A! Aalto University

School of Electrical Engineering
Department of Communications and Networking
ELEC-E7330 Laboratory Course in Internet Technologies

Instructions for

36 – Network Security

Student Edition

22.9.2017 Juho Kaivosoja
12.7.2021 Carolina Mejía López

1 Preliminary Questions

P1   Is it legal in Finland to scan ports of a network or host you do not own? Why / Why not? How about guessing a person's password on a system? Does it change the situation if the person is your friend?

P2   What sorts of security defects are most common in web services(sites)? How could these be avoided? Can you name any web service that has not had a security defect in its history?

P3   What are the characteristics of a good password? How easy is it to remember a good password? Is "correct horse battery staple" a good password? What problems are there when using passwords as security options on computer systems? Are the so-called "security questions" a satisfactory solution to forgotten passwords? Why / Why not? What is brute forcing?

P4   List and analyze the cryptographic weaknesses of the German Enigma machine. What can we learn from them?

P5   Why is WEP the most vulnerable type of security for wireless networks? Describe how it can be cracked.

P6   What is Kali Linux? What is it used for?

2 Laboratory Preparation

Download & Install Virtualbox to your laptop here: https://www.virtualbox.org/wiki/Downloads.
Then download and Install a Kali Linux on your Virtualbox here:
https://www.kali.org/docs/introduction/download-official-kali-linux-images/.
Configure it to use your WiFi connection for hacking tools. You can configure a SSH connection
for management (from your laptop). Prepare the following files for the laboratory a list with com-
mon usernames and passwords, and a html file to upload into a webserver.

3 Laboratory Exercise

You have applied for a position at a company as Security Officer. The day of the interview you
are left alone in a meeting room. There is a sign on the wall, it reads "*Wi-Fi para visitantes...*" the
text is in a language you barely know, the only word you recognize is "WEP." You have Kali
Linux installed in your computer in VirtualBox. You see a USB Wi-Fi adapter and realize *this is*
the interview.

4 Final Report

Write a report commenting your observations, as if you were giving the company feedback on
their network. What kind of host, networks and services can you see? What did you manage to
do with this information? List all your steps and draw a map of the network, you can use screen-
shots to illustrate some of the results. Give suggestions on how to improve the vulnerabilities
you found.