FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE D COIMBRA

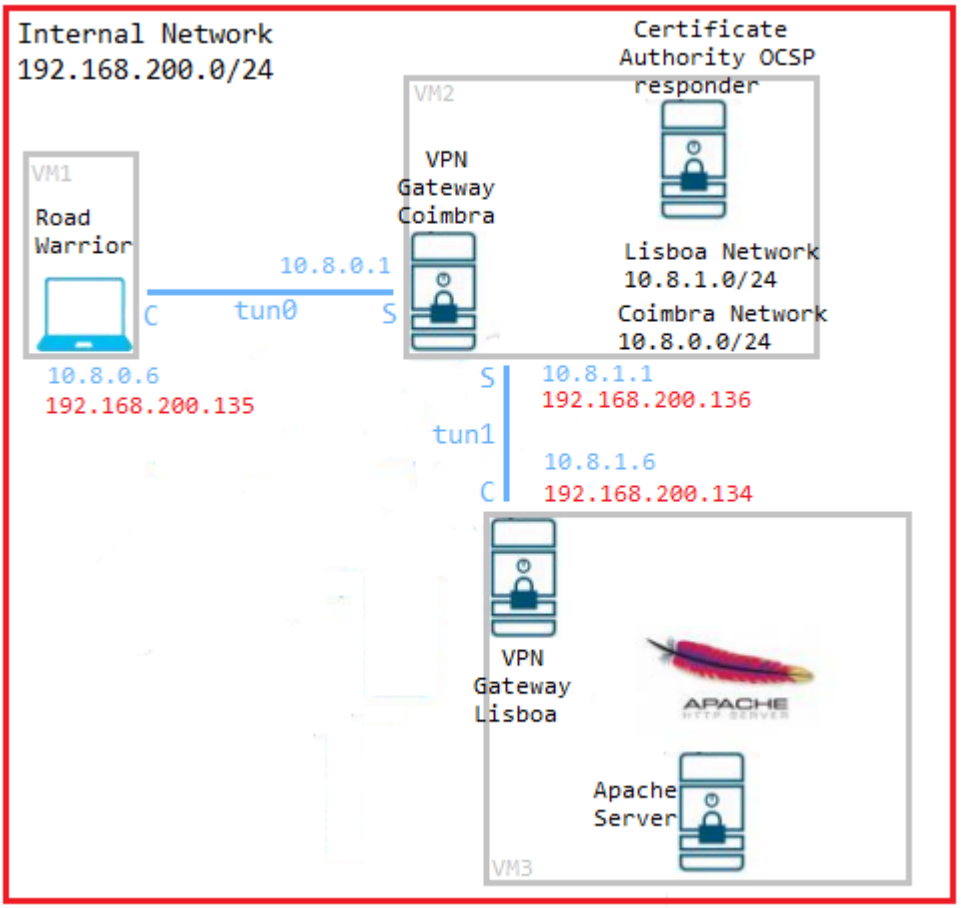
Departamento Engenharia Informática

STI 2021/2022

Relatório Trabalho Prático Nº1:

Trabalho realizado por:
João Calhau 2016255704
Tatiana Simões 2018285812

1. Configurações:



2. Criação da private Certification Authority:

2.1. Criação da chave privada da autoridade de certificação.
openssl genrsa -out ca.key -des3

2.2. Criação do certificado X.509 com a chave privada da CA com as respectivas informações da autoridade de certificação.
openssl req -new -x509 -days 365 -key ca.key -out certs/ca.crt -config validation.cnf

Informações da CA:

Country Name: PT
State or Province Name: Coimbra
Locality Name: Coimbra
Organization Name: UC
Organizational Unit Name: DEI
Common Name: ca
Email Address: ca@dei.pt

3. Certificates issued e revoked usando a private Certification Authority:

Após a criação do certificado de autenticação, passámos à criação dos restantes certificados de servidores e clientes usados no trabalho.

3.1. Criação da chave privada do certificado:
openssl genrsa -out x_nome.key -des3

3.2. Criação do certificado baseado na chave privada criada no ponto anterior:
openssl req -new -x509 -days 365 -key x_nome.key -out x_nome.crt -config validation.cnf

Informações da CA:
Country Name: PT
State or Province Name: Coimbra
Locality Name: Coimbra
Organization Name: UC
Organizational Unit Name: DEI
Common Name: x_nome
Email Address: x_nome@dei.pt

3.3. Criar o certificate signing request(CSR):
openssl x509 -x509toreq -in x_nome.crt -out x_nome.csr -signkey x_nome.key

3.4. Assinar o certificado do cliente usando a CA de coimbra:
openssl ca -batch -startdate 150813080000Z -enddate 250813090000Z -keyfile ca.key -cert ca.crt -policy policy_anything -config validation.cnf -notext -out x_nome.crt -infiles x_nome.csr

3.5. Revogar um certificado:
openssl ca -keyfile ca.key -cert ca.crt -revoke x_nome.crt
Desta forma o certificado passa de ‘good’ para ‘revoked’

4. Two-Factor Authentication:

Para termos two-factor authentication usamos o google authentication. Para isto tivemos de mudar os ficheiros de configuração do servidor de coimbra, do cliente do road warrior e da openvpn.

4.1. Coimbra Gateway (server.conf):
plugin /PATH/openvpn-plugin-auth-pam.so openvpn

4.2. Openvpn (/etc/pam.d/openvpn)

auth requisite lib/x86_64-linux-gnu/security/pam_google_authenticator.so secret=/etc/openvpn/google-authenticator/${USER} user=gauth forward_pass

4.3. Road Warrior (client.conf):

auth-user-pass

Após isto criamos um utilizador de teste ao qual chamamos de test user. Após isto podemos então usar o seguinte comando para gerar um QR code para este utilizador:

su -c "google-authenticator -t -d -r3 -R30 -f -l 'OpenVPN Server' -s /etc/openvpn/google-authenticator/testuser" - gauth

5. OCSP:

Para utilizar o Online Certificate Status Protocol (OCSP), criamos um novo ficheiro de configuração igual ao openssl.cnf ao qual demos o nome de validation.cnf. De seguida acrescentamos as seguintes informações:

```
[ usr_cert ]
authorityInfoAccess = OCSP;URI:http://192.168.200.136:8080

[ v3_OCSP ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = OCSPSigning
```

Todos os certificados criados usaram esta configuração (-config validation.cnf) de forma a terem acesso ao OCSP.
Após termos estas configurações e dado que todos os certificados foram assinados no nosso servidor de coimbra, este ficou com o index.txt preenchido com todos os nossos requests, logo o OCSP consegue revogar qualquer um dos certificados.

Para conseguirmos correr o ocsp server, criamos o certificado do OCSP com os seguintes comandos:

openssl req -new -nodes -out ocspSigning.csr -keyout ocspSigning.key

openssl ca -keyfile ca.key -cert ca.crt -in ocspSigning.csr -out ocspSigning.crt -config validation.conf

De seguida inicializamos o OSCP server com o seguinte comando:
openssl ocsp -index CA/index.txt -port 8080 -rsigner ocspSigning.crt -rkey ocspSigning.key -CA ca.crt -text -out log.txt &

```
ocsp: waiting for OCSP client connections...
```

Para verificar o estado de um certificado corremos o seguinte comando:
*openssl ocsp -CAfile ca.crt -issuer ca.crt -cert x_nome.crt -url http://*192.168.200.136*:8080 -resp_text -noverify*

```
/etc/pki/CA/warrior/warrior_bad.crt: revoked
        This Update: Mar 11 23:22:06 2022 GMT
        Revocation Time: Mar 11 22:52:16 2022 GMT
```

6. Servidor Apache

Para criarmos o servidor apache seguimos os seguintes passos:

6.1. No ficheiro /etc/hosts(na VM de Lisboa, ou host do apache):
192.168.200.134 www.sti.pt
No qual www.sti.pt é o CN do certificado para o servidor de apache

6.2. No ficheiro /etc/apache2/sites-available/default-ssl.conf:
SSLCertificateFile /etc/pki/apache/apache.crt
SSLCertificateKeyFile /etc/pki/apache/apache.key
SSLCACertificateFile /etc/pki/CA/certs/ca.crt

6.3. No ficheiro /etc/hosts(na VM de RoadWarrior):
10.8.1.6 www.sti.pt

6.4. Após isto ligamos o site com SSL(pasta onde está o ficheiro default-ssl.conf)
a2ensite default-ssl.conf
systemctl reload apache2

7. Testes

7.1. Conexão de RoadWarrior para Coimbra

```
2022-03-12 01:32:47 192.168.200.135:42677 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2022-03-12 01:32:47 192.168.200.135:42677 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2022-03-12 01:32:47 192.168.200.135:42677 TLS: Initial packet from [AF_INET]192.168.200.135:42677, sid=2cb1507b a42c3117
2022-03-12 01:32:47 192.168.200.135:42677 VERIFY OK: depth=1, C=PT, ST=Coimbra, L=Coimbra, O=UC, OU=DEI, CN=ca, emailAddress=ca@dei.pt
2022-03-12 01:32:47 192.168.200.135:42677 VERIFY OK: depth=0, C=PT, ST=Coimbra, L=Coimbra, O=UC, OU=DEI, CN=warrior, emailAddress=warrior@dei.pt
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_VER=2.5.1
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_PLAT=linux
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_PROTO=6
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_NCP=2
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_CIPHERS=AES-256-GCM:AES-128-GCM:AES-256-CBC
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_LZ4=1
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_LZ4v2=1
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_LZO=1
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_COMP_STUB=1
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_COMP_STUBv2=1
2022-03-12 01:32:47 192.168.200.135:42677 peer info: IV_TCPNL=1
2022-03-12 01:32:47 192.168.200.135:42677 PLUGIN_CALL: POST /usr/lib/openvpn/openvpn-plugin-auth-pam.so/PLUGIN_AUTH_USER_PASS_VERIFY status=0
2022-03-12 01:32:47 192.168.200.135:42677 TLS: Username/Password authentication succeeded for username 'testuser'
2022-03-12 01:32:47 192.168.200.135:42677 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2022-03-12 01:32:47 192.168.200.135:42677 [warrior] Peer Connection Initiated with [AF_INET]192.168.200.135:42677
```

7.2. Conexão de Lisboa para Coimbra

```
2022-03-11 23:11:19 192.168.200.134:50547 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2022-03-11 23:11:19 192.168.200.134:50547 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2022-03-11 23:11:19 192.168.200.134:50547 TLS: Initial packet from [AF_INET]192.168.200.134:50547, sid=f47054e1 66d93ced
2022-03-11 23:11:19 192.168.200.134:50547 VERIFY OK: depth=1, C=PT, ST=Coimbra, L=Coimbra, O=UC, OU=DEI, CN=ca, emailAddress=ca@dei.pt
2022-03-11 23:11:19 192.168.200.134:50547 VERIFY OK: depth=0, C=PT, ST=Coimbra, L=Coimbra, O=UC, OU=DEI, CN=lisboa, emailAddress=lisboa@dei.pt
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_VER=2.5.1
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_PLAT=linux
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_PROTO=6
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_NCP=2
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_CIPHERS=AES-256-GCM:AES-128-GCM:AES-256-CBC
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_LZ4=1
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_LZ4v2=1
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_LZO=1
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_COMP_STUB=1
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_COMP_STUBv2=1
2022-03-11 23:11:19 192.168.200.134:50547 peer info: IV_TCPNL=1
2022-03-11 23:11:19 192.168.200.134:50547 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2022-03-11 23:11:19 192.168.200.134:50547 [lisboa] Peer Connection Initiated with [AF_INET]192.168.200.134:50547
```

7.3. Ping do RoadWarrior para Lisboa

```
root@debian:~# ping 10.8.1.6
PING 10.8.1.6 (10.8.1.6) 56(84) bytes of data.
64 bytes from 10.8.1.6: icmp_seq=1 ttl=63 time=5.27 ms
64 bytes from 10.8.1.6: icmp_seq=2 ttl=63 time=5.11 ms
64 bytes from 10.8.1.6: icmp_seq=3 ttl=63 time=2.15 ms
64 bytes from 10.8.1.6: icmp_seq=4 ttl=63 time=6.32 ms
64 bytes from 10.8.1.6: icmp_seq=5 ttl=63 time=5.97 ms
```

No.	Time	Source	Destination	Protocol	Length	Info
91	26.402315019	192.168.200.136	192.168.200.135	OpenVPN	152	MessageType: P_DATA_V2
92	26.402676849	10.8.1.6	10.8.0.6	ICMP	100	Echo (ping) reply id
93	27.401570870	10.8.0.6	10.8.1.6	ICMP	100	Echo (ping) request id
94	27.401681598	192.168.200.135	192.168.200.136	OpenVPN	152	MessageType: P_DATA_V2
95	27.403140679	192.168.200.136	192.168.200.135	OpenVPN	152	MessageType: P_DATA_V2
96	27.403249468	10.8.1.6	10.8.0.6	ICMP	100	Echo (ping) reply id
97	28.405689012	10.8.0.6	10.8.1.6	ICMP	100	Echo (ping) request id
98	28.406015900	192.168.200.135	192.168.200.136	OpenVPN	152	MessageType: P_DATA_V2

7.4. Ping de Lisboa para RoadWarrior

```
root@debian:~# ping 10.8.0.6
PING 10.8.0.6 (10.8.0.6) 56(84) bytes of data.
64 bytes from 10.8.0.6: icmp_seq=1 ttl=63 time=5.40 ms
64 bytes from 10.8.0.6: icmp_seq=2 ttl=63 time=4.86 ms
64 bytes from 10.8.0.6: icmp_seq=3 ttl=63 time=1.92 ms
64 bytes from 10.8.0.6: icmp_seq=4 ttl=63 time=5.47 ms
64 bytes from 10.8.0.6: icmp_seq=5 ttl=63 time=2.48 ms
64 bytes from 10.8.0.6: icmp_seq=6 ttl=63 time=1.80 ms
64 bytes from 10.8.0.6: icmp_seq=7 ttl=63 time=5.63 ms
```

No.	Time	Source	Destination	Protocol	Length	Info
205	64.955846629	192.168.200.134	192.168.200.136	UDP	152	58156 → 1195 Len=108
206	64.957317066	192.168.200.136	192.168.200.134	UDP	152	1195 → 58156 Len=108
207	64.957427170	10.8.0.6	10.8.1.6	ICMP	100	Echo (ping) reply id
208	65.979126793	10.8.1.6	10.8.0.6	ICMP	100	Echo (ping) request id
209	65.979292717	192.168.200.134	192.168.200.136	UDP	152	58156 → 1195 Len=108
210	65.984001343	192.168.200.136	192.168.200.134	UDP	152	1195 → 58156 Len=108
211	65.984320544	10.8.0.6	10.8.1.6	ICMP	100	Echo (ping) reply id

```
▸ Frame 1: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0
▸ Linux cooked capture v1
```

7.5. Conexão ao www.sti.pt(servidor de apache) pelo RoadWarrior

7.6. Google authentication(MFA)

```
2022-03-12 01:08:56 192.168.200.135:34698 PLUGIN_CALL: POST /usr/lib/openvpn/openvpn-plugin-auth-pam.so/PLUGIN_AUTH_USER_PASS_VERIFY status=0
2022-03-12 01:08:56 192.168.200.135:34698 TLS: Username/Password authentication succeeded for username 'testuser'
```

```
2022-03-12 01:31:42 PLUGIN_AUTH-PAM: BACKGROUND: user 'testuser' failed to authenticate: Authentication failure
```

8. Referências relevantes:

8.1. Google Auth:
https://ulimit.nl/wp-content/uploads/2019/08/Extending-a-Debian-OpenVPN-server-with-Multi-Factor-Authentication-via-Google-Authenticator.pdf

8.2. OCSP:
https://bhashineen.medium.com/create-your-own-ocsp-server-ffb212df8e63