Lab 18:

Linux in

Active Directory

Windows and Linux Server Security   
 2024-2025

© Daan Pareit

## Introduction

# Lab concept

In this lab, we will make our Debian VM a member of the COMPANY-<firstname>.serverlabs.be Active Directory domain. The machine will be known as debian.COMPANY-<firstname>.serverlabs.be . By adding the VM to the domain, the domain users will also be able to login to this Linux Server.

# Learning goals

* Installing Kerberos authentication and Samba on linux
* Configuring NSS to make linux aware of the Windows AD
* Configuring PAM to allow domain users to login on linux

# Practicalities and prerequisites

You need:

* The pfSense VM
* The Debian VM
* The Windows Server 2022 VM (King)
* The Windows 11 VM (for remote Server Manager and/or WAC)

## Linux within Active Directory

Integrating a Linux server in an AD domain can be done by using Samba (and applying the necessary changes to NSS/PAM). The following steps are based on a tutorial of the official Samba wiki: [https://wiki.samba.org/index.php/Setting\_up\_Samba\_as\_a\_Domain\_Member](https://wiki.samba.org/index.php/Setting_up_Samba_as_a_Domain_Member#Setting_up_a_Basic_smb.conf_File)   
However, it takes quite some effort to execute this correctly. We therefore selected and concretized the necessary steps for your convenience and understanding. They are also adapted to our setup.

# Make domain name resolving work in linux

The first steps are taken to make the linux machine can join the domain:

* Ensure that the DC (KING) is running.
* We assume you start from the Debian image as used previously, without e.g. samba etc. yet installed. If not, uninstall your previous samba installation.
* Log in to your Debian machine as your local user
* Run **apt update** to update your package list

A screenshot of a computer

Description automatically generated

* Change your DNS setting to use the DNS service running at the DC . To this end, change your /etc/resolv.conf to:  
   domain COMPANY-<firstname>.serverlabs.be  
   search COMPANY-<firstname>.serverlabs.be  
   nameserver 192.168.11.50

A screenshot of a computer

Description automatically generated

* Install the packages dnsutils and net-tools (to be able to use tools like nslookup and net)

A screenshot of a computer

Description automatically generated

* Verify if you can resolve king.COMPANY-<firstname>.serverlabs.be with nslookup

A screenshot of a computer

Description automatically generated

Yes, you can

* Active Directory (AD) uses SRV records to locate services, such as Kerberos and LDAP. Verify if you can resolve these records. You should get following output in an interactive nslookup session:

mickey@debian:~# nslookup

> set type=SRV

> \_ldap.\_tcp.COMPANY-<firstname>.serverlabs.be

Server: 192.168.11.50

Address: 192.168.11.50#53

\_ldap.\_tcp.COMPANY-<firstname>.serverlabs.be service = 0 100 389 KING.COMPANY-<firstname>.serverlabs.be.

> exit

A computer screen with white text

Description automatically generated

I think this behaviour is okay, because I do not have LDAP on the server, or at least I think so.

# Install and configure interaction with Kerberos on linux

* Install Kerberos for domain authentication via the krb5-user and libpam-krb5 packages. During installation, set COMPANY-<FIRSTNAME>.SERVERLABS.BE as realm.

A screenshot of a computer error

Description automatically generated

* With dpkg -L <package> one can see which files are installed by a package. What additional pam module has been installed by the previous packages?

Probably this is the pam module (because they have .so extension)

**/lib/x86\_64-linux-gnu/security/pam\_krb5.so**

A screen shot of a computer

Description automatically generated

* Set the following in the Kerberos configuration /etc/krb5.conf

[libdefaults]

default\_realm = COMPANY-<FIRSTNAME>.SERVERLABS.BE

dns\_lookup\_realm = false

dns\_lookup\_kdc = true

A screen shot of a computer

Description automatically generated

* Change your /etc/hosts file to include following entries:

127.0.0.1 localhost

192.168.11.10 debian.COMPANY-<firstname>.serverlabs.be debian

127.0.1.1 debian-<firstname>-<lastname>

A screen shot of a computer

Description automatically generated

# Install and configure samba on linux

* Install the samba package. Choose default values if asked for settings.
* In your /etc/samba/smb.conf file, add the following (and leave other settings untouched):

#======================= Global Settings =======================

[global]

netbios name = DEBIAN

security = ADS

workgroup = COMPANY-<FIRSTNAME>

realm = COMPANY-<FIRSTNAME>.SERVERLABS.BE

############ Misc ############

winbind nss info = template

template shell = /bin/bash

template homedir = /home/%U

idmap config \* : backend = tdb

idmap config \* : range = 3000-7999

idmap config COMPANY-<FIRSTNAME> : backend = rid

idmap config COMPANY-<FIRSTNAME> : range = 10000-999999

A screen shot of a computer

Description automatically generated

A computer screen shot of a program

Description automatically generated

We use the ‘rid’ back end here for simplicity. Check <https://wiki.samba.org/index.php/Idmap_config_rid> for more information .

* Reload your samba configuration:

sudo smbcontrol all reload-config

* You can query the domain info with:

sudo net ads info

A computer screen with white text

Description automatically generated

# Join the AD domain using samba on linux

* Now, we can join our linux machine to the COMPANY-<firstname>.serverlabs.be domain as follows:

sudo net ads join -U "Donald"  
You should obtain following output (you can neglect a DNS Update failure message):

mickey@debian:~# net ads join -U "Donald"

Enter Donald's password:

Using short domain name -- COMPANY-<FIRSTNAME>

Joined 'DEBIAN' to dns domain 'COMPANY-<firstname>.serverlabs.be'

A screen shot of a computer code

Description automatically generated

* Have a look at the ADUC tool in Server Manager, or the Active Directory tab in WAC (on your Windows 11 VM). Verify that DEBIAN is added as domain computer.

It was indeed added

A computer screen shot of a computer

Description automatically generated

# Configure NSS to make linux aware of domain users and groups

In the next steps, we now also want to make domain users and groups available and usable to the local Linux system.

* We first need to install a service to resolve user and group information from Windows servers. This is the winbind service. To this end, install the following packages:   
  winbind libnss-winbind libpam-winbind
* With dpkg -L <package> one can see which files are installed by a package. What additional pam module has been installed by the previous packages?

**/lib/x86\_64-linux-gnu/security/pam\_winbind.so**

**A screen shot of a computer

Description automatically generated**

Also these with winbind, but it does not look like pam modules.

**A screenshot of a computer program

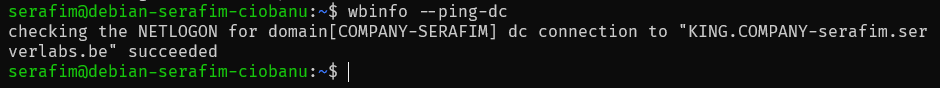
Description automatically generated**

* You can check a successful connection by the winbind service to the DC with:

wbinfo --ping-dc

which should output the following:

checking the NETLOGON for domain[COMPANY-<FIRSTNAME>] dc connection to "KING.COMPANY-<firstname>.serverlabs.be" succeeded



* We need to link the information from the Windows domain into information that can be accessed by Linux. We thus need to enable the information in the Name Service Switch (NSS). This is done by including winbind in the passwd and group entries (not the shadow entry) in /etc/nsswitch.conf file:

passwd: files systemd winbind

group: files systemd winbind

A screenshot of a computer

Description automatically generated

It was there by default

* You can now query information about domain users and groups thanks to winbind in NSS. Try e.g.:

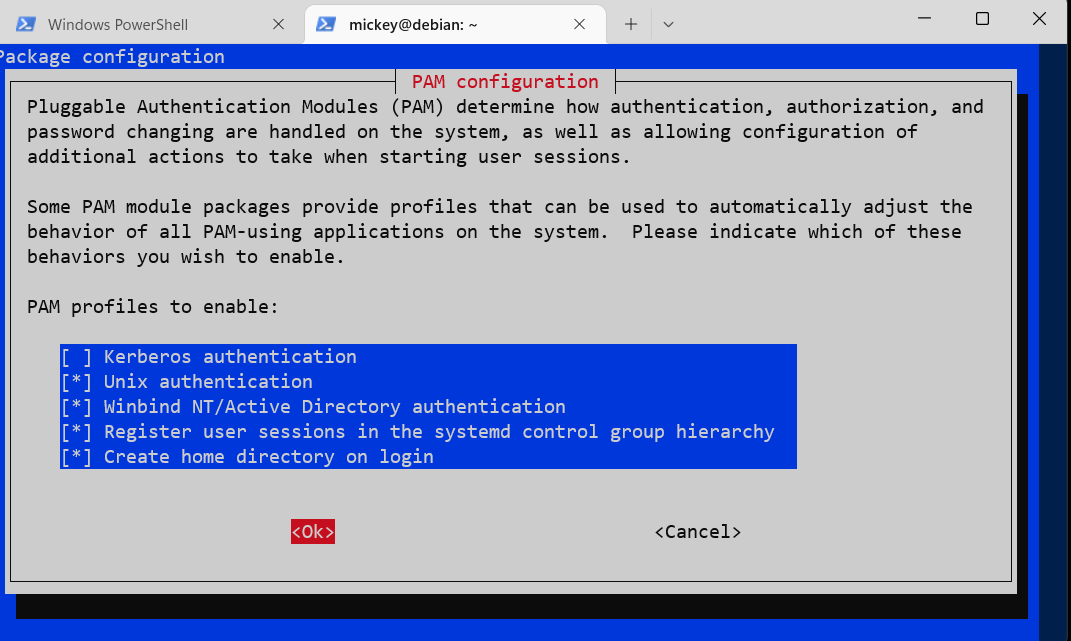
getent passwd "COMPANY-<FIRSTNAME>\\John Doe"  
getent group "COMPANY-<FIRSTNAME>\\Domain Users"  
id "COMPANY-<FIRSTNAME>\\John Doe"

A screen shot of a computer

Description automatically generated

# Configure PAM to enable domain users to login on linux

* Next, to enable domain users to log in locally or to authenticate to services installed on the domain member, such as SSH, we must enable PAM to use the pam\_winbind module. To this end, you can simply execute on Debian: sudo pam-auth-update .   
  Check all options but disable the “Kerberos authentication”.



* Now check the ‘common-auth’ pam configuration file. What PAM module is now used additionally for allowing users to login, besides the traditional pam\_unix.so module (for local users based on /etc/passwd)?

/etc/pam.d/common-auth (**pam\_winbind.so**)

A screen shot of a computer program

Description automatically generated

* Now finally, you can login with a domain user! Go to a local tty and login with: COMPANY-<FIRSTNAME>\John Doe

A screenshot of a computer

Description automatically generated

This feels illegal!

* Besides logging in locally, you can also of course login remotely over SSH. However, note that we’ve configured 2FA in a previous lab for SSH. Thus, first do the initial configuration for 2FA for John Doe, cfr previous lab (or disable 2FA if you’re only interested in the part about your Linux in the AD at this point). Then, try logging in via SSH with your domain user John Doe:

ssh "COMPANY-<FIRSTNAME>\John Doe"@192.168.11.10

Note that quotes are difficult in PowerShell to be used with ssh. Better to do it in cmd.exe .

A screenshot of a computer screen

Description automatically generated

It is alright, it will still work. Ah well, I will have to disable 2FA for the sake of screenshot…

Go to /etc/pam.d/sshd and change this line

A black background with white text

Description automatically generated

And then `sudo systemctl restart sshd`

A screenshot of a computer

Description automatically generated

* Verify that a non-existing account does not work

ssh ["COMPANY-<FIRSTNAME>\random name"@192.168.11.10](mailto:%22COMPANY-%3cFIRSTNAME%3e\random%20name%22@192.168.11.10)

A screenshot of a computer

Description automatically generated

Could have been smarter, but it is alright.

* Create a new domain user in Server Manager or WAC (make sure the user is active!) on your Windows 11 VM and verify he/she can also login immediately to the debian machine.

A screenshot of a computer

Description automatically generated

Password – Howest123!

A screenshot of a computer

Description automatically generated

It worked no issues.

## Resources

* <https://wiki.samba.org/index.php/Setting_up_Samba_as_a_Domain_Member#Setting_up_a_Basic_smb.conf_File>
* <https://wiki.samba.org/index.php/Authenticating_Domain_Users_Using_PAM>