**KCA UNIVERSITY**

**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, 5206/ BISF 3204: ETHICAL HACKING**

**FULL TIME/PART TIME**

**ORDINARY EXAMINATION**

**DATE: APRIL, 2023 TIME: 2 HOURS**

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

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

1. **Discuss any six different attack vectors that a modern organization has to contend with. 6 Marks**
2. **Phishing Attacks**: Phishing involves sending deceptive emails or messages to trick users into revealing sensitive information like login credentials, credit card numbers, or personal data. It often includes malicious links or attachments.
3. **Malware Attacks**: Malware, such as viruses, worms, Trojans, and ransomware, can infect systems through various means like malicious downloads, infected USB drives, or exploit kits, compromising data, and system integrity.
4. **Distributed Denial of Service (DDoS) Attacks**: DDoS attacks overwhelm a target's resources by flooding it with an excessive amount of traffic from multiple sources, rendering the service inaccessible. This disrupts operations and impacts business continuity.
5. **Man-in-the-Middle (MitM) Attacks**: In a MitM attack, an attacker intercepts and possibly alters communications between two parties without their knowledge. This can lead to data theft, unauthorized access, or eavesdropping.
6. **SQL Injection Attacks**: Attackers inject malicious SQL queries into input fields of a web application to manipulate databases and gain unauthorized access to sensitive data. Poorly sanitized user inputs are often exploited.
7. **Social Engineering Attacks**: Social engineering exploits human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security. This can involve pretexting, baiting, or tailgating.
8. **Discuss in detail the security tools you would use in ensuring your web servers are secure. 6 Marks**
9. **Web Application Firewalls (WAF)**: WAFs filter and monitor incoming traffic to web applications, blocking malicious requests and protecting against vulnerabilities like SQL injection, cross-site scripting (XSS), and more.
10. **Intrusion Detection and Prevention Systems (IDPS)**: IDPS monitor network traffic, identifying and responding to suspicious activities or attacks in real-time. They can prevent attacks or alert administrators.
11. **Vulnerability Scanners**: These tools scan web applications and servers for known vulnerabilities. They identify weak points that attackers could exploit and provide recommendations for remediation.
12. **Security Information and Event Management (SIEM)**: SIEM systems collect and analyze log data from various sources to detect and respond to security incidents. They help in monitoring server activity and identifying anomalies.
13. **Patch Management Tools**: These tools help ensure that operating systems, software, and applications are up-to-date with the latest security patches, minimizing the risk of exploitation through known vulnerabilities.
14. **Penetration Testing Tools**: Penetration testing tools simulate real-world attacks to identify vulnerabilities. They provide insights into the effectiveness of security measures and suggest improvements.
15. **Explain in detail the Web Server attack methodology. 5 Marks**
16. **Reconnaissance**: Attackers gather information about the target web server, its architecture, technologies, and potential vulnerabilities. This can involve passive methods like searching online resources or active methods like DNS enumeration.
17. **Scanning**: Attackers use various scanning techniques to identify open ports, services, and potential entry points. Tools like Nmap are commonly used to discover network details and potential vulnerabilities.
18. **Gaining Access**: Once potential vulnerabilities are identified, attackers attempt to exploit them. This could involve exploiting weak authentication mechanisms, known vulnerabilities, or misconfigurations.
19. **Maintaining Access**: After gaining access, attackers aim to maintain their control. They might install backdoors, rootkits, or other malicious software to ensure persistent access even if the initial entry point is discovered and closed.
20. **Covering Tracks**: Attackers try to erase evidence of their presence by deleting logs, altering timestamps, and generally obscuring their activities to evade detection.
21. **Exfiltration**: If the goal is data theft, attackers will attempt to transfer sensitive information from the compromised server to their own systems.
22. **Explain briefly any three scanning methods used to find vulnerable machines. 3 Marks**
23. **Port Scanning**: Port scanning involves sending packets to a range of ports on a target system to identify which ports are open, closed, or filtered. This helps attackers determine potential entry points and services running on the target.
24. **Vulnerability Scanning**: Vulnerability scanners scan systems for known vulnerabilities by comparing their configurations and software versions against a database of known vulnerabilities. This helps identify weak points that could be exploited.
25. **Network Scanning**: Network scanning involves mapping out the network architecture, identifying hosts, services, and their interconnections. It provides attackers with insights into potential pathways for exploitation.

**QUESTION TWO [15 MARKS]**

1. **Discuss the factors you would consider in selecting an appropriate penetration testing type. 5 Marks**
2. **Scope and Goals**: Define the scope of the penetration test and the goals you want to achieve. Are you focusing on a specific application, network, or system? The type of penetration test should align with these objectives.
3. **Regulatory Compliance**: Consider any industry regulations or compliance standards that require specific types of testing. For instance, if you're in the healthcare sector, HIPAA compliance might dictate the type of testing needed.
4. **Risk Tolerance**: Evaluate your organization's risk tolerance. Some penetration tests might involve more aggressive techniques that carry a higher risk of disrupting systems. Choose a type that aligns with your risk appetite.
5. **Level of Knowledge**: Consider the knowledge level of the testers. If you're conducting an internal test with your own team, more advanced techniques might be suitable. For external tests, simpler methods might be preferable.
6. **Time and Resources**: The depth and complexity of penetration testing types can vary. Consider the time and resources available for the testing. A comprehensive test might take longer than a targeted test.
7. **Discuss in detail the system hacking goals and tools and techniques used during gaining access, escalating privileges, executing applications and hiding files. 8 Marks**
8. **Gaining Access**:

* **Goal**: The primary goal is to gain unauthorized access to the target system or network.
* **Tools & Techniques**: Attackers might use password cracking tools (e.g., John the Ripper, Hydra) to guess or crack passwords. Exploiting vulnerabilities in software (e.g., Metasploit) is another approach.

1. **Escalating Privileges**:

* **Goal**: Once access is gained, attackers seek to elevate their privileges to gain administrative control.
* **Tools & Techniques**: Attackers might exploit privilege escalation vulnerabilities (e.g., Windows UAC bypass), manipulate access controls, or abuse misconfigurations to gain higher privileges.

1. **Executing Applications**:

* **Goal**: Attackers might want to run their malicious applications or scripts on the compromised system.
* **Tools & Techniques**: Attackers can use remote access Trojans (RATs), remote code execution vulnerabilities, or backdoors to execute their code on the system.

1. **Hiding Files**:

* **Goal**: Attackers often want to maintain persistence and hide their malicious files.
* **Tools & Techniques**: Rootkits, which modify the operating system to hide malicious files, are commonly used. Attackers might also use steganography to hide data within seemingly innocuous files.

**c) Differentiate between Ethical Hacking and penetration Testing. 2 Marks**

**Ethical Hacking**: Ethical hacking involves simulating real-world cyberattacks to identify vulnerabilities and weaknesses in a system or network. The goal is to discover and fix security flaws before malicious hackers can exploit them. Ethical hackers use the same techniques as malicious hackers but with permission and for the purpose of improving security.

**Penetration Testing**: Penetration testing is a subset of ethical hacking. It focuses on assessing the security of specific systems, applications, or networks by simulating attacks. Penetration testers attempt to exploit vulnerabilities to gain unauthorized access, escalate privileges, and identify potential consequences. The results of penetration tests help organizations understand their security posture and make improvements.

In essence, while ethical hacking is a broader concept that includes all types of security testing carried out with permission, penetration testing specifically involves controlled attacks to evaluate the security of specific targets.

**QUESTION THREE [15 MARKS]**

1. **Discuss in detail how you would defend against SQL injection attacks 6Marks**

SQL injection attacks occur when an attacker injects malicious SQL queries into input fields of a web application. These attacks can lead to unauthorized access, data leakage, and potential manipulation of the database. To defend against SQL injection attacks, consider the following measures:

1. **Input Validation and Sanitization**: Validate and sanitize user inputs before passing them to the database. Use whitelisting to allow only expected characters and reject any input containing potentially harmful characters.
2. **Prepared Statements**: Use parameterized queries or prepared statements provided by your programming language or framework. This separates SQL code from user inputs, making it difficult for attackers to inject malicious code.
3. **Stored Procedures**: Implement stored procedures in your database to encapsulate SQL logic. This restricts the direct execution of arbitrary SQL queries from user inputs.
4. **ORMs (Object-Relational Mapping)**: Use ORM frameworks that generate safe SQL queries based on high-level programming constructs. These frameworks often provide built-in protection against SQL injection.
5. **Least Privilege Principle**: Limit the database user's privileges to only the necessary actions. This reduces the potential damage an attacker can do even if they manage to execute SQL queries.
6. **Web Application Firewall (WAF)**: Deploy a WAF that can detect and block malicious SQL injection attempts by analyzing incoming traffic patterns.
7. **With the aid of a relevant diagram, describe the steps involved in conducting lawful interception. 6 Marks**

Lawful interception refers to the legally authorized interception of communications, often carried out by law enforcement agencies for surveillance purposes. Below are the steps involved:

1. **Authorization Request**: Law enforcement agencies initiate the process by obtaining legal authorization to intercept specific communication targets.
2. **Interception Setup**: Once authorized, the interception process is set up at the service provider's network. This involves configuring monitoring points for the target communication.
3. **Monitoring and Collection**: The authorized communications are monitored and collected in real-time. This can include voice calls, text messages, and internet data.
4. **Filtering and Processing**: Collected data is filtered to extract relevant information related to the authorized interception. Irrelevant data is discarded.
5. **Delivery to LEA**: Extracted data is delivered securely to the requesting law enforcement agency (LEA), where it is stored and analyzed as required.
6. **Data Retention**: Depending on legal requirements, intercepted data may need to be retained for a specified period for future reference.

Here's a simplified diagram illustrating the steps:

**+------------------+**

**| Authorization |**

**| Request |**

**+------------------+**

**|**

**v**

**+------------------+**

**| Interception |**

**| Setup |**

**+------------------+**

**|**

**v**

**+------------------+**

**| Monitoring and |**

**| Collection |**

**+------------------+**

**|**

**v**

**+------------------+**

**| Filtering and |**

**| Processing |**

**+------------------+**

**|**

**v**

**+------------------+**

**| Delivery to LEA |**

**+------------------+**

**|**

**v**

**+------------------+**

**| Data Retention|**

**+------------------+**

**c) Why are indicators of compromise important while investigating an attack on an organization's systems? 3 Marks**

1. **Detection and Attribution**: IoCs help detect ongoing or past attacks by identifying specific patterns, behaviors, or artifacts associated with malicious activity. They provide clues about the attacker's methods, tools, and techniques.
2. **Incident Response**: IoCs guide incident response teams to quickly assess the scope and impact of a security breach. They aid in containing and mitigating the attack, preventing further damage.
3. **Threat Intelligence**: Sharing IoCs with cybersecurity communities and threat intelligence platforms helps other organizations defend against the same attack or similar threats. This collective defense approach improves overall cybersecurity.

IoCs can include IP addresses, domain names, file hashes, URLs, registry keys, and specific patterns in network traffic. By identifying these indicators, organizations can respond effectively to attacks and strengthen their defenses against future threats.

**QUESTION FOUR [15 MARKS]**

1. **You have been given Metasploitable as a vulnerable machine, Virtualbox as your virtualization software and Kali Linux as your attacking machine. Describe in detail the procedure you would follow in setting up and configuring your hacking environment in order to practice hacking of web applications. 8 marks**
2. **Download Metasploitable**: Obtain the Metasploitable virtual machine image from a reliable source. Ensure you download the appropriate version based on your virtualization software.
3. **Install VirtualBox**: Install VirtualBox on your host machine if not already done. VirtualBox is a free and popular virtualization software that allows you to create and manage virtual machines.
4. **Import Metasploitable VM**: Open VirtualBox, go to "File" > "Import Appliance," and select the Metasploitable VM image you downloaded. Follow the import wizard's instructions to configure settings like CPU, memory, and network.
5. **Network Configuration**:

* Configure VM Network: Ensure the Metasploitable VM is connected to the appropriate network. You can use the default NAT network for basic testing or set up a custom network configuration.
* Note IP Address: Metasploitable VM will obtain an IP address. Note this address for future reference.

1. **Start Metasploitable VM**: Start the imported VM from VirtualBox.
2. **Download Kali Linux**: Download the Kali Linux ISO from the official website.
3. **Create Kali Linux VM**: Open VirtualBox, create a new virtual machine for Kali Linux. During the setup, allocate sufficient resources (CPU, memory) for your hacking activities.
4. **Install Kali Linux**:

* Attach Kali Linux ISO: In the Kali Linux VM settings, attach the downloaded Kali Linux ISO to the virtual CD/DVD drive.
* Start Kali Linux VM: Start the Kali Linux VM to initiate the installation process. Follow the installer's prompts to install the OS.

1. **Configure Network in Kali**:

* Set IP Address: Configure the network settings in Kali Linux to ensure it's in the same network range as Metasploitable. This enables communication between the attacking machine and the target.

1. **Install Tools**: Kali Linux comes preloaded with a variety of hacking tools. However, you can install additional tools as needed using the package manager (e.g., apt).
2. **Practice Web Application Hacking**:

* Identify Vulnerabilities: Use tools like Burp Suite, OWASP Zap, or manual methods to identify vulnerabilities in web applications hosted on the Metasploitable VM.
* Exploit Vulnerabilities: Utilize Metasploit Framework or other tools to exploit vulnerabilities and gain access to the target system.
* Learn and Experiment: Practice ethical hacking techniques, learn about different types of attacks, and explore how to remediate vulnerabilities.

1. **Using real world examples, discuss the defence-in-depth strategy for defending enterprise networks. 7 Marks**

The defense-in-depth strategy involves implementing multiple layers of security controls to protect enterprise networks from various threats. Real-world examples of its components are:

1. **Perimeter Security**:

* ***Firewalls:*** Implement both traditional and next-generation firewalls to filter incoming and outgoing traffic.
* ***Intrusion Prevention Systems (IPS):*** Detect and block malicious activities at the network perimeter.
* ***Distributed Denial of Service (DDoS) Protection:*** Deploy solutions to mitigate large-scale DDoS attacks, ensuring uninterrupted services.

1. **Network Segmentation**:

* ***VLANs:*** Use Virtual LANs to segregate network traffic based on departments or functions.
* ***Micro-Segmentation:*** Implement more granular segmentation within segments to isolate critical systems from potential threats.

1. **Endpoint Security**:

* ***Antivirus and Antimalware:*** Deploy endpoint protection solutions to detect and mitigate malware on individual devices.
* ***Endpoint Detection and Response (EDR):*** Monitor endpoints for suspicious activities and provide incident response capabilities.

1. **Access Control and Authentication**:

* ***Multi-Factor Authentication (MFA):*** Require additional authentication factors beyond passwords.
* ***Privileged Access Management (PAM):*** Control and monitor access to sensitive systems by privileged users.

1. **Data Encryption**:

* ***Data-at-Rest Encryption:*** Encrypt data stored on servers, databases, and storage devices.
* ***Data-in-Transit Encryption:*** Encrypt data transmitted between servers, devices, and networks using protocols like SSL/TLS.

1. **Security Monitoring and Incident Response**:

* ***Security Information and Event Management (SIEM):*** Collect, analyze, and correlate security event logs to detect anomalies.
* ***Security Operations Center (SOC):*** Establish a dedicated team to monitor, respond to, and manage security incidents.

1. **User Training and Awareness**:

* ***Security Awareness Programs:*** Train employees to recognize phishing, social engineering, and other common attack vectors.

By layering these security measures, organizations create a more robust defense posture that can detect, prevent, and mitigate various types of threats at different stages of an attack.