UNIVERSITAT D'ANDORRA

Bàtxelor en informàtica

Assignment	Subject	Start Date	Due Date
TV2	Computer Networks II	23/03/2021	30/04/2021

1 Objective

After having familiarized with GNU/Linux and the most common network services in small to large enterprises, the objective of this second assignment is to secure these services using different approaches.

The main objective of this assignment is that students familiarize with PKI (Public Key Infrastructure), certificate authorities, LDAP user authentication and signing processes.

Description	Competences	Weighted grade
Computer Networks Security	UdA04, UdA06, BINFO06	24%

2 Guidelines

- The submitted file should be called: TV2_SurnamesName.{pdf,docx,odt}.
- Only one type of file format should be delivered, preferably a PDF file.
- If the file contains images, please, insert them in the document, **DO NOT** submit them as separate files.
- You can work on this assignment with the host system of your choice: Microsoft Windows, macOS or GNU/Linux.
- No assignment will be accepted after the specified due date.

3 Assignment Description

3.1 Introduction

On this assignment, again, the student will work with GNU/Linux systems. This is, still, the most common operating system used on network servers around the world.

The student will work with the Debian[1] GNU/Linux distribution. At the same time, a virtual network environment will be designed and implemented using VirtualBox[2] and the GNS3

[1] `https://www.debian.org`
[2] `https://www.virtualbox.org`

simulator[3]. The CISCO image file needed for the Routers is located at the moodle Computer Networks II course web page.

3.2 The Network

The environment that is asked to implement has three different networks. All machines have to be under the `cnii.lan` domain. This is the **exact same network** topology used in TV1. Nothing has to be changed, you can use the same you used in TV1 by duplicating the GNS3 project, or continue on the same one. The environment has the following characteristics:

- There is a network where all end-user computers will be allocated. This network has a default gateway in Router **R1** (IP address `172.16.0.1`).
- There is a second network where all servers will be allocated. This second network has a default gateway in Router **R2** (IP address `172.16.1.1`).
- **R1** is directly connected to **R2**.

The three different subnets use addresses from the `172.16.0.0/12` private range:

- Network for the end-user computers: `172.16.0.0/24`
- Network for the servers: `172.16.1.0/24`
- Subnet between Routers **R1** and **R2**: `172.17.0.0/30`

3.3 Docker containers

The Docker containers needed in this assignment are the following:

- DNS Server: Already configured in TV1
- Web Server: Already configured in TV1
- Mail Server: Already configured in TV1
- Client machine (end-user client): Already configured in TV1
- LDAP Server: You can install the `slapd` service in the DNS machine, for example, using the following command: `$ apt install slapd`

3.4 DNS Server

A new entry `files` has to be added to the DNS server. You also need to add a new `apache2` VirtualHost, using the following url: `https://files.cnii.lan`.

3.5 LDAP Server

An LDAP service has to be added to the services network. This LDAP server will have all the information of all the users on the network. All mail services (`smtp`, `imap`, `pop3`) have to be modified to use this LDAP directory to authenticate users.

The relevant information for the directory is the following:

- Domain: `cnii.lan` (`dc=cnii,dc=lan`)

[3] `https://gns3.com`

- Organization: UdA
- Admin user: `cn=admin,dc=cnii,dc=lan`
- A new `Organizational Unit` called `Users` should be added to the directory
- A couple of users should be added as well to test authentication (as with TV1, you can use `user1`, `user2` and so on)

NOTE: To manage the LDAP directory, applications like Apache Directory Studio[4] or phpLDAPAdmin[5] are highly recommended. At the same time, reading of the following two pages can be useful to configure the LDAP service:

- Debian Wiki: `https://wiki.debian.org/LDAP/OpenLDAPSetup`
- OpenLDAP documentation: `https://www.openldap.org/doc/admin24/quickstart.html`

4 Questions

1. Certificate Authority and Service Security
   (a) Implement a Certificate Authority (CA) using OpenSSL for the `cnii.lan` domain. This means that a **self-signed root certificate** will be needed, as well as the certificates that are detailed below. To answer this question detail all commands and files you have used/created/modify to create the CA.

   NOTE: No restrictions are given to the different options available when issuing certificates. It is up to the student to choose these options and justify the chosen parameters.

   (b) Install the `cnii.lan` self-signed root certificate on all machines so that the `cnii.lan` certificates issued by the CA are trusted throughout the whole network. To answer this question detail the process you have followed on the end-user machine.

   (c) Issue new certificates for the `www.cnii.lan` WordPress installation as well as for the `mail.cnii.lan` Roudcube installation and install them accordingly in `apache2`. Verify that the Debian client can access the services securely and that no certificate trust errors are displayed. To do so be sure to include a Wireshark traffic capture showing all SSL connection steps between client and server. At the same time include a screen capture showing the lock on the client Internet browser.

   (d) Create a new VirtualHost in `apache2` with some files in it. Use the `files.cnii.lan` domain name. This area has to be accessed **using personal user certificates**. Issue two different user certificates and install them on the client Internet browser of the Debian desktop client and finally configure `apache2` so that the access to this VirtualHost requires SSL client certificate authentication. Show all configuration files that you have modified in `apache2`.

   (e) Issue a new certificate for the LDAP server (`ldap.cnii.lan`) and install it accordingly on the LDAP service. Show the `ldif` file used to activate TLS and verify that the connection is established using `ldapsearch` and the `-ZZ` option.

   (f) Modify the `dovecot` and the `postfix` configurations so that they use LDAP to authenticate users. At the same time change the Roundcube configuration to ensure that all communications are secured. To answer this question show the modification on all affected files.

[4] `https://directory.apache.org/studio`
[5] `http://phpldapadmin.sf.net`

2. Firewall: Now that services have a *higher* level of security it is time to configure the `iptables` firewall on your `apache2` Docker container (make sure that the `iptables` command is available using: `$ apt install iptables`). Submit the different `iptables` commands used to accomplish the following requirements:
   (a) Drop all packets coming in or out of the container (be careful of not being left out of a SSH connection).
   (b) Discard all fragmented or invalid traffic.
   (c) Accept all traffic on the `lo` interface (this is very important).
   (d) Allow RELATED and ESTABLISHED connections in and out of the Virtual Machine.
   (e) Allow access to `apache2` (request and response), both secure and insecure from the 172.16.0.0/12 network.
   (f) Allow access to `ssh` only from the network the `apache2` machine is on, discard the rest with `ICMP` port unreachable packets.
   (g) Allow all `ICMP` packets (test with `ping` and `traceroute`).
   (h) After having configured the firewall we have left out of the configuration the `smtp` and `imap` ports that Roundcube uses to communicate with the mail server as well as DNS resolution. So, for the whole system to work again, add them to the `iptables` configuration as well.
   (i) Show the result of executing the following command: `$ iptables -nvL`
   (j) On Router R1 add NAT forwarding rules to send all `http` and `https` packets to the `apache2` server. Can you access the WordPress installation from outside the GNS3 simulation using `https://www.cnii.lan`? Why not? Detail the steps to make it possible (Answer this WITHOUT modifying the *hosts* file on your Windows or macOS machine).

3. GnuPG: For this section we are going to need the **Thunderbird** email client application and the **Enigmail** add-on to manage **GPG** keys on the Debian desktop machine.
   (a) Create GPG keys for the two users and install these keys on Thunderbird's Enigmail. To do so you can do it from any machine with the `gpg` command application.
   (b) Send messages between the two users, using the `smtp.cnii.lan` server, *signing* and *encrypting* the contents of the message. Verify that the recipient user can read the encrypted messages and that the signatures verifies. Show the *source code* contents of an encrypted and a signed message.

5 Documentation

Below are listed some Internet resources that may be helpful when solving this assignment:

- Introduction to GNU/Linux: `http://www.tldp.org/LDP/intro-linux/html/`
- Bind server homepage: `https://www.isc.org/downloads/bind/`
- Apache server homepage: `https://httpd.apache.org`
- Postfix server homepage: `http://www.postfix.org`
- Dovecot server homepage: `https://dovecot.org`
- Roundcube webmail application: `https://roundcube.net`

- WordPress documentation: `https://codex.wordpress.org`
- OpenLDAP documentation: `https://www.openldap.org/doc/admin24`
- Debian Wiki (lots of Tutorials and How-Tos): `https://wiki.debian.org`
- OpenSSL documentation: `https://www.openssl.org`
- GnuPG documentation: `https://www.gnupg.org/documentation/manuals/gnupg/`