BRAINWARE UNIVERSITY

Term End Examination 2023-2024
Programme – B.Sc.(ANCS)-Hons-2020/B.Sc.(ANCS)-Hons-2021
Course Name – Hacking Techniques, Tools and Incident Handling
Course Code - BNCSC601
(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) Choose the benefits of Ethical Hacking.

a) Improved Security. b) Reduced Cost of Breaches.
c) Better Compliance with Regulations. d) All of these.

(ii) Select that active attacks and compromises will be identified by_____.

a) Using Antivirus Software b) Conducting Penetration Testing
c) Monitoring Network Traffic d) All of these

(iii) Choose the cybercrime annotation.

a) Hacking for Personal Gain. b) Hacking to Improve Security.
c) Hacking to Cause Harm. d) All of these.

(iv) Show the potential risks of performing foot printing on a live system.

a) None, as Foot Printing is a non-invasive process. b) System instability or downtime.
c) Increased network performance. d) Enhanced system security.

(v) Classify the difference between Active and Passive information gathering.

a) Active information gathering requires the use of specialized tools while Passive information gathering does not b) Passive information gathering involves interacting with the target system while Active information gathering does not
c) Active information gathering is faster than Passive information gathering d) Passive information gathering is performed without the knowledge of the target system while Active information gathering is performed with the knowledge of the target system

(vi) Classify the information gathered during the foot printing phase to gain unauthorized access to a target system.

a) By exploiting vulnerabilities found during the Foot Printing phase b) By launching a DoS attack against the target system

c) By using social engineering techniques to trick system users into revealing sensitive information
d) By deleting critical system files

(vii) Show which methods would be most effective for conducting foot printing on a wireless network.

a) Using packet sniffers to capture network traffic.
b) Performing a port scan on the wireless router.
c) Conducting a DNS lookup on the wireless router.
d) Using a vulnerability scanner to detect weaknesses in the wireless network.

(viii) Choose the characteristics of a good vulnerability assessment tool.

a) Easy to use and configure.
b) Accurate and reliable.
c) Flexible and customizable.
d) All of these.

(ix) Classify the primary goal of vulnerability management.

a) Detect and remediate vulnerabilities
b) Secure the perimeter of the network
c) Monitor network traffic for attacks
d) Identify and report vulnerabilities

(x) Choose two types of system hacking.

a) Passive and active.
b) Internal and external.
c) Remote and local.
d) Host-based and network-based.

(xi) Find the first step in the hacking process.

a) Gaining access to the target system.
b) Identifying the target system.
c) Conducting reconnaissance of the target system.
d) Analyzing network traffic for vulnerabilities.

(xii) Identify the purpose of a keystroke logger.

a) A tool to guess passwords.
b) A tool to capture keystrokes.
c) A tool to generate secure passwords.
d) A tool to scan for vulnerabilities in the system.

(xiii) Identify the best way to remove a keystroke logger.

a) By reinstalling the operating system.
b) By disabling the device driver.
c) By deleting the executable file.
d) By running an anti-malware program on the system.

(xiv) Show the difference between black-box and white-box testing.

a) Black-box testing is for network security, white-box testing is for system security.
b) Black-box testing is for system security, white-box testing is for network security.
c) Black-box testing is a manual process, white-box testing is an automated process.
d) Black-box testing is for testing third-party software, white-box testing is for in-house software.

(xv) Choose a recommended countermeasure against insider attacks.

a) Implementing strong passwords
b) Using multi-factor authentication
c) Educating employees on security
d) Blocking all incoming traffic

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Name some ethical issues that are related to cybercrime and hacking. (3)
3. Explain the importance of Foot Printing and Reconnaissance in Ethical Hacking. (3)
4. Create a plan that includes the necessary resources for the steps needed to complete reconnaissance and footprinting. (3)
5. Explain the Phishing Attacks. (3)
6. Differentiate between backdoors and trojans. (3)

OR

Describe the significance of incident handling for preserving the availability, confidentiality, and integrity of data. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Describe how the mindset of hackers influences cybersecurity. (5)
8. Discuss the various types of viruses. (5)
9. Explain the role of IDS, IPS, and honeypots in incident handling. (5)
10. Explain BOTs/BOTNETs. (5)
11. Summarize the types of social engineering attacks. (5)
12. Explain strategies for preventing cyber attacks and mitigating their impact. (5)

OR

Explain a countermeasure plan to prevent trojan attacks. (5)

****