STI 2022/2023

Practical Assignment #1

1. Goals

- Configure a VPN tunnel in the "road warrior" scenario.
- Enable two-factor user authentication with OpenVPN and Apache services.
- Manage PKI: certification authorities, X.509 certificates, revocation and OCSP.

2. General description

Figure 1 illustrates the scenario considered for our practical assignment. As illustrated, secure communications are supported by a VPN tunnel established between a remote client (road warrior) and the VPN gateway, with the purpose of enabling accesses to services in the Internal Network, particularly a web server running Apache. For enabling the VPN tunnel, we will use OpenVPN (https://openvpn.net).

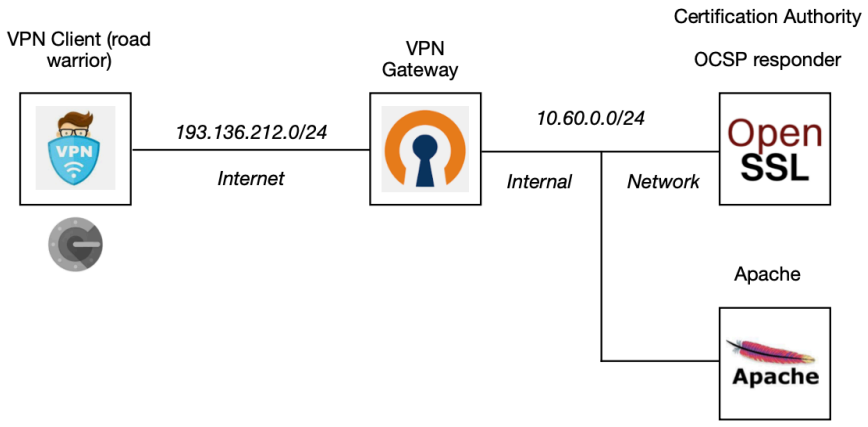

Figure 1 – Scenario for the Practical Assignment #1

Regarding authentication, the two communication entities participating in the VPN tunnel (road warrior and the VPN gateway) should possess valid X.509 certificates, which we will create with a private Certification Authority (CA). Users establishing remote connections to the VPN gateway (road warriors), as well as users connecting to the Apache server, will also use two-factor authentication, as described below. Apache must also implement client authentication via X.509 certificates. Figure 2 provides an illustration of the interactions between all the entities involved in this setup.

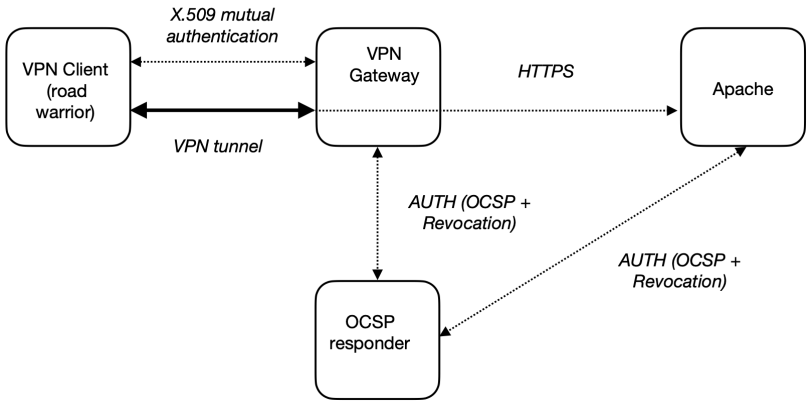

Figure 2 – X.509 mutual authentication and OCSP

As we can observe in Figure 2, the VPN gateway and the Apache web server must verify the status of validity of certificates using OCSP (Online Certificate Status Protocol) and revocation information from the CA. OCSP verification is not required for the road warrior in what respects authentication to the VPN gateway. Next, we describe the configuration requirements for the various components of the assignment.

3. Configuration requirements

VPN tunnel for remote access (road warriors)

As illustrated in Figure 1, remote clients (road warriors) are able to connect to the VPN gateway and, using the tunnel, remotely access hosts in the Internal network. The following configuration requirements should be considered:

- In order to establish a VPN tunnel with the VPN gateway, the road warrior must be in the possession of a valid X.509 certificate, created with the private CA of the scenario.

- The road warrior and the VPN gateway must perform mutual authentication using X.509 digital certificates.

- The VPN gateway should verify the validity of the X.509 certificate presented by the road warrior using OCSP and, in case the certificate is revoked, the gateway should refuse the connection.

- In order to authorize the remote user, the VPN gateway should also enforce two other authentication steps: the user must present a valid username and password, plus a one-time password (authentication token).

Web server

The road warrior user should be able to contact the Apache web server via HTTPS once the VPN tunnel is established. The following configuration requirements should be considered:

- Apache should enforce two-factor authentication in order to authorize accesses from clients: the client (browser) should present a valid X.509 certificate (issued with the private CA of the scenario) and the user should also present a valid one-time password (authentication token).

- As in the VPN scenario, the validity of the X.509 certificate presented by the client should be checked in the CA using OCSP.

Two-factor user authentication

As previously discussed, VPN establishment and HTTPS accesses to Apache make use of one-time passwords (authentication tokens), which may be generated by an appropriate application. One-time passwords may be generated using the TOTP (Time-based One-time Password Algorithm). This algorithm employs a secret key shared between the user (client) and the remote service plus a timestamp (obtained from the current system time), to obtain a one-time password.

In order to generate a one-time password, the user may use an application such as Google Authenticator, illustrated in Figure 3. This application periodically generates a one-time password that can be used to authenticate the user with a remote service. This application is available for iOS and Android [1].

Certification authority

As already discussed, the goal is to use OpenSSL to configure a private Certification Authority, as well as to issue and revoke X.509 digital certificates for the VPN gateways and remote users. The following configuration requirements should be considered:

- The Certification Authority is used to issue certificates for the VPN gateway, VPN client, Apache web server and clients (users) connecting to Apache web server.
- The Certification Authority allows the revocation of certificates previously issued.
- The Certification Authority also supports a OCSP responder.

[1] For Android: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en and for Apple iOS: https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8

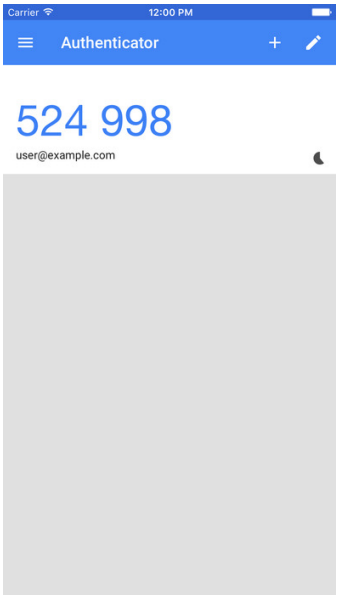

Figure 3 – Google Authenticator app, to generate a one-time password to access services enabled with two-factor authentication

4. Delivery of the Practical Assignment

With the assignment please deliver also a report, containing the following information:

- Descriptions and configuration files for the implementation of the previous requirements.
- A description of how the private Certification Authority was created using OpenSSL.
- A description of how X.509 certificates were issued and revoked using the private Certification Authority.
- A description of the tests performed to validate the functionalities implemented.
- Remaining information considered relevant.

For the delivery of the assignment, put your report, as well as the relevant configuration files, in a single archive. This archive should be signed using your PGP key and encrypted using the PGP key of your PL teacher.

Note: Assignments without PGP will be accepted, although with a discount of 5% in the final grade.

Delivery deadline:

- The deadline for the submission of the assignment (configuration files and report) is March 5th 2023.
- Submission via Inforestudante.