**Answers and grading comments for Assignment 10 – Week 12**

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

**(1) Security logging is:**

a) the recording of events or statistics to provide information about system use and performance  
b) the analysis of log records to present information about the system in a clear and understandable manner  
c) a crucial part of a database transaction  
d) none of the above

**ANS: a**

**(2) Auditing is:**

a) the recording of events or statistics to provide information about system use and performance  
b) the analysis of log records to present information about the system in a clear and understandable manner  
c) a process of securely applying patches to the OS.  
d) none of the above

**ANS: b**

**(3) An auditing system contains which of the following components?**

a) a logger  
b) an analyzer  
c) a password checker  
d) a notifier  
e) a sandbox

**ANS: a, b ,d**

**(4) What determines what information is logged by a logger?**

a) the needs of the analyzer  
b) the needs of the notifier  
c) it's up to the implementer as long as the user id and a timestamp is included.  
d) the space available in the database.

**ANS: a**

**(5) Log sanitization is**

a) removing confidential information from a log before displaying it.  
b) making sure that the log file has proper access permissions.  
c) removing all log records that are more than x days old.  
d) validating the integrity of the log.

**ANS: a**

**(6) Intrusion detection is a form of auditing**

a) true  
b) false

**ANS: a**

**(7) Does your use of a computer at work or at home follow a statistically predictable pattern? Answer yes or no and write a couple of sentences justifying your answer.**

**ANS:** Yes. I often work at home, so the patterns between work and home are similar: I check email, run the browser, run Visual Studio, NetBeans, a text editor, SQL Server. A lot of use of Microsoft Word or PowerPoint would definitely be an anomaly. At home I also occasionally use ITunes and Windows Media Player.

In either place I rarely install new programs.

**(8) A normal user of a system**

a) rarely gets denied access to files  
b) rarely runs a program that he/she is denied access to  
c) is impossible to distinguish from an attacker  
d) never mistypes their password.

**ANS: a, b**  
Why would a normal user frequently get denied access to files or programs? On the other hand, an attacker poking around the system might get denied access. The whole point of the principles of section 22.1 is that it is possible to distinguish a normal user from an attacker. If that were not possible then intrusion detection software would be impossible!

**(9) A virus might cause a program to access files that it doesn't normally access.**

a) true  
b) false

**ANS: a**

**(10) Which of the following are desirable characteristics of an intrusion detection system?**

a) it should minimize false negatives  
b) it should maximize false negatives  
c) it should minimize false positives  
d) it should maximize false positives  
e) none of the above

**ANS: a, c**

**(11) It is not possible for any type of intrusion detection system to detect a zero-day attack**

a) true  
b) false

**ANS: b**  
If the zero-day attack causes a process to behave differently then specification-based detection should notice this. If it breaks some rules then misuse-based detection should notice this. An if it causes an anomaly to occur (e.g., an unusual amount of activity on some port) then anomaly-based dection should notice this. The general nature of the detection methods hopefully will cause many zero-day attacks to be noticed, but not all of them.

**(12) Consider the following situation at Annapurna (the cafeteria at M.U.M.)  
       A diner must show a badge or purchase a meal before eating at Annapurna.  Each diner uses a tray. If the number of trays washed in a day does not equal the number of diners counted by the door checker, then somebody has cheated Annapurna and eaten for free.   By analogy, this is an example of which of the following:**

a) anomaly modelling  
b) misuse modelling  
c) specification-based modelling

**ANS: b**  
There is clearly a non-statistical rule here, namely that the number of trays washed = the number of diners seen by the checker.

**(13) Consider the following policy implemented by Annapurna (the cafeteria at M.U.M.)  
       A student usually accesses only the dining room and the dish room. If a student  is found in the kitchen this is reported (he/she may be trying to put some chicken in the soup).  By analogy, this is an example of which of the following:**

a) anomaly modelling  
b) misuse modelling  
c) specification-based modelling

**ANS: c**  
The student here is a process. The places he/she can visit are like files and programs the process can run. Entering the kitchen is like a process attempting to access a file that its specification says that it shouldn't. This is specification-based modelling.

**(14) Consider the following information about Annapurna, the cafeteria at MUM.  
        From past experience Annapurna has determined that each student on the average drinks one pint of milk per day. Based on this information they budget for X gallons of milk per day. If on some day, all X gallons have been used   
        before the midday meal, there is reason to suspect that someone is stealing milk.  
        By analogy, Annapurna is doing what kind of modelling here?**

a) anomaly modelling  
b) misuse modelling  
c) specification-based modeling

**ANS: a**  
Anomaly modelling is statistical in nature. The phrase "each student **on the average** drinks one pint of milk per day" indicates the statistical nature of this.

**(15) Which statistical model is likely to be used to detect someone guessing passwords?**

a) threshhold metric  
b) statistical moments  
c) markov model

**ANS: a**

**(16) Which of the following are phases of intrusion handling?**

a) logging  
b) auditing  
c) recovery  
d) making a backup  
e) notifying

**ANS: c**  
Logging and auditing make the detection of an intrusion possible. When an intrusion is detected it is necessary to handle it somehow. This is recovery. Making a backup after an intrusion has been detected is not a good idea because you might be saving a root kit planted by the intruder.