** task group: secure communication **

Context

Sometimes you need to debug your HTTP(S) network traffic.

An often used tool for analyzing HTTP(S) (and other Internet) traffic is Wireshark (http://www.wireshark.org). NOTE: by sniffing the network possibly the Confidentially is in danger.

Two other tools come in handy when testing for HTTP connections: `telnet` (or `netcat`) for HTTP and `openssl` for HTTPS. HTTP is a ASCII based protocol, which you can easily play yourself.

Deliverables

- Show screenshots/screencast of a HTTP connection to your test host
- Show screenshots/screencast of a HTTPS connection to your personal bank

Task

1. Download a Kali VirtualBox VM (https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/)

2. Download the Windesheim BBT VM from the elo.

3. Start your Kali VM

4. Start the Windesheim BBT VM

   - Obtain your IP number via `$ ip address`

5. Kali: Run

   ```
   $ telnet IP_OF_BBT 80
   ```

   Now you can 'speak' HTTP (send the HTTP request optionally with headers)

   ```
   GET / HTTP/1.0
   [ENTER]
   ```

   You should see the server responding with the contents of the index.html file.

6. Kali: using telnet for HTTPS connections is very cumbersome (you have to type binary). Therefore we use `openssl` for debugging a TLS connection:

   ```
   $ openssl s_client -connect IP_OF_BBT:443
   ```

You should see the TLS cryptography exchange Again now you can 'speak' HTTP (send the HTTP request optionally with headers)

```
GET / HTTP/1.0
[ENTER]
```

You should see the server responding with the contents of the index.html file.

7. Kali: Start Wireshark and start sniffing on the host_only interface
8. Kali: Start a browser and surf with to your Windesheim BBT VM
   - Analyse the packages: show the response
9. Kali: Surf to your personal bank
   - Analyse the packages: which encryption algorithm is used?

Done