BRAINWARE UNIVERSITY

Term End Examination 2023
Programme – B.Sc.(IT)-AI-2020
Course Name – Information Security
Course Code - BAID601A
(Semester VI)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Identfy the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.

a) Network Security
b) Database Security
c) Information Security
d) Physical Security

(ii) Which of them is not a threat to information security?

a) Disaster
b) Eavesdropping
c) Information leakage
d) Unchanged default password

(iii) A systems engineer has discovered that a web server supports only 56- bit SSL connections. Relate the systems engineer deduce from this?

a) Web communications with this server are highly secure
b) The server does not support remote administration
c) Web communications with this server are not secure
d) The server is running the Windows operating system

(iv) A systems engineer is designing a system that consists of a central computer and attached peripherals. For fastest throughput, Choose of the following technologies should be used for communication with peripheral devices:

a) USB 2.0
b) Firewire 400
c) USB 1.1
d) IDE

(v) A user, Bill, has posted a link on a web site that causes unsuspecting users to transfer money to Bill if they click the link. The link will only work for users who happen to be authenticated to the bank that is the target of the link. This is known as:

a) Cross site request forgery
b) Cross-site scripting
c) Broken authentication
d) Replay attack

(vi) Select Compromising confidential information comes under

a) Bug
b) Threat
c) Vulnerability
d) Attack

(vii) Identify Lack of access control policy is a

a) Bug
b) Threat
c) Vulnerability
d) Attack

(viii) Select the right one Why Would A Hacker Use A Proxy Server?

a) The System Configuration
b) The Business Strategy Of The Company
c) The Education Of The Attacker
d) The Network Architecture

(ix) To Hide Information Inside A Picture, select the Technology

a) Rootkits
b) Bitmapping
c) Steganography
d) Image Rendering

(x) An intruder wishes to break in to an application in order to steal information stored there. Because the application utilizes strong authentication, what is the most likely approach the intruder will take?

a) Dictionary attack
b) Malicious code attack
c) Application bypass attack
d) Password guessing attack

(xi) Select Performing Hacking Activities With The Intent On Gaining Visibility For An Unfair Situation Is Called

a) Cracking
b) Analysis
c) Hacktivism
d) Exploitation

(xii) Select hacking tools and techniques hackers' do not use for maintaining access in a system?

a) Trojans
b) Rootkits
c) Backdoors
d) Wireshark

(xiii) Identify the ability of an individual to gain physical access to an authorized area?

a) Remote accessing
b) Physical accessing
c) Network accessing
d) Remote accessing

(xiv) An organization that is performing a disaster recovery planning project has determined that it needs to have on-site electric power available for as long as ten days, in the event of an electric utility failure. The best approach for this requirement is:

a) Uninterruptible power supply (UPS) and power distribution unit (PDU)
b) Electric generator
c) Uninterruptible power supply (UPS)
d) Uninterruptible power supply (UPS) and electric generator

(xv) An organization wants to prevent SQL and script injection attacks on its Internet web application. The organization should implement a/an:

a) Intrusion detection system
b) Firewall
c) Application firewall
d) SSL certificate

Group-B

(Short Answer Type Questions) 3 x 5=15

2. What is business continuity management? (3)
3. What is a security policy and why do we need one? (3)
4. What is packet filtering? (3)
5. Why are internal threats often more successful than external threats? (3)
6. Illustrate that IT security audit? (3)

OR

How can you ensure backups are secure? Illustrate it. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Discuss the various security process? How do we control it? (5)
8. Choose the first three steps when securing a Linux server? (5)

9. Explain the common method of disrupting enterprise systems? (5)
10. Explain different kind of attack is a standard Diffie-Hellman exchange vulnerable . (5)
11. Explain with a few examples of security architecture requirements. (5)
12. What does an intrusion detection system do? Analyze it? (5)

OR

Explain that what are the primary design flaws in HTTP, and how would you improve it? (5)

****