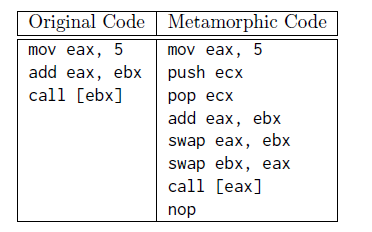
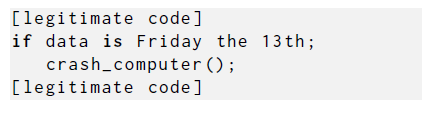
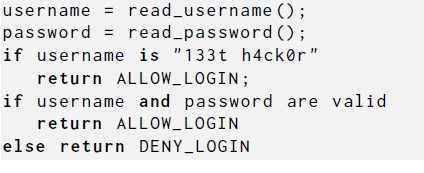
1. What mechanisms can a virus use to conceal itself?
   1. The mechanisms are encryption, stealth, polymorphism and metamorphism
2. What is a *logic bomb****?***
   1. Code embedded in the malware to make it explode, hence the name bomb, when something specific happens. Once it does, then it does whatever the malware is set to do, aka the payload.
3. How does a Trojan enable malware to propagate? How common are Trojans on computer systems? Or on mobile platforms?
   1. The only way a trojan can propagate is when the user allows it to run, which executes the hidden code, harms whatever it has to harm and goes on to the next person in the network. Trojans are common on computers and mobile devices but more Andriod OS phones over iOS phones.
4. What is the difference between machine executable and macro viruses?
   1. Executables infect files specific to the OS or hardware in some cases. Viruses infect files with macros or scripts that is needed to support the current programs that are running.
5. The following code fragments show a sequence of virus instructions and a metamorphic version of the virus. Describe the effect produced by the metamorphic code.
   1. 
   2. The signature has been changed but the structure of the code is still the same.
6. Consider the following fragment. What type of malware is this?
   1. 

It is a logic bomb.

1. 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?
   1. The CIA triad is threatened. It could have a virus set to execute when you plug it in, or a doc with a macro virus, a worm that autoruns. A trojan horse that can threaten the work computer. What you could do is use anti-virus software to analyze and determine its contents that way. Or you could use a linux distro that doesn’t change if the USB does manage to execute whatever malware it may have.
2. Consider the following fragment in an authentication program. What type of malware is this?:
   1. 
   2. A backdoor malware
3. Suppose you receive a letter from a finance company stating that your loan payments are in arrears (in default), and that action is required to correct this. However, as far as you know, you have never applied for, or received, a loan from this company! What may have occurred that led to this loan being created? What type of malware, and on which computer systems, might have provided the necessary information to an attacker that enabled them to successfully obtain this loan?
   1. A hacker has enough info from you to open a loan for themselves, making you pay the bill. They may have used spyware that spied on your information when you used a credit or debit card using your name online to spy. Maybe even a keystroke logger that made sure it would register all the keys correctly.
4. 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 counter- measures would help block the spread of macro viruses spread using email attachments? Which would block the use of backdoors on the system?
   1. A firewall can protect you from getting malicious software from online and only allows data necessary for you. An antivirus blocks viruses from running or executing on your system. Backdoors are blocked by firewalls. An antivirus blocks macro viruses.