1. An example of a host-based intrusion detection tool is the tripwire program. This is a file integrity checking tool that scans files and directories on the system on a regular basis and notifies the administrator of any changes. It uses a protected database of cryptographic checksums for each file checked and compares this value with that recomputed on each file as it is scanned. It must be configured with a list of files and directories to check and what changes, if any, are permissible to each. It can allow, for example, log files to have new entries appended, but not for existing entries to be changed. What are the advantages and disadvantages of using such a tool? Consider the problem of determining which files should only change rarely, which files may change more often and how, and which change frequently and hence cannot be checked. Consider the amount of work in both the configuration of the program and on the system administrator monitoring the responses generated.

2. The question arises as to whether it is possible to develop a program that can analyze a piece of software to determine if it is a virus. Consider that we have a program D that is supposed to be able to do that. That is, for any program P, if we run D (P), the result returned is TRUE (P is a virus) or FALSE (P is not a virus). Now consider the following program:

   ```
   Program CV :=
   {. . .
   main-program :=
   {if D(CV) then goto next:
   else infect-executable;
   }
   next:
   }
   ```

   In the preceding program, infect-executable is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus.

3. Consider the following fragment:

   ```
   legitimate code
   if data is Friday the 13th;
   crash_computer();
   legitimate code
   ```

What type of malware is this?

4. Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms we discuss could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

5. Suppose you have a new smartphone and are excited about the range of apps available for it. You read about a really interesting new game that is available for your phone. You do a quick Web search for it, and see that a version is available from one of the free marketplaces. When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to "Send SMS messages" and to "Access your address-book". Should you be suspicious that a game wants these types of permissions? What threat might the app pose to your smartphone, should you grant these permissions and proceed to install it? What types of malware might it be?

6. List the types of attacks on a personal computer that each of a (host-based) personal firewall, and anti-virus software, can help you protect against. Which of these countermeasures would help block the spread of macro viruses spread using email attachments? Which would block the use of backdoors on the system?

7. Research and list any three malwares that occurred in 2017. If possible, classify them as virus, worm or Trojan. Provide technical details of how the attack occurred, what vulnerability was exploited, what was the impact of the attack. Briefly provide countermeasures that could have possibly prevented these attacks. Provide proper references and citations.