BRAINWARE UNIVERSITY

Library
Brainware University
398, Ramkrishnapur Road, Barasat
Kolkata, West Bengal-700125

Term End Examination 2024-2025
Programme – B.Sc.(ANCS)-Hons-2022
Course Name – Security Incident Handling
Course Code - BNCSD501A
(Semester V)

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) What are the key phases involved in the hacking process?

a) Reconnaissance, scanning, gaining access, maintaining access, covering tracks
b) Footprinting, scanning, enumeration, system hacking, escalation of privileges
c) Phishing, ransomware, identity theft, cyberstalking, DDoS attacks
d) Malware, spyware, adware, ransomware, phishing

(ii) What are some common techniques used by hackers to gain unauthorized access to systems?

a) Brute force attacks, social engineering, and exploiting vulnerabilities
b) Ransomware, phishing, and DDoS attacks
c) Malware, spyware, and adware
d) Ethical hacking and penetration testing

(iii) What is the primary goal of a DDoS attack?

a) Encrypting data
b) Crashing or disrupting services
c) Stealing information
d) Gaining unauthorized access

(iv) What is the primary goal of reconnaissance in the hacking process?

a) Disrupt systems
b) Gather information
c) Hide evidence
d) Gain control

(v) What is the term for the process of identifying vulnerabilities in a system?

a) Vulnerability Assessment
b) Penetration Testing
c) Ethical Hacking
d) Security Audit

(vi) What is the main goal of footprinting?

a) To create a vulnerability report
b) To exploit security weaknesses
c) To identify potential entry points
d) To install malware

(vii) Which type of footprinting involves gathering information without direct interaction?

a) Passive Footprinting
b) Active Footprinting
c) Network Scanning
d) Social Engineering

(viii) Identify common tools used for network sniffing.

a) Wireshark, Tcpdump, Ettercap, Fiddler.
b) Metasploit, Nmap, Burp Suite, Netcat.
c) Aircrack-ng, Snort, NetFlow, Nessus.
d) Hydra, John the Ripper, Hashcat, Patator.

(ix) Name the strategies to protect against Trojan Horse attacks.

a) Use security software and maintain regular updates.
b) Disable all network services.
c) Install only trusted applications.
d) Use outdated software to avoid vulnerabilities.

(x) Define the types of Trojans and their impact on systems.

a) RATs, keyloggers, backdoors, ransomware.
b) Worms, viruses, spyware, adware.
c) Phishing, social engineering, cryptojacking.
d) Rootkits, bootkits, logic bombs, data breaches.

(xi) Identify methods for verifying system file integrity.

a) Checksum and hash verification, digital signatures, and FIM.
b) Network monitoring and traffic analysis.
c) User access control and permissions management.
d) Regular backups and antivirus scanning.

(xii) Identify the common method used in social engineering attacks.

a) Phishing
b) DOS Attack
c) SQL Injection
d) Encryption

(xiii) Locate the type of phishing attack that specifically targets high-level executives.

a) Whaling
b) Smishing
c) Spear Phishing
d) Vishing

(xiv) Identify which security mechanism is used to monitor security events across a network and provide incident management.

a) Snort IDS
b) OSSIM
c) Suricata IDS
d) Lynis

(xv) Choose the correct approach used to mitigate Session Hijacking attacks by encrypting the entire communication channel.

a) Use of HTTPS
b) Secure Cookie Flag
c) Temporary Session IDs
d) Session Expiry

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain the process and significance of covering tracks in the hacking lifecycle. (3)
3. Justify the information gathering process in the context of footprinting. (3)
4. What are Keystroke Loggers, and how can they be detected? (3)
5. How do Intrusion Prevention Systems (IPS) differ from IDS in responding to incidents? (3)
6. Illustrate Identity Theft and its impact on individuals. (3)

OR

Distinguish a "Smurf" attack and its method of operation. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

Library
Brainware University
398, Ramkrishnapur Road, Barasat
Kolkata, West Bengal-700125

7. Evaluate the SYN Flood attack and its impact on servers. (5)
8. Evaluate the role of Honeypots in condition of detecting and analyzing network incidents. (5)
9. How can organizations effectively identify and respond to active attacks and compromises? (5)
10. Write the strategies that organizations can implement to defend against these password cracking methods. (5)
11. Evaluate DNS Spoofing and its impact on network security. (5)
12. Analyze the passive and active footprinting techniques. What are the potential risks associated with each? (5)

OR

Explain the potential consequences of failing to secure information that can be easily gathered during the foot printing phase. (5)

****