**Answers and grading comments for Assignment 8 – Week 10**

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**

**(1) The Melissa virus is a**

a) executable infector  
b) boot sector virus  
c) macro virus  
d) multipartite virus

**ANS: c**

**(2) A great text editor is UltraEdit. It lets you download a trial version that you can use for 30 days before having to pay for it. After 30 days, however, the trial program ceases to work. Is this an example of a logic bomb?**

a) Yes  
b) No

**ANS: b**You are warned when you download the trial version that it will expire in a certain amount of time. This is a feature of the program, not a bomb. And besides, this behavior does not violate any security policy.

**(3) The Father Christmas worm was effective because it employed what kind of engineering?**

a) computer engineering  
b) social engineering  
c) software engineering  
d) desktop engineering

**ANS: b**  
It is social engineering because it was designed to appear to be a reasonable email, just like a phone call for a password is meant to sound reasonable. And it was probably released around Christmas when it is normal to receive Christmas cards, especiallly from friends. Because the virus used addresses from the email program, chances are people knew the person who sent the virus. Software engineering is not correct because it focuses on errors and mischance, not on malicious programming.

**(4) From the textbook "Defending against malicious logic takes advantage of several different characteristics of malicious logic to detect, or to block, its execution. The mechanisms are imprecise". Given this, which of the following statements are true?**

a) A defense mechanism is secure if it allows malicious logic that does not exhibit the given characteristic to proceed  
b) A defense mechanism is precise if it allows malicious logic that does not exhibit the given characteristic to proceed  
c) A defense mechanism is broad if it allows malicious logic that does not exhibit the given characteristic to proceed  
d) A defense mechanism is secure if it prevents programs from executing that are not malicious but do exhibit the given characteristic.  
e) A defense mechanism is precise if it prevents programs from executing that are not malicious but do exhibit the given characteristic.  
f) A defense mechanism is broad if it prevents programs from executing that are not malicious but do exhibit the given characteristic.

**ANS: c, d**  
See definition 1-3 in Chapter 1 of the textbook

**(5) The textbook gave the following example of a rabbit:**

while true  
 mkdir x (create a directory named x)  
 chdir x (make the newly created directory the current directory)  
done

**Would this still be a rabbit if you removed the chdir x?**

a) Yes  
b) No  
c) It depends on whether the user has administrative privileges  
d) It depends on whether the user has permission to create nested directories.

**ANS: b**  
If you don't have the chdir, then only the first mkdir will succeed. Every other one will give an error because the directory already exists and the disk won't fill up with directories. Several students commented that it is a rabbit because it wastes CPU cycles. I gave them credit for their observation, but please be aware that rabbits exhaust (i.e., use up completely) system resources not just waste them.

**(6) Traditional access controls are powerless to defend against Trojan horse programs.**

a) True  
b) False

**ANS: a**  
A Trojan runs with the identity of the user that it tricked, so access controls let it access everything the user has permission to access.

**(7) Which of the following are possible spread conditions for a computer virus?**

a) today's date  
b) number of times infected program has been executed since it was infected  
c) the type of the virus  
d) existence of a file in a certain directory  
e) the covert action

**ANS: a, b, d**  
The spread condition is what has to be true for the virus to infect. It has to be tested for by the virus. The virus doesn't have to test for its type, that is a given. An a covert action is what the virus does, not what it tests for. See beginning of section 19.3 of the textbook

**(8) Let's say you got an email that told you that the file dvpsetup.exe in the windows system32 directory (c:\windows\system32 on my machine) was a dangerous virus and you should delete it immediately. The message claimed to come from SANS. Furthermore the message told you to forward it to everybody in your address book. So use windows explorer to see if you have dvpsetup.exe on your computer and you notice that its icon is an X which looks very suspicious. So you delete the file and tell all your friends to do so also.  Unfortunately this is part of the Winows operating system (It is the Microsoft DirectPlay Voice Test.)  
What is the best way to describe this email?**

a) It's a hoax  
b) It's a virus  
c) It's a worm  
d) It's a rabbit.  
e) none of the above

**ANS: a**  
Any unsolicited email you get about warning of some danger is almost always a hoax.

**(9) How can a Trojan horse assume a user's identity?**

a) By using a dictionary attack.  
b) Effortlessly, because the user is logged on when he/she runs the trojan horse program.  
c) Effortlessly, because you have to have administrative privileges to run a trojan horse program.

**ANS: b**

**(10) Which of these types of malicious logic are designed to avoid detection by a virus detection program?**

a) TSR viruses  
b) encrypted viruses  
c) trojan horses  
d) boot sector infectors  
e) polymorphic viruses

**ANS: b, e**  
The book is clear that encrypted viruses and polymorphic viruses were meant to trick a virus detection program.

**(11) Rabbit attacks which one of the following?**

a) Availability  
b) Confidentiality  
c) Integrity

**ANS: A**

**(12) A manipulation detection code is based on:**

a) permission bits  
b) timestamps  
c) a keyed cryptographic checksum  
d) a keyless cryptographic checksum

**ANS:  a, d**  
See section 19.6.4. The checksum algorithms mentioned are keyless. Permission bits can be included in the signature so I accepted that. The end of section 19.6.4 mentions encryption, not sure how it is used but if you said "keyed cryptographic checksum" I gave you that also. What I didn't accept was timestamps. These are used to prevent replay attacks which do not apply here.

**(13) An MDC is**

a) a prevention mechanism  
b) a detection mechanism  
c) a way of enforcing a confidentiality policy  
d) a way of enforcing an integrity policy  
e) a way of enforcing an availability policy

**ANS: b, d**  
The purpose of an MDC is to detect if a file has changed. Changing a file affects its integrity (i.e., it introduces a virus). An MDC does not prevent somebody from altering the file, it doesn't enforce a confidentiality policy because it can't detect if somebody has read the file, and it has nothing to do with availability.

**(14) I have described how the Email new password button on the login page works.   Let's say that instead of resetting the password to a random password, I reset the password to a default value such as "password". This default password would be used to reset any password. If I did this, briefly describe what would be involved for a student to get administrative privileges. (Hint, I have administrative privileges.)**

**ANS:** With this policy, if an attacker knew my login name he could type it into the logon dialog, click the email new password button, and then log in using the default password. He wouldn't have to read my email.  
It has nothing to do with the weakness of the password. This would still be a design flaw if the default password was er\*ada33ada!!a. To receive full credit you had to mention that you needed the user name of the administrator and you pushed the email new password button.

**(15)  What is malicious logic?**

**ANS:** Set of instructions that cause site security policy to be violated.

**(16) Give some suggestions about how to stop spreading viruses?  
ANS:**

1. Update your anti viruses software to the latest one.  
2. Install the important security updates for your computer.  
3. Do not click any suspicious link or email.  
4. Do not use cd or flash disk or any kind of mobile storage before antiviruse software scan it.  
5. Hold down shift key when inserting flash drive to be protected from auto run attack  
6. Never run a program from browser.  
7. If a computer in a network is infected, remove the computer from the network until the virus is removed;  
etc.

**(17) Virtual machines are useful in protecting a computer from viruses.**

a) True  
b) False

**ANS: a**  
See http://www.vmware.com/appliances/directory/browserapp.html

**DO NOT COPY, SHARE OR REPRODUCE THIS MATERIAL AS IT CAN GET YOU EXPELLED FROM M.U.M.**