MARIS STELLA COLLEGE (AUTONOMOUS), VIJAYAWADA -8
(Affiliated to Krishna University, Machilipatnam)
SYLLABUS

Subject: Computer Science **Semester: V/VI**

Course Title: Cyber Security & Malware **Course Code: 20CSSEC22CM3**

No. of Hours: 45 **LTP: 300** **Credits: 3**

Objectives

- To learn the importance of computer networks and network tools.
- To describe NIST Cyber Security Framework
- To apply Malware analysis tools for various issues.

Course Outcomes

CO1: Explain the computer networks, networking tools and cyber security.
CO2: Describe about NIST Cyber Security Framework.
CO3: Explain the OWASP Vulnerabilities.
CO4: Implement various Malware analysis tools.
CO5: Explain about Information Technology act 2000.

UNIT-I (9 Hrs.)

Introduction to Networks & cyber security: Computer Network Basics • Computer network types • OSI Reference model • TCP/IP Protocol suite • Difference between OSI and TCP/IP • What is cyber, cyber-crime and cyber-security • All Layer wise attacks • Networking devices: router, bridge, switch, server, firewall • How to configure: router • How to create LAN - Programming Exercises

UNIT-II (9 Hrs.)

NIST Cyber security framework: Introduction to the components of the framework • Cyber security Framework Tiers • What is NIST Cyber security framework • Features of NIST Cyber security framework • Functions of NIST Cyber security framework • Turn the NIST Cyber security Framework into Reality/ implementing the framework - Programming Exercises.

UNIT-III (9 Hrs.)

OWASP: • What is OWASP? • OWASP Top 10 Vulnerabilities –
Injection - Broken Authentication - Sensitive Data Exposure - XML External Entities (XXE) - Broken Access Control - Security Misconfiguration - Cross-Site Scripting (XSS) - Insecure Deserialization - Using Components with Known Vulnerabilities - Insufficient Logging and Monitoring • Web application firewall - Programming Exercise.

UNIT-IV **(9 Hrs.)**

MALWARE Analysis: • What is malware • Types of malware - Key loggers - Trojans - Ran some ware - Rootkits • Antivirus • Firewalls • Malware analysis - VM ware - How to use sandbox - Process explorer - Process monitor - Programming Exercises.

UNIT-V **(9 Hrs.)**

CYBER SECURITY: Legal Perspectives • Cybercrime and the legal landscape around the world • Indian IT ACT 2000 -- Cybercrime and Punishments • Challenges to Indian law and cybercrime scenario in India - Programming Exercises.

Co-Curricular Activities

- Assignments on problem solving
- Group discussions
- Student presentations and seminars
- Online quizzes
- Project work

Prescribed Books

1. Computer Networks | Fifth Edition | By Pearson (6th Edition)|Tanenbaum, Feamster & Wetherill
2. Computer Networking | A Top-Down Approach | Sixth Edition | By Pearson | Kurose James F. Ross Keith W.
3. Cyber Security by Sunit Belapure, Nina Godbole|Wiley Publications
4. TCP/IP Protocol Suite |Mcgraw-hill| Forouzan|Fourth Edition

References

1. https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide
2. https://owasp.org/www-project-top-ten/
3. https://owasp.org/www-project-juice-shop/

MARIS STELLA COLLEGE (AUTONOMOUS), VIJAYAWADA – 8
(Affiliated to Krishna University)
Blueprint

Subject: Computer Science | **Semester: V/VI**
Course Title: Cyber Security & Malware | **Course Code: 20CSSEC22CM3**
Time: 3 Hrs. | **Max. Marks: 100**

SECTION – A

Answer **ALL** questions **20 x 1 = 20M**

Q. No.	UNIT	Marks Weightage	RBT LEVEL
1	I	1	**No. of questions to be set** RBT1 – 8 RBT2 – 8 RBT3 – 2 RBT4 – 2
2	I	1	
3	II	1	
4	II	1	
5	III	1	
6	III	1	
7	IV	1	
8	IV	1	
9	V	1	
10	V	1	
11	I	1	
12	I	1	
13	II	1	
14	II	1	
15	III	1	
16	III	1	
17	IV	1	
18	IV	1	
19	V	1	
20	V	1	

SECTION – B

Answer any **FOUR** questions **4 x 8 = 32M**

Q. No.	**UNIT**	**Marks Weightage**	**RBT LEVEL**
21	I	8	**No. of questions to be set** RBT1 – 2 RBT2 – 2 RBT3 – 1 RBT4 – 1
22	II	8	
23	III	8	
24	IV	8	
25	V	8	
26	I / II / III / IV / V	8	

SECTION – C

Answer any **FOUR** questions **4 x 12 = 48M**

Q. No.	**UNIT**	**Marks Weightage**	**RBT LEVEL**
27	I	12	**No. of questions to be set** RBT1 – 2 RBT2 – 2 RBT3 – 1 RBT4 – 1
28	II	12	
29	III	12	
30	IV	12	
31	V	12	
32	I / II / III / IV / V	12	

MARIS STELLA COLLEGE (AUTONOMOUS), VIJAYAWADA – 8
(Affiliated to Krishna University)
Model Question Paper

Subject: Computer Science	**Semester: V/VI**
Course Title: Cyber Security & Malware	**Course Code: 20CSSEC22CM3**
Time: 3 Hrs.	**Max. Marks: 100**

SECTION – A

Answer **ALL** questions **20 x 1 = 20M**

1. What is the of layers in the OSI model?
   A. 2 layers
   B. 4 layers
   C. 6 layers
   D. 7 layers

2. Identify the network which extends a private network across a public network.
   A. Virtual Private Network
   B. Storage Area Network
   C. Enterprise Private Network
   D. Local Area Network

3. When there is harm, threat, or damage to a network or system, the term is broadly known as _____________.
   A. System Hijacking
   B. Digital crime
   C. Cyber crime
   D. Cyber attack

4. Among these ___________ is the encrypted text.
   A. Secret Text
   B. Cipher Text
   C. Cipher Script
   D. Secret Script

5. Which category includes XSS in OWASP Top 10 2021?
   A. Broken Access Control
   B. Insecure Design
   C. Software and Data Integrity Failure
   D. Injection

6. In what way(s) can a XXE attack be exploited?
   A. Denial Of Service
   B. Leakage Of sensitive Data
   C. Remote Code Execution

D. Explorer

7. Which of the following malware do not replicate or reproduce through infection?

A. Worms

B. Trojans

C. Viruses

D. Rootkits

8. What is known as sandbox?

A. It is a program which can be molded to do desired task

B. It is program that is controlled or emulated section of OS

C. It is a special mode of antivirus

D. It is a special mode of firewall

9. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information?

A. Cyber attack

B. Computer security

C. Cryptography

D. Digital hacking

10. Governments hired some highly skilled hackers for providing cyber security for the country or state. These types of hackers are termed as _______.

A. Nation / State sponsored hackers

B. CIA triad

C. Special Hackers

D. Hackerthon

11. Government HackersCross Site Scripting_________ is the father of computer security.

12. ________ do Cyber attackers commonly target for fetching IP address of a target or victim user.

13. ________defines the framework core on its official website as a set of cyber security activities, desired outcomes, and applicable informative references common across critical infrastructure sectors.

14. _________ Framework Components includes three components; the Framework Core, the Framework Implementation Tiers, and the Framework Profile.

15. XSS is__________.

16. ________ are network based security measures that control the flow of incoming and outgoing traffic.

17. ______ short form of malicious software.

18. _________ are the special type of programs used for recording and tracking user’s keystroke.

19. _____________ is the full form of ITA-2000.

20. In _____________ year the Indian IT Act, 2000 got updated.

SECTION – B

Answer any **FOUR** questions **4 x 8 = 32M**

21. Explain about computer network types.
22. Discuss any 4 Networking devices.
23. Write about Cyber security Framework Tiers.
24. Analyse the OWASP Top 10 Vulnerabilities.
25. Write about the types of malware.
26. Explain the Cybercrime and the legal landscape around the world.

SECTION – C

Answer any **FOUR** questions **4 x 12 = 48M**

27. Differentiate the concepts OSI and TCP/IP models.
28. Discuss the features of NIST Cyber security framework.
29. Analyse the features of XML External Entities (XXE).
30. Elaborate about malware and firewall.
31. Discuss about Indian IT ACT 2000 and its Cybercrime and Punishments.
32. Explain the challenges to Indian law and cybercrime scenario in India