ALEXANDRIA UNIVERSITY
FACULTY OF ENGINEERING
Specialized Scientific Programs
Computer & Communication Program
Course Title: Computer and Network Security
Course Code: CC551

جـامـعـة الإسـكـنـدريـة
كـلـيـة الـهـنـدسـة
البرامج العلمية المتخصصة
برنـامج الحاسبات و الإتصالات

Date: 9/ January/ 2016
Time allowed: Two hours

اسم الطالب: --

Student's Name : --- Student ID: --------------------

<u>Question 1 [50 points]:</u> *Choose* the correct answer for the following statements and ***briefly** state* the reason (each statement is worth one point)

1) What is the difference between Data Integrity and Data Security?
   a. Limiting physical access to computer systems; assigning passwords to users.
   b. Consistent, accurate and reliable data; protection of data from unauthorized access.
   c. Encryption; Audit trails.
   d. Distributing work to preserve integrity; installing system passwords.

<u>Reason:</u>

2) Once a worm infects a computer it has two primary tasks; one is to send itself to another computer and the other is to replicate itself.
   a. Ture
   b. False

<u>Reason:</u>

3) Which of the following asymmetric encryption keys is used to encrypt data to ensure only the intended recipient can decrypt the ciphertext?
   a. Private
   b. Escrow
   c. Public
   d. Preshared

<u>Reason:</u>

4) In Public/Private key cryptography, even the sender will no longer be able to read the message after encrypting it with the receiver’s public key.
   a. Ture
   b. False

<u>Reason:</u>

5) The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric
   key cryptography uses:
   a. Multiple keys for non-repudiation of bulk data.

b. Different keys on both ends of the transport medium.
c. Bulk encryption for data transmission over fiber.
d. The same key on each end of the transmission medium.

Reason:

6) A buffer overflow happens with a C program tries to store too much information in the random access memory and causes an excess of data in the storage buffer.
a. Ture
b. False

Reason:

7) Which of the following MUST a programmer implement to prevent cross-site scripting?
a. Validate input to remove shell scripts
b. Validate input to remove hypertext
c. Validate input to remove batch files
d. Validate input to remove Java bit code

Reason:

8) The attack where bad web site sends browser request to good web site, using credentials of an innocent victim is called
a. SQL injection
b. Cross Site Request Forgery (CSRF)
c. Cross-site Scripting (XSS)

Reason:

9) Which of the following allows an attacker to identify vulnerabilities within a closed source software application?
a. Fuzzing
b. Compiling
c. Code reviews
d. Vulnerability scanning

Reason:

10) CAPTCHA provides mitigation against flooding of your service by bots masking as new customers.
a. Ture
b. False

Reason:

11) DNS cache poisoning attack can be done by:
a. Breaking into the DNS server and creating false entries
b. Sending false zone transfers to the DNS server and creating false name records
c. Creating a fraudulent DNS server to redirect computers
d. Hijacking the web browser

Reason:

12) Which of the following concepts ensures that the data is only viewable to authorized users?
a. Availability
b. Biometrics
c. Integrity
d. Confidentiality

Reason:

13) Firewalls are used by network administrators to resist attacks to the network by filtering all the packets as they arrive. Another name for a firewall is a packet filter.
   a. Ture
   b. False

Reason:

14) Which of the following devices BEST allows a security administrator to identify malicious activity after it has occurred?
   a. Spam filter
   b. Intrusion detection system (IDS)
   c. Firewall
   d. Malware inspection

Reason:

15) An instance where an IDS identifies legitimate traffic as malicious activity is called which of the following?
   a. False positive
   b. True negative
   c. False negative
   d. True positive

Reason:

16) Which of the following methods BEST describes the use of hiding data within other files?
   a. Digital signatures
   b. PKI
   c. Transport encryption
   d. Steganography

Reason:

17) The purpose of digitally signing a message is to ensure:
   a. Integrity of the sender
   b. Confidentiality of the message
   c. Authenticity of the sender
   d. Confidentiality of the sender

Reason:

18) An Access Control List is a set of permissions that are attached to an object.
   a. Ture
   b. False

Reason:

19) A security administrator needs to implement a site-to-site VPN tunnel between the main office and a remote branch. Which of the following protocols should be used for the tunnel?
   a. TLS
   b. DNS-SEC
   c. IPSec
   d. 802.1X

Reason:

20) When examining HTTP server logs the security administrator notices that the company's online store crashes after a particular search string is executed by a single external user. Which of the following BEST describes this type of attack?

a. Rebinding
b. DDoS
c. Spoofing
d. DoS

Reason:

21) The purpose of digitally signing a message is to ensure:

a. Integrity of the message
b. Confidentiality of the message
c. Integrity of the sender
d. Confidentiality of the sender

Reason:

22) Which of the following logs would MOST likely indicate that there is an ongoing brute force attack against a server local administrator account?

a. Firewall
b. System
c. Performance
d. Access

Reason:

23) Which of the following type of attacks requires an attacker to sniff the network?

a. Man-in-the-Middle
b. DDoS attack
c. MAC flooding
d. DNS poisoning

Reason:

24) Which of the following is used to perform denial of service (DoS) attacks?

a. Privilege escalation
b. Botnet
c. Adware
d. Spyware

Reason:

25) DNS-SEC uses SSL between different name servers to certify that the results of DNS queries match those that the name servers are authorized to provide.

a. True
b. False

Reason:

26) DNS-SEC is effective against DNS-rebinding attacks.

a. True
b. False

Reason:

27) Syncookies can prevent massive (>200Gbs) DoS floods.

a. Ture
b. False

Reason:

28) A stateless packet filter can prevent internal hosts from connecting to an external DNS server.

a. True
b. False

Reason:

29) In encryption, CBC mode is considered preferable and more secure to ECB mode.
a. True
b. False

Reason:

30) Message authentication codes can provide authentication.
a. True
b. False

Reason:

31) Some DoS attacks would be possible even if every autonomous system on the Internet implemented ingress filtering.
a. True
b. False

Reason:

32) Different iOS applications may be installed with different permissions, enforced by an application sandbox.
a. Ture
b. False

Reason:

33) Choosing random initial sequence numbers in the TCP handshake ensures that a network attacker cannot inject packets into the session.
a. True
b. False

Reason:

34) A□SYN□flood□exhausts□what□resource□at□its□target?
a. Ability□of□the□machine's□network□card□to□handle□incoming□packets
b. Entries□in□the□process□table
c. Entries□in□the□TCP□connection□table
d. Processing□power

Reason:

35) Android applications may be installed with different permissions, enforced by vendors' signatures.
a. True
b. False

Reason:

36) Different Windows Phone 8 applications may be installed enforced by the principles of isolation and least privilege.
a. True
b. False

Reason:

37) Snort is considered as a network-based anomaly-based intrusion detection system.
a. True
b. False

Reason:

38) IPSec operation depends on employing mutual authentication algorithms between agents at the beginning of the communication session.
   a. True
   b. False

Reason:

39) Firewalls might use various application proxies to enforce policies for specific protocols, such as FTP and Telnet.
   a. True
   b. False

Reason:

40) Route Attestations are used in S-BGP to enable adding easily new routes between autonomous systems.
   a. True
   b. False

Reason:

41) The ------ is a cryptographic network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers.
   a. SSH
   b. SSL
   c. DES
   d. AES

Reason:

42) The statement, "Information systems should be configured to require strong passwords," is an example of a/an:
   a. Security requirement
   b. Security policy
   c. Security objective
   d. Security control

Reason:

43) Public key cryptography is another name for:
   a. Secure Sockets Layer
   b. Asymmetric cryptography
   c. Symmetric key cryptography
   d. Kerberos

Reason:

44) A particular encryption algorithm transforms plaintext to ciphertext by XORing the plaintext with the encryption key. This is known as:
   a. Electronic codebook
   b. Cipher block chaining
   c. Block cipher
   d. Stream cipher

Reason:

45) A banker is concerned foremost with protecting the of bank account information.
   a. Confidentiality.
   b. Integrity.
   c. Availability.
   d. Size.

Reason:

46) A denial of service attack is an attempt to prevent users from having access to a service exploiting design flaws in some networking protocols.
   a. True
   b. False

Reason:

47) The principle of least privilege is the idea that a subject should be given the maximum privileges needed to perform its prescribed task.
   a. True
   b. False

Reason:

48) The ------------- protocol was created to ensure secure transactions between web servers and browsers. The protocol uses a third party, a certificate authority, to identify one end or both end of the transactions.
   a. SSL
   b. SSH
   c. TLS
   d. SBGP

Reason:

49) It is possible to have DoS attacks at different network layers in the TCP/IP stack.
   a. True
   b. False

Reason:

50) Backscatter attack can be considered as a high rate TCP SYN flood attack.
   a. True
   b. False

Reason:

Good Luck ....

Dr. Bassem Mokhtar