

**Computer Security**

**Tutorial 3**

**Part 1: Test you AV Software**

One key element of any good anti-virus software is to prevent it from being able to execute on a specific host. The following exercise will test your AV software using a fake virus file. Please read through each of the steps **before** undertaking the activity. Once you have read through each of the steps, start from point 1 and continue the steps.

1. Go to http://www.eicar.org/anti\_virus\_test\_file.htm and have a read of the "Anti-virus or Anti-malware test file" information carefully. This file you will be testing is not an actual virus but rather designed to appear as a virus to your AV software.
2. Click on *eicar.com*  which contains a fake virus. A dialog box opens that asks if you want to download the file. Wait to see what happens.

What does your antivirus software do? Close your antivirus message and click *Cancel* to stop the download procedure.

1. Now click *eicar\_com.zip*. This file contains a fake virus inside a compress zip file. What happened when you attempted to click the file?
2. If your antivirus software did not prevent you from accessing the eicar\_com.zip file when the file download dialog box appears click *Save* and download the file to your desktop.
3. When the download is complete, click *Close* if necessary.
4. How is your antivirus program detecting this file as malicious?
5. Thinking back to a few weeks ago, how is it that a fake virus can be detected by your antivirus scanner, yet not be malicious? (Hint, you may need to do some research on this).

**Part 2: Questions:**

The following questions are designed to test your knowledge of what you have learnt so far and to allow you to apply your analytical skills to a given problem. Whilst solutions to each of the questions are provided, it is recommended that you attempt to solve the problem yourself first, as similar style of questions may be present in the final exam.

1. John is a ~~malicious~~ software developer, and designed an online banking system. John included a feature that would email him the bank account information for any account where the total balance exceeds $1,000.

What kind of malware attack is this and why?

1. Suppose that you are a malware developer; hence, you know that you need to store a

copy of the code for your virus inside the virus itself. Moreover, suppose you know that a security administrator is also aware of this fact and will be using it to detect the presence of your malware in operating systems files.

Explain how you (the malware developer) can hide the embedded copy of your malware so that it is difficult for the security administrator to find.

1. Based on a true story. Suppose, a network malware specimen is designed so that as soon as it is copied onto a computer, X, it copies itself to six of X's neighbouring computers. Each time it copies itself it uses a random file name, so as to evade detection.

The malware itself does no other harm, in that it doesn't read, delete or modify any files. What harm would be done by such malware and how would it be detected?

1. In a salami-slicing attack, a program performs a large number of small, hardly noticeable malicious actions, which add up to a large aggregate malicious action. As an example, a programmer for a bank has 1 cent of the monthly interest calculation on each bank customer's account transferred into his account.

Thus, if the bank has 1,000,000 customers, then the developer would get $10,000 each month from the salami slicing attack. What type of malware is such a program based on?

1. Viruses that perform no explicit malicious behaviours are called bacteria or rabbits. Explain how such seemingly benign viruses can still have negative impacts on a computer systems.
2. Bart told his teacher that the reason he is unable to submit his Microsoft Word assignment is that malware ate his homework. What type of malware would be the most likely culprit?
3. Explain why it is often beneficial for an adware author to include spyware in his adware.
4. Laura installed spyware software on 100 USB flash drives and designed this software to load automatically from these drives along with some nude photos. She then painted the logo of a well-known adult magazine on each one and randomly scattered these flash drives in the parking lots of several of the big defence companies in her town.

What type of malware attack is this and what vulnerability is she trying to exploit in order to get her malware code past the network firewalls of these companies?

1. What would be the financial advantage for a malware designer to create lots of different malicious code instances that all exploit the same vulnerability yet have different malware signatures?
2. Describe the process of a malware attack that would cause a victim to receive physical advertisements.