BRAINWARE UNIVERSITY

Term End Examination 2023
Programme – B.Sc.(ANCS)-Hons-2020
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. *Choose the correct alternative from the following :* 1 x 15=15

(i) Analyze URL obfuscation work

a) By hiding the real URL
b) By redirecting the user to a fake URL
c) By encrypting the URL
d) By blocking the user from the URL

(ii) predict the phase of Hacking involves identifying vulnerabilities and potential entry points?

a) Reconnaissance
b) Scanning and Enumeration
c) Gaining Access and Maintaining Access
d) Covering Tracks

(iii) justify,Which of the following is a common Hacking methodology?

a) Fuzzing
b) SQL Injection
c) Social Engineering
d) All of the above

(iv) Write the phase of Hacking involves gaining and maintaining access to a system

a) Reconnaissance
b) Scanning and Enumeration
c) Gaining Access and Maintaining Access
d) Covering Tracks

(v) Identify Foot Printing in ethical hacking

a) Testing a website's functionality
b) Gathering information about a target system
c) Injecting malicious code into a system
d) Launching a DoS attack

(vi) Write tool would be best used for performing DNS Foot Printing

a) Traceroute
b) Whois
c) Nmap
d) Dig

(vii) Write the vulnerability management life cycle

a) Identifying, assessing, prioritizing and patching
b) Assessing, exploiting, patching, retesting
c) Testing, identifying, prioritizing and patching
d) Patching, testing, identifying and exploiting

(viii) Identify approach is used for vulnerability assessment

a) Manual
b) Automated
c) Both manual and automated
d) None of the above

(ix) Identify a tool is commonly used for password cracking

a) Wireshark
b) Nmap
c) John the Ripper
d) Cain and Abel

(x) Comapre the difference between an IDS and an IPS in incident handling

a) An IDS detects and alerts of potential incidents, while an IPS prevents them
b) An IDS prevents incidents, while an IPS detects them
c) An IDS is used for recovery, while an IPS is used for backup
d) There is no difference between the two

(xi) Explain a recommended action to take in response to a DDoS attack in incident handling

a) Shutting down all systems
b) Blocking traffic from the attacking IP addresses
c) Allowing the attack to continue and monitor it for information
d) Disconnecting from the network

(xii) Define the two types of sniffers

a) Active and passive
b) Online and offline
c) Internal and external
d) Invasive and non-invasive

(xiii) Compare the difference between ARP spoofing and ARP poisoning

a) There is no difference, the terms are interchangeable
b) ARP spoofing is a passive attack, while ARP poisoning is an active attack
c) ARP poisoning is a type of ARP spoofing attack that involves sending large numbers of ARP messages
d) ARP spoofing is a type of ARP poisoning attack that involves spoofing the MAC address of the gateway

(xiv) Write from the following is an example of an online scam

a) Nigerian prince scam
b) Smurf attack
c) SYN flooding
d) DNS amplification attack

(xv) Identify is the concept of Ethical Hacking?

a) Hacking to cause harm
b) Hacking to break the law
c) Hacking to improve security
d) Hacking to steal data

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Identify Insider Attacks. (3)
3. Identify common types of Online Scams. (3)
4. Explain the purpose and process of Reconnaissance in hacking. (3)
5. Develop a strategy to identify indications of a trojan attack. (3)
6. Compare and contrast Social Engineering and Phishing Attacks. (3)

OR

Analyse the effectiveness of different session hijacking tools. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Summarize the different techniques used by hackers to carry out cyber attacks. (5)
8. Determine the concept of a computer hole and its role in system hacking. (5)
9. Evaluate the effectiveness of different incident handling strategies. (5)

10. Apply Social-Engineering Countermeasures to prevent identity theft. (5)
11. Evaluate the effectiveness of DoS/DDoS countermeasures. (5)
12. Illustrate the steps involved in vulnerability management life cycle. (5)

OR

Compare various methods of password cracking and their effectiveness. (5)

****