17706

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – M.Sc.(ANCS)-2024
Course Name – Network Penetration Testing
Course Code - MNC30112
(Semester III)

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 ICMP type–code pair that a firewall returns when a closed UDP port is probed during enumeration.

a) Echo Reply (0) b) Port Unreachable (3/3)
c) Time-Exceeded (11/0) d) Source Quench (4)

(ii) Select the DNS record whose disclosure in a zone-transfer immediately reveals authoritative name-server details.

a) MX b) SOA
c) TXT d) CNAME

(iii) Choose the option for nslookup that specifically queries IPv6 (AAAA) resource records.

a) -type=A b) -type=ptr
c) -type=aaaa d) -type=soa

(iv) Choose the immediate indicator, in traceroute, that a router intentionally suppresses TTL-exceeded messages.

a) *** timeouts for every hop b) ICMP type 11 returned twice
c) Sudden drop to <1 ms latency d) Hop duplicates its own IP

(v) Choose the standard algorithm used in TLS handshake for key exchange.

a) RSA b) MD5
c) SHA1 d) DES

(vi) Select the most secure version of TLS supported in modern browsers.

a) TLS 1.0 b) TLS 1.1
c) TLS 1.2 d) TLS 1.3

(vii) Select the key benefit of using TLS over SSL.

a) Faster key exchange b) Backward compatibility
c) Enhanced cryptographic strength d) Support for VPN tunneling

(viii) Select the full form of DLL as described in the module.

a) Dynamic Link Library b) Direct Load Library

c) Device Level Logic
d) Distributed Logic Layer

(ix) Choose the application state required for a hijacked DLL to execute.

a) Idle
b) Running in Safe Mode
c) Restarted
d) Scheduled in Task Manager

(x) Select the privilege escalation outcome from a successful DLL hijack.

a) Guest access
b) Administrator or SYSTEM access
c) No privilege change
d) Kernel panic

(xi) Select the purpose of port forwarding in an attacker's post-exploitation phase.

a) To scan open ports from an external network
b) To redirect traffic from a compromised host to internal systems
c) To encrypt shellcode for obfuscation
d) To detect proxy usage in the network

(xii) Choose the correct example of local port forwarding.

a) ssh -L 8080:10.10.10.5:3389 user@remote
b) ssh -R 53:127.0.0.1:4444 user@remote
c) ssh -D 1080 user@remote
d) ssh user@remote -X

(xiii) Select the tool that can convert a compromised host into a TCP-over-HTTP/HTTPS tunnel endpoint.

a) Nmap
b) Chisel
c) Wireshark
d) Responder

(xiv) Select the method that detects unauthorized port forwarding behavior.

a) Monitor DNS queries
b) Track memory usage
c) Analyze netstat output for high ports in LISTEN state
d) Check disk I/O performance

(xv) Choose the typical attack step that follows a successful pivot in an internal network.

a) Disable the local firewall
b) Install proxychains
c) Scan the new subnet for high-value targets
d) Encrypt local drives

Group-B

(Short Answer Type Questions) 3 x 5=15

2. List any four tools used for reconnaissance. (3)
3. Explain the risk of leaving NetBIOS enabled in modern networks. (3)
4. Justify the use of NFS in enterprise environments. (3)
5. Describe the security implication of Kerberoasting. (3)
6. Explain the concept of Copy-On-Write (COW) in memory management. (3)

OR

Compare User Mode and Kernel Mode in Windows architecture. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Describe how SMB enumeration is used by attackers and name two tools used for it. (5)
8. Define HTTP status codes and categorize them with examples. (5)
9. Assess the security challenges posed by unprotected NFS shares. (5)
10. Assess the impact of manipulating EPROCESS and ETHREAD structures. (5)
11. Explain how attackers use UAC bypass techniques in Windows to escalate privileges. (5)
12. Explain the process of identifying and exploiting a vulnerable application for DLL Hijacking. (5)

OR

Explain the concept of mounting in Unix-like operating systems with an example. (5)

****