45493

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – M.Sc.(ANCS)-2025
Course Name – Privilege Escalation
Course Code - MNC27503 (T)
(Semester II)

Full Marks : 40 **Time : 2:0 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 10=10

1. *Choose the correct alternative from the following :*

(i) Identify a service commonly targeted using weak credentials.
   a) DNS b) FTP
   c) DHCP d) NTP

(ii) Name one category of attack vectors.
   a) Encryption-based b) Credential-based
   c) Backup-based d) Audit-based

(iii) Identify the main goal of system enumeration.
   a) Patch system b) Encrypt files
   c) Identify weaknesses d) Disable AV

(iv) Locate where Linux OS distribution details are stored.
   a) /etc/shadow b) /boot
   c) /etc/os-release d) /var/log

(v) Choose the vulnerability type exploited by Dirty COW.
   a) Integer overflow b) Race condition
   c) Logic flaw d) Permission misconfig

(vi) Enumerate one Windows mechanism abused by potato attacks.
   a) Secure Boot b) BIOS firmware
   c) BitLocker d) NTLM authentication

(vii) Choose the primary abuse in DLL hijacking.
   a) Token reuse b) Kernel memory
   c) Password cracking d) DLL search order

(viii) Define container-based privilege escalation.
   a) VM escape via BIOS b) User enumeration
   c) Abusing container misconfigurations to gain higher privileges d) Kernel panic induction

(ix) Choose the Windows DLL search location most dangerous when writable.

a) System32 b) Windows directory
c) Application directory d) Driver store

(x) Choose the necessary condition for unquoted service path exploitation.

a) No antivirus installed b) Path contains spaces and is unquoted
c) Service runs in user context d) Registry key is missing

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain how stored passwords contribute to privilege escalation. (3)
3. Summarize the importance of port forwarding in post-exploitation. (3)
4. Explain the getSystem technique used in Windows privilege escalation. (3)
5. Describe how DLL hijacking leads to privilege escalation. (3)
6. Compose an explanation of how token impersonation is abused for privilege escalation in Windows systems. (3)

OR

Write how unquoted service paths and binary path misconfigurations allow attackers to gain elevated privileges. (3)

Group-C

(Long Answer Type Questions) 5 x 3=15

7. Differentiate between network-based, application-based, and credential-based attack vectors. (5)
8. Summarize the objectives and importance of system enumeration in privilege escalation. (5)
9. Illustrate how DLL hijacking can lead to privilege escalation when targeting Windows services. (5)

OR

Analyze how SSH key mismanagement can lead to immediate privilege escalation or lateral movement. (5)

****