ANNEX A · SSH AND TLS

Name: _____ **Group:** _____ **Date:** _____

The lab. `pc1` is your office PC. `srv` (`203.0.113.10`, name `intranet.tramuntana.internal`) is a server on the other side of the router. The user on `srv` is `marta`, password `Tramuntana2027`. You need **two terminals in `pc1`**: A captures, B works.

```
cd ~/lab/office && containerlab deploy -t office.clab.yml
docker exec -it clab-office-pc1 bash          (twice: terminal A and terminal B)
```

1 Which doors are open?

```
nc -zv 203.0.113.10 23        (then 22, 80 and 443)
```

Port 23 is _____ 22 is _____ 80 is _____ 443 is _____

2 Telnet: read a password off the wire

```
A:  tcpdump -i eth1 -w /tmp/telnet.pcap port 23
B:  telnet 203.0.113.10          (log in, type  whoami , then  exit )
A:  Ctrl+C
A:  tshark -r /tmp/telnet.pcap -q -z follow,tcp,ascii,0
```

What can you read in the capture? Tick: ☐ user name ☐ password ☐ the command ☐ its answer

Which machine between `pc1` and `srv` could have made the same capture? _____

DONE WHEN you can point at the password in your own capture.

3 SSH: the same login in a sealed envelope

```
on the PC, in a third terminal (the true fingerprint, straight from the server):
    docker exec clab-office-srv ssh-keygen -lf /etc/ssh/ssh_host_ed25519_key.pub
A:  tcpdump -i eth1 -w /tmp/ssh.pcap port 22
B:  ssh marta@203.0.113.10       (STOP at the question. Compare. Then: yes)
B:  whoami ;  exit        A:  Ctrl+C
A:  tshark -r /tmp/ssh.pcap -q -z follow,tcp,ascii,0 | head -20
```

Last 6 characters of the fingerprint: on the server _____ shown by `ssh` _____

Same? _____

What is still readable in the capture? _____

What can a spy on the path still learn? _____

DONE WHEN the two fingerprints match and you cannot find `Tramuntana2027` in the SSH capture.

4 HTTP against HTTPS

```
A:  tcpdump -i eth1 -w /tmp/web.pcap port 80 or port 443
B:  curl http://intranet.tramuntana.internal/
B:  curl https://intranet.tramuntana.internal/         (read the error)
B:  curl -k https://intranet.tramuntana.internal/      (-k = do not check the certificate)
A:  Ctrl+C
A:  tshark -r /tmp/web.pcap -q -z follow,tcp,ascii,0            (the HTTP conversation)
A:  tshark -r /tmp/web.pcap -q -z follow,tcp,ascii,1 | head -30   (the HTTPS one)
B:  openssl s_client -connect intranet.tramuntana.internal:443 -brief </dev/null
```

a) The secret you can read in the HTTP conversation: _____

b) The error of `curl https://…` (the last words): _____

Which of the browser's three checks failed? _____

c) From `openssl`: Protocol version _____ Certificate name (CN) _____

DONE WHEN you read the secret in stream 0 and cannot read it in stream 1.

5 A real certificate (on the Ubuntu PC, not in the lab)

```
openssl s_client -connect example.com:443 -servername example.com -brief </dev/null
```

Protocol version: _____ Verification: _____ Certificate name: _____

Open any site you use in the browser and click the padlock. Site: _____

Issued by: _____

Valid until: _____

DONE WHEN `Verification: OK` appears. Then in the lab folder: `containerlab destroy -t office.clab.yml --cleanup`.

6 Close the clear-text doors of your MikroTik (group)

```
/ip service print
/ip service disable telnet,ftp,www,api
/ip ssh set strong-crypto=yes
from a PC:  nc -zv 10.G.0.1 23      then      ssh admin@10.G.0.1
```

Services still enabled: _____

`nc` to port 23, before: _____ after: _____

DONE WHEN Telnet is refused and one of you has a RouterOS prompt over SSH.

Exit ticket — alone, no notes. Tick one answer.

1. Why must Telnet not be used to manage a router?

☐ **A)** It only works inside a LAN ☐ **B)** It sends the password as readable text
☐ **C)** It is slower than SSH ☐ **D)** It needs a certificate

2. `ssh` says: REMOTE HOST IDENTIFICATION HAS CHANGED. What does it mean?

☐ **A)** Your password has expired ☐ **B)** The server is switched off
☐ **C)** Your user was deleted ☐ **D)** The server's key is not the one you saved

3. A browser rejects a self-signed certificate. Which check failed?

☐ **A)** It is not signed by a trusted authority ☐ **B)** The connection is not encrypted
☐ **C)** The port is not 443 ☐ **D)** The page uses TLS 1.3

4. Which port and which protocol protect HTTPS?

☐ **A)** 80, SSH ☐ **B)** 22, TLS
☐ **C)** 443, TLS ☐ **D)** 443, Telnet

5. You use HTTPS on the café's Wi-Fi. What can the café still see?

☐ **A)** The page you read ☐ **B)** Which server you talk to, and when
☐ **C)** Your password ☐ **D)** The form you sent