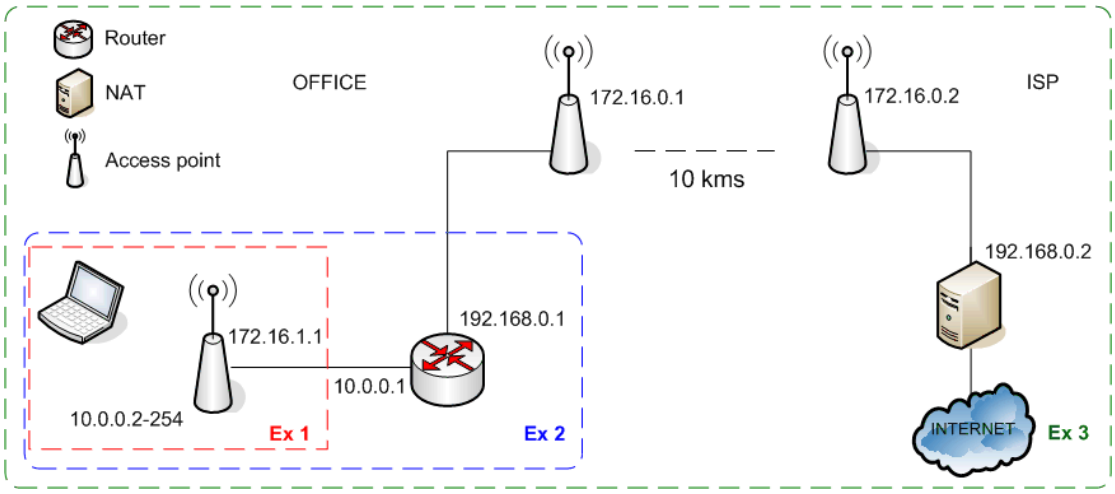
ITRAINONLINE MMTK

Exercise guidelines: Wireless Security

Developed by: Alberto Escudero Pascual IT+46



Let us consider the following scenario. A laptop is wireless connected to an office network (Ex1) by means of an access point. The laptop receives IP addresses from a DHCP server and router (Ex2.)

The whole office is connected to the internet by a dedicated a PtP wireless link to an ISP. The wireless PtP link is composed by two access points that are acting as bridges.

The ISP border router is a NAT server (Ex3)

Exercise 1: Data Confidentiality and Integrity

Consider the diagram (Ex1), where a laptop is connected via wireless to the office network.

Question 1: How can you guarantee data confidentiality and integrity?

- *Which functionality can you implement and how?*

Possible topics for discussion:

Implement WPA2-Enterprise to ensure overall link level encryption IEEE 802.1X

Implement WPA2-Personal and agree in a shared secret in the office. Discuss if it is appropriate.

Train your staff to understand which services are sensitive and use application security and NO link level encryption at all.

Implement a VPN solution and force all clients to communicate via the VPN-Concentrator

- *Discuss all possible alternatives to ensure data confidentiality in the "first-hop" (between the laptop and the access point)*

Possible topics for discussion:

Pros and cons of using WPA2 with and without IEEE 802.1X, Disable encryption, introduce VPN solution (interoperability, costs), network management etc.

Now, consider the diagram (Ex3)

Question 3: How can the ISP guarantee data donfidentiality and Integrity in the PtP link?

- *Discuss the advantages and disadvantages of each solution.*

Possible topics for discussion:

The ISP should implement authentication in their PtP link to avoid link hijacking.

The ISP could decide NOT to implement link encryption due to:

a) regulations (is it legal?), b) the physical difficulty of an unauthorised user to listen the traffic (very directive antennas in the PtP and high towers), (c) reduce the network management overhead.

Exercise 2: Authentication – access control

Consider diagram (Ex2): the router is providing IP addresses to the wireless clients by means of DHCP.

Question 1: How can you prevent that unauthorised users from obtaining an IP address from your network?

Possible topics for discussion:

Implement AP Authentication by means of WPA or WPA2

Use static IP addresses and "monitor DHCP requests" (making things a bit harder to the attacker)

Not broadcasting the SSID and limiting the wireless coverage (making things a bit harder to the attacker)

Question 2: How can you prevent that unauthorised users can not reach the internet from your network?

Possible topics for discussion:

Blocking IP traffic in the office router

Allowing only certain MAC/IP addresses in the router

Implementing a "Captive Portal" type solution in the Office Router

Consider diagram (Ex3): the ISP is proving connectivity to the office by means of a NAT server.

Question 3: How can the ISP ensure that only your office is connected to their network?

Possible topics for discussion:

Allowing only incoming IP traffic from the MAC address of the office router

Implementing a Captive Portal in the NAT server and allowing per-user authentication

Ensuring that the PtP is fully authenticated

Exercise 3: Availability and prevention of DoS

Consider the office diagram (Ex1, Ex2) and the ISP (Ex3)

Question 1 : Describe what can go wrong in every communication "hop" in the whole picture. What can make the network unavailable?

Possible topics for discussion:

Radio Jamming in both wireless links

Unauthorised users associate with any AP and send bogus traffic

Malicious software floods the wireless links

Unauthorised users impersonate the routers (IP/MAC hijacking)

Unauthorised users impersonate an AP (radio channel hijacking)

Question 2 : Describe how to solve each of the security problems and who should be responsible of implementing them?

Possible topics for discussion:

Radio Jamming in both wireless links: monitor periodically your wireless links, report the attack to the Telecommunication Authority

Unauthorised users associate with any AP and send bogus traffic: implement WPA2, include traffic shaping policies in the routers/AP, limit your wireless coverage

Malicious software floods the wireless links: monitor the IP traffic, include intrusion detection systems, include traffic shaping, disconnected infected stations.

Unauthorised users impersonate the routers (IP/MAC hijacking): implement authentication in your PtP links, monitor the SNR to detect big changes

Unauthorised users impersonate an AP (radio channel hijacking): implement authentication in your PtP links, monitor the SNR to detect big changes

Question 3 :Think in one concrete scenario (hospital, school, telecenter etc) and describe the security requirements. Suggest security measures.