Chapter 16

Multiple Choice Questions

1. To protect the systems we have to ensure security on the following level:
A. physical
B. network
C. operating system
D. all of the above

Ans: D
Feedback: 16.1
Difficulty: Easy

2. ________ is a type of social-engineering attack, in which a legitimate-looking e-mail misleads a user into entering confidential information.
A. spamming
B. phishing
C. attack surface
D. denial-of-service

Ans: B
Feedback: 16.1
Difficulty: Easy

3. Trojan mule is a type of the Trojan horse which emulates ____________
A. a legitimate email
B. a system shell
C. a login program
D. a legitimate webpage

Ans: C
Feedback: 16.2.1
Difficulty: Medium

4. ________________ encrypts the information on the target computer and renders it inaccessible to the owner
A. Spyware
B. Ransomware
C. Logic bomb
D. all of the above

Ans: B
Feedback: 16.2.1
Difficulty: Medium

5. _____________ virus changes each time it is installed to avoid detection by antivirus software.
A. A polymorphic
B. A source code
C. An encrypted
D. A macro

Ans: B
Feedback: 16.2.3
Difficulty: Medium

6. Port scanning allows a hacker to_________________
A. known users' passwords
B. disrupt legitimate use of a system
C. detect a system's vulnerabilities
D. modify a transmission between a remote user and a system

Ans: D
Feedback: 16.3.3
Difficulty: Medium

7. TLS provides security at the _______ layer.
A. network
B. transport
C. application
D. none of the above

Ans: B
Feedback: 16.4.2
Difficulty: Medium

8. IPSec uses ______ encryption.
A. asymmetric
B. symmetric
C. one-time password
D. Caesar cipher

Ans: B
Feedback: 16.4.2
Difficulty: Easy

9. User authentication can be based on_______________
A. the user’s possession of something
B. the user’s knowledge of something
C. an attribute of the user
D. all of the above

Ans: B
Feedback: 16.5
Difficulty: Medium

10. Vulnerability scans can check:
A. unexpected long-running processes
B. hidden network daemons
C. unauthorized programs in system directories
D. all of the above

Ans: D
Feedback: 16.5
Difficulty: Medium

11. IPSs (Intrusion Prevention Systems) can detect zero-day attack if they employ_____________
A. signature-based detection
B. anomaly detection
C. all of the above
D. none of the above

Ans: B
Feedback: 16.6.3
Difficulty: Medium

12. Using a firewall, the following connection is allowed:
A. from Internet to company’s computers
B. from Internet to DMZ (demilitarized zone)
C. from computers in DMZ (demilitarized zone) to company computers
D. none of the above

Ans: B
Feedback: 16.6.5
Difficulty: Medium

13. Address Space Layout Randomization (ASLR) technique protects an operating system against_______________
A. a macro virus
B. zero-day attack
C. Denial of Service
D. a code-injection attack

Ans: D
Feedback: 16.6.7
Difficulty: Medium

Essay Questions

1. Describe the principle of least privilege.
Ans: Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job. The purpose of this principle is to reduce the number of potential interactions among privileged programs to the minimum necessary to operate correctly, so that one may develop confidence that unintentional, unwanted, or improper uses of privilege do not occur.

Feedback: 16.2.1
Difficulty: Easy

2. Describe the problem of a buffer overflow.
Ans: The function strcpy() copies with no regard to the buffer size in question, halting only when a NULL (\0) byte is encountered. If such a byte occurs before the BUFFER SIZE is reached, the program behaves as expected. But the copy could easily exceed the buffer size, then
a) If the overflow exceeds the padding, the next automatic variable on the stack will be overwritten with the overflowing contents. The outcome here will depend on the exact positioning of the variable and on its semantics. This overflow could lead to a program crash, as an unexpected value in a variable could lead to an uncorrectable.
b) If the overflow greatly exceeds the padding, all of the current function's stack frame is overwritten. At the very top of the frame is the function's return address, which is accessed when the function returns. The flow of the program is subverted and can be redirected by the attacker to another region of memory, including memory controlled by the attacker (for example, the input buffer itself, or the stack or the heap). The injected code is then executed, allowing the attacker to run arbitrary code as the processes' effective ID.

Feedback: 16.2.2
Difficulty: Hard

3. Why UNIX does not suffer from viruses?
Ans: UNIX and other multiuser operating systems generally are not susceptible to viruses because the executable programs are protected from writing by the operating system. Even if a virus does infect such a program, its powers usually are limited because other aspects of the system are protected.

Feedback: 16.2.3
Difficulty: Hard

4. Describe the idea of masquerading attack.
Ans. During a masquerading, an attacker pretends to be an authorized user in order to gain access to a system or to gain greater privileges than are authorized for her/him.

Feedback: 16.3.1
Difficulty: Medium

5. Describe the idea of main-in-the-Medium attack.
Ans. The man-in-the-Medium attack takes place in between two legitimate peers. This attack allows an attacker to eavesdrop and to modify the communication between them.

Feedback: 16.3.1
Difficulty: Medium

6. What is the reason to use a stream cipher?
Ans. A stream cipher is designed to encrypt and decrypt a stream of bytes or bits rather than a block. This is useful when the length of a communication would make a block cipher too slow. The key is input into a pseudo–random bit generator, which is an algorithm that attempts to produce random bits. The output of the generator when fed a key is a keystream. A keystream is an infinite set of bits that can be used to encrypt a plaintext stream through an XOR operation. (XOR, for "exclusive OR" is an operation that compares two input bits and generates one output bit. If the bits are the same, the result is 0. If the bits are different, the result is 1.)

Feedback: 16.4.1.2
Difficulty: Medium

7. Why an asymmetric encryption algorithm uses two keys?
Ans. In an asymmetric encryption algorithm, there are different encryption and decryption keys. An entity preparing to receive encrypted communication creates two keys and makes one of them (called the public key) available to anyone who wants it. Any sender can use that key to encrypt a communication, but only the receiver who owns the key can decrypt the communication.

Feedback: 16.4.1.2
Difficulty: Medium

8. How does one distribute a key for symmetric algorithms?
Ans. With symmetric algorithms, both parties need the key, and no one else should have it. Sometimes it is performed out-of-band, but usually it is sent through an existing encryption channel using e.g., asymmetric key algorithms.

Feedback: 16.4.1.4
Difficulty: Medium

9. How are one-time password systems implemented?
Ans. One-time password systems are implemented in various ways. Commercial implementations use hardware calculators with a display or a display and numeric keypad. Software running on computers or smartphones provides the user with H(pw, ch); pw can be input by the user or generated by the calculator in synchronization with the computer. Sometimes, pw is just a personal identification number (PIN). The output of any of these systems shows the one-time password. A one-time password generator that requires input by the user involves two-factor authentication. Two different types of components are needed in this case—for example, a onetime password generator that generates the correct response only if the PIN is valid. Two-factor authentication offers far better authentication protection than single-factor authentication because it requires "something you have" as well as "something you know."

Feedback: 16.5.4
Difficulty: Hard

10. What does a security policy include?
Ans. Policies vary widely but generally include a statement of what is being secured.

Feedback: 16.6.1
Difficulty: Easy

True/False Questions

1. The attack surface is the set of points at which an attacker can try to break into the system.

Ans: T
Feedback: 16.1
Difficulty: Easy

2. A virus is a fragment of code embedded in a malware.

Ans: F
Feedback: 16.2.3
Difficulty: Easy

3. The purpose of denial-of-service attacks is to gain information or steal resources.

Ans: F
Feedback: 16.3.2
Difficulty: Easy

4. In a symmetric encryption algorithm, one key is used to encrypt and a different one is used to decrypt.

Ans: F
Feedback: 16.4.1
Difficulty: Easy

5. It is much faster for a computer to encode and decode ciphertext by using the usual symmetric algorithms than by using asymmetric algorithms.

Ans: T
Feedback: 16.4.1
Difficulty: Medium

6. Transport Layer Security (TLS) employs server’s certificate from certification authority (CA).

Ans: T
Feedback: 16.4.3
Difficulty: Medium

7. MS Word documents in RTF format are resistant to macro viruses.

Ans: T
Feedback: 16.6.4
Difficulty: Easy

8. A firewall is installed between the trusted and the untrusted.

Ans: T
Feedback: 16.6.6
Difficulty: Medium

9. When a user logs on, MW Windows 10 creates a list of files which can be used by the user.

Ans: F
Feedback: 16.7
Difficulty: Medium