1. **Review 6.1** What are the three broad mechanisms that malware can use to propagate?

   Propagation mechanisms include **infection of existing executable or interpreted content** by viruses that is subsequently spread to other systems; **exploit of softwares vulnerability** either locally or over a network by worms or drive-by-downloads to allow the malware to replicate; **social engineering attacks** that convince users to bypass security mechanism to install Trojans or to respond to phishing attacks.
   (Page 186)

2. **Review 6.11** What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit?

   The definition of each is the following:
   Backdoor - Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
   Boot - A bot is a program installed on an infected machine that is activated to launch attacks on other machines.
   Keylogger - A keylogger captures keystrokes on a compromised system.
   Spyware - A spyware is a software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.
   Rootkit - A rootkit is a set of hacker tools used after attacker has broken into a computer system and gained root-level access.

   Now, the difference is basically the different ways of attacking, a **backdoor** can be created by the attacker or is sometimes already in the system because it was used before by an specific user to debug, but these doors are used to get access to places/code where they are not authorized. The **bot** does not get access like a backdoor to the program, instead, is its own program that is install into a computer without the user knowing this program is being installed, so there's no authorization process since most of the times the user doesn't even know it's being installed. This can control your entire computer. Now a **keylogger** is different from the two previous on because this one is used to collect data, is like a surveillance software that is creating a file with all the inputs by keyboard given to the computer. The **spyware** in difference with the other ones, comes in free downloads or some downloads you do from the browser. Having spyware will make your computer crash or will generate system instability. Lastly **rootkit** are difficult to detect because they are activated before your system's Operating System has completely booted up and they are able to intercept data from terminals, network connections, and the keyboard.

3. **Problem 6.3** The following code fragments show a sequence of virus instructions and a metamorphic version of the virus. Describe the effect produces by the metamorphic code.

Original Code	Methamorphic Code
mov eax, 5	
add eax, ebx	
call [eax]	mov eax, 5
	push ecx
	pop ecx
	add eax, ebx
	swap eax, ebx
	swap ebx, eax
	call[eax]
	nop

In the metamorphic code we can see the key instructions that we know are used to affect the code, **push and pop** one after another one and the same variable, and also **swap**, same one after another one and the same variables, in addition to **nop**. Dan told us this changes the behavior of the code. The push and pop and swaps and nop, change the behavior of the code. So with these operation the signature gets corrupted because the code is being changed, however the semantics of the original code are not being modify.

4. **Problem 6.5** Consider the following fragment:

```
legitimate code
\textbf{if} data is Friday the 13th;
       crash_computer();
legitimate code
```

What type of malware is this?

They are using **Logic Bomb** . I know is logic bomb because we can see the instruction **crash_computer()** AFTER the condition of checking the date to see if its Friday the 13th. So this means that he function to crash the computer will be called when the date condition is met.

5. **Problem 6.6**. Consider the following fragment in an authentication program:

```
username = read_username();
password = read_password();
if username is "133t h4ck0r"
     return ALLOW_LOGIN;
if username and password are valid
     return ALLOW_LOGIN
else return DENY_LOGIN
```

   What type of malicious software is this?

   This is a **Backdoor** because after checking a username is giving access with the "return ALLOW_LOGING" So the authentication logarithm its allowing secret admission to the username, and letting the right user and password have the security access.

6. **Problem 6.10**. Suppose you have a new smarthphone 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 did 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 access permissions granted to it. You see that it wants permission to "Send SMS messages" and to "Access you adress-book". Should you be suspicious that a game wants these types of permissions? What threat might the app pose to your smarthphone, should you grant these permissions and proceed to install it? What types of malware might it be?

   I think you SHOULD be really suspicious about this game wanting access to send messages and access your address book. The threat this game posses is that IF you grant the access to send messaged and read your contact list, then the attacker can collect all that data and send that info to himself since he can send messages from your phone to any phone. Also, since it has your contacts book, it can send messages to any contact you have in your phone. Therefore, you SHOULD NOT grant these permissions and DO NOT install it. The malware that will be installed into your phon IF you grant these permission will be **Trojan Horse**. If you have an iPhone they can put a jail-break malware and if you have an Android it would be a DriodDream malware.

7. **Problem 6.11** Assume you receive an e-mail, which appears to come from a senior manager in your company, with a subject indicating that it concerns a project that you are currently working on. When you view the e-mail, you see that it asks you to review the attached revised press release, supplied as a PDF document, to check that all details are correct before management releases it. When you attempt to open the PDF, the viewer pops up a dialog labeled "Launch File" indicating that "the file and its viewer application are set to be launched by this PDF file". In the section of this dialog labeled "File" there are a number of black lines, and finally the text "Click the 'Open' button to view this document". You also note that there is a vertical scroll-bar visible for this region. What type of threat might this pose to your computer system should you indeed select the "Open" button? How could you check your suspicious without threatening your system? What type of attack is this type of message associated with? How many people are likely to have received this particular e-mail?

   The threat this pose to your computer is that this PDF file can contain malicious script code that will cause an installment of a malware, so the user should click on "open" to review the code.
   To check the suspicious without threatening your system you would need to scroll through ALL the code that is in there and check that there is nothing weird about it or some weird statements that will run if some conditions are met or will get installed or would get some info or something that a PDF shouldn't do. You can also check the code's behavior while you click on the "Open" button to see if there's anything weird.
   The type of attack associated with this is **spear phishing attack** because this type of attack asks the user to click on a button or link or something that will cause the installation of the malware, the malware can be a worm or a trojan horse. If the malware is installed then it can start to steal data.
   Since the email seems to come from the senior manager in the company, then I would think that the email could have been sent to all the people who works with that manager, or in that company since it won't be weird that a Senior Manager is sending the email.