Linnaeus University
Computer Science
Ola Flygt

2021-11-22

2DV703 Mobile and Wireless Data Security
Assignment #3

A. Theoretical part

Each group is given a new area of responsibility that you will study, prepare and present for the class on **Monday 29 November and Thursday 2 December** (30 minutes/group). Group 1 -3 can use whatever material you can find, but try to use different types of sources (books, scientific articles and the web). Group 4 and 5 can mainly use the textbook, but feel free to add other related material.

Group 1 How is positioning working using different methods? You should cover GPS and GPS and GSM/3G/4G/5G. Are there any advantages or disadvantages with each positioning service from functional and security points of view? What are the typical application areas for this type of positioning?

Group 2 How is positioning working using different methods? WiFi and RFID/NFC positioning but with a focus on WiFi positioning (including the upcoming standard 802.11az). Are there any advantages or disadvantages with each positioning service from functional and security points of view? What are the typical application areas for this type of positioning?

Group 3 VPN protocols and products. Look for support for different protocols in devices and network equipment we already have. Things you could cover: PPTP, L2TP over IPSec, Cisco IPSec (IKEv1, IPsec/XAuth), IKEv2, SSTP, Shadowsocks, Cisco AnyConnect, Windows DirectAccess, OpenVPN and Wireguard.

Group 4 Chapter 6 WLAN and IP Networking Threat and Vulnerability Analysis.

Group 4 Chapter 9 WLAN Auditing Tools.

Linnaeus University
Computer Science
Ola Flygt

2021-11-22

B. Practical part

This practical assignment focuses on configuring an WPA2 or WPA3 Enterprise solution. Each group is going to set up a Radius server on their internal server. Furthermore, there are tasks regarding wireless penetration testing.

1. WPA2/3 Enterprise wireless solution - make your Windows Server act as Radius Server (alternatively you could set up some other Radius server). It should then be able to work with the AP and authenticate users based on their credentials in the local database. These authenticated users should then be granted access to the internal network and the Internet. Set up the AP on the "Trusted" VLAN to WPA2/3 Enterprise mode and establish the connection with the RADIUS server.

2. Create Kali Live USB-sticks or use the ones that are in the lab.

3. Wireless penetration testing - Each group should perform attacks within the lab premise and on the lab equipment. You are encouraged to cooperate among the groups (attacking another groups AP) but this is not mandatory - you may also perform these within the group itself, and even at home as long as the whole group is present and the setup is documented in some detail. The APs should be configured to use WPA and WPA2 with PSK. Try to crack the security to gain access to the network of the AP's. You might also need to generate some background traffic and/or normal logins from legitimate users for some of these tasks.

   Also perform the following attacks:
   - Deauthenticate clients to gain a handshake from a running session
   - Gain a simple password either by brute force on a short password or using a dictionary attack on a word-based password
   - Find an AP with hidden SSID (with some client connected to it that generates traffic)
   - Bypass a MAC filter.
   - Perform a **directed** wireless DoS (Denial of Service) attack. This could be done in a few different ways but **make sure not to disturb other wireless networks or exceed legal transmission powers*.** Can you make the network completely unusable? How close do you need to be? Can you make it unusable for just one client?

4. Voluntary work

   a. Use WireShark to capture and decrypt WPA/WPA2 (PSK) traffic.
   b. When is it possible to crack/listen to WPA Enterprise?
   c. Test the KRACK vulnerability in WPA2 (mainly for android clients).
   d. Test performing ARP and/or DNS poisoning attacks using the tool Bettercap https://github.com/bettercap/bettercap

Linnaeus University
Computer Science
Ola Flygt

2021-11-22

Written report about the practical work

Discuss and document your reflections on the practical part in a group report that is submitted in MyMoodle (PDF format). Summarize the results you got for the different tasks. You don't need to quote every command used, but an overview of what guide you used and what modifications you made to it. Also be prepared to present your results to the class on the **9 December**.

The report and the presentation slides should be submitted to MyMoodle. Deadline is **12 December**.

Remember to continue to document all your work in in the lab in your group Wiki whenever you make any changes in the lab!

To get the legal Transmission levels in Sweden (See the lecture notes on antennas)
#Start with running this command:
sudo iw reg get
#That should give you your current country codes registered. Remember that value/notation.
#Then change to:
sudo iw reg set SE
#should put your kali box to a Swedish country code and TX power restrictions and you can then later reset your country code register:
sudo iw reg set BU for instance