Introduction to IT security
Exercise set 1

DIKU, block 4, 2015

In this exercise we take a closer look at two phases of typical cyber attacks, the reconnaissance and exploitation phases.

Reconnaissance

In the reconnaissance phase a common task is to profile the target organisation using publicly or readily available information.

Imagine you are tasked to profile KU.

Question 1. Download a copy of the ku.dk index page and find all subdomains of ku.dk listed on the page, and their IP addresses. Automate as much as you can of the process using a combination of shell commands or a scripting language of your choice.

Question 2. What are the name servers of KU? What are the mail servers? When was ku.dk first registered as a domain and when does it expire?

Question 3. How could you go about profiling KU without interacting with any systems under KU control?

Exploitation

Question 1. What is the difference between client-side and server-side exploitation?

A client-side application that is commonly targeted for exploitation is Java. In the past recent years many serious software vulnerabilities have been reported in Java. As Java is often installed and enabled in browsers, delivery of code to exploit the vulnerabilities is often done in the form of Java Applets delivered to the user while browsing infected websites. When run, the applet exploits the vulnerability and caries out it mal-doing.

You are given such a malicous Java Applet in the form of a JAR file, JAR1. (Get it from Absalon.)

Question 2. Extract and inspect the embedded Java class files from the JAR file with a tool such as JD GUI and try to determine as well as you can what the JAR file does, what you could do to prevent it from successfully executing and how to find signs of successful exploitation, i.e. infected machines. Assume any evaluation of `System.getSecurityManager()==null` returns `true`.