Exercise 2
Scanning + Enumeration

Assignment 1 (Discussion):

Pair up, and discuss the following topics from today's lesson:

- Scanning
  - Intro
  - Live systems
  - Scanning types
  - OS fingerprinting
  - Vulnerabilities
  - Network mapping
  - Proxies
- Enumeration
  - Intro
  - Windows basics
  - Linux basics
  - SNMP
  - Unix/Linux enumeration
  - LDAP
  - NTP
  - SMTP

Assignment 2 (Group work):

Go through the review questions of Chapter 5 + 6. For each question, discuss and see if you can agree on the answer, before checking with the answers section.

Assignment 3 (Scanning):

Exercise in chapter 5: 5.1.

Further, test other tools mentioned in Chapter 5:

- Ping
- Nmap
- Hping3
- P0f
- Netcraft
- Maltego
- LANState

Peter Justesen

Exercise2.docx

Assignment 4 (Enumeration):

Exercises in chapter 6: 6.1, 6.2, 6.3.

Further, test other tools mentioned in Chapter 6:

- Nbtstat
- PsTools
- Unix commands (slide 32)
- NTP commands (slide 34)
- SMTP commands (slide 35)