Exercise 3
System Hacking + Malvare + Sniffers

Assignment 1 (Discussion):

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

- System Hacking
- Malvare
  - Overt and covert channels
- Sniffers
  - Understanding sniffers
  - Using a sniffer
  - Switched network sniffing

Assignment 2 (Group work):

Go through the review questions of Chapter 7 + 8 + 9. For each question, discuss and see if you can agree on the answer, before checking with the answers section.

Assignment 3 (System Hacking):

Exercise in chapter 7: 7.1, 7.2, 7.3, 7.4, 7.5 (optional), 7.6, 7.7.

Further, test other tools mentioned in Chapter 7.

Note: Some tools are perceived as viruses by e.g. Symantec.

Assignment 4 (Malvare):

Exercises in chapter 8: 8.1, 8.2.

Further, test other tools mentioned in Chapter 8.

Note: Be careful when experimenting with malware! Only execute in sandbox environments!

Assignment 5 (Sniffers):

Exercises in chapter 9: 9.1, 9.2, 9.3.

Note: You may user other tools/programs than telnet to create traffic, e.g. firefox.

Further, test other tools mentioned in Chapter 9.

Peter Justesen

Exercise3.docx

Assignment 6 (Metasploit framework):

Check out the metasploit framework docs and videos (msframework): https://www.metasploit.com/

Also check out the video: https://www.youtube.com/watch?v=sHS4kHKcQhc

User guide, including meterpreter: http://cs.uccs.edu/~cs591/metasploit/users_guide3_1.pdf

Meterpreter independent guide: https://dev.metasploit.com/documents/meterpreter.pdf

Assignment 7 (Nessus scanner):

Check out the Nessus vulnerability scanner: https://www.tenable.com/products/nessus/nessus-professional

Assignment 8 (Hackthissite):

Check out hackthissite for further excersises: https://www.hackthissite.org/