



APUNTES 04


**ADMINISTRACIÓN DE
CREDENCIALES PARA EL
ACCESO A
SISTEMAS INFORMÁTICOS**

BASTIONADO DE REDES Y SISTEMAS

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información



ÍNDICE

1. Gestión de credenciales.
2. Infraestructura PKI.
3. Firma Electrónica.
4. Sistemas NAC.
5. Gestión de cuentas privilegiadas.
6. Protocolo RADIUS y TACACS.

Caso práctico

En la empresa de María, las cuentas de usuario consisten en un nombre de usuario y una contraseña (password). En los sistemas operativos estos dos elementos forman un conjunto de credenciales y sirven para identificar a una persona. Utilizar contraseñas es un método para autenticarse, pero no es el único, hay otros métodos como, por ejemplo, el uso de tarjetas inteligentes que tiene la identidad grabada. La administración de credenciales de acceso es algo fundamental debido a los numerosos ataques de contraseñas que hoy día pueden producirse.

De hecho, los sistemas de control de acceso protegidos con contraseña, suelen ser un punto crítico de la seguridad y por ello suelen recibir distintos tipos de ataques, siendo los más comunes los ataques de fuerza bruta y los ataques de diccionario.

Objetivos: Ya vimos en la unidad tres los diferentes elementos que componen el control de acceso a un servicio, sistemas y factores. En esta unidad explicaremos cuáles son los mecanismos más apropiados para gestionar las credenciales además de mencionar ejemplos con tecnologías de utilidad en las infraestructuras TIC como las claves públicas y la gestión de acceso a las redes entre otros.

El alumno al finalizar la unidad habrá asimilado conceptos relacionados con la implementación de clave pública, los controles de acceso a la red así como la gestión adecuada de cuentas privilegiadas. Para terminar, se llevará a cabo una aproximación a los protocolos de acceso basados en autenticación, autorización y conteo como RADIUS y TACACS.

1.- GESTIÓN DE CREDENCIALES.**Caso práctico**

En la empresa de María, todos los empleados utilizan el mismo usuario y la misma contraseña para acceder al sistema. Se trata de una práctica que para ellos es de relativa comodidad pero que a la larga, podría suponer más de un problema ya que no se permite la trazabilidad de los usuarios. Sin duda, se trata de una práctica de riesgo que se debe evitar.

Antes de adentrarnos en diferentes tecnologías, es necesario conocer que, para acceder a los sistemas y servicios, será necesario disponer de algún tipo de credencial que facilite la autorización. En este sentido, la autorización se puede llevar a cabo de dos maneras, bien a nivel local, donde para acceder al recurso, la configuración, llevar a cabo tareas de mantenimiento, etc. será necesario introducir las credenciales en el propio dispositivo; o bien a través de un acceso remoto mediante una consola, un escritorio remoto o cualquier otro tipo de tecnología.

Si a estas dos cuestiones sumamos que estas credenciales pueden estar en manos de diversos técnicos o que no se usan los canales de comunicación con la seguridad necesaria, nos encontramos en un nivel de exposición que es muy favorable para los posibles atacantes y que sin duda será un problema para la empresa u organización.

Riesgos o problemas comunes en el uso de credenciales

A continuación, enumeraremos cuáles son los inconvenientes más habituales en la gestión de credenciales:

1. Contraseñas : se trata del supuesto menos habitual hoy en día, aunque hasta hace años aún se podían encontrar dispositivos con credenciales que no era posible modificar de ningún modo. No obstante, si nos movemos al mundo de las tecnologías “hardcodeadas” de la operación (OT) es posible encontrar dispositivos con esta característica. El mayor inconveniente, viene dado porque las credenciales suelen ser conocidas, bien porque aparecen en el manual o bien porque se pueden encontrar de manera sencilla en Internet. Cualquier persona con acceso al activo podría obtener la autorización.

2. Contraseñas por defecto: cuando se adquiere un dispositivo, antes de su puesta en marcha y parametrización, es posible acceder a través de contraseñas por defecto que el fabricante ha dispuesto. Lo habitual es que una vez que comencemos a parametrizar el dispositivo, aplicación o servicio, lo primero que hagamos sea modificar las credenciales. En cualquier caso, siempre podrá existir el error humano, donde por un descuido u otra razón se dejen dichas contraseñas con el riesgo que supone, aunque en ocasiones, se dejan de manera voluntaria por el trastorno que supondría conocer todas las credenciales de todos los sistemas, algo que no es una buena práctica.

3. Incremento en el uso de credenciales: en la actualidad es habitual necesitar una credencial para cada servicio, además los procesos de autorización habitualmente discurren a través de la red. Esto significa que, si no tenemos los mecanismos de cifrado adecuados, alguien que sea capaz de interceptar el tráfico, podría acceder a un gran número de usuarios y contraseñas.

4. Compartir contraseñas: a pesar de que pueda parecer algo inaudito, nos son pocas las personas que no tienen ningún problema en compartir las contraseñas, sobre todo en aquellos servicios relativos al ámbito laboral. Por ejemplo, alguien que necesita acceder a un recurso para el que no recuerda su acceso, solicita la contraseña a un compañero y este se la facilita. Sin duda no es una buena práctica ya que se pierde la trazabilidad entre otros problemas.

5. Credenciales privilegiadas: aunque lo trataremos en un punto específico en esta unidad, en la actualidad, en todas aquellas organizaciones que no existe una política de gestión de contraseñas, es habitual emplear las credenciales de administrador para la operación de los servicios con los riesgos que eso entraña. Del mismo modo que ocurre con la compartición de contraseñas, la utilización de este tipo de cuentas impide la trazabilidad entre otras cosas.

Características básicas para una correcta gestión de credenciales

Existen numerosas tecnologías y aplicaciones que nos van a permitir llevar a cabo esta tarea de una manera mucho más cómoda, no obstante, antes de entrar en ese plano, es necesario especificar algunas características que se han de considerar:

- Descubrimiento de credenciales: una de las cuestiones más importante, es conocer qué activos de la organización necesitan credenciales para su gestión. Por ello, el disponer de un inventario actualizado es esencial para determinar cuáles son los datos para la autorización de cada servicio. Existen algunas aplicaciones que son capaces de inspeccionar la red para llevar a cabo el descubrimiento de credenciales mediante la monitorización de equipos. Esta tarea será la primera a llevar a cabo para construir la base de datos inicial.

- Modificación periódica de contraseñas: a pesar de que sabemos que es una de las cuestiones que más incomoda a los usuarios, llevar a cabo una rotación periódica es necesario. Imaginemos que un empleado lleva usando la misma clave durante 5 años. En ese periodo es posible que dicha contraseña haya sido sustraída, incluso que sea conocida por gente que ya no está en la organización. Una política de gestión de contraseñas junto con una herramienta tecnológica facilitará esta cuestión.

- Segmentación por roles: es imperativo que las credenciales para los diferentes activos sean únicamente conocidas por los usuarios que los van a operar. Esta medida no permitirá que usuarios que no tienen permisos puedan llevar a cabo alguna acción no intencionada o intencionada.

- Auditoría de accesos: es necesario implementar una medida de este tipo para garantizar la trazabilidad de las acciones que llevan a cabo los usuarios. Imaginemos que varios usuarios comparten una contraseña, en caso de haber algún problema, no se podría determinar quién ha llevado a cabo la acción. Para ello, sería adecuado implementar tecnologías que, por ejemplo, impidan el acceso a un recurso por parte de un usuario que no se encuentra en su puesto de trabajo.

- Acceso único o SSO: una solución de acceso único, en muchas ocasiones puede resultar interesante para ofrecer al usuario la autorización para gestionar todos los activos para los que tenga permiso, de esa manera se encontrará con las opciones para las que se le ha dado acceso y ninguna otra.

Para finalizar, hay que mencionar que existen aplicaciones comerciales que facilitan la gestión de las cuentas que tienen algún tipo de particularidad o privilegio y que han de ser gestionadas adecuadamente:

Shared Account & Credential Vault.

Safeguard for Privileged Passwords.

Gestores de credenciales

Existen opciones más básicas para la gestión de credenciales y que se pueden utilizar a título individual como los gestores de contraseñas. Estas aplicaciones básicamente almacenan la información de nuestras credenciales en una base de datos cifrada con un algoritmo seguro para la que necesitaremos una contraseña, denominada “contraseña maestra” (o “clave maestra”). Lo práctico de estas aplicaciones es que únicamente necesitaremos memorizar una contraseña para acceder al resto.

Existen numerosas alternativas tanto comerciales como gratuitas. En cualquier caso, las características comunes que comparten serían:

- Multidispositivo: es posible acceder a la base de datos con las aplicaciones desarrolladas para las diversas plataformas (Windows, Android, iOS, etc.). Aquellas que además dispongan de servicio en la nube, las podremos sincronizar.

- Acceso online y offline: en este punto se debe valorar la usabilidad ¿Por qué?, esencialmente porque en un servicio online (nube) necesitaremos disponer de conexión a Internet para acceder al listado o haber exportado las contraseñas si es posible. En el caso de las aplicaciones offline como Keepass, necesitaremos una copia de la base de datos si queremos abrirla en varios dispositivos.

- Generador de contraseñas: la totalidad de aplicaciones disponen de generadores de claves que crearán contraseñas con buenos niveles de seguridad.

- Identificación de debilidad en contraseñas: como la característica anterior, esta está disponible en todos los gestores y básicamente nos informará de cuándo una contraseña no es considerada segura y por ende no debe ser utilizada.

- Verificación en dos pasos: limitado a los gestores en la nube como LastPass, que dotarán de una capa de seguridad para acceder al servicio.
- Integración con navegadores: casi la totalidad de los gestores de claves en la nube, disponen de esta funcionalidad, bien de manera nativa con el navegador o a través de un plugin. Su utilización será más cómoda a la hora de autorizarse en servicios mediante clientes web o similar.

2.- INFRAESTRUCTURA PKI.

Caso práctico

Manuel tiene una página web con un formulario para realizar pedidos en su web. Un día un conocido, le informa que los datos que se transmiten desde su formulario, pueden ser inspeccionados por alguien malintencionado. Manuel se informa y el servicio técnico del hosting que tienen contratado, le indica que ha de instalar un certificado para cifrar las comunicaciones. Manuel accede y desde entonces su web es más segura.

Tal y como se indica en numerosas referencias, “La infraestructura de clave pública (PKI) es un conjunto de roles, políticas, hardware, software y procedimientos necesarios para crear, administrar, distribuir, usar, almacenar y revocar certificados digitales y administrar el cifrado de clave pública”. Esto que a priori, si uno no está familiarizado con el tema puede resultar un poco abrumador, para entenderlo mejor, usaremos un ejemplo. Imaginemos que queremos llevar a cabo una transacción en un portal de eCommerce en Internet y considerando un contexto en el que no existen los certificados. Al otro lado no sabríamos si se lo estamos comprando al comerciante legítimo o a un ciberdelincuente. Bien, considerando el supuesto y teniendo en cuenta la información inicial en torno a las PKI, lo que se consigue con esto es crear una infraestructura de autoridades de certificación, autoridades de registro y certificados, que garantizarán en gran medida, la seguridad en las comunicaciones y por ende según el ejemplo, en las transacciones. Lo que va a conseguir la infraestructura de clave pública, es certificar que alguien es quien dice ser, en algunas ocasiones incluso aunque las claves le sean robadas. Indicar que la infraestructura PKI es un sistema de cifrado asimétrico por la existencia de un par de claves (privada y pública).

Para ello, la parte principal de la infraestructura se podría decir que son los certificados, que aportarán información acerca de quién es el dueño del mismo. En España podemos decir que todos los ciudadanos disponemos de un certificado digital personal gracias al DNI y que está disponible en todos los documentos nacionales de identificación que expide la Policía Nacional. En este caso se trata de un certificado un poco especial, ya que no puede exportarse, pero es el que nos identifica de manera unívoca a cada individuo para cuestiones de ámbito digital. Volviendo al DNI, un certificado digital podría considerarse como una “especie de DNI”, que tiene aplicabilidad en multitud de servicios digitales. Por ejemplo, en el caso de una página web, nos ofrecerá información relacionada con el propietario, la autoridad de certificación, la clave pública de la web, el algoritmo de cifrado utilizado o la fecha de caducidad del certificado entre otra información. Veamos la información que podemos obtener desde el certificado de CIDEAD en su página web:
<https://www.educacionyfp.gob.es/mc/cidead/el-cidead.html>.

Mediante el certificado de la web de CIDEAD, nos va a permitir llevar a cabo una comunicación segura entre nuestro cliente (navegador) y el servidor remoto. Dicha conexión estará cifrada mediante la clave pública de cifrado que nosotros podemos usar en nuestro navegador. Para ello además existe una Autoridad de Certificación que vela porque la información del certificado sea cierta. En este caso tenemos dos niveles de verificación, por un lado la AC de componentes informáticos y por otro la AC de la Fábrica Nacional de Moneda y Timbre que sería la Autoridad de Registro (RA).

¿Pero cómo se sabe que esa web pertenece a esa empresa? La CA de manera autónoma o mediante otra entidad llamada Autoridad de Registro, realizará una serie de comprobaciones donde si todo es correcto, generará el certificado para cifrarlo con su clave privada. De este modo el que reciba el certificado sabrá que los datos que se muestran en el detalle de ese certificado los ha validado una CA ya que el dato de la autoridad de certificación es público.

También podría surgir la duda de que quizás una CA no sea legítima. En estos casos existe lo que se denomina un certificado raíz que será validado por otras Autoridades reconocidas como podrían ser Verisign, Symantec, etc.

Antes comentamos que podría ser posible el robo de la clave privada de un servidor y que un atacante nos suplante la web. ¿Qué hacer en estos casos? Tenemos la posibilidad de revocar un certificado para que no sea válido. Este tipo de acciones se hacen casi de manera inmediata y evita que se produzca una suplantación. Para ello hemos de solicitarlo a la CA que firmó dicho certificado. Posteriormente podremos solicitar uno nuevo.

En este punto puede surgir la pregunta de ¿Si al conectarme a una web, recibo un certificado que está cifrado, cómo es posible descifrarlo? Muy sencillo, la mayoría de los clientes web, correo, etc. tienen instaladas las claves públicas de las CAs más conocidas, por esta razón el descifrado es transparente. No obstante, y por cuestiones de seguridad implementadas por los desarrolladores de navegadores, podemos encontrarnos situaciones un poco confusas como por ejemplo, si nos conectamos a un servicio web que tiene un certificado autofirmado, obtendremos un mensaje de advertencia de que “el sitio no es seguro” y en el formulario de URL, en función del navegador, aparecerá un candado tachado (en vez de verde) y las letras “https” tachadas.

Usos de la infraestructura PKI

En el punto anterior hemos usado el ejemplo de una conexión web cifrada para explicar el modelo de infraestructura, pero tiene muchos más usos como:

- Firma digital de documentos: con reconocimiento legal y al emplear tecnología en vez de papel, se pueden trazar las operaciones, se gana en agilidad y se aumenta la seguridad.
- Cifrado de datos: cualquier individuo con un certificado válido, podrá cifrar cualquier tipo de documento para transmitirlo con seguridad.
- Gestión de credenciales e implementación de sistemas SSO: eliminando la necesidad de recordar usuarios y contraseñas como hemos visto en puntos previos.
- Operar con otras instituciones de manera segura: como por ejemplo con algunos servicios digitales de la Administración Pública Española (Puntos del carnet, ventanas online, etc.)

3.- FIRMA ELECTRÓNICA.

Caso práctico

Sonia y Fernando, dueños de una asesoría, desconocen que es posible otorgar validez jurídica a los documentos a través de la firma digital. Tras informarse en la Administración Pública, donde les confirmaron esta cuestión y les indicaron que sería posible además contar con un certificado de empresa, implementaron el proceso en su negocio. Desde entonces son mucho más ágiles.

La firma electrónica es un concepto originado hace unas décadas que consiste en un concepto legal cuyo propósito es dar fe de la voluntad del firmante. Cuando la firma se hace electrónicamente, esta consiste en un conjunto de datos que están vinculados a un documento que identifica al autor y garantiza la integridad. Por ejemplo y tal y como se ha mencionado anteriormente, en España podemos firmar electrónicamente con el DNI.

¿Para qué se usan actualmente los procesos de firma electrónica? Por ejemplo, en muchas aplicaciones móviles y más en concreto en las de carácter financiero, cuando llevamos a cabo una operación como una transferencia, el programa suele solicitar la acción de firma ¿Y cómo se lleva a cabo esa acción? Pues de diferentes maneras:

- Con contraseñas: básicamente a través de una clave que hemos concretado con el banco.
- Con datos biométricos: por ejemplo, a través de la huella dactilar. Aclarar antes que los datos relativos a la huella nunca se envían al banco, se almacenan en el dispositivo móvil y se autoriza con la clave existente que sí es la que se envía al banco.
- Claves criptográficas de carácter privado: en este caso, la validez de la firma electrónica dependerá de los acuerdos a los que se haya llegado con la entidad.

Como dato, indicar que la situación pandémica generada por el COVID19, promovió el uso de la firma electrónica elevando su uso. Esto es lógico pues la ausencia de contacto físico y las restricciones de acceso a oficinas motivaron este incremento.

Si quieres conocer más acerca de la firma electrónica, puedes visitar la siguiente entrada del Blog de Protege tu Empresa de INCIBE.

4.- SISTEMAS NAC

Caso práctico

Juan, un pequeño administrador de sistemas con un negocio familiar, necesita añadir en la oficina, una funcionalidad que a los comerciales que visitan su empresa, les permita conectarse a un servidor de ficheros para actualizar determinada información. El problema es que no quiere que tengan acceso al resto de la red. Un conocido del gremio, le ha dicho a Juan que puede implementar acceso a nivel de red para permitir el acceso a los comerciales, exclusivamente a los archivos y equipos que necesitan.

Hasta ahora hemos visto cómo el modo de acceder a servicios a través de credenciales para obtener la autorización. En este punto vamos a abordar como se logra dicho acceso a través de los dispositivos e interfaces que forman parte de la electrónica de red. Esto se consigue a través de las soluciones NAC (Network Access Control) o de control de acceso a la red.

Un sistema NAC va a permitir controlar de manera muy específica qué dispositivos están autorizados para acceder a una determinada red o a un segmento de esta. Para lograrlo, las soluciones que usan esta tecnología emplean políticas y directivas de seguridad para la gestión de dispositivos tanto fijos como móviles e incluso, dispositivos de terceros o BYOD.

Este tipo de soluciones están dirigidas a empresas por encima de un tamaño medio y con una dependencia tecnológica media/alta. Es importante el disponer de NAC en estas organizaciones porque habitualmente sufren cambios que van desde la evolución de otras tecnologías como sistemas operativos o aplicaciones hasta el crecimiento de su parque informático con el incremento de terminales, servidores, etc.

Implementación NAC

A continuación vamos a ver algunos casos de uso en la implementación de este tipo de soluciones. A primera vista quizás pueda parecer que también se podría solucionar con la configuración de redes virtuales, pero NAC va más allá.

1. NAC para IoT: el crecimiento de estos dispositivos es exponencial en los últimos años. Si a esto le añadimos que muchos fabricantes no integran seguridad desde el diseño, podemos encontrarnos con un conjunto de activos que podría poner en riesgo a parte de la organización. Implementando NAC sobre estos dispositivos limitaríamos la exposición a través de políticas y directivas específicas que garanticen la seguridad de la organización.
2. NAC para BYOD: de manera similar a lo anterior, el integrar dispositivos en la red de la empresa que no están amparados por las políticas generales, podría suponer un riesgo. Mediante la implementación de NAC se limitaría el alcance de las operaciones que pueden realizar estos elementos ofreciendo mayor seguridad a la empresa.
3. NAC para terceros o visitas: en línea con lo anterior, pero de una manera más restrictiva, se implementaría políticas en la solución NAC que permitieran conectarse a la red de la compañía, pero de manera segregada por ejemplo con respecto a los empleados.
4. NAC para OT: las redes industriales en ocasiones son consideradas como críticas en función del sector. Las tecnologías NAC permiten diferenciar las diferentes redes y aplicar políticas para cada una de ellas.

Soluciones OpenSource

En el ámbito comercial, existen numerosas soluciones facilitadas por los principales proveedores de tecnologías de red como Cisco, HP, FortiGate, etc. pero también encontramos soluciones de acceso gratuito. Obviamente no suelen contar con toda la funcionalidad y facilidad de configuración que las marcar comerciales, pero pueden ser una solución para aquellas organizaciones que no necesiten grandes cosas en este ámbito. Algunas de ellas serían:

FreeNAC
PacketFence

5.- GESTIÓN DE CUENTAS PRIVILEGIADAS.

Caso práctico

Francisco y Luis son dos administradores de sistemas que aunque trabajan en la misma empresa, se encuentran en ubicaciones diferentes. Un día se produjo un borrado de varios archivos de manera accidental. Tras consultar los registros se comprobó que el borrado se llevó a cabo por el usuario "administrador". Tanto Fran como Luis usan esa cuenta de manera indiscriminada por lo que salvo que uno de ellos lo admita, va a ser difícil saber quién llevó a cabo la operación.

Podemos abrir este punto con la siguiente pregunta ¿Quién no ha utilizado alguna vez una cuenta de administrador para casi todo? Desgraciadamente la respuesta es demasiado común, "todo el mundo".

Al igual que en otros ámbitos de la vida, a veces, más es menos, abarcar demasiado puede conducir a perder todo y en términos de seguridad de servidores, abrir las puertas al mundo es una práctica más común de lo habitual entre administradores y enormemente peligrosa, muchas veces es involuntaria o por desconocimiento y otras es por una gestión ineficiente.

Debemos tener siempre en mente la premisa de ir de menos a más, de máxima restricción (es decir, mínimo impacto en seguridad) a la restricción justa y necesaria cuando sea necesario. En este sentido, invertir tiempo en organizar, mantener y compartir información y formarse es siempre una buena idea cuando se trata de proteger la privacidad de la información en un servidor.

Un administrador o equipo de administradores formado y organizado es siempre una apuesta segura. Pero nos centraremos en lo importante: las cuentas de usuario con privilegios, sus riesgos y consecuencias y cómo se han de configurar para minimizar los riesgos.

• Cuentas de usuario en servidores

Aunque usuarios, ordenadores y servicios cambian en el tiempo, los roles de los servidores y las reglas de seguridad tienden a permanecer estables; en una empresa con determinados roles de servicio instalados, es fácil encontrar que varios usuarios han estado gestionando esos roles a lo largo del tiempo, por este motivo, no es sensato administrar una red empresarial asignando derechos y permisos a usuarios individuales, ordenadores o identidades de servicio.

Lo lógico, es asignar las tareas de administración por medio de grupos de usuarios con permisos bien definidos y diferenciados, por tanto, es importante para un administrador conocer a la perfección el funcionamiento de los grupos para identificar adecuadamente los roles administrativos y de usuario, para filtrar las directivas y asignar políticas de contraseñas únicas y para administrar derechos y permisos. Además, debe contar con los conocimientos necesarios en las técnicas de ataques más comunes y los mecanismos para mitigarlos, así como las herramientas de gestión de privacidad y seguridad más habituales.

En este punto con carácter general, veremos de modo somero, cómo lograr una administración más eficiente y segura de los usuarios teniendo siempre en mente que una gestión consistente es la que aplica buenas prácticas en seguridad mediante cambios y adaptaciones estudiadas y testeadas previamente por los equipos de TI. Pero centrémonos en lo importante, para maximizar la seguridad, cada usuario debe utilizar su propia cuenta (salvo excepciones) y su propia contraseña, la cual debe cumplir unas características mínimas de complejidad que deben ser definidas en las políticas de administración de servidores.

Elegir el nombre de las cuentas de usuario es igual a decir que: "Definir, evita errores", pero además ayuda a otros administradores a no cometer errores a la hora de asignar derechos y permisos sobre un usuario. En materia de seguridad, los atributos de las cuentas de usuario también juegan un papel muy importante que veremos a continuación. Y esos atributos son los responsables de una gestión segura y eficiente de los usuarios. Entre ellos destacan:

- Inicio de sesión en franja horaria: limitando los tiempos en los que pueden operar los sistemas.
- Iniciar sesión en: opción para logarse en algunos equipos,
- La cuenta expira en: útil para cuentas temporales.
- El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
- La contraseña nunca caduca: opción recomendable en contraseñas relativas a servicio.
- El usuario no puede cambiar la contraseña: usado en cuentas de servicio.
- Almacenar contraseña usando cifrado reversible: no se recomienda activar esta opción
- La cuenta es confiable para la delegación: en el caso de delegar algún tipo de función a esa cuenta como por ejemplo operadores de copias de seguridad.

Sobre tecnología Microsoft, el aspecto que tendría sería el que muestra la imagen de la derecha.

• Grupos por defecto

Tal y como comentamos antes, las cuentas de usuario deben organizarse en grupos, hay dos tipos de grupos:

- De distribución: no tienen identificador, no puede darle permisos, se usan solo con aplicaciones de correo.
- De seguridad: tienen un identificador, se le puede dar permisos.

Estos grupos definen los derechos y permisos que tendrá cada usuario, recordemos que no es buena idea dar permisos de forma individual a un usuario, ya que el directorio se haría muy difícil de gestionar con el tiempo y no habría una clara organización en cuanto a los permisos de acceso a recursos compartidos, para estos casos es mejor crear un grupo de permisos especiales para determinados usuarios que dar el permiso de forma individual. En los servidores suele existir una serie de grupos por defecto que tienen una serie de permisos y derechos predefinidos. Estos grupos están protegidos por defecto y no se pueden eliminar o modificar. Es importante conocer su existencia y funciones para implementar una administración del servidor más eficiente, pero sobre todo más consistente y segura. Los grupos por defecto o entidades de seguridad integradas los podemos encontrar al dar de alta un usuario, pudiendo elegir si va a ser un usuario que tendrá funciones administrativas en mayor o menor medida dentro del dominio empresarial.

• Administración delegada

La administración delegada pretende evitar el acceso de un "superusuario" o usuario con privilegios totales a todas las áreas del sistema, además, acota las personas que pueden acceder a ciertas características y al mismo tiempo, reparte las tareas de administración en entornos productivos altamente densos. Pero no todo, son ventajas, una administración delegada, requiere una organización bien estudiada, para ello, podemos contar con los grupos o en tecnologías Microsoft con las OU's o Unidades Organizativas.

La clave del diseño de una base de datos de usuarios consistente es que ayude a organizar la jerarquía dentro de la organización, de esta forma, tendremos una idea clara de quien, como y donde puede acceder a la información. La mejor práctica para crear una jerarquía organizativa es que controlen los objetos para delegación de control, aplicación de políticas o directivas y para ambas cosas. La organización debería estar basada en la localización geográfica o física, las características del departamento, los tipos de recursos accesibles, la estructura de administración y una combinación de todas ellas.

Anteriormente hemos visto los tipos de grupos por defecto asignados a funciones específicas de administración, pero esto no quiere decir que no podamos delegar determinadas tareas específicas a otros usuarios, para ello disponemos de los permisos, pudiendo hablar de permisos de distinta granularidad según su concreción y especificidad.

- **Protección del acceso con privilegios**

La protección del acceso con privilegios es un paso crítico para establecer la seguridad de los recursos empresariales de una organización, la seguridad de estos recursos depende en su gran mayoría de la integridad de las cuentas con privilegios que realizan tareas administrativas, de gestión y desarrollo y normalmente, esto suele suceder diariamente.

Estas cuentas son el foco principal de los ciberdelincuentes, ya que les permite acceder a datos y sistemas rápidamente, tan “solo” robando las credenciales mediante dos técnicas conocidas como “pass the hash” o “pass the ticket”, no vamos a entrar extensamente en ellas, pero básicamente son ataques que consiguen robar las credenciales en menos de 48 horas utilizando técnicas de phishing e ingeniería social. En un primer estadio la mayoría de las empresas no detectan el acceso no autorizado a la red y mientras tanto acceden a recursos compartidos con credenciales robadas, una vez dentro de la red el siguiente escalón es elevar los privilegios del usuario o robar otros más elevados, permitiéndoles acceder a máquinas y configuraciones para pasar finalmente al control de servidores, controladores de dominio y robo de credenciales de toda la organización.

- **Reducción de privilegios y consecuencias de una gestión ineficaz**

Habitualmente el entorno más grande, es el más difícil de proteger y administrar, no es ningún misterio. Dada la dificultad de esta tarea e incluso a veces la imposibilidad de llevarla a cabo, debemos centrarnos en proteger primero las cuentas cuyo privilegio crea el mayor riesgo en la organización, que normalmente son aquellas integradas en la base de datos por defecto y utilizadas por los administradores, así como también las cuentas locales con privilegios en estaciones de trabajo, no olvidemos revisar también aquellos grupos de usuarios con privilegios críticos, ya que varios administradores de sistemas diferentes pueden tomar decisiones diferentes basadas en su experiencia.

Los ataques frecuentemente se centran en hosts individuales, por tanto, es necesario proteger las cuentas de administrador local de cada equipo, ya sabemos a esta altura, que estas cuentas vienen deshabilitadas por defecto, sin embargo, en dominios con sistemas operativos heredados o en los que se han habilitado cuentas de administrador local, estas cuentas se pueden utilizar para propagar compromisos de seguridad entre los servidores y estaciones de trabajo.

Las cuentas de administrador locales no deben usarse nunca para iniciar sesión en equipos locales ni mucho menos como cuentas de servicio en servidores asociados, su uso está más bien concebido para solucionar incidencias del sistema con arranques en modo seguro. Mencionar aquí por cierto que una buena práctica es cambiar el nombre de la cuenta de Administrador. El objetivo de implementar estas medidas de protección es reducir significativamente la probabilidad de éxito de un ataque que tenga como destino las cuentas de administrador local.

- Algunos de los posibles riesgos o problemas de no llevar a cabo una gestión de credenciales adecuadas serían Robo de credenciales: a través de diversas técnicas o simplemente por mantener los datos durante mucho tiempo, intercambiarse, etc.

- Propagación de Ransomwares y secuestros de información: si no se previenen técnicas de ataque como “pass the hash of the ticket”.

- Robo de datos personales: u otro tipo de información accesible en el activo.

- Eliminación accidental o no de información: a la hora de realizar tareas de administración que no están controladas.

- Desestabilización de la red o de la infraestructura: al configurar opciones o características que el usuario no domina.

Sin duda, se trata de riesgos que podrían paralizar cualquier empresa o sector, imaginemos una mala gestión en un hospital, en una central nuclear o en un sistema armamentístico de misiles, aunque pueda parecer de película, lo cierto es que en la escala empresarial, los riesgos son diferentes pero no igualmente menos importantes.

Para saber más acerca de las técnicas de robo de credenciales visita:

Pass the hash

Pass the ticket

6.- PROTOCOLO RADIUS Y TACACS.

Caso práctico

A Paco, ingeniero de telecomunicaciones, le han pedido desde la alcaldía de su pueblo, que implemente un sistema wifi para la localidad. Lo que también le ha dicho el alcalde, es que quiere que la red únicamente esté disponible para los empadronados en el ayuntamiento, que no quiere que “los de otros pueblos” se conecten. Para ello, Paco implementará un portal cautivo mediante RADIUS que permitirá conectarse únicamente a los ciudadanos de la localidad.

En este punto explicaremos algunos protocolos de la familia AAA, que facilitan el acceso a las redes, del mismo modo que NAC pero en este caso, de manera remota. Esta familia de protocolos fue desarrollados inicialmente para desplegarse mediante líneas analógicas a través de módems pero se usan en la actualidad con las tecnologías existentes. Entre los protocolos más utilizados destacan:

- RADIUS: protocolo creado para autorizar el acceso a las redes a través de módems.
- DIAMETER: evolución del protocolo RADIUS.
- TACACS y TACAS+: (Terminal Access Controller) se trata de protocolos propietarios de CISCO
- EAP: protocolo utilizado para habilitar el acceso en redes de tipo Wireless.
- LDAP: protocolo utilizado para acceder a servicios de directorio en un entorno de red.

RADIUS

Desarrollado en 1991, su acrónimo atiende a Remote Authentication Dial-In User Service. Se trata de un protocolo utilizado para ofrecer acceso a una red a un cliente previa autenticación de este. Si lo trasladamos a un ejemplo concreto, la red wifi de un aeropuerto como la ofrecida por Aena en España, estaría gestionado por un portal cautivo bajo una arquitectura con RADIUS (o similar). Eso significa que para poder disfrutar del acceso wifi, previamente tendremos que habernos registrado para que nos envíen unas credenciales de acceso. Esto mismo lo vemos en muchos hoteles, redes de ayuntamientos, etc.

Para implementar una arquitectura de este tipo, necesitaremos tres elementos:

- Cliente: va a ser quien trate de conectarse a la red. Lo hará a través del Servicio NAS.
- Servicio NAS (Network Access Server): se trata de un servidor intermedio que actuará como un cliente de RADIUS y facilitará la comunicación entre cliente y servidor RADIUS.
- Servidor RADIUS: será el servicio que permitirá el acceso a la red.

El modo de operar de los servidores RADIUS es relativamente sencillo. Primero reciben la petición del cliente y llevan a cabo la autenticación en función de los datos recibidos entregando posteriormente la configuración con la información necesaria para que el cliente pueda acceder al servicio.

6.1. PROBLEMAS DE SEGURIDAD EN RADIUS

Como muchos protocolos, este fue creado sin algunas cuestiones relacionadas con la seguridad que más tarde serían necesarias. Alguno de los problemas relacionados con este protocolo:

- La comunicación se lleva a cabo a través del protocolo UDP, lo que permitiría a un atacante suplantar direcciones IP o directamente falsearlas.
- La información que se transmite en las distintas peticiones de este protocolo no viaja cifrada a excepción de las contraseñas, lo que permitiría a atacantes acceder a la información que se intercambia.
- Para el cifrado de hash, usa el algoritmo MD5 que es vulnerable a ataques de colisión.

6.2. EVOLUCIÓN DE RADIUS

Para corregir los problemas iniciales de RADIUS, se diseñó protocolo DIAMETER basado en este, pero con notables mejoras. Entre ellas podemos destacar:

- Usa protocolos de transportes fiables como TCP o SCTP.
- Usa seguridad a nivel de transporte para el encapsulado de tráfico evitando que se pueda inspeccionar.
- Tiene compatibilidad transicional con RADIUS.
- Pueden usarse modelos con y sin estado.

- Tiene notificación de errores que permiten la depuración del servicio.
- Tiene mejor compatibilidad con roaming, lo que lo hace ideal para cuestiones relacionadas con movilidad.

TACACS

Se trata de un protocolo similar a RADIUS pero específico de tecnología CISCO. Esto significa que deberemos contar con elementos de dicha marca como routers, para poder implementar este tipo de control de acceso a la red.

Si deseas ampliar información acerca de cómo se configuran estos dispositivos, puedes visitar el siguiente enlace: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xr-16/sec-usr-tacacs-xr-16-book/sec-cfgtacacs.html Creado con eXeLearning

Autoevaluación I

¿Cuál no es un uso de la infraestructura KPI?

- a) Firma digital
- b) Gestión de credenciales
- c) Operar con las instituciones de manera segura
- d) Ninguna de las anteriores es cierta

Autoevaluación II

Las aplicaciones que permiten una correcta gestión de credenciales se denominan:

- a) Gestor de contraseñas.
- b) Gestor de permisos
- c) Gestor de accesos

TEST I

1- En un servidor RADIUS todas las peticiones viajan cifradas ¿Verdadero o falso?

- a) Verdadero
- b) Falso

2- Para cubrir las necesidades de protocolos de tipo AAA, Cisco creo:

- a) FreeRadius.
- b) Ninguna respuesta es correcta.
- c) DIAMETER.
- d) TACACS.

3-La firma electrónica es un concepto electrónico que no tiene validez legal ¿Verdadero o falso?

- a) Verdadero
- b) Falso

4- Una de las tecnologías más populares que usa la tecnología PKI es:

- a) icmp.
- b) Ninguna respuesta es correcta.
- c) https.
- d) tcp.

5- RADIUS Y TACACS son protocolos orientados a la autenticación, autorización y conteo ¿Verdadero o falso?

- a) Verdadero
- b) Falso

6- Las contraseñas harcodeadas no son un problema en la gestión de acceso ¿Verdadero o falso?

- a) Verdadero
- b) Falso

7- Un certificado https nunca se puede revocar. Hay que adquirir uno nuevo. ¿Verdadero o falso?

- a) Verdadero
- b) Falso

8- Uno de los principales problemas de un servidor RADIUS es usa el protocolo **** en su implementación:

- a) ICMP.
- b) Ninguna respuesta es correcta.
- c) UDP.
- d) SMTP.

- 9- Un certificado autofirmado, es vulnerable por naturaleza y sería inseguro usarlo ¿Verdadero o falso?
- a) Verdadero
 - b) Falso
- 10- Un certificado web que se ha expedido, ya no es posible revocarlo, habría que adquirir uno nuevo ¿Verdadero o falso?
- a) Verdadero
 - b) Falso

TEST II

- 1- Uno de los usos más extendidos de la tecnología PKI es la firma digital ¿Verdadero o falso?
- a) Verdadero
 - b) Falso
- 2- La segmentación por roles y la modificación periódica de una contraseña forman parte de:
- a) De los marcos de confianza.
 - b) Una correcta gestión de credenciales.
 - c) De los estándares de seguridad.
 - d) Las dimensiones de la seguridad.
- 3- Los grupos por defecto en los servidores y con carácter general son:
- a) De administración y de autenticación
 - b) De seguridad y de administración
 - c) De distribución y de seguridad
 - d) Ninguno de los anteriores
- 4- La implementación NAC es útil para entornos:
- a) Ninguno de los anteriores
 - b) BYOD, el acceso de terceros y para lot
 - c) Solo para el acceso de terceros
 - d) Para lot exclusivamente
- 5- El robo de contraseñas es un resultado de una gestión ineficaz de credenciales ¿Verdadero o falso?
- a) Verdadero
 - b) Falso
- 6- El protocolo https no utiliza la tecnología PKI ¿Verdadero o falso?
- a) Verdadero
 - b) Falso
- 7- Algunas de las soluciones NAC opensource son:
- a) FreeNAC y FenceFirewall.
 - b) FreeNAC y PacketFence.
 - c) FreeNAC y WordFence.
 - d) Ninguna respuesta es correcta.
- 8- DIAMETER no es compatible con RADIUS ¿Verdadero o falso?
- a) Verdadero
 - b) Falso
- 9- Para cubrir las carencias en seguridad de RADIUS se creo TACACS ¿Verdadero o falso?
- a) Verdadero
 - b) Falso
- 10- Las cuentas de administración locales se deberían usar para iniciar sesión ¿Verdadero o falso?
- a) Verdadero
 - b) Falso

Solución

Autoevaluación I: c)

Autoevaluación II: a)

TEST I 8/10: 1 b), 2 d), 3 b), 4 b), 5 a), 6 b), 7 b), 8 c), 9 a) 10 b)

TEST II /10: 1 a), 2 b), 3 c), 4 b), 5 a), 6 b), 7 b), 8 a), 9 b) 10)

Caso práctico

En la empresa de María, las cuentas de usuario consisten en un nombre de usuario y una contraseña (password). En los sistemas operativos estos dos elementos forman un conjunto de credenciales y sirven para identificar a una persona. Utilizar contraseñas es un método para autenticarse, pero no es el único, hay otros métodos como, por ejemplo, el uso de tarjetas inteligentes que tiene la identidad grabada. La administración de credenciales de acceso es algo fundamental debido a los numerosos ataques de contraseñas que hoy día pueden producirse.

De hecho, los sistemas de control de acceso protegidos con contraseña, suelen ser un punto crítico de la seguridad y por ello suelen recibir distintos tipos de ataques, siendo los más comunes los ataques de fuerza bruta y los ataques de diccionario.

Apartado 1: tarea de investigación e implementación

Para elaborar la práctica el alumno deberá investigar cómo llevar a cabo un despliegue de este tipo en un entorno doméstico. Existen numerosas fuentes en Internet que explican cómo llevarlo a cabo.

El alumno mostrará a través de capturas de pantalla el proceso que ha llevado a cabo.

En caso de no disponer de un router compatible, bastará con la explicación detallada del proceso en ese dispositivo.

Elementos necesarios:

- Máquina virtual Ubuntu (u otro Linux)
- Aplicación FreeRADIUS para instalar en Ubuntu
- Router compatible con seguridad RADIUS. Habitualmente los routers actuales de los proveedores de Internet suelen disponer de él.
- Cliente wifi que puede ser un ordenador, móvil, etc.

INTRODUCCIÓN

RADIUS (Remote Authentication Dial-In Service) es un protocolo estándar de red, diseñado para gestionar desde un punto central, tres funciones (AAA): autenticación, verificación de credenciales, certificados o tokens, autorización, definición de los recursos a los que puede acceder un usuario y contabilidad, registro de actividades hechas por el usuario. Este protocolo de Internet se utiliza en redes inalámbricas Wi-fi, VPS y otros servicios para proporcionar seguridad, control de accesos y aplicar políticas. RADIUS opera con tecnologías 802.1X para redes Wi-fi y emplea protocolos PAP, CHAP o EAP para la autenticación. Su comunicación con servidores NAS (de acceso) se realiza mediante UDP a través del puerto 1812.

Implementar este protocolo de seguridad en un servidor (servidor RADIUS) es útil para que una empresa con múltiples ubicaciones o redes complejas porque permite gestionar de manera centralizada el acceso seguro a su red, permitiendo autenticar y autorizar tanto empleados y dispositivos desde un único punto. Esto garantiza que únicamente las personas autorizadas tengan acceso a los recursos, fortaleciendo la seguridad y haciendo posible llevar un monitoreo y cumplimiento normativo.

FreeRADIUS es un servidor RADIUS de código abierto que centraliza la autenticación, autorización y contabilidad de usuarios en redes y servicios. Se utiliza para validar credenciales, gestionar permisos y registrar actividades, siendo clave en redes Wi-fi, VPS, empresas...

Funciona integrándose con bases de datos como LDAP o Active Directory y dispositivos como puntos de acceso Wi-fi o Switches, garantizando seguridad y control de acceso. Su flexibilidad, escalabilidad y compatibilidad con protocolos como 802.1X o EAP lo hacen ideal para gestionar usuarios en redes modernas de forma eficiente y gratuita.

En mi caso el router del que dispongo, no tiene la opción de activar la seguridad WPA2- Enterprise para poder configurar RADIUS con todos sus requisitos, así que intentaré recrear esta práctica con:

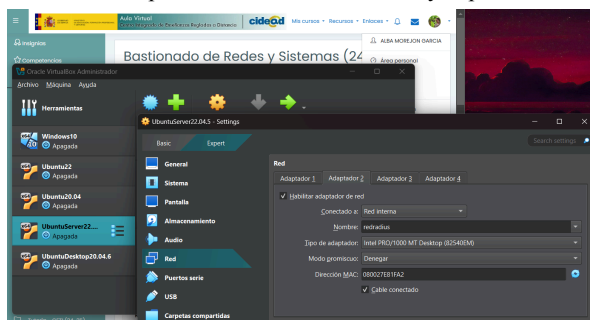
FUNCIÓN	VERSIÓN	IP
Servidor RADIUS	Ubuntu Server 22.04.5	192.168.50.1
Cliente Linux	Ubuntu Desktop 20.04.6	192.168.50.2

PROCESO DE DESPLIEGUE

1. CONFIGURAR RED

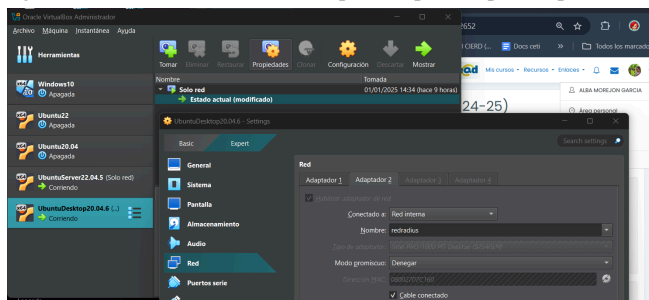
ADAPTADORES

En el Servidor RADIUS ponemos el adaptador 1 en la opción NAT y habilitamos el adaptador 2 en Red Interna eligiendo el nombre de "redradius". enp0s3 - nat - 080027CDF1B2 y enp0s8 - redinterna - 080027E81FA2



En el ClienteLinux elegimos la misma configuración que la máquina UbuntuServer22, Red interna: redradius

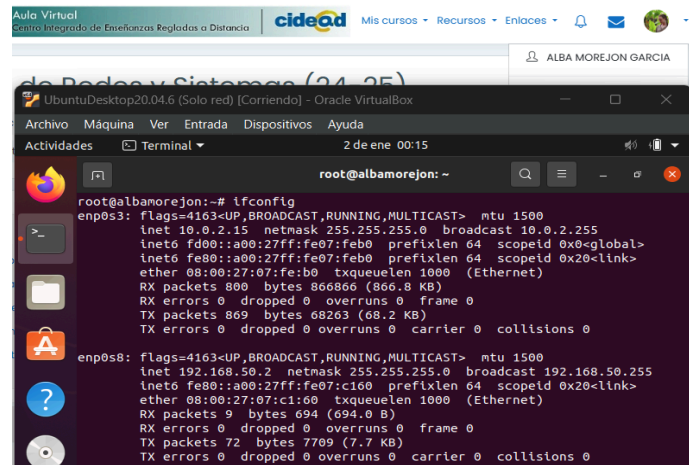
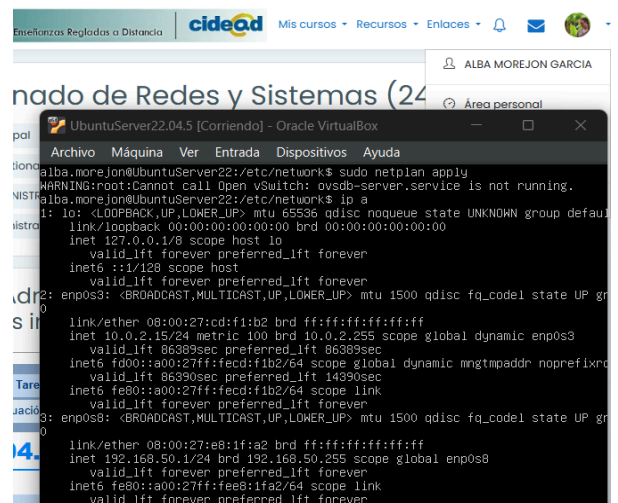
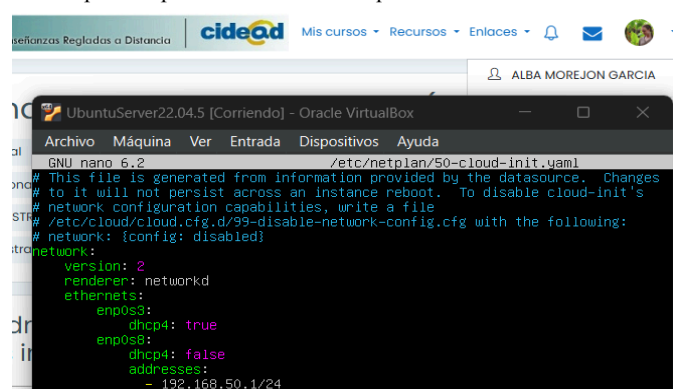
*en principio la idea iba a ser que la máquina ubuntu server 22 fuera la única que saliese a internet pero tras encontramos posteriormente algún error en la resolución DNS optamos por la opción aplicada.



enp0s3 - nat- 08002707FEB0 y enp0s8 - redinterna - 08002707C160
IPs

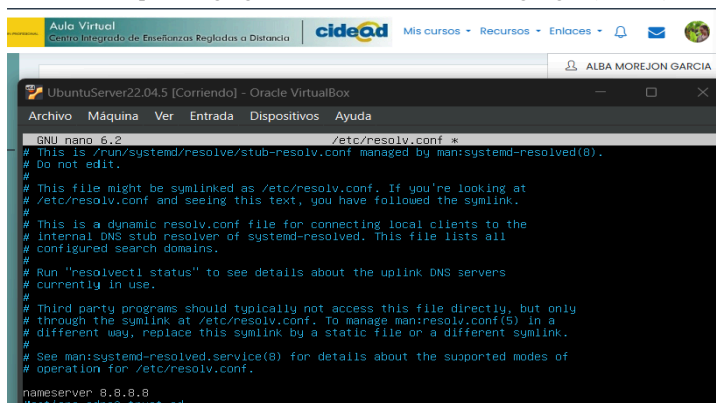
Para la configuración de redes utilizaremos netplan, añadimos los datos necesarios en el siguiente fichero: “/etc/netplan/nom_fichero” y aplicamos los cambios con “sudo netplan apply”.

Con la ip correspondiente en cada máquina.



DNS

En ambas máquinas agregamos los servidores dns de google (8.8.8.8) en el fichero “/etc/resolv.conf”



Con esto, ambas máquinas tendrían salida a internet y se conectarán entre ellas.

2. CONFIGURAR SERVIDOR RADIUS

Primero haremos una mejora y una actualización de las máquinas con los siguientes comandos:

“sudo apt update && sudo apt upgrade -y”

Instalamos el paquete principal del servidor y herramientas adicionales con el comando

“sudo apt install freeradius freeradius-utils -y” que sería

```

UbuntuServer22.04.5 (Solo red) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
alba.morejon@UbuntuServer22:~$ sudo apt install freeradius freeradius-utils -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done

```

Modificamos el fichero de configuración para clientes “/etc/freeradius/3.0/clients.conf”, que enviará las solicitudes de autenticación al servidor radius (que sería en este caso el UbuntuServer22)

```

UbuntuServer22.04.5 (Solo red) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 6.2 /etc/freeradius/3.0/clients.conf
# the "ipaddr" or "ipv6addr" fields. For compatibility, the I.X
# format is still accepted.
#
client Ubuntu {
    ipaddr = 192.168.50.1
    secret = testing123
}

```

Los datos serían la ip del dispositivo que hará de router (la propia máquina), la contraseña entre el cliente y el servidor.

A continuación, editamos el archivo de usuarios para añadir el usuario con el que haremos las pruebas de autenticación, el fichero es:

“/etc/freeradius/3.0/mods-config/files/authorize”

```

UbuntuServer22.04.5 (Solo red) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 6.2 /etc/freeradius/3.0/mods-config/files/authorize
#
# The canonical testing user which is in most of the
# examples.
#
bob ClearText-Password := "hello"
    Reply-Message := "Hello, %(User-Name)"
#
# testuser ClearText-Password := "password"

```

Modificamos el archivo eap “/etc/freeradius/3.0/mods-available/eap” para que la autenticación sea WPA2-Enterprise (PEAP) que es la más común en redes Wi-fi.

```

UbuntuServer22.04.5 (Solo red) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 6.2 /etc/freeradius/3.0/mods-available/eap
# users then cannot use ANY other authentication method.
#
eap {
    # Invoke the default supported EAP type when
    # EAP-Identity response is received.
    #
    # The incoming EAP messages DO NOT specify which EAP
    # type they will be using, so it MUST be set here.
    #
    # For now, only one default EAP type may be used at a time.
    #
    # If the EAP-Type attribute is set by another module,
    # then that EAP type takes precedence over the
    # default type configured here.
    #
    default_eap_type = md5
    default_eap_type = peap
    #
    # A list is maintained to correlate EAP-Response
    # packets with EAP-Request packets. After a
    # configurable length of time, entries in the list
    # expire, and are deleted.
    #
    timer_expire = 60
}

```

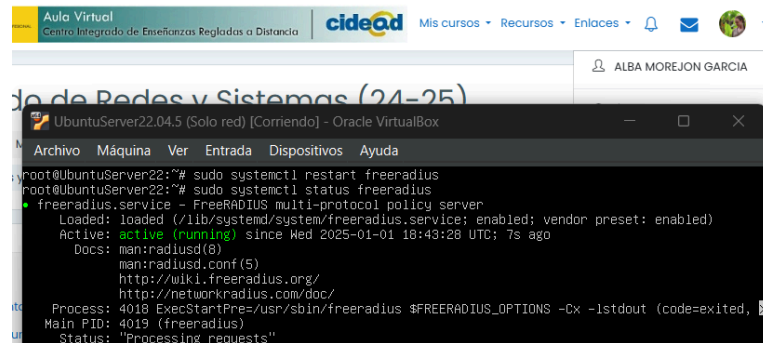
Aseguramos que el usuario/grupo freerad tengan propiedad y total sobre los archivos de configuración para freeradius, así como permisos de lectura y modificación.

```

UbuntuServer22.04.5 (Solo red) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@UbuntuServer22:~# sudo chown -R freerad:freerad /etc/freeradius/3.0/
root@UbuntuServer22:~# sudo chown -R 640 /etc/freeradius/3.0/
root@UbuntuServer22:~#

```

Después de las modificaciones, reiniciamos el servicio.



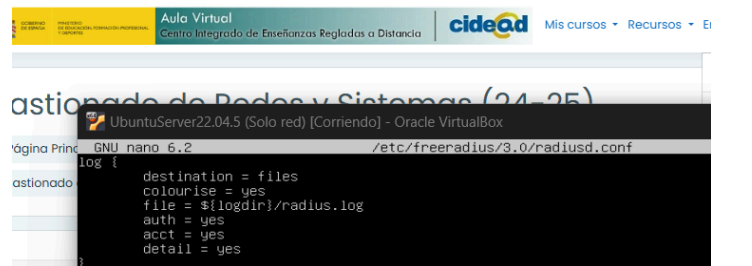
```

root@UbuntuServer22:~# sudo systemctl restart freeradius
root@UbuntuServer22:~# sudo systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
   Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2025-01-01 18:43:28 UTC; 7s ago
     Docs: man:radiusd(8)
           man:radiusd.conf(5)
           http://wiki.freeradius.org/
           http://networkradius.com/doc/
   Process: 4018 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cx -lstdout (code=exited,
   Main PID: 4019 (freeradius)
   Status: "Processing requests"
  
```

Monitorear los accesos en el servidor

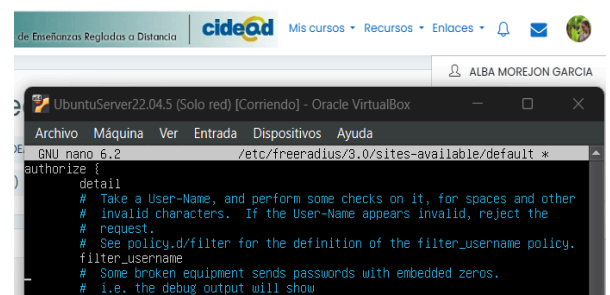
Definimos el comportamiento del log, para que se guarden en archivos en la ruta que le indicamos, que se registren las autenticaciones con los detalles y los inicios rechazados. En el fichero:

“/etc/freeradius/3.0/radiusd.conf” y “/etc/freeradius/3.0/sites-available/default”



```

log {
    destination = files
    colourise = yes
    file = $logdir/radius.log
    auth = yes
    acct = yes
    detail = yes
}
  
```



```

authorize {
    detail
    # Take a User-Name, and perform some checks on it, for spaces and other
    # invalid characters. If the User-Name appears invalid, reject the
    # request.
    # See policy.d/filter for the definition of the filter_username policy.
    filter_username
    # Some broken equipment sends passwords with embedded zeros.
    # i.e. the debug output will show
  
```



```

authenticate {
    Auth-Type Reject {
        reject
    }
    # PAP authentication, when a back-end database listed
    # in the 'authorize' section supplies a password. The
    # password can be clear-text, or encrypted.
    Auth-Type PAP {
        pap
    }
  
```

Reiniciamos el servicio con “sudo systemctl restart freeradius”

3. PRUEBAS

Recordemos:

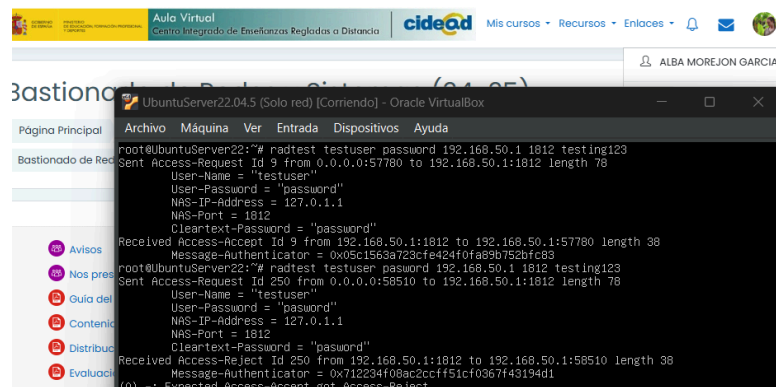
Client: 192.168.50.1 - testing123

User: testuser - password

Probamos la autenticación con usuario que habíamos creado, utilizando el comando:

“radtest testuser password 192.168.50.1 1812 testing123”

Hacemos dos intentos de inicio uno bien y el siguiente con un error



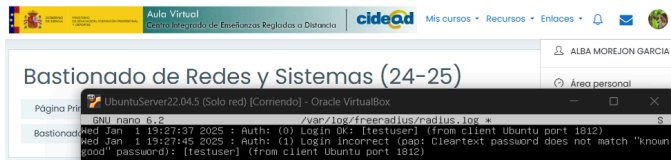
```

root@UbuntuServer22:~# radtest testuser password 192.168.50.1 1812 testing123
Sent Access-Request Id 9 from 0.0.0.0:57780 to 192.168.50.1:1812 length 78
  User-Name = "testuser"
  User-Password = "password"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Cleartext-Password = "password"
Received Access-Accept Id 9 from 192.168.50.1:1812 to 192.168.50.1:57780 length 38
  Message-Authenticator = 0x05c1563a723cfe424f0fa89b752bfc83
root@UbuntuServer22:~# radtest testuser password 192.168.50.1 1812 testing123
Sent Access-Request Id 250 from 0.0.0.0:58510 to 192.168.50.1:1812 length 78
  User-Name = "testuser"
  User-Password = "password"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Cleartext-Password = "password"
Received Access-Reject Id 250 from 192.168.50.1:1812 to 192.168.50.1:58510 length 38
  Message-Authenticator = 0x712234f08ac2ccff51cf0367f43194d1
(0) -> Expected Access-Accept got Access-Reject
  
```

En la primera conexión, el servidor radius ha aceptado la solicitud de autenticación, el mensaje proviene de la dirección ip 192.168.50.1:1812, la respuesta fue enviada de vuelta al cliente por el puerto 42163 y el mensaje de autenticación es un código hash que garantiza la seguridad.

El segundo intento ha sido rechazado (Received Access-Reject)

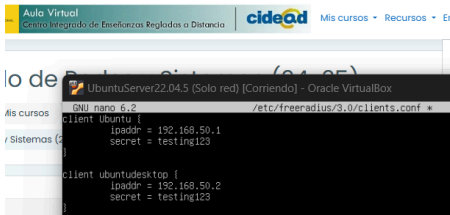
Verificamos los logs en el fichero “/var/log/freeradius/radius.log” en el que se nos mostrarían todos los detalles como el día, la hora, la autenticación, etc.



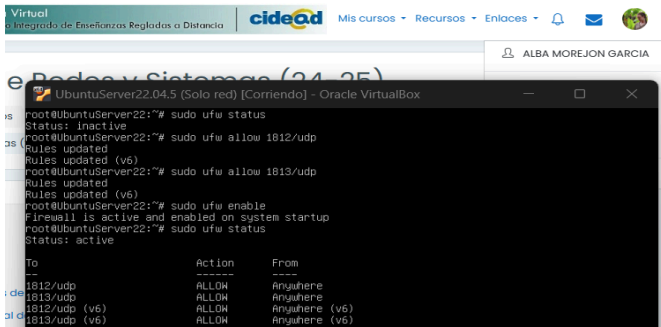
4. CONFIGURAR CLIENTE

Configuramos la máquina UbuntuDesktop20 como cliente para que se pueda autenticar en el servidor freeradius (UbuntuServer22)

En el UbuntuServer22 modificamos el fichero de configuración del cliente para permitir la autenticación desde la otra máquina: “/etc/freeradius/3.0/clients.conf”

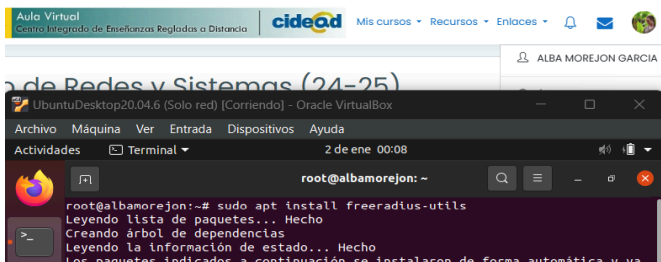


(Opcional) Para evitar que nos de algún problema habilitamos el firewall y abrimos los puerto 1812 y 1813 que son los que utiliza el servicio radius

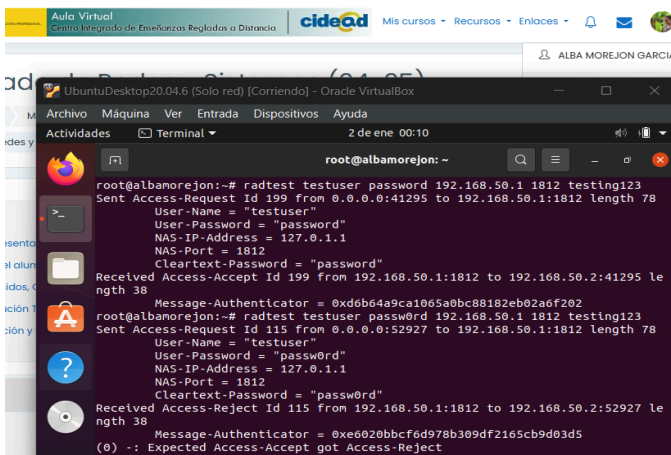


Ahora configuramos el cliente UbuntuDesktop20

Instalamos las herramienta adicionales con el comando “sudo apt install freeradius-utils”



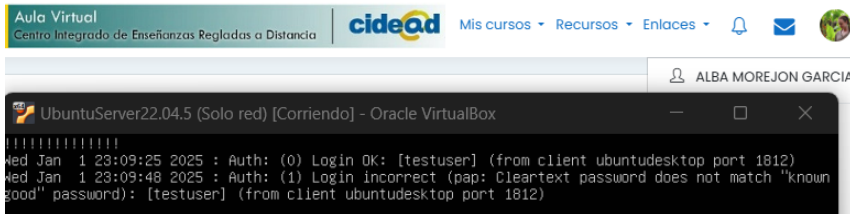
Hacemos dos pruebas de acceso, una con los datos bien y otra con los datos mal.



En la primera conexión vemos que ha sido aceptada (Received Access-Accept) y la segunda rechazada (Received Access-Reject)

Para mostrar los logs a tiempo real, utilizamos el comando:

“tail -f /var/log/freeradius/radius.log”



```

Aula Virtual
Centro Integrado de Enseñanzas Regladas a Distancia
cideaod Mis cursos Recursos Enlaces
ALBA MOREJON GARCIA

UbuntuServer22.04.5 (Solo red) [Corriendo] - Oracle VirtualBox
#####
Wed Jan 1 23:09:25 2025 : Auth: (0) Login OK: [testuser] (from client ubuntu desktop port 1812)
Wed Jan 1 23:09:48 2025 : Auth: (1) Login incorrect (pap: Cleartext password does not match "known
good" password): [testuser] (from client ubuntu desktop port 1812)

```

Adicional:

En caso de querer borrar todo lo instalado para el servidor radius los comandos serían:

sudo rm -rf /etc/freeradius

sudo rm -rf /var/log/freeradius

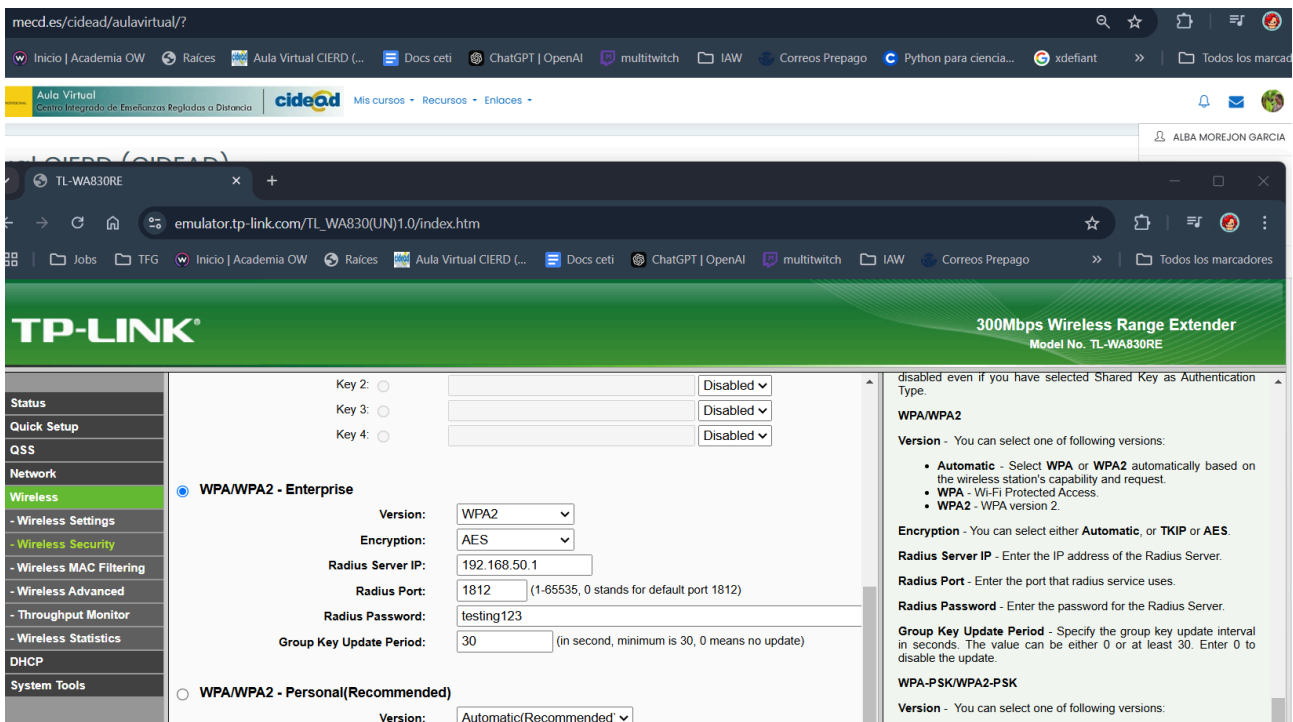
sudo rm -rf /usr/lib/freeradius

sudo apt purge freeradius freeradius-utils freeradius-config -y

El único router que he encontrado con la posibilidad de activar la seguridad RADIUS es:

TL-WA830RE, V1, Versión de firmware: 111108

Así se haría la configuración en caso de tener un router compatible y después solo haría falta loguearse con los usuarios creados, en la red Wi-fi



meed.es/cideaod/aulavirtual/?

Inicio | Academia OW | Raíces | Aula Virtual CIERD (...) | Docs ceti | ChatGPT | OpenAI | multitch | IAW | Correos Pre pago | Python para ciencia... | xdefiant | Todos los marcadores

Aula Virtual
Centro Integrado de Enseñanzas Regladas a Distancia

cideaod Mis cursos Recursos Enlaces

ALBA MOREJON GARCIA

TL-WA830RE

emulator.tp-link.com/TL_WA830(UN)1.0/index.htm

TP-LINK® 300Mbps Wireless Range Extender Model No. TL-WA830RE

Key 2: Disabled
Key 3: Disabled
Key 4: Disabled

☒ WPA/WPA2 - Enterprise

Version: WPA2
Encryption: AES
Radius Server IP: 192.168.50.1
Radius Port: 1812 (1-65535, 0 stands for default port 1812)
Radius Password: testing123
Group Key Update Period: 30 (in second, minimum is 30, 0 means no update)

☐ WPA/WPA2 - Personal(Recommended)
Version: Automatic(Recommended)

disabled even if you have selected Shared Key as Authentication Type.

WPA/WPA2
Version - You can select one of following versions:
• Automatic - Select WPA or WPA2 automatically based on the wireless station's capability and request.
• WPA - Wi-Fi Protected Access.
• WPA2 - WPA version 2.

Encryption - You can select either Automatic, or TKIP or AES.

Radius Server IP - Enter the IP address of the Radius Server.

Radius Port - Enter the port that radius service uses.

Radius Password - Enter the password for the Radius Server.

Group Key Update Period - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

WPA-PSK/WPA2-PSK
Version - You can select one of following versions: