Summer 2016 CS6035 Exam I

25 questions at 4 points each; total: 100 points

TRUE/FALSE QUESTIONS:

1. (T) The three essential security goals are confidentiality, integrity, and availability.
2. (F) Accidentally overflowing the stack by just one byte is acceptable from a security standpoint because it doesn't overwrite the whole return address.
3. (F) Address Space Layout Randomization (ASLR) can effectively mitigate the OpenSSL Heartbleed vulnerability exploitation because the technique makes the address of sensitive data unpredictable.
4. (T) Alice wants to write a program. If she uses system calls in her code, she can access the operating system section of the address space.
5. (T) The principle of least privileges states that a subject is given only the minimum privileges necessary to complete the subject's task.
6. (F) Authentication determines if the source of a request is allowed to read a file.
7. (F) A user with read-only access to a file can change the ownership of that file in order to obtain write access.
8. (T) Under the BLP (confidentiality) model, a subject with a low security clearance is allowed to write to an object of higher classification (i.e., an object that requires a higher security clearance).
9. (T) A polymorphic virus can effectively bypass the signature-based anti-virus software.
10. (T) A botnet is a network of machines (desktops, laptops, servers, cell phones, etc.) called bots controlled by an attacker to perform coordinated malicious activities.
11. (T) Role-based access control (RBAC) is an example of mandatory access control (MAC).
12. (F) While it may not be safe to open a Microsoft Word document sent as an email attachment, it is always safe to open a PDF attachment.
13. (F) Since signature-based anti-virus solutions are not always effective, we should get rid of them.

MULTIPLE CHOICE QUESTIONS:

1. ____D__ is a basic design principle for secure systems that requires that every access to every object be checked for authorization.
   A. Defense-in-depth
   B. Least common mechanism

C. Fail-safe defaults
D. Complete mediation

2. Which of the following contributes to buffer overflow attacks? Answer: __B__
A. Stack Canaries
B. Using strcpy without boundary checks
C. Address Space Layout Randomization (ASLR)
D. Non-executable stack (NX)

3. Which operating system does not provide isolation from application code? Answer: __C__
A. Windows
B. Linux
C. DOS
D. OS X

4. In the UNIX file access control model, given a file with the following access control list (ACL): "-rwxr-xr--" (that is, the user has read/write/execute, the group has read/execute and the world has read), which of the following cases violate this ACL? Answer: __B__
A. The user under a different group can make copy of the file.
B. The user under the same group can add additional content to the file.
C. The owner can modify the content of the file.
D. All users can read the file.

5. The Clark-Wilson Policy is an example of __B__:
A. Discretionary Access Control
B. Mandatory Access Control
C. Rule-based Access Control
D. Role-based Access Control

6. Data mining (or in general, data analysis) techniques can be used to analyze data in order to illegitimately gain knowledge about a database. Which of the following database attacks use such a technique? Answer: __B__
A. SQL injection attack
B. Inference attack
C. Privilege escalation attack
D. Brute-force attack for cracking admin passwords

7. In 2015, XCodeGhost in China drew the public's attention. XCode is a developer tool from Apple used for application development. Almost all big software companies use it to develop and compile their applications for Mac OS / iOS. Companies in China do the same, but some of them download XCode from third party servers because they experience poor connections to Apple servers. However, these third-party XCode downloads were reported to contain malicious

code. These infected third-party XCode versions have since been called XCodeGhost. When a company uses XCodeGhost to compile their application, additional code snippets, which have the capabilities to do various malicious actions, are injected by XCodeGhost. In terms of malicious software classification, XCodeGhost can be classified as a __C__:

A. Trap door
B. Logic bomb
C. Trojan horse
D. Virus

8. A parasitic virus's intent is to __B___.
A. Be embedded in documents, run/spread when opened
B. Scan/infect programs
C. Run/Spread whenever the system is booted
D. None of the above

9. Which of these is a characteristic of an advanced persistent threat (APT)? Answer: __F__
A. Users do not realize they have been compromised
B. The malware sends data to a bot master
C. The malware remains undetected
D. Both A and B
E. Both B and C
F. A, B, and C

10. Which of these are required for an operating system to be considered as a trusted computing base (TCB)? Answer: __F__
A. Tamper-proof
B. Complete-mediation
C. Correctness
D. Both A and B
E. Both B and C
F. A, B, and C

11. Which of these is example(s) of two-factor authentication? Answer: __C__
A. Using both your password and birthday
B. Using both your fingerprint and retinal scan
C. Using both your password and a pin number sent to your phone by the bank
D. Both A and B
E. Both B and C
F. Both A and C
G. A, B, and C

12. Need-to-know is an example of __A__.
A. Mandatory access control policy

B. Discretionary access control policy
C. Integrity protection policy
D. Authentication policy