



Academic year 2022-2023 (Odd Semester)

## DEPARTMENTS OF COMPUTER SCIENCE/ INFORMATION SCIENCE AND ENGINEERING

Date	March 2023	Maximum Marks	10+50
Course Code	22MCE3E2T	Duration	120 Min
Sem	III	CIE - I	
<b>CYBER SECURITY(Elective common to PGCSE/PGCNE)</b>			

SL No.	Part A- Quiz	M	BT	CO
1	----- is an activity on the internet of the victim, gather all information in the background, and send it to someone else.	1	L2	CO1
2	----- is a type of software designed to help the user's computer detect viruses and avoid them.	1	L2	CO1
3	Define Cryptanalyst?	1	L1	CO2
4	Write three key elements of CIA triad.	2	L3	CO3
5	It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the-----	1	L3	CO2
6	Define Piracy, Plagiariasm	2	L2	CO4
7	-----refers to exploring the appropriate, ethical behaviors related to the online environment and digital media platform?	1	L2	CO2
8	-----refers to the violation of the principle if a computer is no more accessible	1	L2	CO2

SL No.	Part B -Test	M	BT	CO
1.a	Illustrate with examples why do cyber security is important. Briefly discuss the types of cyber-attacks.	5+5	L1	CO2
2.	Describe the principles of Confidentiality, Integrity and Availability with a neat diagram depicting cyber cube.	5+5	L2	CO2
3	Illustrate with a neat diagram concept of DNS and the associated attacks	5+5	L3	CO4
4	Illustrate with examples the following terms and the characteristics in each case with respect to damage they create in cyber security arena. (i)Virus (ii)Worm (iii) Trojan Horse (iv)Logic Bomb (v) Boot sector Virus	2x5	L3	CO2
5	Define Symmetric Encryption ? Discuss in detail the working principles involved in the design of public key encryption technique with an example.	5+5	L2	CO2



Academic year 2023-2024 (Odd Semester)

## DEPARTMENTS OF COMPUTER SCIENCE/ INFORMATION SCIENCE AND ENGINEERING

Date	7 <sup>th</sup> March 2024	Maximum Marks	10+50
Course Code	22MCE3E2T	Duration	120 Min
Sem	III	CIE - II	
<b>CYBER SECURITY(Elective common to PGCSE/PGCNE)</b>			

SL No.	Part A- Quiz	M	BT	CO
1	What type of rootkit will patch, hook, or replace the version of system call in order to hide information	1	L2	CO1
2	_____ the sequence of a TCP connection?	1	L2	CO1
3	The first phase of hacking an IT system is comprised of which foundation of security?	1	L1	CO2
4	How is IP address spoofing detected?	2	L3	CO3
5	Why would a ping sweep be used?	1	L3	CO2
6	What are the port states determined by Nmap?	2	L2	CO4
7	_____ is the most important activity in system hacking?	1	L2	CO2
8	Phishing is a form of _____.	1	L2	CO2

SL No.	Part B -Test	M	BT	CO
1.	Illustrate with examples why do attackers use proxies ? Discuss types of proxies being used in attacks.	5+5	L1	CO2
2.	Describe the principles of SSH used in tunneling techniques.	10	L2	CO2
3	Illustrate with a neat diagram concept of Phishing, Smishing, Vishing, and Mobile Malicious Code	5+5	L3	CO4
4	Illustrate with examples threat infrastructure taking botnet as case study with centralized and decentralized botnet infrastructure.	2x5	L3	CO2
5	Discuss in detail , victim interaction to Fast-Flux, Advanced Fast-Flux architectures.	5+5	L2	CO2

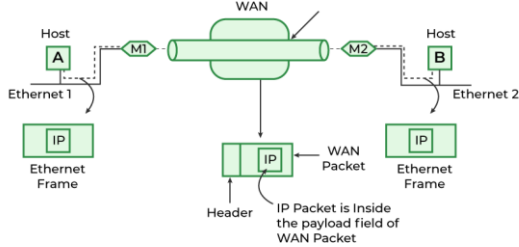


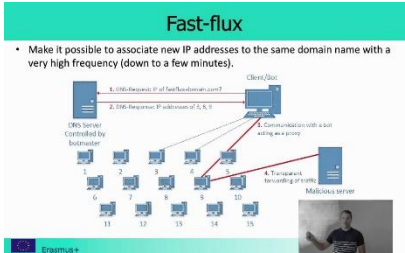
Academic year 2022-2023 (Odd Semester)

**DEPARTMENTS OF COMPUTER SCIENCE/ INFORMATION SCIENCE AND  
ENGINEERING**

Date	March 2024	Maximum Marks	10+50
Course Code	22MCE3E2T	Duration	120 Min
Sem	III	CIE - II	
<b>CYBER SECURITY(Elective common to PGCSE/PGCNE)</b>			

SL No.	Part A- Quiz	M	BT	CO
1	What type of rootkit will patch, hook, or replace the version of system call in order to hide information?  Library level root kits	1	L2	CO1
2	_____ the sequence of a TCP connection?  SYN-SYN ACK-ACK	1	L2	CO1
3	The first phase of hacking an IT system is comprised of which foundation of security? confidentiality	1	L1	CO2
4	How is IP address spoofing detected?  Comparing the TTL values of the actual and spoofed addresses	2	L3	CO3
5	Why would a ping sweep be used?  A ping sweep is intended to identify live systems. Once an active system is found on the network, other information may be distinguished, including location. Open ports and firewalls.	1	L3	CO2
6	What are the port states determined by Nmap? Open, filtered, unfiltered	2	L2	CO4
7	_____ is the most important activity in system hacking?  Cracking passwords	1	L2	CO2
8	Phishing is a form of _____.  Impersonation	1	L2	CO2

SL No.	Part B -Test	M	BT	CO
1.a	<p>Illustrate with examples why do attackers use proxies ? Discuss types of proxies being used in attacks.</p> <p><b>Types of Proxy Servers</b></p> <ul style="list-style-type: none"> <li>• Forward Proxy.</li> <li>• Transparent Proxy.</li> <li>• Anonymous Proxy.</li> <li>• High Anonymity Proxy.</li> <li>• Distorting Proxy.</li> <li>• Data Center Proxy.</li> <li>• Residential Proxy.</li> <li>• Public Proxy.</li> </ul>	5+5	L1	CO2
2.	<p>Describe the principles of SSH used in tunneling techniques.</p> <p>Tunneling is <b>redirecting network traffic from one port to another to enable secure access to network traffic and services across firewalls and also from outside the network</b>. Simply put, tunneling is a port redirection technique in which traffic is received at one port and forwarded to another port.</p>  <p><b>Steps</b></p> <ul style="list-style-type: none"> <li>• Host A constructs a packet that contains the IP address of Host B.</li> <li>• It then inserts this IP packet into an Ethernet frame and this frame is addressed to the multiprotocol router M1</li> <li>• Host A then puts this frame on Ethernet.</li> <li>• When M1 receives this frame, it removes the IP packet, inserts it in the payload packet of the WAN network layer packet, and addresses the WAN packet to M2. The multiprotocol router M2 removes the IP packet and sends it to host B in an Ethernet frame.</li> </ul>	5+5	L2	CO2
3	<p>Illustrate with a neat diagram concept of Phishing, Smishing, Vishing, and Mobile Malicious Code</p>	5+5	L3	CO4

	Phishing: fraudulent e-mails and websites meant to steal data. Vishing: fraudulent phone calls that induce you to reveal personal information. Smishing: fraudulent text messages meant to trick you into revealing data.			
4	<p>Illustrate with examples threat infrastructure taking botnet as case study with centralized and decentralized botnet infrastructure.</p> <p>Bot herders control their botnets through one of two structures: <b>a centralized model with direct communication between the bot herder and each computer, and a decentralized system with multiple links between all the infected botnet device</b></p> <p>An attacker builds a botnet by taking control of a large number of network-connected machines. While it is possible to build a botnet using cheap computing power, such as cloud infrastructure, <b>botnets are usually created by infecting computers with malware.</b></p>	2x5	L3	CO2
5	<p>Discuss in detail, victim interaction to Fast-Flux, Advanced Fast-Flux architectures.</p> <p><i>Fast flux</i> is a DNS technique used by botnets to phishing and malware delivery sites behind an ever-changing network of compromised hosts ..</p> <p>Fast flux is <b>a technique used by cybercriminals to hide malware delivery and phishing websites by rapidly cycling through IP addresses tied to a malicious domain.</b> 2. What Are the Types of Fast-Flux Network? The two types of fast-flux networks are single-flux and double-flux networks.</p> 	5+5	L2	CO2



Academic year 2022-2023 (Odd Semester)

## DEPARTMENTS OF COMPUTER SCIENCE/ INFORMATION SCIENCE AND ENGINEERING

Date	March 2023	Maximum Marks	10+50
Course Code	22MCE3E2T	Duration	120 Min
Sem	III	CIE - I	
<b>CYBER SECURITY (Elective common to PGCSE/PGCNE)</b>			

SL No.	Part A- Quiz	M	BT	CO
1	-----is also referred to as malicious software?	1	L2	CO1
2	In Wi-Fi Security, name the protocol which is used often?	1	L2	CO1
3	The response time and transit time is used to measure the _____ of a network.	1	L1	CO2
4	Write three key elements of CIA triad.	2	L3	CO3
5	It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the _____	1	L3	CO2
6	Define Piracy, Plagiarism	2	L2	CO4
7	When was the first computer virus created?	1	L2	CO2
8	In the computer networks, the encryption techniques are primarily used for improving the _____	1	L2	CO2

SL No.	Part B -Test	M	BT	CO
1.a	Discuss information assurance fundamentals essential in cyber security.	5+5	L1	CO2
2.	Describe the principles of basic cryptography compare that with symmetric encryption and public key encryption	5+5	L2	CO2
3	Illustrate with a neat diagram concept of Firewalls and type of firewalls with examples	5+5	L2	CO3
4	Illustrate with examples attacker techniques and motivations.	5+5	L3	CO2
5	Discuss Virtual Machine Obfuscation related to cyber security? Justify how it is useful in a virtual environment to mitigate modern threats?	5+5	L3	CO4