BRAINWARE UNIVERSITY

Term End Examination 2022
Programme – M.Sc.(ANCS)-2021
Course Name – Vulnerability Analysis and Penetration Testing
Course Code - MNCS302
(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) In which of the following, a person is constantly followed/chased by another person or group of several peoples?

a) Phishing b) Bulling
c) Stalking d) Identity theft

(ii) Which of the following refers to the violation of the principle if a computer is no more accessible?

a) Access control b) Confidentiality
c) Availability d) All of the above

(iii) In ethical hacking and cyber security, there are _______ types of scanning:

a) 1 b) 2
c) 3 d) 4

(iv) Which Nmap output formats are supported by searchsploit?

a) JSON b) XML
c) Text d) Graphical

(v) What is the purpose of a pen test?

a) To simulate methods that intruders take to gain escalated privileges
b) To see if you can get confidential network data
c) To test the security posture and policies and procedures of an organization
d) To get passwords

(vi) Which framework made cracking of vulnerabilities easy like point and click.

a) .NET b) Metasploit
c) Zeus d) Ettercap

(vii) Which tool was made by OWASP Foundation

a) Metasploit b) Nessus
c) ZAP d) Nmap

(viii) Maltego used for

a) OSI
b) Information gathering
c) Forensic
d) Traffic analyzer

(ix) What are the major components of the intrusion detection system?

a) Analysis Engine
b) Event provider
c) Alert Database
d) All of the mentioned

(x) What is the preferred communications method used with systems on a bot-net?

a) IRC
b) E-mail
c) ICMP
d) TFTP

(xi) What are the forms of password cracking techniques?

a) AttackBrute Forcing
b) AttacksHybrid
c) AttackSyllable
d) All of the above

(xii) HTTPs uses which port number?

a) 21
b) 53
c) 80
d) 443

(xiii) Banner grabbing is an example of what?

a) Footprinting
b) Application analysis
c) Active operating system fingerprinting
d) Passive operating system fingerprinting

(xiv) In an any organization, company or firm the policies of information security come under___________

a) CIA Triad
b) Confidentiality
c) Authenticity
d) None of the above

(xv) What are the types of scannings used in Ethical hacking?

a) Port scanning
b) Network scanning
c) Vulnerability scanning
d) All of the above

Group-B

(Short Answer Type Questions) 3 x 5=15

2. What is CIA triad in Cyber Security? Explain. (3)
3. What is vulnerability management? explain the difference between a risk and a vulnerability? (3)
4. What is nmap ? Report about the common ports to focus on during penetration testing? (3)
5. What is an SSL Certificate? Compare between Authentication vs Authorization? (3)

OR

Analyze Content Security Policy (CSP)? How to use Content Security Policy (CSP) against clickjacking? (3)

6. What is patch management? Express about SSL session or SSL connections? (3)

OR

What Is a Penetration Testing Report? Invent the diffrence between Manual Penetration and automated penetration testing. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Explain honeypots? What is a firewall and how does it work? What is the difference between an IDS and an IPS? (5)
8. what is API ? Describe API Lifecycle Management? (5)
9. Explain bug bounty? How to mitigate the risk of Sensitive Data Exposure? (5)
10. What is ClickJacking? Illustrate how to prevent a clickjacking attack? (5)
11. Analyze PCI Compliance? What is HIPAA Compliance? What is Protected Health Information? What are the HIPAA Rules? (5)

OR

Explain Vulnerability Testing ? what are the types of a vulnerability scanner ? describe the Vulnerability Assessment Process. (5)

12. What is buffer overflow? How can DNS and ARP be exploited by attackers? What is privilege escalation? Provide a few examples (5)

OR

What are LFI and RFI ? What is IDOR, what are its consequences and how can you prevent it? (5)

****