5. University Questions / Question Bank (2marks and 10 Marks)

NARSIMHA REDDY ENGINEERING COLLEGE
UGC AUTONOMOUS INSTITUTION
Maisammaguda (V), Kompally - 500100, Secunderabad, Telangana State, India
Accredited by NBA & NAAC with 'A' Grade
Approved by AICTE
Permanently affiliated to JNTUH

CYBER SECURITY - 23CY601

Department of CSE (Cyber Security)

UNIT WISE QUESTION BANK

UNIT-I					
S. No		**Questions**	**BT**	**CO**	**PO**
Part –A (Short Answer Questions)					
1		Who are called computer criminals?	L1	CO1	PO1
2		Define passive attacks and active attacks	L1	CO1	PO1
3		Illustrate about CIA Triad.	L1	CO1	PO1
4		Explain short notes on Network and Security Concepts	L1	CO1	PO1
5		What is Domain Name System (DNS)?	L1	CO1	PO1
6		List the types of Cyber Security threats.	L1	CO1	PO1
7		What is basic Cryptography	L1	CO1	PO1
8		Write a short note on public key encryption?	L1	CO1	PO1
9		Discuss about Firewalls	L1	CO1	PO1
10		Define Radio- Frequency Identification	L1	CO1	PO1
11		What is Windows Tokens?	L1	CO1	PO1
12		Explain about Window Messaging	L1	CO1	PO1
Part– B(Long Answer Questions)					
13	a)	Differentiate between active attacks and passive attacks	L2	CO1	PO1
	b)	Explain in detail about Network and Security Concepts.	L2	CO1	PO1
14	a)	Discuss in detail the Symmetric Encryption and Public Key Encryption.	L2	CO1	PO1
	b)	Write a detailed note on Domain Name System (DNS)?	L2	CO1	PO1
15	a)	What is Internet Governance? Use Firewalls.	L2	CO1	PO1
	b)	Distinguish between Software attacks and Hardware attacks.	L1	CO1	PO1
16	a)	Explain and briefly Virtualization with examples.	L2	CO1	PO1
	b)	What is meant by Windows Tokens with briefly expand?	L2	CO1	PO1
17	a)	Explain in detail about Windows Program	L1	CO1	PO1
	b)	What are the Windows firewalls?	L1	CO1	PO1

your roots to success...

UNIT- II				
S. No	**Questions**	**BT**	**CO**	**PO**
Part –A (Short Answer Questions)				
1	What is the difference between cyber forensics and digital forensics?	L1	CO2	PO1
2	List various techniques used in cyber forensic investigation?	L1	CO2	PO1
3	Write a short note on cyber forensics	L1	CO2	PO1
4	Explain briefly about forensics investigation	L1	CO2	PO1
5	How Hackers Cover Their Tracks (Antiforensics) with any four points.	L1	CO2	PO1
6	What is digital evidence?	L1	CO2	PO1
7	How Hackers Cover Their Tracks (Antiforensics)	L1	CO2	PO1
8	Compression of Detection and Prevention	L3	CO2	PO1
9	Short notes on Malicious Code.	L1	CO2	PO1
10	What is a Mobile Malicious Code?	L1	CO2	PO1
11	Explain about Click Fraud Motivations.	L1	CO2	PO1
12	Explain about Advanced Fast-Flux.	L3	CO2	PO1

Part– B (Long Answer Questions)					
13	a)	How Hackers Cover Their Tracks (Antiforensics) with Define and expand	L2	CO2	PO1
	b)	Explain and Types of Proxies and Detecting the Use of Proxies	L2	CO2	PO1
14	a)	What is a Tunneling Techniques and expand: HTTP, DNS and ICMP?	L2	CO2	PO1
	b)	Explain in detail of Fraud Techniques.	L6	CO2	PO1
15	a)	Expand each and every information of Phishing, Smishing, Vishing, and Mobile Malicious Code.	L2	CO2	PO1
	b)	Compressions of Mobile Malicious Code and Phishing against Mobile Devices	L1	CO2	PO1
16	a)	Explain about Detection and Prevention with suitable information.	L2	CO2	PO1
	b)	Explain a Pay-per-Click and Click Fraud Motivations.	L2	CO2	PO1
17	a)	What is Rogue Antivirus and briefly explain about Click Fraud	L2	CO2	PO1
	b)	What and explain Threat Infra structure with write on a). Botnets b). Fast-Flux and 3). Advanced Fast-Flux?	L2	CO2	PO1

your tools to success...

UNIT-III					
S. No		**Questions**	**BT**	**CO**	**PO**
Part –A(Short Answer Questions)					
1		What is a cybercrime?	L1	CO3	PO1
2		Explain about Shellcode.	L1	CO3	PO1
3		What are the challenges faced in securing mobile devices?	L1	CO3	PO1
4		What is SQL Injection.	L1	CO3	PO1
5		Expand of little note on Malicious PDF Files	L1	CO3	PO1
6		Write a short note on trends in mobility?	L1	CO3	PO1
7		Explain about a Reducing the Risks of Malicious	L1	CO3	PO1
8		Write a any four points of PDF Files?	L3	CO3	PO1
9		What is meant by Web Exploit Tools	L1	CO3	PO1
10		Explain about Proliferation of Web Exploit Tools.	L1	CO3	PO1
11		Write short notes on Misdirection, Reconnaissance.	L3	CO3	PO1
12		What is Cross-Site Scripting (X SS)?	L1	CO3	PO1
Part– B (Long Answer Questions)					
13	a)	Explain about exploitation and stack-based buffer over flows	L2	CO3	PO1
	b)	What is the Techniques to Gaina Foothold?	L2	CO3	PO1
14	a)	Define and explain Integer Over flow Vulnerabilities with examples.	L2	CO3	PO1
	b)	Explain about Format String Vulnerabilities.	L6	CO3	PO1
15	a)	What is meant by SQL Injection and expand Protecting against SQL Injection?	L2	CO3	PO1
	b)	Write a Malicious PDF Files and Reducing the Risks of Malicious PDF Files	L1	CO3	PO1
16	a)	What is Race Conditions and Detecting and Preventing Race conditions	L2	CO3	PO1
	b)	Explain about Web Exploit Tools and DoS Conditions	L1	CO3	PO1
17	a)	Compressions of Brute Force and Dictionary Attacks	L2	CO3	PO1
	b)	What is Misdirection, Reconnaissance, and Disruption Methods	L2	CO3	PO1

your tools to success...

UNIT-IV					
S. No		**Questions**	**BT**	**CO**	**PO**
Part –A (Short Answer Questions)					
1		Define a malicious code.	L1	CO3	PO1
2		Explain about Self-Replicating Malicious Code	L1	CO3	PO1
3		Write a short note on Worms and Viruses?	L1	CO3	PO1
4		Explain about a Basic Input–Output System (BIOS)/Complementary Metal-Oxide Semiconductor (CMOS).	L1	CO3	PO1
5		What is Master Boot Record (MBR) Malicious Code?	L1	CO3	PO1
6		Explain about a Token Kidnapping	L1	CO3	PO1
7		What is a Token Kidnapping?	L1	CO3	PO1
8		Explain about a Virtual Machine Detection.	L3	CO3	PO1
9		Write short notes on Detecting Communication with the Outside World?	L1	CO3	PO1
10		Compressions of Man-in-the-Middle Attacks and dynamic-link library Injection.	L1	CO3	PO1
11		Explain about a Stealing Information and Exploitation.	L3	CO3	PO1
12		What is meant by Injecting Applications.	L1	CO3	PO1
Part– B (Long Answer Questions)					
13	a)	Explain in detail about Evading Detection and Elevating Privilege.	L2	CO3	PO1
	b)	What are the Evading Detection and Elevating Privileges?	L2	CO3	PO1
14	a)	Compressions of basic Input–Output System (BIOS)/ Complementary Metal-Oxide Semiconductor (CMOS) and Master Boot Record (MBR)	L2	CO3	PO1
	b)	Explain about Persistent Software Techniques with complete details.	L6	CO3	PO1
15	a)	What is meant by Attacks against Privileged User Accounts?	L2	CO3	PO1
	b)	Write a long note on Virtual Machine Detection	L1	CO3	PO1
16	a)	What is Stealing Information and Exploitation with briefly information?	L2	CO3	PO1
	b)	Explain about Man-in-the-Middle Attacks (MITM) with examples.	L1	CO3	PO1
17	a)	Explain in complete detail of a dynamic-link library(DLL)Injection	L2	CO3	PO1
	b)	What is Browser Helper Objects with examples.	L2	CO3	PO1

your tools to success...

Dept. of CSE - CS Mr. K. SRINIVASA RAO

UNIT-V				
S. No	**Questions**	**BT**	**CO**	**PO**
Part –A (Short Answer Questions)				
1	Define a Memory Forensics.	L2	CO3	PO1
2	Write a short note on Capabilities of Memory Forensics?	L1	CO3	PO1
3	Explain about a Dumping Physical Memory.	L2	CO3	PO1
4	What is Finding Hidden Processes?	L2	CO3	PO1
5	Explain about a Volatility Analyst Pack	L2	CO3	PO1
6	What is a Memory Analysis Frameworks?	L1	CO3	PO1
7	Explain about a Honeypots.	L2	CO3	PO1
8	Write short notes on Malicious Code Naming?	L3	CO3	PO1
9	Compressions of Passive Analysis and Active Analysis.	L1	CO3	PO1
10	Explain about a Automated Malicious Code Analysis Systems.	L2	CO3	PO1
11	What is meant by Physical or Virtual Machines.	L3	CO3	PO1
12	Explain about a Intrusion Detection Systems	L1	CO3	PO1

Part– B(Long Answer Questions)					
13	a)	Explain about defense and analysis techniques with general awareness.	L2	CO3	PO1
	b)	What are the Memory Forensics in completer details?	L2	CO3	PO1
14	a)	Define and expand Capabilities of Memory Forensics.	L2	CO3	PO1
	b)	Explain about a Dumping Physical Memory with examples.	L6	CO3	PO1
15	a)	What is meant by Finding Hidden Processes	L2	CO3	PO1
	b)	Write a long note on Honeypots with examples?	L1	CO3	PO1
16	a)	What is a Malicious Code Naming with suitable examples?	L2	CO3	PO1
	b)	Explain about Automated Malicious Code Analysis Systems.	L1	CO3	PO1
17	a)	Compressions of Passive Analysis and Active Analysis with examples.	L2	CO3	PO1
	b)	What is Physical or Virtual Machines and IntrusionDetectionSystems?	L2	CO3	PO1

NRCM
your roots to success...

Dept. of CSE - CS Mr. K. SRINIVASA RAO