Mind Map

Access Control

This mind map covers the security fundamentals for the SSCP/ CISSP / CompTIA Security+ exams. All these concepts are extremely important from an exam point of view.

How to use this mind map?

Yellow Circle represents the concept while the White Box next to it represents a short explanation for it. Move from LEFT to RIGHT to study this. This mind map focuses only on the most important concepts of a particular domain.

Note - This is just a learning tool. Studying in detail about all the concepts is highly recommended. Check out more such learning tools for free on www.mayurpahwa.com

1. Identification Process of Process of 2 Authentication providing providing an Access 3. Authorization evidence to identity. **Controls Steps** 4. Accountability Identification Authentication 3 factors of prove the authentication identity. Ex- Username, Also, known as user ID etc.. the IAAA Password, PIN Something you know - Type 1 Information Individual's bio Which is known by an possessed by an metrics. individual Something individual Something Something you Something Ex- Fingerprint , voice print., retina You Have You Are have - Type Ex- Access Card Ex- PIN, scan . Iris scan. . Hardware token. password . pet's Something you Software token are - Type 3 name etc. etc., FAR - False Individual to specifying Acceptance Rate be made access rights/privileges accountable Authorization FRR - False Accountability **Biometric** Single Sign to resources for his/her Rejection Rate actions. ACL, Capability CER is FAR=FRR Logs Single sign on protocol. Terms User Users to Security authenticates Assertion authenticate in to know - TGT, Markup once and then different ticket granting Language - to the system uses **Federated** Kerberos networks by SAML server , session ticket . Provides provide SSO the same Access using the same over the credentials for identity issued internet. the entire confidentiality by oné. and integrity. session. Central server Every device Credentials are authenticates has its own set stored in the every device on of memory cache the network. Decentralized Centralized authentication Offline of the device. Subject authentication Authentication Authentication credentials. Used when the device is offline Entity that Entity that is Data owners Security Admin accesses the being accessed can assign will grant resource. by the subject. permissions to Discretionary access/ Non DAC Model Object A subject can subjects privileges. Users also be an Control Model themselves. have no control obiect. over the resources Users are Administrators Grants access granted all the create rules that based on the privileges and Role based Rule based determine Attribute value of the access to Based Access attributes of the Access Access access to resources when Control Control Control subjects and resources. they are obiects. Firewall has assigned a rules. particular role

Mind Map

Access Control

This mind map covers the security fundamentals for the SSCP/ CISSP / CompTIA Security+ exams. All these concepts are extremely important from an exam point of view.

How to use this mind map?

Yellow Circle represents the concept while the White Box next to it represents a short explanation for it. Move from LEFT to RIGHT to study this. This mind map focuses only on the most important concepts of a particular domain.

Note - This is just a learning tool. Studying in detail about all the concepts is highly recommended. Check out more such learning tools for free on www.mayurpahwa.com

NON DAC Models 1.Bell La Padula 2.BIBA 3.Clark Wilson 4.Chinese Wall

Bell La Padula Model Ensures Confidentiality. Rule - No Read Up , No write down.

BIBA Model

Ensures Integrity. Rule -No read down , No write up.

Clark Wilson Model

Ensures Integrity. Uses certification rules and enforcement rules to enforce separation of duties.

Chinese Wall (Brewer Nash) Ensures separation of duties and prevents conflict of interest.

Access Control Matrix List of objects mapped to the permissions they have.

Capability Table List of subjects mapped to the permissions they have.

Provisioning

Creation of user accounts

Deprovisioning Deactivation and deletion of user accounts

Clipping Levels Threshold value, which when crossed results in a event being logged or an activity to be performed.

Replay Attack

Network attack in which a valid data transmission is fraudulently repeated with the goal of obtaining unauthorized access.

Rainbow table Single sign on protocol. Terms to know - TGT, ticket granting server, session ticket. Provides confidentiality and integrity.

Service Provisioning Markup Language Allows for automation of user management

Simple Object Access Protocol Protocol specification for exchanging structured information in the implementation of web services and networked environments.

Threat modeling

Identifies potential threats and attack vectors