 2002)

[9]Intranet access management and single sign on "Microsoft" URL http://www.microsoft.com/technet/security/topics/identity/idmanage/P3Intran_3.mspx (March 25, 2004)

Upcoming Training

San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event