Total points: 60

Simon Fraser University
CMPT 403
Mid-term exam

Date:	30th June, 2022
Time:	12:30 PM to 1:50 PM
Duration:	80 minutes
Final page number:	5

Name: _____

Student ID: _____

1. Write your name and student ID in the space above.
2. Circle the correct answer.

Solution: THIS IS THE ANSWER KEY.

. (1) Disabling third-party cookies has the effect of:

A. Preventing third-parties from knowing what sites I'm visiting.

B. Reducing the amount of information collected by web bugs.

C. Disabling web bugs, as they rely on third-party cookies.

D. Stopping third-party advertisements on the websites I'm visiting.

(2) Why does Microsoft release patches on "Patch Tuesday" and usually not any other date?

A. To minimize the damage caused by "Exploit Wednesday".

B. To minimize the damage caused by vulnerable users.

C. To minimize the damage caused by malware exploiting patched vulnerabilities.

D. To minimize the damage caused by patching.

(3) Which of the following classifications best describes the mechanism used by Stuxnet to penetrate into a nuclear reactor?

A. Spread by network

B. Spread by trojan

C. Spread by removable media

D. Spread by planted malware

(4) A format string vulnerability occurs when:

A. Insecure formats such as %n are used.

B. Improper bounds checking is done for a printf or fprintf function.

C. User input is treated as a format string.

D. The return address is overwritten by a printf or frptinf function.

(5) Which of the following is FALSE concerning the weakness of a substitution cipher, which replaces each of the 128 ASCII characters with another ASCII character?

A. Given enough ciphertext, it is easy to guess the key using frequency analysis.

B. It is easier to break this cipher with brute force than it is to break DES.

C. If the same word appears twice in the plaintext, it will appear twice in the ciphertext at the same locations.

D. It assumes the communicating parties can establish another secure channel to deliver the secret key to each other.

(6) Why is a botnet especially useful for malware spreading?

A. Bots can more easily launch worm attacks.

B. Trojan horses from bots are more believable.

C. Its network capacity allows DDoS attacks.

D. A botnet has more computational power in total than a single machine.

(7) Which of the following is a way to achieve authenticity?

A. Using an asymmetric key encryption algorithm to establish secret keys.

B. Using Two-Factor Authentication to check for user credentials.

C. Displaying your server's public key upon connection.

D. Adding a Message Authentication Code based on a symmetric key encryption algorithm.

(8) Which of the following is not a feature of Flame?

A. When news about Flame broke out, infected computers received a kill command and attempted to remove all traces of Flame.

B. Infected computers would attack a Microsoft server's weak cryptography to obtain a fake certificate.

C. It records the victim's keystrokes.

D. It changes its behavior depending on the victim's programs, such as antivirus programs.

(9) Which of the following statements about Trojans is false?

A. Some Trojans can be defeated with a software patch.

B. Trojans can involve privilege escalation attacks.

C. Buffer overflows vulnerabilities can lead to Trojans.

D. One way to infect someone with a Trojan is to use a SQL Injection attack.

(10) When Heartbleed was disclosed, the Tor Project blog posted that "If you need strong anonymity or privacy on the Internet, you might want to stay away from the Internet entirely for the next few days while things settle." What does "while things settle" mean?

A. Wait for law enforcement to find and arrest the attackers responsible.

B. Wait for OpenSSL server owners to install the required patch.

C. Wait for researchers to figure out how to fix the bug.

D. Wait for firewalls to start blocking code that can exploit the Heartbleed bug.

(11) In this course, polymorphic code is:

A. A way to disguise file patterns.

B. A way to randomize code so that malware cannot exploit it.

C. A way to encrypt files for ransom.

D. A way to cause false negatives in anti-virus software.

(12) Which of the following statements about a secure cryptographic hash is false?

A. Hashes of common words are easy to reverse.

B. For password storage, we may want to choose a hash with long computational time.

C. In the context of password storage, hashes are used to secure confidentiality.

D. A hash should be used with a salt when used as a MAC.

(13) Which of the following is an incorrect description of TOCTTOU attacks?

A. TOCTTOU attacks rely on malformed input to cause unexpected behavior.

B. TOCTTOU attacks can be used to gain root privileges.

C. TOCTTOU attacks can be used to bypass authentication.

D. In a TOCTTOU attack, the attacker changes an object between the time it is checked and the time it is used.

(14) Which of the following is NOT a difference between XSS and XSRF attacks?

A. XSRF attacks use malicious links; XSS attacks do not.

B. XSRF succeeds because the web server trusts the web client; XSS succeeds because the web client trusts the web server.

C. In XSRF, the HTTP request is malicious; in XSS, the HTTP response is malicious.

D. XSS attacks may be launched after maliciously taking over a server; XSRF attacks do not attack the server.

(15) What is the implication of the "dancing pig" problem?

A. From the security perspective, there is nothing we can do if the user chooses an insecure option.

B. Trojan Horses should be defeated by forcing users to install patches.

C. Trojan Horses succeed because users emphasize functionality.

D. The average user cannot notice a rootkit on their computer.

(16) Which of the following is NOT a desirable property for an encryption function Enc(K, M), where K is the key and M is the message?

A. Given K and M, it should be easy to find Enc(K, M).

B. Given M, but not K, it should be hard to find Enc(K, M).

C. Given Enc(K, M) and M, it should be easy to find K.

D. Given Enc(K, M) and K, it should be hard to find M.

(17) The DigiNotar problem tells us that when a Certificate Authority is compromised, it should immediately announce this. Why is that?

A. Browser users will be able to check the issuer of the certificate for websites they go to.

B. It is easy for browsers to revoke a Certificate Authority's key.

C. Webservers that use a certificate from the compromised Certificate Authority should immediately get a new certificate to avoid compromise.

D. Other Certificate Authorities can help by removing a compromised authority from the web of trust.

Solution: B, D, C, C, B B, C, B, D, B, D, D, A, A, C, D, B