Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No.....

Faculty of Science
End Sem Examination Dec-2023
BC3ET01 Ethical Hacking

Programme: B.Sc. Branch/Specialisation: Computer Science / All

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. Which of the following is a tool for performing footprinting undetected? **1**

(a) Whois search (b) Traceroute
(c) Ping sweep (d) Host scanning

ii. Banner grabbing is an example of what? **1**

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

iii. For discovering the OS running on the target system, the scanning has a specific term. What is it? **1**

(a) Footprinting (b) 3D Printing
(c) Fingerprinting (d) Screen-printing

iv. In order to prevent a hacker from using SMB session hijacking, which TCP and UDP ports would you block at the firewall? **1**

(a) 167 and 137 (b) 80 and 23
(c) 1277 and 1270 (d) 139 and 445

v. _____ is the world's most popular vulnerability scanner used in companies for checking vulnerabilities in the network. **1**

(a) Wireshark (b) Nessus
(c) Snort (d) WebInspect

vi. What is a virtual private network (VPN)? **1**
(a) A device used to encrypt network traffic
(b) A device used to monitor network traffic
(c) A device used to block network traffic
(d) A device used to analyze system logs

vii. This is a type of cyber attack that has a program running on your server to bypass the authorization. **1**
(a) DoS (b) Phishing (c) Sniffing (d) Backdoor

viii. What is enumeration? **1**
(a) Identifying active systems on the network
(b) Cracking passwords
(c) Identifying users and machine names
(d) Identifying routers and firewalls

ix. What is the purpose of a penetration test? **1**
(a) To identify vulnerabilities in a system or network
(b) To exploit vulnerabilities in a system or network
(c) To fix vulnerabilities in a system or network
(d) To steal sensitive information from a system or network

x. _____ framework made cracking of vulnerabilities easy like point and click. **1**
(a) .Net (b) Ettercap
(c) Zeus (d) Metasploit

Q.2 i. Compare Remote Access vs Local access. **2**
ii. How to take full permissions control to edit protected Registry Keys? **3**
iii. Enumerate the different methodology used for footprinting. Explain the footprinting through search engine? **5**
OR iv. What is the importance of Network Enumeration with example? **5**

Q.3 i. Explain in detail the pre attack phase of penetration testing. **2**
ii. Illustrate the open-source tools for scanning. Explain any one of them in detail. **8**
OR iii. Discuss gaining access phase of the attack including how the attack occurs. **8**

Q.4 i. Discuss about network sniffing in detail. **3**
ii. Explain with example: **7**
(a) Voice mail hacking (b) VPN hacking
OR iii. Expressing valuable thought about the Private Branch Exchange hacking. **7**

Q.5 i. Identifying the Tools that exploiting WEP Weakness. **4**
ii. Examining the Wireless Foot printing, Wireless Scanning and discuss how enumeration play a role in wireless hacking. **6**
OR iii. What is Denial of Service Attacks? Discuss Motivation of DoS Attackers. Also explain the types of DoS attacks. **6**

Q.6 Write short note on any two:
i. SQL injection attacks **5**
ii. Client-side browser **5**
iii. Metrpreter **5**

******

Scheme of Marking

Ethical Hacking-BC3ET01(T)

Q.1	i)	Which of the following is a tool for performing footprinting undetected? a) Whois search	**1**
	ii)	Banner grabbing is an example of what? c) Passive operating system fingerprinting	**1**
	iii)	For discovering the OS running on the target system, the scanning has a specific term. What is it? c) Fingerprinting	**1**
	iv)	In order to prevent a hacker from using SMB session hijacking, which TCP and UDP ports would you block at the firewall? d) 139 and 445	**1**
	v)	_____ is the world's most popular vulnerability scanner used in companies for checking vulnerabilities in the network. b) Nessus	**1**
	vi)	What is a virtual private network (VPN)? a) A device used to encrypt network traffic	**1**
	vii)	This is a type of cyber attack that has a program running on your server to bypass the authorization. d) Backdoor	**1**
	viii)	What is enumeration? c) Identifying users and machine names	**1**
	ix)	What is the purpose of a penetration test? b) To exploit vulnerabilities in a system or network	**1**
	x)	_____ framework made cracking of vulnerabilities easy like point and click. d) Metasploit	**1**

Q.2	i.	Define Remote Access vs Local access	**1 mark** **1 mark**	**2**
	ii.	Simulating to take full permissions control to edit protected Registry Keys		**3**
	iii.	Different methodology used for footprinting	**2 marks**	**5**
		Footprinting through search engine	**3 marks**	
OR	iv.	What is the Importance of Network Enumeration With example	**4 marks** **1 mark**	**5**

Q.3	i.	Explain in detail the pre attack phase of penetration testing		**2**
	ii.	Illustrate the Open source tools for scanning explains any one of them in detailed	**2 marks** **6 marks**	**8**
OR	iii.	Gaining Access phase of the attack including how the attack occurs	**2 marks** **6 marks**	**8**

Q.4	i.	Discuss about network sniffing in detail	**3**
	ii.	Develop a case study to product your system into Brute force attack	**2 marks** **5 marks**	**7**
OR	iii.	Expressing valuable thought about the Private Branch Exchange hacking Explanation		**7**

Q.5	i.	Identifying the Tools that exploiting WEP Weakness	**1 mark** **3 marks**	**4**
	ii.	Examining the Wireless Foot printing Wireless Scanning Enumeration does play a role in wireless hacking	**2 marks** **2 marks** **2 marks**	**6**
OR	iii.	Detecting Denial of Service Attacks Motivation of Dos Attackers Types of DoS attacks	**2 marks** **2 marks** **2 marks**	**6**

Q.6		Attempt any two:	
	i.	SQL injection attacks 5 marks	**5**
	ii.	Client-side browser 5 marks	**5**
	iii.	Metrpreter 5 marks	**5**

******

P.T.O.