

**UNIVERSITY EXAMINATIONS: 2021/2022**

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

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

**DATE: DECEMBER, 2021 TIME: 2 HOURS**

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

**QUESTION ONE – COMPULSORY [20 MARKS]**

1. **Discuss in detail each of the phases of the hacking cycle. 5 Marks**
2. **Reconnaissance:** In this phase, the attacker gathers information about the target system or network. This can be done through passive or active reconnaissance methods. Passive reconnaissance involves gathering information from publicly available sources such as social media, websites, and other open sources. Active reconnaissance involves actively scanning the target network or system for vulnerabilities, open ports, and services.
3. **Scanning:** In this phase, the attacker scans the target network or system to identify vulnerabilities and weaknesses. This can be done using automated tools such as port scanners and vulnerability scanners, or manual methods such as analyzing network traffic and system logs.
4. **Gaining access:** In this phase, the attacker exploits the vulnerabilities identified in the previous phase to gain unauthorized access to the target system or network. This can be done using a variety of methods, including exploiting software vulnerabilities, brute force attacks, and social engineering.
5. **Maintaining access:** Once the attacker has gained access to the target system or network, they try to maintain access for as long as possible. This can be done by installing backdoors, creating user accounts, and modifying system files.
6. **Covering tracks:** In this phase, the attacker tries to cover their tracks by deleting logs, modifying system files, and erasing any evidence of their presence on the target system or network.
7. **Explain the goals and techniques used in system hacking for the following phases:**
   1. **Gaining access 2 Marks**

The goal of this phase is to gain unauthorized access to the target system or network. This can be done using techniques such as exploiting software vulnerabilities, brute force attacks, and social engineering. Techniques used in this phase include port scanning, network sniffing, and password cracking.

* 1. **Escalating privileges 2 Marks**

Once the attacker has gained access to the target system or network, the goal of this phase is to escalate their privileges to gain access to more sensitive data or systems. This can be done by exploiting vulnerabilities in the operating system or applications, or by using social engineering techniques to trick system administrators into granting them higher privileges. Techniques used in this phase include privilege escalation exploits, password cracking, and social engineering.

* 1. **Executing applications 2 Marks**

Once the attacker has escalated their privileges, they can execute applications to steal data or take control of the target system or network. This can be done using malware such as keyloggers, backdoors, and remote access trojans (RATs). Techniques used in this phase include exploiting vulnerabilities in applications, social engineering, and using phishing emails to distribute malware.

1. **Explain briefly any five information technology attack vectors. 5 Marks**

Information technology attack vectors are methods used by attackers to exploit vulnerabilities in IT systems. Here are five examples:

1. **Phishing attacks:** This involves sending fake emails or messages to trick users into revealing sensitive information or clicking on a link that downloads malware onto their system.
2. **SQL injection:** This involves inserting malicious SQL code into a web form or application to gain unauthorized access to a database.
3. **Denial of Service (DoS) attacks:** This involves overwhelming a target system or network with traffic to make it unavailable to legitimate users.
4. **Social engineering:** This involves tricking people into revealing sensitive information or performing actions that they wouldn't normally do, such as downloading malware or giving away passwords.
5. **Man-in-the-middle (MitM) attacks:** This involves intercepting and altering data as it passes between two parties, allowing the attacker to steal sensitive information or gain unauthorized access to a system.
6. **Explain briefly the any four reasons why penetration testing is conducted 4 Marks**
7. To identify vulnerabilities in a system or network before attackers can exploit them. Penetration testing involves simulating an attack on a system or network to identify weaknesses and vulnerabilities that attackers could exploit. By conducting a penetration test, organizations can proactively identify security weaknesses and take corrective action before an actual attack occurs.
8. To test the effectiveness of security controls and procedures. By conducting simulated attacks, organizations can identify gaps in their security controls and make improvements to better protect their systems and data.
9. To comply with regulatory requirements or industry standards. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires regular penetration testing of systems that store or process credit card data.
10. To evaluate the security of third-party vendors or partners. By conducting a penetration test on a third-party system, organizations can ensure that their data is not at risk due to vulnerabilities in the third-party's systems.
11. To provide assurance to stakeholders that the organization's systems and data are secure. By conducting regular penetration testing, organizations can demonstrate their commitment to security and provide assurance to customers, investors, and other stakeholders that their systems and data are protected from attack.

**QUESTION TWO [15 MARKS]**

1. **Discuss in detail the methodology you would follow in conducting a vulnerability assessment of an organization. 8 Marks**
2. **Planning and Preparation:** The first step is to plan and prepare for the assessment, which includes identifying the assets that need to be assessed, the scope of the assessment, the methodology to be used, and the team that will conduct the assessment. The team should consist of experienced security professionals with the necessary skills and knowledge to identify and assess vulnerabilities.
3. **Scanning:** The next step is to conduct a vulnerability scan of the organization's network, applications, and systems. This is done using automated tools that scan the network for known vulnerabilities. The scan should be conducted from both internal and external perspectives to identify vulnerabilities that can be exploited by an attacker.
4. **Vulnerability Assessment:** Once the scan is complete, the vulnerabilities identified need to be assessed. This involves analyzing the results of the scan to determine the severity of the vulnerabilities, the likelihood of exploitation, and the potential impact of an attack. The assessment should be conducted by experienced security professionals who can provide an accurate assessment of the risk posed by each vulnerability.
5. **Reporting:** The next step is to report the findings of the vulnerability assessment to the relevant stakeholders. This includes a detailed report that outlines the vulnerabilities identified, their severity, and recommendations for remediation. The report should be presented in a way that is easily understood by both technical and non-technical stakeholders.
6. **Remediation:** The final step is to remediate the vulnerabilities identified during the assessment. This involves implementing the recommended fixes and patches to ensure that the organization's systems, networks, and applications are secure. Remediation should be done as quickly as possible to minimize the risk of exploitation.
7. **Discuss the activities in each of the phases of penetration testing. 7 Marks**
8. **Planning:** The first phase of penetration testing is planning, which involves defining the scope of the test, identifying the systems and applications to be tested, and creating a testing plan. The testing plan should define the testing methodology, the tools to be used, and the timelines for the test.
9. **Information Gathering:** The next phase is information gathering, which involves collecting as much information as possible about the organization's systems, networks, and applications. This includes identifying the IP addresses, network architecture, and system configurations. The information gathering phase is critical as it provides the tester with the necessary information to conduct the test effectively.
10. **Vulnerability Assessment:** The vulnerability assessment phase involves identifying vulnerabilities in the organization's systems, networks, and applications. This is done using a variety of tools and techniques, including network scanners, port scanners, vulnerability scanners, and manual testing. The objective of this phase is to identify all vulnerabilities that could be exploited by an attacker.
11. **Exploitation:** Once vulnerabilities have been identified, the exploitation phase begins. This involves attempting to exploit the vulnerabilities identified during the vulnerability assessment phase. The objective is to determine the level of access that an attacker could gain if the vulnerability were successfully exploited.
12. **Reporting:** The reporting phase involves creating a detailed report that outlines the findings of the penetration test. The report should include details of the vulnerabilities identified, the severity of each vulnerability, and recommendations for remediation. The report should be presented in a way that is easily understood by both technical and non-technical stakeholders.
13. **Remediation:** The final phase is remediation, which involves implementing the recommended fixes and patches identified during the penetration testing process. The objective of this phase is to ensure that the organization's systems, networks, and applications are secure and that the vulnerabilities identified during the test have been remediated. Remediation should be done as quickly as possible to minimize the risk of exploitation.
14. **Verification:** After the remediation phase, the verification phase begins. This involves retesting the organization's systems, networks, and applications to ensure that the vulnerabilities identified during the initial test have been successfully remediated. The objective is to ensure that the remediation efforts have been effective and that the organization's systems are now secure.

**QUESTION THREE [15 MARKS]**

1. **Explain in detail the Web Server attack methodology. 5 Marks**
2. **Footprinting and reconnaissance:** Attackers gather information about the target web server, such as the IP address, the operating system, and the applications running on the server. They also gather information about the web application and any vulnerabilities that may be present.
3. **Scanning:** Attackers scan the web server to identify open ports, services, and applications. This is done using automated tools that scan for known vulnerabilities and weaknesses in the web server.
4. **Enumeration:** Attackers use enumeration techniques to identify the users, groups, and resources on the web server. This is done to gather information that can be used to launch further attacks.
5. **Exploitation:** Once vulnerabilities have been identified, attackers attempt to exploit them to gain access to the web server. This can be done using a variety of techniques, such as cross-site scripting (XSS), SQL injection, and remote file inclusion (RFI).
6. **Privilege escalation:** If the attacker gains access to the web server, they may attempt to escalate their privileges to gain access to sensitive information or other resources on the server.
7. **Maintaining access:** Once access has been gained, attackers may install backdoors or other malicious software to maintain access to the web server.
8. **Discuss in detail the SQL injection methodology 6 Marks**
9. **Reconnaissance:** The attacker gathers information about the target web application, such as the URL, parameters, and input fields.
10. **Identification:** The attacker identifies the input fields that are vulnerable to SQL injection attacks.
11. **Exploitation:** The attacker injects SQL code into the vulnerable input fields to manipulate the database and retrieve sensitive information or perform unauthorized actions.
12. **Escalation:** If the attacker gains access to the database, they may attempt to escalate their privileges to gain access to sensitive information or other resources on the server.
13. **Maintaining access:** Once access has been gained, attackers may install backdoors or other malicious software to maintain access to the database.
14. **Explain briefly any four scanning methods used to find vulnerable machines.**

**4 Marks**

1. **Port scanning:** Port scanning involves scanning a network or system for open ports. This is done using automated tools that scan for known vulnerabilities and weaknesses in the network or system.
2. **Vulnerability scanning:** Vulnerability scanning involves using automated tools to scan for vulnerabilities in the network or system. This can include scanning for known software vulnerabilities, misconfigurations, or weak passwords.
3. **Banner grabbing:** Banner grabbing involves retrieving information about the target system or application by examining the response headers from the server. This can be useful in identifying the type of server, the version of software running, and other information that can be used to launch further attacks.
4. **Operating system fingerprinting:** Operating system fingerprinting involves identifying the type and version of the operating system running on a target system. This can be useful in identifying vulnerabilities that are specific to the operating system and in determining the best methods for exploitation.

**QUESTION FOUR [15 MARKS]**

1. **Discuss the necessity for Ethical Hacking. 3 Marks**
2. **Identifying vulnerabilities:** Ethical hacking can help organizations identify vulnerabilities in their systems and networks before attackers can exploit them. This can help organizations improve their security posture and prevent potential breaches.
3. **Compliance:** Many organizations are required to comply with security standards and regulations, such as PCI DSS, HIPAA, and GDPR. Ethical hacking can help organizations identify vulnerabilities and ensure that they are in compliance with these standards.
4. **Incident response:** Ethical hacking can be used to test an organization's incident response capabilities. By simulating a real-world attack, ethical hackers can help organizations identify gaps in their incident response plans and improve their ability to respond to security incidents.
5. **Discuss the technical and non-technical skills of an Ethical Hacker. 6 Marks**

Technical skills of an ethical hacker include:

1. Proficiency in programming languages such as Python, C, C++, and Java
2. Knowledge of networking protocols such as TCP/IP, DNS, HTTP, and SMTP
3. Understanding of operating systems such as Windows, Linux, and MacOS
4. Knowledge of penetration testing tools such as Nmap, Metasploit, and Burp Suite
5. Familiarity with web application security and common vulnerabilities such as SQL injection and cross-site scripting (XSS)

Non-technical skills of an ethical hacker include:

1. Excellent communication skills to effectively communicate findings to clients or management
2. Strong analytical and problem-solving skills to identify and assess vulnerabilities in systems and networks
3. Ability to work well independently or as part of a team
4. Good time management and organizational skills to manage multiple projects and deadlines
5. High ethical standards and the ability to maintain confidentiality and trust with clients.
6. **Discuss the methodology you would follow in discovering WiFi networking using Wardriving. 6 Marks**

Wardriving is the act of driving around a geographic area while scanning for wireless access points or WiFi networks. The methodology for discovering WiFi networks using wardriving typically involves the following steps:

1. **Planning:** Identify the geographic area to be covered and plan the route for driving. This can be done using online mapping tools.
2. **Preparation:** Prepare the wardriving equipment, which typically includes a laptop or mobile device with WiFi scanning software installed.
3. **Scanning:** Drive around the target area while scanning for WiFi networks. This can be done using automated tools that scan for open wireless access points and record their location, SSID, and other information.
4. **Mapping:** Record the location and other information about the discovered WiFi networks on a map. This can be done using online mapping tools or specialized mapping software.
5. **Analysis:** Analyze the data collected during the wardriving exercise to identify patterns, trends, and potential security vulnerabilities. This can include identifying open wireless access points or networks with weak encryption or default passwords.
6. **Reporting:** Create a report of the findings and recommendations for improving the security of the WiFi networks discovered during the wardriving exercise. This report should be communicated to the organization or individual responsible for the WiFi networks.