

**UNIVERSITY EXAMINATIONS: 2022/2023**

**EXAMINATIONS FOR THE DEGREE OF BACHELOR OF SCIENCE IN INFORMATION SECURITY AND FORENSICS/ BACHELOR OF SCIENCE IN APPLIED COMPUTING**

**BAC 3213/ BISF 3204/: ETHICAL HACKING FULL TIME/PART TIME**

**DATE: DECEMBER, 2022 TIME: 2 HOURS**

**INSTRUCTIONS:** Answer **QUESTION ONE and ANY OTHER TWO** questions.

# QUESTION ONE – COMPULSORY [20 MARKS]

1. **Discuss the different ways of classifying malware and the motivations for each class of malware. 6 Marks**
2. **Behavior-based classification:** This classification is based on how the malware behaves and what it is designed to do. For example, viruses, worms, Trojans, ransomware, spyware, adware, and rootkits are different types of malware with distinct behaviors.
3. **Propagation-based classification:** This classification is based on how the malware spreads. Malware can propagate through various means, including email, removable media, peer-to-peer networks, social engineering, and software vulnerabilities.
4. **Target-based classification:** This classification is based on the intended victim of the malware. Some malware is designed to attack specific industries or groups, such as banking malware, while others are more general-purpose and can affect anyone.
5. **Sophistication-based classification:** This classification is based on the level of technical expertise required to create the malware. Some malware is relatively simple, while others are highly sophisticated and require advanced knowledge of programming and computer systems.
6. **Classification by payload:** This classification is based on the malicious actions that the malware performs on an infected system. For example, some malware is designed to steal sensitive data, while others are used to control a compromised system.
7. **Classification by target:** This classification is based on the intended victim of the malware. Some malware is designed to target specific industries, such as finance or healthcare, while others are more broadly targeted.
8. **Classification by platform:** This classification is based on the operating system or platform that the malware targets. For example, some malware is designed specifically for Windows systems, while others target mobile devices or IoT devices.
9. **Classification by origin:** This classification is based on the source of the malware, such as whether it was created by a government agency or a criminal organization.
10. **Discuss in detail each of the top information security attack vectors. 8 Marks**
11. **Phishing:** This is a social engineering technique that involves tricking individuals into providing sensitive information or clicking on a malicious link. Phishing attacks are often carried out through email, but can also occur through text messages or phone calls.
12. **Malware:** Malware is any malicious software that can harm computer systems or steal sensitive data. Malware can be delivered through a variety of means, including email attachments, infected websites, and social engineering techniques.
13. **Denial of Service (DoS) attacks:** These attacks involve overwhelming a computer system with traffic, making it inaccessible to users. DoS attacks can be carried out through botnets, which are networks of infected computers controlled by the attacker.
14. **Man-in-the-middle (MitM) attacks:** These attacks involve intercepting communications between two parties and stealing or altering the information being transmitted. MitM attacks can be carried out through various means, including WiFi network spoofing or DNS hijacking.
15. **SQL injection:** This is a type of web application attack that involves injecting malicious SQL code into a website's input fields to gain unauthorized access to the website's database. SQL injection attacks can be used to steal sensitive data or to modify or delete data in the database.
16. **Discuss in any four techniques that attackers use to cover their tracks on the target system. 4 Marks**
17. **Encryption:** Attackers may use encryption to conceal their activities or the data they have stolen from the victim's system.
18. **Steganography:** This technique involves hiding data within other files or data to avoid detection. For example, an attacker may hide data within an image file.
19. **Rootkits:** A rootkit is a type of malware that allows an attacker to gain persistent access to a system while hiding their presence from the victim. Rootkits can be difficult to detect and remove.
20. **Anti-forensics tools:** These are specialized tools that can be used to delete or modify log files, erase disk space, or otherwise cover an attacker's tracks on a system.
21. **Why is ethical hacking necessary? 2 Marks**

Ethical hacking is necessary because it helps organizations identify vulnerabilities in their computer systems and networks before attackers can exploit them. By using ethical hacking techniques, organizations can proactively identify and fix security weaknesses, reducing the risk of data breaches, financial loss, and damage to their reputation. Ethical hacking also helps organizations comply with regulatory requirements and best practices for information security. Additionally, ethical hacking can improve the overall security posture of an organization, making it more resilient to future attacks.

# QUESTION TWO [15 MARKS]

1. **Using real world examples, discuss in the different categories of indicators of compromise. 6 Marks**

Indicators of compromise (IOCs) are signs that a security breach has occurred or that a system has been compromised by malware or unauthorized access. There are different categories of IOCs, including:

1. **Network IOCs:** These are signs of network traffic that may indicate a security breach. Examples include unusual network traffic patterns or connections to known malicious IP addresses. For example, the WannaCry ransomware outbreak in 2017 was detected through the presence of network IOCs.
2. **Host-based IOCs:** These are signs of activity on an individual system that may indicate a security breach. Examples include changes to system files, unexpected system shutdowns, or the presence of unauthorized software. For example, the detection of a suspicious file on a system could be a host-based IOC.
3. **Behavioral IOCs:** These are signs of unusual or unexpected behavior on a system or network. Examples include large amounts of data being transferred to an external location or user accounts being created with unusual privileges. For example, detecting an unusual pattern of user activity on a network could be a behavioral IOC.
4. **Discuss in detail the Threat Modeling Process steps. 6 Marks**

The threat modeling process is a systematic approach to identifying and assessing potential security threats to a system or organization. The steps in this process are:

1. **Define the system:** Identify the scope of the system to be analyzed, including its components, boundaries, and functions.
2. **Identify threats:** Identify potential threats to the system, including both internal and external threats. This can be done through brainstorming or by using threat intelligence sources.
3. **Identify assets:** Identify the assets that are at risk, including data, hardware, software, and personnel.
4. **Identify vulnerabilities:** Identify the weaknesses in the system that could be exploited by a threat actor, including technical vulnerabilities and human factors.
5. **Assess risks:** Assess the likelihood and potential impact of each identified threat, taking into account the assets and vulnerabilities.
6. **Develop mitigations:** Develop a set of mitigations to address the identified risks, including technical controls, policies, and procedures.
7. **Prioritize:** Prioritize the mitigations based on the level of risk and available resources.
8. **Describe the roles of the people that are involved in incident management. 3 Marks**
9. **Incident manager:** The incident manager is responsible for coordinating the incident response team, communicating with stakeholders, and ensuring that the incident is resolved as quickly and effectively as possible.
10. **Technical experts:** Technical experts provide expertise in areas such as network security, malware analysis, and forensic analysis. They are responsible for identifying the root cause of the incident and developing technical solutions.
11. **Communications specialist:** The communications specialist is responsible for managing communications both internally and externally during an incident. This includes notifying stakeholders, providing updates, and managing the public relations aspect of the incident.

# QUESTION THREE [15 MARKS]

1. **Describe the steps an attacker follows to hack a network using sniffers. 5 Marks**
2. **Identify the target network:** The attacker identifies the network they want to attack, usually by scanning for vulnerable systems.
3. **Gain access to the network:** The attacker gains access to the network, either by exploiting a vulnerability or by using a stolen credential.
4. **Install the sniffer:** The attacker installs the sniffer tool on the compromised system, which allows them to intercept and analyze network traffic.
5. **Monitor network traffic:** The attacker monitors the network traffic for sensitive information, such as usernames and passwords, credit card numbers, or other confidential data.
6. **Steal data:** Once the attacker has identified sensitive data, they can use the sniffer to steal the information and use it for malicious purposes.
7. **Discuss the techniques you will use in defending your network against sniffing.**

## **6 Marks**

1. **Encryption:** Use encryption technologies to encrypt sensitive data in transit, making it harder for attackers to read the traffic they intercept.
2. **Network segmentation:** Segment the network into smaller, isolated subnets, so that even if one subnet is compromised, the attacker will have limited access to the rest of the network.
3. **Use secure protocols:** Use secure protocols, such as HTTPS or SSL/TLS, to transmit sensitive data over the network.
4. **Implement network monitoring:** Implement network monitoring tools to detect unusual traffic patterns and identify potential sniffing attacks.
5. **Use intrusion detection and prevention systems:** Implement intrusion detection and prevention systems to detect and block malicious traffic, including traffic generated by sniffers.
6. **Strong access control:** Implement strong access control measures, such as two-factor authentication, to prevent unauthorized access to the network.
7. **Explain any four processes that help in achieving information assurance. 4 Marks**
8. **Risk assessment:** Conducting a risk assessment helps to identify potential threats and vulnerabilities to the organization's information assets. It involves identifying the assets, analyzing the threats, and assessing the risks.
9. **Security policy development:** Developing security policies and procedures helps to establish guidelines for protecting information assets. Policies should cover areas such as access control, data backup, and incident response.
10. **Training and awareness:** Providing regular training and awareness programs to employees helps to ensure that everyone understands their role in protecting the organization's information assets. This includes topics such as password security, phishing, and social engineering.
11. **Continuous monitoring:** Implementing continuous monitoring tools and techniques helps to detect and respond to security incidents in real-time. This includes monitoring network traffic, log files, and security alerts.

# QUESTION FOUR [15 MARKS]

1. **Discuss the challenges you would expect to encounter in your role as an Ethical Hacker. 4 Marks**
2. **Legal and ethical considerations:** Ethical hackers must operate within legal and ethical boundaries, and must ensure that their activities do not harm the organization they are hired to protect.
3. **Scope limitations:** Ethical hackers must work within the scope of their engagement, which may limit their ability to identify all vulnerabilities.
4. **Complexity of systems:** Modern systems are complex, and ethical hackers must have a deep understanding of various technologies and platforms to be effective.
5. **Evolving threat landscape:** The threat landscape is constantly evolving, and ethical hackers must keep up with the latest techniques and tools used by attackers.
6. **Discuss the methodology you would follow in compromising WLANs. 7 Marks**
7. **Reconnaissance:** Gather information about the target WLAN, such as the network name (SSID), encryption type, and MAC address filtering.
8. **Enumeration:** Identify the wireless access points (APs) and client devices connected to the WLAN, and determine their operating systems and versions.
9. **Scanning:** Use tools such as NetStumbler, Kismet, or Aircrack-ng to scan for wireless networks and access points.
10. **Exploitation:** Exploit any vulnerabilities in the wireless network, such as weak encryption, default passwords, or unpatched software.
11. **Persistence:** Maintain access to the WLAN by creating backdoors or installing remote access tools.
12. **Covering tracks:** Erase evidence of the attack, such as log files or network traffic.
13. **What are the special challenges that wireless networks pose to security professionals compared to wired networks while trying to defend their systems. 4 Marks**
14. **Eavesdropping:** Wireless signals can be intercepted and eavesdropped on, allowing attackers to capture sensitive information.
15. **Rogue access points:** Attackers can set up rogue access points to trick users into connecting to their network and stealing sensitive information.
16. **Unauthorized devices:** Wireless networks are more susceptible to unauthorized devices connecting to the network, such as smartphones or laptops brought in from outside the organization.
17. **Signal leakage:** Wireless signals can leak outside the physical boundaries of the organization, making it harder to control access to the network.