FIT9137 Workshop Session
Week 11

Topics

- Virtual Private Networks (VPNs)
- Digital Inclusion

Covered Learning Outcomes:

- identify and describe fundamental concepts of network security mechanisms against common threats and countermeasures.

Instructions

- One of the main purposes of an applied session is to build the learning community, create connections and include the learners. The other goal is to give and receive feedback from your peers and or your tutors.
- Form groups of 2 students (online) or more face-to-face to work through the exercises. If you meet a problem, try to solve it by asking direct questions to your peers. If the issue was not solved within peers, ask your tutor. If you did not get a chance to solve the problem during your applied session with your peer or tutor, jump into one of many consultation hours and ask any of the tutors to help you. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

• ACTIVITY A: VPN

Find the core file `FIT9137_Week-11_Activity_VPN.imn` inside **workshop_files** folder. Open the file in core. The configuration contains a network design with a private network on the right, some public (Internet) routers in the middle, and a client in the top left that wants to connect to the private network. Start the emulation and perform the following tasks:

STEP 1.

See if you can reach the devices inside the private network. You can for instance ping the clients or run `lynx` with the address of the server.

yes, we can reach the web server

```
lynx 10.0.6.10
```

STEP 2.

Run a `traceroute` between `vpnclient` and `web`. What do you see?

```
traceroute 10.0.6.10
traceroute to 10.0.6.10 (10.0.6.10), 64 hops max
  1   10.0.200.1 0.445ms 0.321ms 0.388ms
  2   10.0.6.10  0.402ms  0.321ms  0.323ms
```

checking local network interfaces we find the `tun0` interface:

```
2: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast state\
    UNKNOWN group default qlen 100
    link/none
    inet 10.0.200.4 peer 10.0.200.1/32 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::10b5:f2b:3bef:247b/64 scope link flags 800
       valid_lft forever preferred_lft forever
```

checking the routing table, we find all traffic is redirected through `tun0` interface:

```
0.0.0.0/1 via 10.0.200.1 dev tun0
default via 10.0.0.1 dev eth0
10.0.0.0/24 dev eth0 proto kernel scope link src 10.0.0.20
10.0.1.10 via 10.0.0.1 dev eth0
10.0.6.0/24 via 10.0.200.1 dev tun0
10.0.200.1 dev tun0 proto kernel scope link src 10.0.200.4 128.0.0.0/1
via 10.0.200.1 dev tun0
```

STEP 3.

Run Wireshark on one of the routers. Then run `lynx` again from `vpnclient` accessing `web` or ping `web`. Can you see the HTTP protocol messages or the ICMP echo request and replies?

No, we only see OpenVPN packets as all traffic is redirected through VPN.

STEP 4.

Run Wireshark on the interface `eth1` (with IP `10.0.6.1`) of the `vpnserver`. Run `lynx` as before. What can you see in the captured traffic?

We see the communication between `vpnclient` and `web`. This is because the VPN connection terminates on the external interface of `vpnserver` so the packets are decrypted.

STEP 5.

Check the file `client.conf` on `vpnclient` and `server.conf` on `vpnserver` and use `openvpn` manual (`man openvpn`) to learn more about the settings. For instance, what encryption algorithm is used, what key exchange algorithm is used, what are the client and server key pairs etc. the location of the keys depend on the session as shown below.

client.conf

```
client
dev tun
proto udp
remote 10.0.1.10 1194
nobind
ca /tmp/pycore.50682/certs/ca-cert.pem
cert /tmp/pycore.50682/vpnclient.conf/vpnclient.pem
key /tmp/pycore.50682/vpnclient.conf/vpnclient.key
dh /tmp/pycore.50682/certs/dh2048.pem
cipher AES-256-CBC
log /var/log/openvpn-client.log
verb 4
daemon
```

server.conf

```
local 10.0.1.10
server 10.0.200.0 255.255.255.0
push redirect-gateway def1
push route 10.0.6.0 255.255.255.0
keepalive 10 120
ca /tmp/pycore.50682/certs/ca-cert.pem
cert /tmp/pycore.50682/vpnserver.conf/vpnserver.pem
key /tmp/pycore.50682/vpnserver.conf/vpnserver.key
dh /tmp/pycore.50682/certs/dh2048.pem
cipher AES-256-CBC
status /var/log/openvpn-status.log
log /var/log/openvpn-server.log
ifconfig-pool-linear
ifconfig-pool-persist /tmp/pycore.50682/vpnserver.conf/ippool.txt
port 1194
proto udp
dev tun
verb 4
daemon
```

- # ACTIVITY B: Digital Inclusion

Digital inclusion is about ensuring all Australians are able to access information and communications technology to benefit from the resulting socio-economic opportunities. In 2018, the Regional Telecommunications Independent Review Committee presented the *2018 Regional Telecommunications Review - Getting it right out there (the Review)*. For Indigenous Australians, the report highlighted the need for those living in remote communities to have better access to phone and Internet services.

In this exercise we will investigate the following problem: How to provide proper Internet access to remote Indigenous communities?

Steps to follow:

1. Form groups of 5-8 students.
2. Pick a "cool" group name and a representative.
3. Read the two main articles (and more as you like).
4. Discuss potential issues (financial, technical, cultural, etc) around the problem.
5. Come up with solutions to the problem.
6. Bring something from your own cultural, educational, professional background
7. Report the following in PollEv and to your class:
    a. Your group name
    b. List of issues identified (with brief explanations)
    c. Proposed solutions
    d. Input from your own background

Resources:

1. https://theconversation.com/for-remote-aboriginal-families-limited-phone-and-internet-services-make-life-hard-heres-what-they-told-us-201295
2. https://www.creativespirits.info/aboriginalculture/economy/internet-access-in-aboriginal-communities

Resources:

1. https://www.niaa.gov.au/sites/default/files/documents/publications/indigenous-digital-inclusion-plan-discussion-paper.pdf
2. https://researchbank.swinburne.edu.au/file/a67b7e2c-0717-4974-8c98-06730bd91426/1/PDF%20(Accepted%20manuscript).pdf

Sample Answers:

1. Group name
2. List of potential issues

- Issue 1: brief explanation
- Issue 2: brief explanation

3. List of proposed solutions issues
    - Soln 1: brief explanation
    - Soln 2: brief explanation
4. Individual 1's personal input
5. Individual 2's personal input