18267

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – M.Sc.(ANCS)-2025
Course Name – Network Penetration Testing
Course Code - MNC10500
(Semester I)

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) Select the DNS record whose disclosure in a zone-transfer immediately reveals authoritative name-server details.
a) MX b) SOA
c) TXT d) CNAME

(ii) Choose the reconnaissance tool that passively enumerates sub-domains via certificate-transparency logs.
a) Sublist3r b) crt.sh
c) theHarvester d) Amass

(iii) Select the Burp Suite feature that must be configured in a browser to intercept HTTP requests transparently.
a) Intruder b) Repeater
c) Proxy listener d) Decoder

(iv) Recollect the Nmap timing template that maximises speed without disabling reliability checks, often used on LANs.
a) -T2 (Polite) b) -T3 (Normal)
c) -T4 (Aggressive) d) -T5 (Insane)

(v) Select the protocol layer where TLS/SSL operates.
a) Application b) Transport
c) Network d) Session

(vi) Choose the standard algorithm used in TLS handshake for key exchange.
a) RSA b) MD5
c) SHA1 d) DES

(vii) Assess the importance of TLS in underpinning HTTPS and its role in ensuring secure web transactions.
a) SSL b) SSH
c) TLS d) IPSec

(viii) Identify a directory where DLL execution should be monitored.

a) C:\ProgramData\Logs
b) Temp or user directories
c) C:\SystemVolumeInformation
d) C:\Boot

(ix) Assess the security and stealth implications of using port 22 for SSH pivot tunneling.

a) 23
b) 443
c) 3389
d) 22

(x) Recall the main risk of enabling unrestricted outbound traffic on corporate networks.

a) Data loss through HTTP only
b) Limited access to internet resources
c) Facilitates covert command-and-control channels
d) Prevents DNS poisoning

(xi) Recall the port often used in dynamic port forwarding for general SOCKS proxy services.

a) 1080
b) 80
c) 3389
d) 22

(xii) Choose the primary goal of an attacker when setting up multiple chained tunnels.

a) Gain faster bandwidth access
b) Bypass time-based detection mechanisms
c) Obfuscate traffic path and reach deeper assets
d) Interfere with monitoring tools

(xiii) Assess which mitigation strategy would be most effective to counter SQL injection attacks in production environments.

a) Parameterized Queries
b) Input Validation
c) IDS Monitoring
d) WAF Blocking

(xiv) Predict which malware type would pose the greatest risk in a scenario where attackers require stealthy persistence at kernel level.

a) Worm
b) Rootkit
c) Trojan
d) Spyware

(xv) Predict the most likely attacker objective when exploiting SMBv1 vulnerabilities.

a) Privilege Escalation
b) Remote Code Execution
c) Password Cracking
d) Denial of Service

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define passive reconnaissance with examples. (3)
3. Write any two techniques used for maintaining access in hacking. (3)
4. Distinguish between DLL Hijacking and DLL Sideloading. (3)
5. Estimate the key security implications of improper detection of pivoting attempts. (3)
6. Differentiate between local and remote port forwarding in penetration testing. (3)

OR

Analyze the role of dynamic port forwarding using SOCKS proxies in pivoting. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Describe tools and techniques used in DNS enumeration. (5)
8. Compare and contrast TCP SYN, NULL, and FIN scans. (5)
9. Evaluate the effectiveness of using HTTP tunneling as an evasion technique against modern firewalls. (5)
10. Evaluate the risks associated with poor credential hygiene and password reuse in enterprise environments. (5)
11. Evaluate the effectiveness of SSH dynamic port forwarding in advanced penetration testing. (5)
12. Design a defense-in-depth strategy to detect and prevent pivoting in a corporate network. (5)

OR

Develop a complete attack chain using pivoting, port forwarding, and privilege escalation to compromise a segmented network. (5)

****