AS PER AP-CBCS SYLLABUS 2023-2024

COMPUTER APPLICATIONS(MAJOR/MINOR)

3RD YEAR – SEMESTER - V

CYBER SECURITY

(Common to All Universities in AP)

UNIT I: CYBER SECURITY FUNDAMENTALS

Network Security Concepts: Information Assurance Fundamentals, Basics of Cryptography: Symmetric and Asymmetric, DNS, Firewalls, Virtualization, Radio-Frequency Identification Microsoft Windows Security Principles: Windows Tokens, Window Messaging, Windows Program Execution, Windows Firewall

Case Study: Install any Virtualization Software and perform various tasks

UNIT – II: ATTACKER TECHNIQUES AND MOTIVATIONS

Anti forensics, Tunneling Techniques, Fraud Techniques, and Threat Infrastructure

Case Study: Working with Free and commercial proxies available from web-hack.ru.

UNIT-III: EXPLOITATION

Techniques to gain a Foothold, Misdirection, Reconnaissanse, and Disruption Methods

Case Study: Working with SQL Injection attacks and DDoS attacks

UNIT-IV: MALICIOUS CODE

Self-Replicating Malicious Code, Evading Detection and Elevating Privileges, Stealing Information and Exploitation.

Case Study: Identify latest Malwares and differentiate different types of malwares

UNIT-V: DEFENSE AND ANALYSIS TECHNIQUES

Memory Forensics, Honeypots, Malicious Code Naming, Automated Malicious Code Analysis Systems, Intrusion Detection Systems

Case Study: Identify latest Anti-Virus Softwares in the market and compare the functionality of each Anti-Virus

IMPORTANT QUESTIONS

LEVEL – 1

UNIT-I: CYBER SECURITY FUNDAMENTALS

- Discuss the fundamental concepts of Network Security and how they contribute to protecting information systems. 4
- Explain the principles of Information Assurance and their role in maintaining data integrity and availability. 7
- Differentiate between Symmetric and Asymmetric Cryptography, including their use cases and advantages. 9
- Describe the Domain Name System (DNS) and its significance in network operations and security. 12
- Analyze the function of Firewalls in network security and how they mitigate potential threats. 14
- Discuss the concept of Virtualization and its impact on enhancing cybersecurity measures. 17
- Explain how Radio-Frequency Identification (RFID) technology works and its security implications. 20
- Evaluate the challenges and best practices in implementing comprehensive cybersecurity strategies in organizations. 24

UNIT-II: ATTACKER TECHNIQUES & MOTIVATIONS

- Define Anti-Forensics and discuss various techniques used by attackers to evade detection. 37

- Explain Tunneling Techniques in cybersecurity and how they are utilized to bypass network security measures. 39
- Describe common Fraud Techniques employed in cyber attacks and their impact on individuals and organizations. 41
- Discuss the concept of Threat Infrastructure and its role in facilitating cyber attacks. 44
- Analyze the motivations behind cyber attacks and how they influence the choice of attack techniques. 46
- Evaluate the challenges faced by cybersecurity professionals in detecting and mitigating Anti-Forensics methods. 48
- Assess the effectiveness of current strategies in combating cyber fraud and suggest improvements. 53
- Propose comprehensive measures to counteract the various attacker techniques and strengthen cybersecurity defenses. 57

UNIT-III: EXPLOITATION

- Define exploitation in cybersecurity and explain its significance in the context of cyber attacks. 70
- Discuss various techniques attackers use to gain an initial foothold in a target system. 72
- Explain the concept of misdirection in cyber-attacks and how it aids attackers in evading detection. 74
- Describe the reconnaissance phase in cyber-attacks and outline the methods employed during this phase. 76
- Analyze the disruption methods used by attackers to impair or disable target systems. 79
- Discuss the importance of anti-forensics techniques in maintaining attacker anonymity and persistence. 85

- Explore the ethical implications of using deception and misdirection in cybersecurity defense strategies. 87
- Propose comprehensive measures to detect and prevent exploitation techniques in organizational networks. 89

UNIT-IV: MALICIOUS CODE

- Define malicious code and explain the characteristics of self-replicating malicious code, such as viruses and worms. 102
- Discuss various techniques employed by malicious code to evade detection by security systems. 104
- Explain the methods used by malicious code to elevate privileges within a system and the potential risks involved. 106
- Analyze how malicious code is utilized to steal sensitive information from users and organizations. 108
- Describe the lifecycle of a malicious code attack, from initial infection to exploitation. 111
- Examine the role of anti-forensics techniques in aiding malicious code to avoid detection and analysis. 115
- Discuss the challenges faced by cybersecurity professionals in detecting and mitigating advanced malicious code threats. 118
- Propose comprehensive strategies to prevent, detect, and respond to malicious code attacks in organizational environments. 122

UNIT-V: MALICIOUS CODE

- Define memory forensics and explain its role in digital investigations. 135
- Discuss the purpose and functioning of honeypots in

cybersecurity. 137
- Describe the conventions used in malicious code naming and their significance. 140
- Explain how automated malicious code analysis systems operate and their benefits. 142
- Analyze the role of intrusion detection systems (IDS) in network security. 144
- Discuss the challenges involved in memory forensics and how they can be addressed. 151
- Examine the importance of standardized naming conventions for malicious code in threat intelligence sharing. 154
- Propose a comprehensive strategy integrating memory forensics, honeypots, automated analysis, and IDS for robust cybersecurity defense. 157

LEVEL – 2

- Define Cyber Security and explain its importance in today's digital landscape. 1
- Outline the security principles of Microsoft Windows, focusing on Windows Tokens, Messaging, Program Execution, and Windows Firewall. 22

Case Study:
- Install any Virtualization Software and perform various tasks 26
- Examine the use of Tunneling Techniques in advanced persistent threats (APTs) and their implications for network security. 51

Case Study:
- Explore the components of Threat Infrastructure and how they are leveraged in orchestrating large-scale cyber attacks. 55

- Working with Free and commercial proxies available from web-hack.ru. 60
- Evaluate the role of social engineering in facilitating exploitation and gaining unauthorized access. 81
- Examine the use of tunneling techniques in cyber-attacks and their impact on network security. 83

Case Study:

- Working with SQL Injection attacks and DDoS attacks 91
- Evaluate the impact of self-replicating malicious code on network security and system performance. 113
- Explore the ethical and legal implications of deploying malicious code in cyber warfare and espionage. 119

Case Study:

- Identify latest Malwares and differentiate different types of malwares 125
- Compare and contrast host-based and network-based intrusion detection systems. 147
- Evaluate the effectiveness of honeypots in detecting and analyzing cyber threats. 149

Case Study:

- Identify latest Anti-Virus Softwares in the market and compare the functionality of each Anti-Virus 161

List of Questions

UNIT-I: CYBER SECURITY FUNDAMENTALS

LONG ANSWER QUESTIONS

1. Define Cyber Security and explain its importance in today's digital landscape. 1
2. Discuss the fundamental concepts of Network Security and how they contribute to protecting information systems. 4
3. Explain the principles of Information Assurance and their role in maintaining data integrity and availability. 7
4. Differentiate between Symmetric and Asymmetric Cryptography, including their use cases and advantages. 9
5. Describe the Domain Name System (DNS) and its significance in network operations and security. 12
6. Analyze the function of Firewalls in network security and how they mitigate potential threats. 14
7. Discuss the concept of Virtualization and its impact on enhancing cybersecurity measures. 17
8. Explain how Radio-Frequency Identification (RFID) technology works and its security implications. 20
9. Outline the security principles of Microsoft Windows, focusing on Windows Tokens, Messaging, Program Execution, and Windows Firewall. 22

10. Evaluate the challenges and best practices in implementing comprehensive cybersecurity strategies in organizations. 24

Case Study:

11. Install any Virtualization Software and perform various tasks 26

SHORT ANSWER QUESTIONS

12. Cyber Security 30
13. Network Security Concepts 30
14. Information Assurance 31
15. Symmetric Cryptography 32
16. Asymmetric Cryptography 32
17. Domain Name System (DNS) 33
18. Firewalls 34
19. Virtualization 34
20. Radio-Frequency Identification (RFID) 35
21. Windows Security Principles 36

UNIT-II: ATTACKER TECHNIQUES & MOTIVATIONS

LONG ANSWER QUESTIONS

1. Define Anti-Forensics and discuss various techniques used by attackers to evade detection. 37
2. Explain Tunneling Techniques in cybersecurity and how they are utilized to bypass network security measures. 39

3. Describe common Fraud Techniques employed in cyber attacks and their impact on individuals and organizations. 41
4. Discuss the concept of Threat Infrastructure and its role in facilitating cyber attacks. 44
5. Analyze the motivations behind cyber attacks and how they influence the choice of attack techniques. 46
6. Evaluate the challenges faced by cybersecurity professionals in detecting and mitigating Anti-Forensics methods. 48
7. Examine the use of Tunneling Techniques in advanced persistent threats (APTs) and their implications for network security. 51
8. Assess the effectiveness of current strategies in combating cyber fraud and suggest improvements. 53
9. Explore the components of Threat Infrastructure and how they are leveraged in orchestrating large-scale cyber attacks. 55
10. Propose comprehensive measures to counteract the various attacker techniques and strengthen cybersecurity defenses. 57

Case Study:

11. Working with Free and commercial proxies available from web-hack.ru. 60

SHORT ANSWER QUESTIONS

12. Anti-Forensics 63
13. Tunneling Techniques 63

14. Phishing 64
15. DNS Tunneling 65
16. Steganography 66
17. Threat Infrastructure 66
18. Motivations for Cyber Attacks 67
19. Data Wiping 68
20. Virtual Private Network (VPN) 68
21. Credential Stuffing 69

UNIT-III: EXPLOITATION

LONG ANSWER QUESTIONS

1. Define exploitation in cybersecurity and explain its significance in the context of cyber attacks. 70
2. Discuss various techniques attackers use to gain an initial foothold in a target system. 72
3. Explain the concept of misdirection in cyber-attacks and how it aids attackers in evading detection. 74
4. Describe the reconnaissance phase in cyber-attacks and outline the methods employed during this phase. 76
5. Analyze the disruption methods used by attackers to impair or disable target systems. 79
6. Evaluate the role of social engineering in facilitating exploitation and gaining unauthorized access. 81

7. Examine the use of tunneling techniques in cyber-attacks and their impact on network security. 83
8. Discuss the importance of anti-forensics techniques in maintaining attacker anonymity and persistence. 85
9. Explore the ethical implications of using deception and misdirection in cybersecurity defense strategies. 87
10. Propose comprehensive measures to detect and prevent exploitation techniques in organizational networks. 89

Case Study:

11. Working with SQL Injection attacks and DDoS attacks 91

SHORT ANSWER QUESTIONS

12. Exploitation 95
13. Initial Foothold 95
14. Misdirection 96
15. Reconnaissance 97
16. Disruption Methods 97
17. Social Engineering 98
18. Tunneling Techniques 98
19. Anti-Forensics 99
20. Phishing 99
21. Denial of Service (DoS) 100

UNIT-IV: MALICIOUS CODE

LONG ANSWER QUESTIONS

1. Define malicious code and explain the characteristics of self-replicating malicious code, such as viruses and worms. 102
2. Discuss various techniques employed by malicious code to evade detection by security systems. 104
3. Explain the methods used by malicious code to elevate privileges within a system and the potential risks involved. 106
4. Analyze how malicious code is utilized to steal sensitive information from users and organizations. 108
5. Describe the lifecycle of a malicious code attack, from initial infection to exploitation. 111
6. Evaluate the impact of self-replicating malicious code on network security and system performance. 113
7. Examine the role of anti-forensics techniques in aiding malicious code to avoid detection and analysis. 115
8. Discuss the challenges faced by cybersecurity professionals in detecting and mitigating advanced malicious code threats. 118
9. Explore the ethical and legal implications of deploying malicious code in cyber warfare and espionage. 119

10. Propose comprehensive strategies to prevent, detect, and respond to malicious code attacks in organizational environments. 122

Case Study:

11. Identify latest Malwares and differentiate different types of malwares 125

SHORT ANSWER QUESTIONS

12. Malicious Code 127
13. Self-Replicating Malware 128
14. Code Obfuscation 129
15. Privilege Escalation 130
16. Information Stealer 130
17. Sandbox Evasion 131
18. Keylogger 131
19. Trojan Horse 132
20. Rootkit 133
21. Backdoor 133

UNIT-V: MALICIOUS CODE

LONG ANSWER QUESTIONS

1. Define memory forensics and explain its role in digital investigations. 135
2. Discuss the purpose and functioning of honeypots in cybersecurity. 137
3. Describe the conventions used in malicious code naming and their significance. 140

4. Explain how automated malicious code analysis systems operate and their benefits. 142
5. Analyze the role of intrusion detection systems (IDS) in network security. 144
6. Compare and contrast host-based and network-based intrusion detection systems. 147
7. Evaluate the effectiveness of honeypots in detecting and analyzing cyber threats. 149
8. Discuss the challenges involved in memory forensics and how they can be addressed. 151
9. Examine the importance of standardized naming conventions for malicious code in threat intelligence sharing. 154
10. Propose a comprehensive strategy integrating memory forensics, honeypots, automated analysis, and IDS for robust cybersecurity defense. 157

Case Study:

11. Identify latest Anti-Virus Softwares in the market and compare the functionality of each Anti-Virus 161

SHORT ANSWER QUESTIONS

12. Memory Forensics 164
13. Honeypot 165
14. Malicious Code Naming 165
15. Automated Malware Analysis 166
16. Intrusion Detection System (IDS) 166
17. Host-Based IDS 167
18. Network-Based IDS 168

19. Signature-Based Detection 168
20. Anomaly-Based Detection 169
21. Threat Intelligence 170