|  |  |  |
| --- | --- | --- |
| **CSC 312 Cybersecurity** | **Assignment 03** | **50 Points** |

***Elijah Chong Tay***

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

An attack that takes advantage of a specific vulnerability

Exploit

A file security policy in which users have read access to other users' files by default

File-sharing policy

A file security policy that is applied to all users on the system

Global Policy

A file security policy in which users have no access to other users' files by default

Isolation policy?

A file security policy that is modified to apply special permissions to particular users or groups

Tailored policy

A list of access rights associated with a single file, directory, or other resource

Access Control List (ACL)

A set of files and other records that records significant actions for later review and analysis

audit trail

A mechanism in recent Windows systems that demands authorization for administrative tasks

User Account Control (UAC)

A set of flags that specify access rights for a specific file or directory

file permission flags

An extra code value included with data that detects changes to the data

Error Detecting Code (EDC)

Dynamic inheritance is the condition in which files automatically take on the same permissions as the folder in which they reside is called.

Transitive trust is described as the implicit spreading of trust.

Administrative groups provide special privileges for managing the system.

Window of vulnerability is the period of time during which a system is unprotected an exploit.

The process of security flaws involves applying software updates to address known vulnerabilities.

Patches

Monitoring system events through security information and event management (SIEM) can help detect and respond to security threats.

Broken access control vulnerability is caused by a system that is not set up properly, allowing an attacker to gain unauthorized access.

* Vulnerabilities that allow an attacker to gain unauthorized access to a system are known as Unauthorized Access vulnerabilities.
* The Vulnerability Prioritization process involves categorizing vulnerabilities based on their potential impact and the level of risk they pose to the system or organization.
* A backdoor vulnerability is a type of vulnerability that can be exploited by an attacker to bypass security controls and execute malicious code on a system.

**Multiple-choice questions: (10 points)**

* Two mechanisms to apply initial access rights are:
* Default rights / Inherit rights
* Read rights / Write rights
* Mandatory access control rights / Role based access rights
* Object / Directory
* In Windows, when you copy a file from one folder to another and the folders have different access permissions, the file:
* takes on the access rights of the destination folder
* must be assigned a new set of permissions manually
* retains its original access rights
* none of the above
* When something important (an event) takes place inside a program, the program creates
* Event log
* User profile
* Log entry
* Extract files
* What are the risks of logging into a system routing as “root” or some other administrative identity?
* Files could be erased
* Files could be altered
* Exposed system to a virus or malicious website
* All of the above
* A zero-day exploit:
* occurs immediately after a software patch is applied
* has no software patch
* does not pose a security threat
* refers to an exploit that never occurs
* A security database that contains entries for users and their access rights for files and folders is:
* an access security list (ASL)
* an access control list (ACL)
* a security policy
* an administrative group
* Which of the following is not a type of firewall?
* Network Address Translation (NAT) firewall
* Application firewall
* Stateful Packet Inspection (SPI) firewall
* Intrusion Detection System (IDS) firewall
* What is the process of evaluating a vulnerability and determining its potential risk and impact called?
* Scoring
* Exploiting
* Patching
* Monitoring
* Which type of vulnerability allows an attacker to obtain sensitive information such as passwords?
* Privilege escalation vulnerability
* Authentication bypass vulnerability
* Injection vulnerability
* Information disclosure vulnerability
* What is the process of remediating a vulnerability in a system called?
* Scoring
* Patching
* Monitoring
* Exploiting

**True or False Questions (10 points):**

|  |  |  |
| --- | --- | --- |
| # | Statement | True or False |
| 1 | When a system process starts another, the parent process often inherits the child’s access rights. | F |
| 2 | Modern operating systems protect files according to administrator identity | T |
| 3 | Mac OS-X allows you to add ACL entries for groups as well as users. | T |
| 4 | Windows does not deny an access right by omitting it, but it allows you to explicitly deny a right. | T |
| 5 | If a group member (who is not the file’s owner) accesses the file, the system does not apply the group rights. | F |
| 6 | Dynamic ACL’s make it more difficult to establish tailored access rights. | T |
| 7 | Vulnerabilities that allow an attacker to execute arbitrary code on a system are known as denial-of-service vulnerabilities. | F |
| 8 | Vulnerability scoring is an exact science and there is always a correct score for a given vulnerability. | F |
| 9 | Vulnerability management is a one-time process that is performed when a system is first set up. | F |
| 10 | Exploiting vulnerabilities is an acceptable practice if done for educational purposes. | T |

**Essay Questions (10 points):**

* Briefly explain the purpose of file permission flags and these user classes: Owner, System, and World.

File permission flags provide permissions and access rights to users and groups, these perms are used for handling files, to ensure how the system handles attempts to access files.

Owner: the file owner who determines the actions to be carried out.

can have perms like read, write execute and delete

System: a user class that determines the OS and perms which can carry out certain actions to groups.

World: perms given to all files and public users where actions performed can be global

* How does the OS decide what permissions to apply when a user creates a new file?

umask

When we create a directory the default file permissions are assigned by the user mask. If the file is already created we can use chmod.

* What is role-based access control, and how does it differ from discretionary access control?

RBAC (Role based access control) is based on defining a list of business roles, and adding each user in the system to one or more roles.

Discretionary Access Control (DAC) allows a user or administrator to define an Access Control List (ACL) on a specific resource (e.g. file, registry key, database table, OS object, etc), this List will contain entries (ACE) that define each user that has access to the resource, and what her privileges are for that resouce.

* What is a port scan, and how can it be used to identify vulnerabilities in a system?

A port scanner is an application which is made to probe a host or server to identify open ports. These port scannors can be used by *bad actors* to exploit vulnerabilities.