|  |  |
| --- | --- |
| Course | Access Controls |
| Assignment | Assignment- Week 11 |
| Name of the Student | Maisha Khatoon |
| Student ID | 100899259 |

**Week 11: Assignment – Network AAA Worksheet**

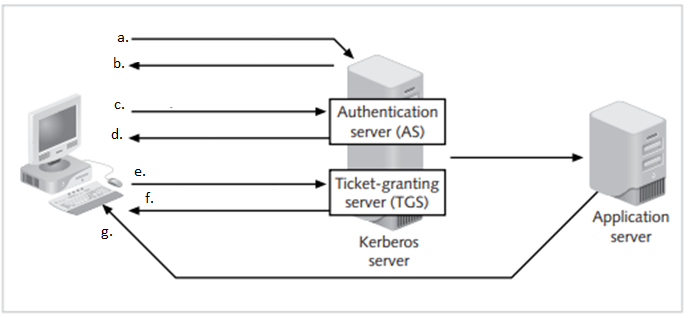
1. What is the difference between a mandatory and discretionary access control system?

Ans. In terms of managing access to resources, Mandatory access control (MAC) and Discretionary access control (DAC) are two different strategies.

Strict access guidelines established by system administrators are enforced through Mandatory access control. Based on hierarchical security labels assigned to subjects (users, processes), and objects (files, directories), these policies are constructed. Subjects are only permitted access to things if their security label satisfies the system's predetermined requirements. Access permissions cannot be changed by users, making it rigorous but incredibly secure. In high-security settings like government and military systems, MAC is frequently employed.

Contrarily, Discretionary access control gives power to resource owners by enabling them to control access to their resources using Access Control Lists (ACLs). More flexibility is offered by the ability for users to grant read, write, or execute permissions to other users or groups. This method works well with general-purpose systems where users have different access requirements.

In conclusion, MAC focuses on rigorous standards and system-defined security labels, restricting user discretion for increased security. Resource owners are given additional control over access permissions by DAC, which provides flexibility but may also increase system vulnerability if access restrictions are not effectively handled. The decision between MAC and DAC is made based on the system's security requirements and the appropriate amount of user flexibility against stringent control.

1. Describe each of the steps shown in this diagram:   
   
   1. By requesting a Ticket Granting Ticket (TGT), the client opens a line of communication with the authentication server (AS). The client contacts the AS to seek a Ticket Granting Ticket (TGT) at the initial step of the authentication procedure.
   2. If the user's login information, which is frequently a username and password, is accurate, the Ticket Granting Server (TGS) will issue a TGT that has been encrypted with a secret key that is only known to the client and the TGS.
   3. To get service tickets that will provide them access to the needed resources (such as the Application Server), clients send a TGT request to the Ticket Granting Server (TGS).
   4. Issuance of Service Tickets: A client who presents a TGT is given a service ticket that has been encrypted with a session key that is specific to both the client and the service that the Ticket Granting Server (TGS) has requested.
   5. The customer can formally request the service from the Application Server (the service provider) once they have the Service Ticket in hand. e. Using the Application Server to send a request. The AS decrypts the ticket's encryption when validating a Service Ticket using the shared secret key it has with the TGS. Additionally, it guarantees that the client is eligible for the service.
   6. The Application Server permits the client access to the service if the Service Ticket is valid, and the client has access rights. The session key created at that time can be used to continue communication between the client and Application Server after a ticket has been issued.
   7. Permitting Use of the Service: h. The service will be made accessible to the client when the Application Server (AS) verifies the validity of the Service Ticket and their request to use the service.
   8. The client can communicate with the application server and access the requested service once a session key has been established (during the issuance of the service ticket). Until the session is over (for example, when the user logs out), the session key ensures a secure connection between the client and the application server.
2. What are the benefits of using TACACS+ as an authentication method?

Ans. The advantages of utilizing TACACS+ as a method of authentication are:

* Enhanced Security: By encrypting all client and server communications, TACACS+ offers a strong and secure authentication mechanism that lowers the risk of unauthorized access.
* Centralized Management of User Authentication and Authorization: TACACS+ enables central administration of user authentication and authorization, simplifying access management for network assets and services.
* User Accountability: TACACS+ enables thorough user activity logging, assisting in auditing and accountability—both of which are essential for compliance and security reasons.
* Granular Access Control: Using TACACS+, administrators can create fine-grained access policies that grant various network resources access at different levels according to user roles or privileges.
* Vendor-Independent: TACACS+ is a vendor-independent protocol, making a variety of networking devices and platforms compatible with it.

1. Describe each of the components of a TACACS+ system.
   1. TACACS+ Client: A network device or application that asks the TACACS+ server for authentication and authorization services.
   2. TACACS+ Server: A centralized server for authentication, authorization, and accounting that manages client requests for authentication and upholds access regulations.
   3. TACACS+ Database: This database is used by the TACACS+ server to manage access privileges and store user accounts, credentials, and access control policies.
2. What are the benefits of using RADIUS as an authentication method?

Ans. The advantages of utilizing RADIUS as a technique for authentication are:

* RADIUS supports centralized user authentication, which makes it simpler to handle user accounts and credentials from a single location.
* Scalability: RADIUS is appropriate for large-scale deployments since it is extremely scalable and can accommodate many users and devices.
* Reduced Network Traffic: RADIUS has a client-server architecture, reducing network traffic by performing local user authentication on the RADIUS server as opposed to directly on network devices.
* Enhanced Security: RADIUS enables encryption for safe communication between clients and servers, lowering the danger of unauthorized access and data eavesdropping.
* Flexibility: RADIUS is widely supported and is vendor-neutral, enabling interoperability with a range of network hardware and authentication sources.

1. Draw an example of a *mesh* topology for a VPN solution.

Ans. In this analysis, let’s look at a specific instance of a virtual private network (VPN) solution utilizing a mesh topology. The network consists of five distinct network nodes, denoted as A, B, C, D, and E. In this instance, every node is directly linked to each and every other node, thus creating a network that is totally integrated.

The interconnections inside the mesh topology can be visually represented as follows:

* Node A is directly connected to nodes B, C, D, and E through point-to-point connections.
* Node B is directly connected to nodes A, C, D, and E through point-to-point connections.
* Node C is directly connected to nodes A, B, D, and E through point-to-point connections.
* Node D is directly connected to nodes A, B, C, and E through point-to-point connections.
* Node E is directly connected to nodes A, B, C, and D through point-to-point connections.

In the context of this mesh topology, it is observed that every node within the network possesses a direct and individual link to all other nodes. This arrangement results in the establishment of a communication infrastructure that is both redundant and capable of withstanding faults. In the event of a failure in an individual connection between nodes, alternative channels remain accessible for communication, thereby guaranteeing a VPN solution with a high level of availability and dependability.

1. Draw an example of a *hub and spoke* topology for a VPN solution.

Ans. Let's consider an instance of a hub and spoke topology in the context of a virtual private network (VPN) solution, encompassing four distinct network locations: a central hub (H) and three peripheral spokes (S1, S2, and S3). Every individual spoke is connected to the central hub to gain access to resources within the virtual private network (VPN). In the given illustration:

+-----+

| H | (Hub)

+--+--+

|

|

+---------+--------+

| | |

+-v-+ +-v-+ +-v-+

|S1 | |S2 | |S3 |

+---+ +---+ +---+

* The hub (H) refers to the central location housing the primary VPN server or concentrator. The central point for all virtual private network (VPN) connections is provided by this entity.
* The Spoke S1 establishes a connection with the central hub (H) to securely access the resources that are available within the Virtual Private Network (VPN).
* The Spoke S2 device can establish a connection with the central hub (H) to securely access resources within the virtual private network (VPN).
* The Spoke S3 establishes a connection with the central hub (H) to gain access to the resources that are accessible within the Virtual Private Network (VPN).

The central hub (H) serves as the intermediary for all communication among the spokes (S1, S2, and S3). The utilization of a hub and spoke topology in network architecture has the advantage of streamlined network management and enhanced security control through centralization. The central hub (H) possesses the capability to implement security policies, facilitate authentication, and administer access control for all the interconnected spokes, hence simplifying the maintenance and fortification of the VPN solution.

The utilization of the hub and spoke architecture is prevalent in situations where a central data center, referred to as the hub, houses essential resources, while outlying offices or users, known as the spokes, necessitate secure connectivity to access those resources.

1. When might an organization implement an “always on” VPN system?

Ans. An organization may choose to deploy an "always on" virtual private network (VPN) system in situations when there is a need for uninterrupted and secure connectivity to internal network resources by remote users or devices. This configuration guarantees that all network traffic originating from remote users or devices is consistently encrypted and directed through the virtual private network (VPN), even in situations when there is no active interaction with specific resources. The technology improves security measures, safeguards data, and ensures adherence to regulatory requirements, while simultaneously providing a continuous and secure connection for remote users or devices.

1. What are the differences between a hardware and a software VPN?

Ans. The difference between a hardware and a software VPN:

* A hardware VPN creates secure connections using routers with built-in VPN functionality or standalone VPN hardware appliances. Whereas Software applications that run on general-purpose devices like PCs, cellphones, or virtual machines are used to establish a software VPN.
* Due to the use of specialized hardware for encryption and decryption, it delivers improved performance and throughput. On the other hand, users are given the option to select from a variety of software clients and protocols thanks to its flexibility and customizability.
* Given their greater scalability, hardware VPNs are frequently better suited for large-scale deployments and high-traffic situations. They are less adaptable than software VPNs because they are made for hardware platforms and might not have as much configuration flexibility. Hardware VPNs could have greater up-front costs due to the need to buy special hardware. However, the processing power of the host device may have an impact on the performance of software VPNs. They are more affordable because they can operate on current devices without the need for new hardware, which makes them better for small to medium-sized deployments. To maintain security and compatibility with the most recent operating systems and protocols, software VPNs need constant updates and maintenance.

1. What should be specified in a VPN policy?

Ans. The following should be stated in a VPN policy:

* The VPN's goal.
* Authenticated users and access management.
* methods for authorization and authentication.
* procedures for data protection and encryption.
* Device specifications and security precautions.
* prohibited behaviors.
* processes for reporting and responding to incidents.
* Legal and compliance considerations.
* practices for monitoring and auditing.
* penalty for breaking the rules.
* Review and updating of policy.