Linnaeus University
Computer Science
Ola Flygt

2021-11-15

2DV703 Mobile and Wireless Data Security
Assignment #2

A. Theoretical part

Each group is to prepare a 20 minutes presentation for the class to be given on the seminar **22 November and possibly 25 November**. Make best possible use of the time! Use the material assigned you, but feel tree to find other material in the area and select the most important part to present. Make sure to both give an overview of the area and possible solutions and make an in-depth technical presentation of a few of the most important protocols. There is a potential overlap between some of the groups. Try to avoid presenting something belonging to another group and if in doubt discuss this between the groups. Also do not repeat things covered in previous courses except to give an introduction and context on how things are related. The areas each group should cover is:

Group 1 Chapter 3 - Anywhere, Anytime, on Anything: “There’s an App for That!”

Group 2 Chapter 4 - Security Threats Overview: Wired, Wireless, and Mobile

Group 3 Back end authentication (Radius, Access Server, LDAP, certificates)

Group 4 Chapter 7 - Basic WLAN Security Measures

Group 5 Chapter 8 - Advanced WLAN Security Measures

Each group should also look at what is currently going on in respective area. Are there any new standards, protocols or products in the pipeline? Also look at the equipment we have in the lab. What do they support?

Linnaeus University
Computer Science
Ola Flygt

2021-11-15

B. Practical work

You should by now have a basic infrastructure. We start to look into different ways to segment and secure the network. This week we will focus on VLANs and making these segments safe both from outside and each other. We are also going to do a basic setup of our wireless access points.

1. Use the switch to separate the VLANs: “Trusted”, “Admin”, “IoT” and “DMZ” and make a **trunk port** to the firewall. Trusted will be the VLAN for regular users within the organization. The DMZ is for the public services the company provides and for wireless guests that visit the company. Think about how the other VLANs might work and be used! Confirm that the VLANs are properly segmented by testing traffic between them and to/from “Internet”.

2. Configure VLAN interfaces on the firewall to handle the incoming VLANs. Setup DHCP pools for the newly created VLANs.

3. Setup new NAT and filtering rules, and configure the security levels for the VLAN interfaces. Both “DMZ” and “Trusted” should be able to reach the Internet. In addition, the external server on “DMZ” should be reachable from outside. How do you want to the other two VLANs to work?

4. Connect the provided access points. You should place one on “Trusted” and one on “DMZ” VLAN. Configure them with different level of security; Open for “DMZ” and WPA2 (with PSK) for “Trusted”. Test to see if the wireless connection is working by accessing your network as well as the Internet with different wireless clients.

Make sure you have properly documented your work so far. Each group should have proper documentation (in the Wiki in MyMoodle) of both the physical and abstract layered design. This includes, but is not limited to: VLANs, IP addresses, interfaces, subnets, physical ports, DHCP ranges etc. of equipment.

You are also strongly recommended to document how you solved the assignment e.g. “for NAT rules I used the following commands [...] that did [...]”.

The practical part of the assignment must be completed at least Friday 26th November.