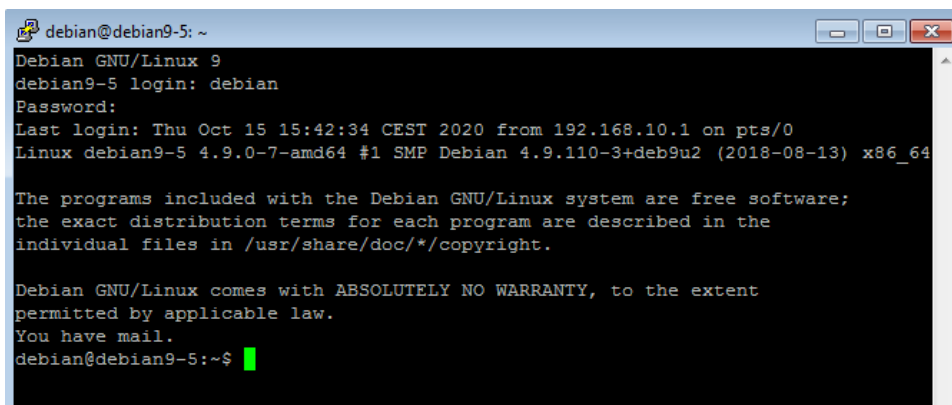


Compte rendu certificats

1 Accès à un serveur à distance

1 Telnet

Connexion Telnet avec Putty :



```
debian@debian9-5: ~
Debian GNU/Linux 9
debian9-5 login: debian
Password:
Last login: Thu Oct 15 15:42:34 CEST 2020 from 192.168.10.1 on pts/0
Linux debian9-5 4.9.0-7-amd64 #1 SMP Debian 4.9.110-3+deb9u2 (2018-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
debian@debian9-5:~$
```

Les trames entre la VM chrome et le switch ainsi qu'entre le switch et la debian :

12	9.711393	192.168.10.1	192.168.10.2	TELNET	55 Telnet Data ...
13	9.711851	192.168.10.2	192.168.10.1	TELNET	60 Telnet Data ...
14	9.922050	192.168.10.1	192.168.10.2	TCP	54 49158 → 23 [ACK] Seq=2 Ack=2 Win=254 Len=0
15	9.973471	192.168.10.1	192.168.10.2	TELNET	55 Telnet Data ...
16	9.973993	192.168.10.2	192.168.10.1	TELNET	60 Telnet Data ...
17	10.188220	192.168.10.1	192.168.10.2	TCP	54 49158 → 23 [ACK] Seq=3 Ack=3 Win=254 Len=0
18	10.276281	aa:bb:cc:00:01:10	Spanning-tree-(for-...	STP	60 RST. Root = 32768/1/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8002
19	11.301382	192.168.10.1	192.168.10.2	TELNET	56 Telnet Data ...
20	11.302238	192.168.10.2	192.168.10.1	TELNET	60 Telnet Data ...
21	11.515633	192.168.10.1	192.168.10.2	TCP	54 49158 → 23 [ACK] Seq=5 Ack=5 Win=254 Len=0
22	11.515905	192.168.10.2	192.168.10.1	TELNET	280 Telnet Data ...
23	11.735124	192.168.10.1	192.168.10.2	TCP	54 49158 → 23 [ACK] Seq=5 Ack=231 Win=253 Len=0

13	13.895695	192.168.10.1	192.168.10.2	TELNET	55 Telnet Data ...
14	13.896866	192.168.10.2	192.168.10.1	TELNET	60 Telnet Data ...
15	14.105942	192.168.10.1	192.168.10.2	TCP	54 49158 → 23 [ACK] Seq=2 Ack=2 Win=254 Len=0
16	14.157278	192.168.10.1	192.168.10.2	TELNET	55 Telnet Data ...
17	14.159022	192.168.10.2	192.168.10.1	TELNET	60 Telnet Data ...
18	14.372197	192.168.10.1	192.168.10.2	TCP	54 49158 → 23 [ACK] Seq=3 Ack=3 Win=254 Len=0
19	14.460891	aa:bb:cc:00:01:00	Spanning-tree-(for-...	STP	60 RST. Root = 32768/1/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8001
20	15.485312	192.168.10.1	192.168.10.2	TELNET	56 Telnet Data ...
21	15.487269	192.168.10.2	192.168.10.1	TELNET	60 Telnet Data ...
22	15.699689	192.168.10.1	192.168.10.2	TCP	54 49158 → 23 [ACK] Seq=5 Ack=5 Win=254 Len=0
23	15.700941	192.168.10.2	192.168.10.1	TELNET	280 Telnet Data ...
24	15.919156	192.168.10.1	192.168.10.2	TCP	54 49158 → 23 [ACK] Seq=5 Ack=231 Win=253 Len=0

2 La méthode sécurisée : SSH

Capture des trames lors de la connexion SSH depuis Putty :

386	467.239172	192.168.10.1	192.168.10.2	SSHv2	326 Client: Encrypted packet (len=272)
387	467.257534	192.168.10.2	192.168.10.1	SSHv2	102 Server: Encrypted packet (len=48)
388	467.276724	192.168.10.1	192.168.10.2	SSHv2	134 Client: Encrypted packet (len=80)
389	467.289221	192.168.10.2	192.168.10.1	SSHv2	582 Server: Encrypted packet (len=528)
390	467.498224	192.168.10.1	192.168.10.2	TCP	54 49160 → 22 [ACK] Seq=1757 Ack=2048 Win=65024 Len=0
391	467.499589	192.168.10.2	192.168.10.1	SSHv2	118 Server: Encrypted packet (len=64)
392	467.500219	192.168.10.1	192.168.10.2	SSHv2	230 Client: Encrypted packet (len=176)
393	467.502748	192.168.10.2	192.168.10.1	SSHv2	214 Server: Encrypted packet (len=160)
394	467.503101	192.168.10.2	192.168.10.1	SSHv2	454 Server: Encrypted packet (len=400)
395	467.503210	192.168.10.2	192.168.10.1	SSHv2	278 Server: Encrypted packet (len=224)
396	467.503323	192.168.10.1	192.168.10.2	TCP	54 49160 → 22 [ACK] Seq=1933 Ack=2672 Win=64256 Len=0
397	467.644043	192.168.10.2	192.168.10.1	SSHv2	150 Server: Encrypted packet (len=96)
398	467.644330	192.168.10.1	192.168.10.2	TCP	54 49160 → 22 [ACK] Seq=1933 Ack=2992 Win=65536 Len=0

387	463.055096	192.168.10.1	192.168.10.2	SSHv2	326 Client: Encrypted packet (len=272)
388	463.072039	192.168.10.2	192.168.10.1	SSHv2	102 Server: Encrypted packet (len=48)
389	463.092777	192.168.10.1	192.168.10.2	SSHv2	134 Client: Encrypted packet (len=80)
390	463.102450	192.168.10.2	192.168.10.1	SSHv2	582 Server: Encrypted packet (len=528)
391	463.314311	192.168.10.1	192.168.10.2	TCP	54 49160 → 22 [ACK] Seq=1757 Ack=2048 Win=65024 Len=0
392	463.314569	192.168.10.2	192.168.10.1	SSHv2	118 Server: Encrypted packet (len=64)
393	463.315949	192.168.10.1	192.168.10.2	SSHv2	230 Client: Encrypted packet (len=176)
394	463.317617	192.168.10.2	192.168.10.1	SSHv2	214 Server: Encrypted packet (len=160)
395	463.317834	192.168.10.2	192.168.10.1	SSHv2	454 Server: Encrypted packet (len=400)
396	463.317933	192.168.10.2	192.168.10.1	SSHv2	278 Server: Encrypted packet (len=224)
397	463.319023	192.168.10.1	192.168.10.2	TCP	54 49160 → 22 [ACK] Seq=1933 Ack=2672 Win=64256 Len=0
398	463.458801	192.168.10.2	192.168.10.1	SSHv2	150 Server: Encrypted packet (len=96)
399	463.460070	192.168.10.1	192.168.10.2	TCP	54 49160 → 22 [ACK] Seq=1933 Ack=2992 Win=65536 Len=0

Connexion à l'utilisateur nvu avec un mot de passe :

```

192.168.10.2 - PuTTY
login as: nvu
nvu@192.168.10.2's password:
Linux debian9-5 4.9.0-7-amd64 #1 SMP Debian 4.9.110-3+deb9u2 (2018-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 19 12:25:23 2020 from 192.168.10.1
Could not chdir to home directory /home/nvu: No such file or directory
$

```

3 Etablissement d'une connexion SSH avec clé asymétrique

Connexion a nvu2 :

```

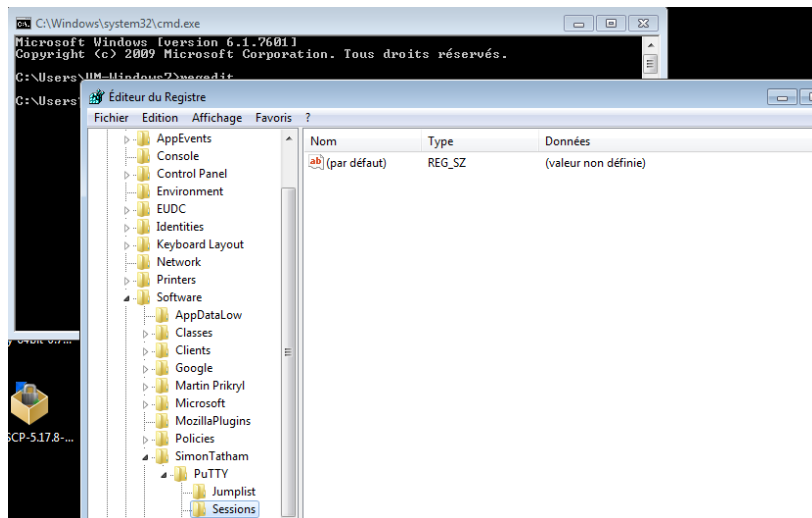
192.168.10.2 - PuTTY
login as: nvu2
nvu2@192.168.10.2's password:
Linux debian9-5 4.9.0-7-amd64 #1 SMP Debian 4.9.110-3+deb9u2 (2018-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Oct 15 17:21:29 2020 from 192.168.10.1
Could not chdir to home directory /home/nvu2: No such file or directory
$

```

Regedit de la VM :



```

                                debian@debian9-5: /etc/ssh

Fichier  Édition  Affichage  Rechercher  Terminal  Aide

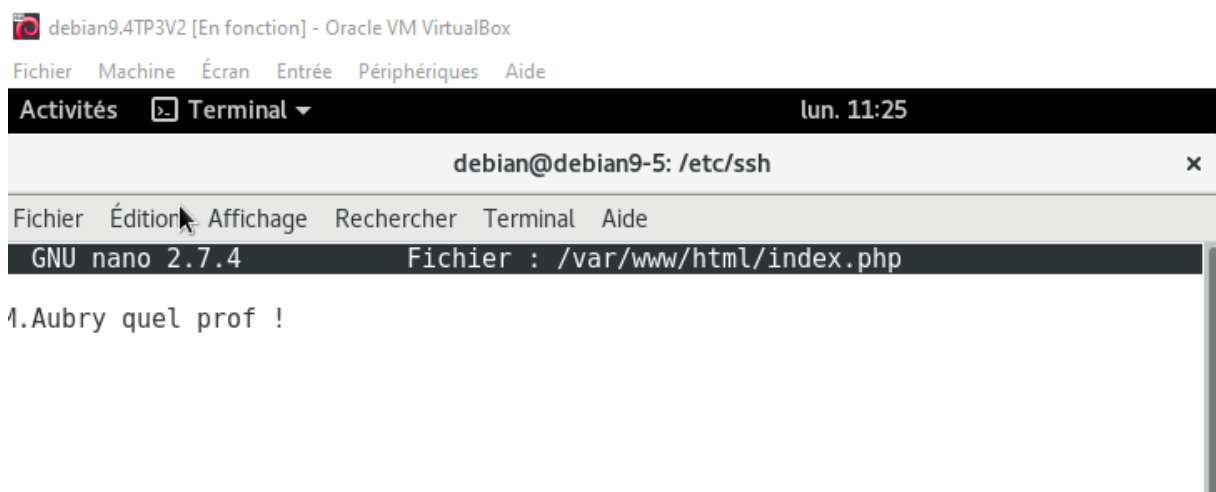
debian@debian9-5:~$ cd /etc/ssh
debian@debian9-5:/etc/ssh$ ls
moduli          ssh_host_ecdsa_key      ssh_host_ed25519_key.pub
ssh_config      ssh_host_ecdsa_key.pub  ssh_host_rsa_key
sshd_config     ssh_host_ed25519_key    ssh_host_rsa_key.pub

```

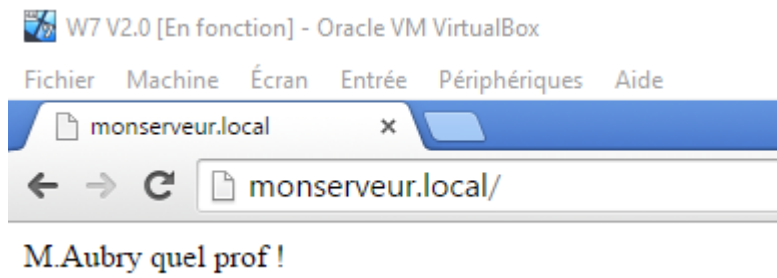
2 Mise en place d'un serveur web sécurisé

1 Connexion HTTP

Modification du fichier /var/www/html/index.php



⇒ Affichage de la page modifié



2 Connexion HTTPS

```
debian@debian9-5:/etc/apache2$ ls
apache2.conf      envvars          mods-enabled      sites-enabled
conf-available    magic            ports.conf        ssl
conf-enabled      mods-available  sites-available
```

1 Création d'un certificat serveur

```
root@debian9-5:/etc/apache2/ssl# openssl genrsa 2048 > monserveur.key
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x010001)
```

```
root@debian9-5:/etc/apache2/ssl# openssl req -new -key monserveur.key > monserveur.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:DOUBS
Locality Name (eg, city) []:Besak
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LLB
Organizational Unit Name (eg, section) []:BTSINFO
Common Name (e.g. server FQDN or YOUR name) []:monserveur.local
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Signature du certificat par le CA :

```
root@debian9-5:/etc/apache2/ssl# openssl x509 -req -in monserveur.csr -out monserveur.crt
t -CA ca.crt -CAkey ca.key -CAcreateserial -CAserial ca.srl
Signature ok
subject=C = FR, ST = DOUBS, L = Besak, O = LLB\09, OU = BTSINFO, CN = monserveur.local
Getting CA Private Key
Enter pass phrase for ca.key:
unable to load CA Private Key
140360974914816:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt
:../crypto/evp/evp_enc.c:535:
140360974914816:error:0906A065:PEM routines:PEM_do_header:bad decrypt:../crypto/pem/pem_
lib.c:445:
```

W7 V2.0 [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

https://monserveur.local x

← → ↻  https://monserveur.local

M.Aubry quel prof !