**CSC 312 Cybersecurity**

|  |  |  |
| --- | --- | --- |
| **50 Points** |  | **Assignment 02** |

**Fill in the Blank (20 Points)**

1. Process state - Information representing the current condition of the process within the computer
2. Puzzle - Access control that is based on the knowledge of secret information
3. Process - An entity that consists of a computer program being executed by a CPU
4. Machine instructions - Binary data that executes a program when interpreted by the CPU
5. Data selection - An area in RAM that contains data used by a program, as opposed to instructions
6. Dispatcher - A program used by the OS to manage the execution of processes by the CPU
7. Buffer - An area in RAM used for temporary storage, often used with input/output operations
8. Return Address - The program counter address to which a called program returns to a calling program
9. Kernel mode - A CPU mode that provides unrestricted access to the computer's instructions and RAM
10. Stack - An area in RAM that stores data in a last-in-first-out manner; often used in procedure calls
11. Steganography - A method of hiding information by encoding it within another data object
12. CPU - The computer circuits that execute instructions and perform calculations
13. Input/Output - Computer circuits that connect the CPU and RAM to external devices
14. BIOS - Built-in software on a PC that takes control when the computer starts up
15. Read only memory (ROM) - Access right that allows data to be read but not modified
16. Kerckhoff's Principle - The principle that security mechanisms should be published, and rely on changeable secrets
17. In the role-based access control category, each request want to use a resource is checked to ensure the process has permission to use it.
18. Pattern-based access control is unreliable because pattern matching is rarely perfect and there is always a risk of a mismatch.
19. In the islands access control category, the process or group of processes are isolated and mediation is used to mediate its access to other resources.
20. In access, Remediation correction is the process of restoring the security of a system after an unauthorized access attempt.

**Multiple-choice questions: (8 points)**

1. The fundamental job of every operating system is to run programs, and this relies on:
2. process management
3. random access memory (RAM) management
4. input/output (I/O) management
5. all of the above
6. The type of computer-based access control that involves a process that uses secret or hidden information in order to retrieve particular data items is:
7. island
8. vault
9. puzzle
10. pattern
11. What are the four categories of computer-based access control?
12. Discretionary, Mandatory, Role-Based, and Accessible
13. Islands, Vaults, Puzzles, and Patterns
14. Prevention, Detection, Correction, and Open Design
15. Confidentiality, Integrity, Availability, and Encryption
16. The two primary program modes are:
17. user mode
18. CPU mode
19. kernel mode
20. a and c
21. In practice, computer-based access control begins by making each process into its own \_\_\_\_\_\_\_\_\_\_\_\_
22. Island
23. House
24. Apartment
25. Planet
26. Which of the following is an example of a detection strategy in access control?
27. Firewalls
28. Password management
29. Encryption
30. Intrusion Detection Systems (IDS)
31. The security controls used to protect processes rely on CPU features, but they are all implemented by the \_\_\_\_\_\_ software.
32. Delivery
33. Dispatcher
34. Post office
35. Network
36. \_\_\_\_\_\_\_\_\_\_\_\_ flaws in the software such as finger service are often exploited.
37. Buffer Overflow
38. Blue Screen of Death
39. Shell Shock
40. Windows

**True or False Questions (12 points):**

|  |  |  |
| --- | --- | --- |
| # | Statement | True or False |
| 1 | Two processes are running the same program on a computer. The operating system can set up an access restriction on the control section to prevent one process from changing the control section while the other process is using it. | T |
| 2 | These three functions process management, RAM management and I/O management appear in every operating system no matter how basic or complex. | T |
| 3 | Cryptography provides us with a variety of mathematical techniques to hide data through encryption or to authenticate its contents. | T |
| 4 | Everything a computer does, right or wrong, results from running a computer program written by people. | T |
| 5 | The process of loading and running a program from a mass storage device like a hard drive or CD-ROM is called Chaining | F |
| 6 | In buffer overflow vulnerability, a program fails to keep track of its output | F |
| 7 | Open Design is a principle that relies on keeping security mechanisms secret. | F |
| 8 | Encryption is an example of a detection strategy in access control. | F |
| 9 | Prevention, restoration, and correction are the three access control strategies. | F |
| 10 | Incident response is a correction strategy that involves taking steps to restore the security of the system after an unauthorized access attempt. | T |

**Essay Questions (12 points):**

1. Explain the difference between a program and a process. What information makes up the process state?

Program is a set of instructions to be executed by a computer. A process in an instance of a program. The process state is a current status of a process at a certain point in time.

1. Explain how a buffer overflow can allow an attacker to take over a computer.

An attacker can exploit a buffer overflow vulnerability by crafting input data that overflows the buffer in a specific way. An attacker can cause overwritten memory to execute malicious code.

1. What are the three access control models and how do they differ?

Mandatory Access Control (MAC) is a strict security model that assigns security labels to resources and users, and access is granted based on a set of predefined rules.

Discretionary Access Control (DAC) is a more flexible model that allows resource owners to control access to their own resources. Access decisions are made by the resource owner, who can choose to grant or deny access to specific users or groups.

Role-Based Access Control (RBAC) is a model where access to resources is based on the role or job function of the user. Users are assigned roles that define the types of resources they can access and the actions they can perform on those resources