Practical Network Defense - Lab 6

LDAP on ACME co.

Alessandro Serpi - 1647244

3 May 2019

Contents

1 Introduction

LDAP stands for Lightweight Directory Access Protocol, an open standard for accessing and maintaining directory information services.

In this laboratory, we will use LDAP to perform centralised authentication. Username and password of administrative users will be stored into a Zentyal domain controller and the firewalls will perform verification queries at each login attempt.

Zentyal is an open source groupware supporting Samba (among other protocols) based on Ubuntu LTS. The assignment was completed in a local environment with the latest major free release, Zentyal Server Development Edition 6.0.

2 Zentyal configuration

2.1 Network

Enable the *Network* module in *Module status* and reboot the server. In *System* ▷ *General*, change the hostname to `dc` and the domain to `pndeflab.edu`. Then, enable *Network* in *Module status* and reboot the server.

In *Network* ▷ *Interfaces* configure the internal interface `eth0` with static address `100.64.1.2`. Then, in *Network* ▷ *Gateways*, assign to the gateway on interface `eth0` (modifying an existing gateway or creating a new one, if necessary) the IP address `100.64.1.2`.memorise

2.2 Firewall and DNS

Enable *Firewall* and *DNS* modules in *Module status* and reboot the server. While the former module is already configured, it is necessary to set up the latter.

In *DNS*, section *Forwarders*, add a known DNS server. In section *Domains*, click on the cog wheel in row `pndeflab.edu` and column *Hostnames*. Then, add all relevant hosts in the network, inserting for each one all their local IP addresses.

Open a terminal (either using the virtual machine graphical interface or through an SSH connection) with root privileges and edit the file `etc/zentyal/dns.conf`, appending `100.64.0.0/16` to the line starting with `intnets =` . Then, reboot the server.

2.3 Remote logging

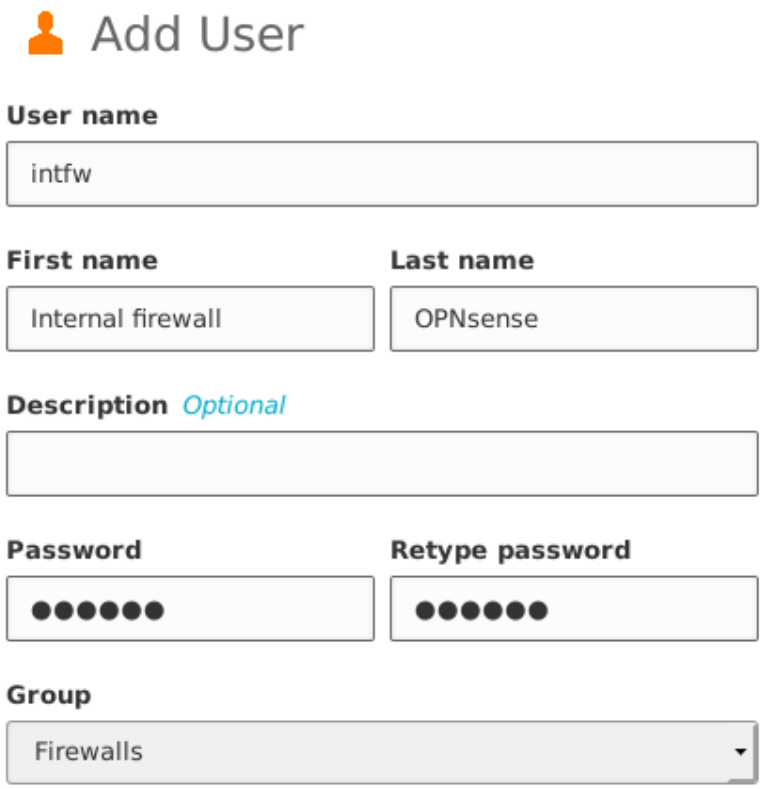
Open a terminal with root privileges and append the line `*.* @100.64.1.3` to the file `/etc/rsyslog.d/50-default.conf` and reboot the server.

2.4 LDAP

Enable the *Domain Controller and File Sharing* module in *Module status* and reboot the server.

In *Users and Computers* ▷ *Manage*, add a new group `Firewalls` clicking on the *Groups* folder, then on the green plus sign and completing the form. Similarly, add a new `PND_Group` group for the administrators.

Add a new computer account for the internal firewall clicking on the *Groups* folder, then on the green plus sign and filling the form as follows (taking care to choose a secure password):



Then, add another account for the main firewall in the same fashion.

Finally, add a new User account for each admin, inserting them in the `PND_Group` group.

3 OPNsense internal firewall configuration

3.1 Server

Create a new authentication server in *System* ▷ *Access* ▷ *Server* with the following settings:

Descriptive name	**Domain controller**
Type	**LDAP**
Hostname or IP address	100.64.1.2
Port value	389
Transport	TCP - Standard
Peer Certificate Authority	VPN Certificate Authority
Protocol version	3
Bind credentials	User DN: CN=Main firewall OPNsense,CN=Computers,DC=pnd … Password: ●●●●●●
Search scope	One Level
Base DN	CN=Users,DC=pndeflab,DC=edu
Authentication containers	CN=Users,DC=pndeflab,DC=edu Select
Extended Query	memberOf=CN=PND_Group,CN=Groups,DC=pndefl …
User naming attribute	CN

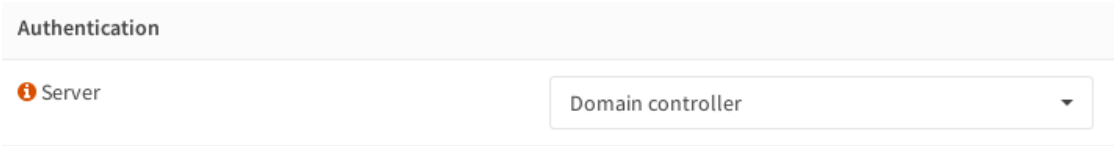
In field *Bind credentials*, insert the distinguished name and password for the *intfw* account created in the domain controller. In field *Extended query*, specify that the users must be member of the `PND_Group` group. After completing the form up to *Base DN*, press the *Select* button adjacent to field *Authentication containers* and choose the only option available.

3.2 Users

In *System* ▷ *Access* ▷ *Users*, import start importing new users clicking on the cloud icon. Select all showed users and insert them in the `admin` group.

3.3 Settings

In *System* ▷ *Settings* ▷ *Administration*, change the authentication server to *Domain controller*. Since superuser access is disabled, it may be advisable to add `admin` to the list of sudoers.



If SSH is enabled, add `admin` to the SSH login groups and disable root login.

4 OPNsense main firewall configuration

Follow the configuration section for the internal firewall, changing the bind account to the one created for `mainfw`. In the internal firewall, create a rule for allowing LDAP traffic from the main firewall to the domain controller.

	Protocol	Source	Port	Destination	Port
▶	IPv4 TCP	mainfw_address	*	dc_address	389 (LDAP)

5 Test of the configuration

Testing was performed manually, trying to login in the two firewalls, both in the web GUI and the physical terminal. Using the built-in root user had a negative outcome, while using a LDAP account gave access to both the web GUI and the shell.

6 Final remarks

OPNsense has a lacklustre LDAP support.

The primary shortcoming is the manual user configuration: the usefulness of a central domain controller is greatly diminished if admins must import locally and configure new users in each firewall.

Another deficiency is the non-existent group support. A sensible approach would be inserting newly-imported users into local groups with the same names as their LDAP groups (optionally creating those which do not exist) in order to ease privilege assignment; instead, LDAP groups are completely ignored.

Lastly, the documentation is not up to date: some icons are different (e.g. the user import icon) and some settings are located in different sections (e.g. the active authentication servers).