LAB

Laboratory – Introduction

- Introduction to the exercises, explanation of the structure of the exercises.
- Explanation of the lab network (red network, white network)
- Connection of the lab computers to the red network
- Eavesdropping with wireshark
  - Introduction to the program
  - Eavesdropping of the network communication (local computer at this moment)
  - Search query with a search engine not using SSL/TLS
  - Login (username/password) of a service not using SSL/TLS
  - SSL protected connections
  - File transfer over http without SSL/TLS – data recovery

Laboratory – Introduction

- IDS - snort
  - snort -W
  - packet dump mode: snort -i -1
  - packet headers – default: snort -v
  - dump application layer data : snort -d (or -dv)
  - dump second layer header info: snort -e (or -dev)
  - data log (binary): md xxx; snort -dev -l xxx
  - data log (ascii): -K ascii
  - IDS – simple 2 rules to catch the http communication
    - snort -c ..\etc\s_test.conf -l ..\log -r E.pcap
  - standard rules
    - snort -c ..\etc\snort.conf -l ..\log -r attack-trace.pcap

Homework

- Analyze a sample PCAP file with snort. Prepare a written report. [3 points maximum]
  - Use standard snort rules (or find additional rules)
  - Use nessus_against_20.pcap file for analyses
  - Select one reported alert
    - Analyze the alert
      - Which packet was flagged?
      - Why the packet was flagged?
      - Is this a serious issue? What exactly does this alert mean?
  - Expected 1-2 A4 pages of text.