Tarea 2

Autenticación multifactor

AAA en IT y CLOUD

Ciberseguridad Módulo 4

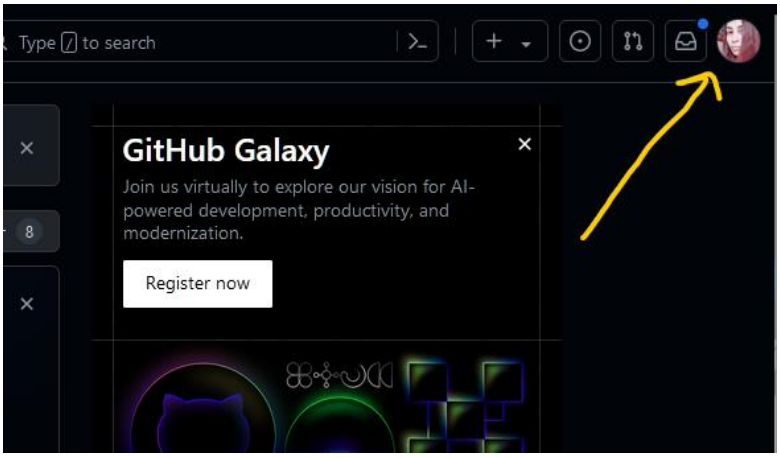
AAA23

Índice

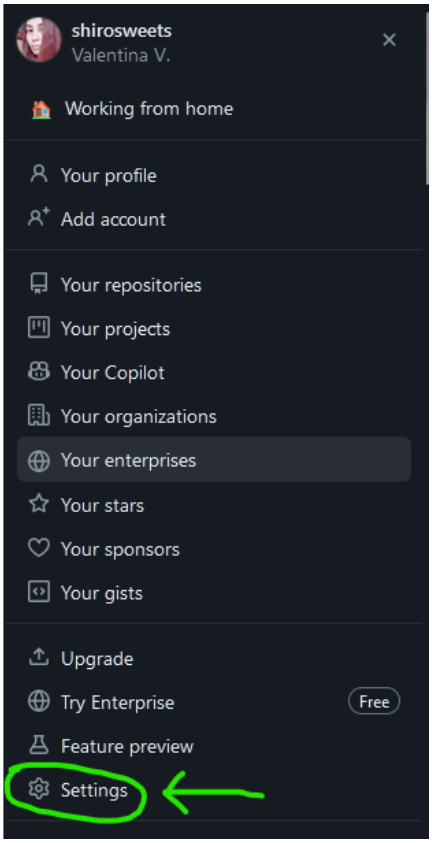
OTP

OTP, *"One-Time Password"* ("Contraseña de un Solo Uso"), es un método de autenticación que proporciona una contraseña temporal que se utiliza para acceder a una cuenta o servicio en línea una sola vez. Estas contraseñas son generadas por un sistema (software) y son válidas por un período corto de tiempo, generalmente unos pocos minutos, antes de expirar. El propósito principal de las contraseñas de un solo uso es aumentar la seguridad al proporcionar una capa adicional de protección contra el acceso no autorizado a cuentas en línea.

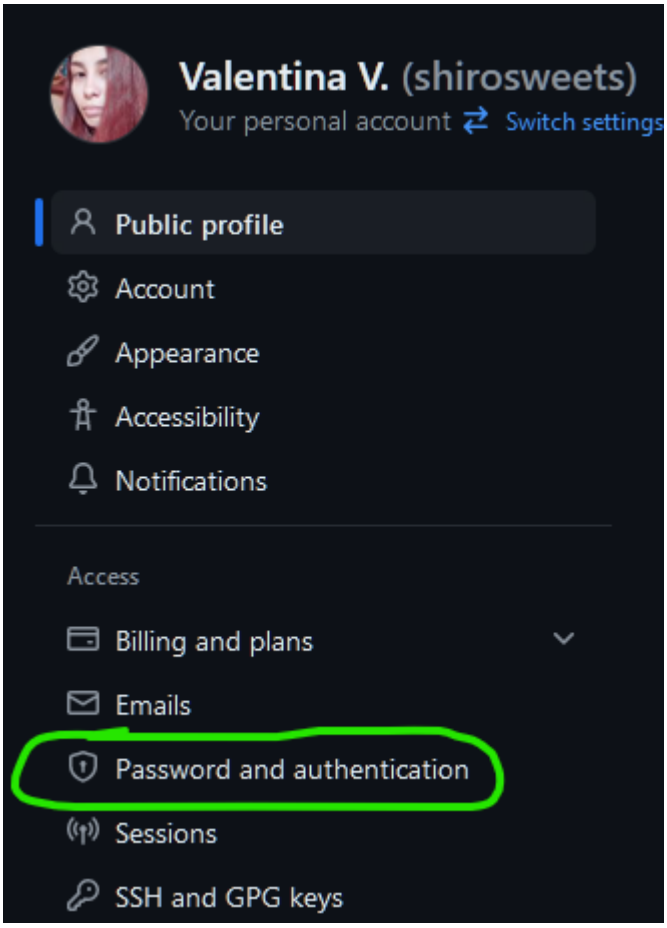
¿Cómo utilizar Google Authenticator en GitHub?

1. Descargar Google Authenticator.
2. Ingresar a GitHub con nuestro usuario y contraseña.
3. Hacer click en la imagen de perfil.
   a. 

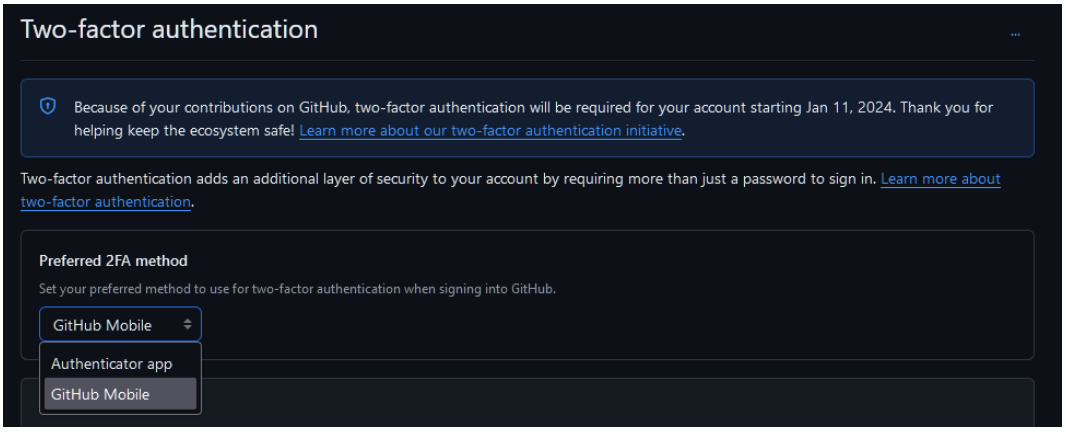
4. Ir a configuración, en la esquina superior derecha de la página.

a. 

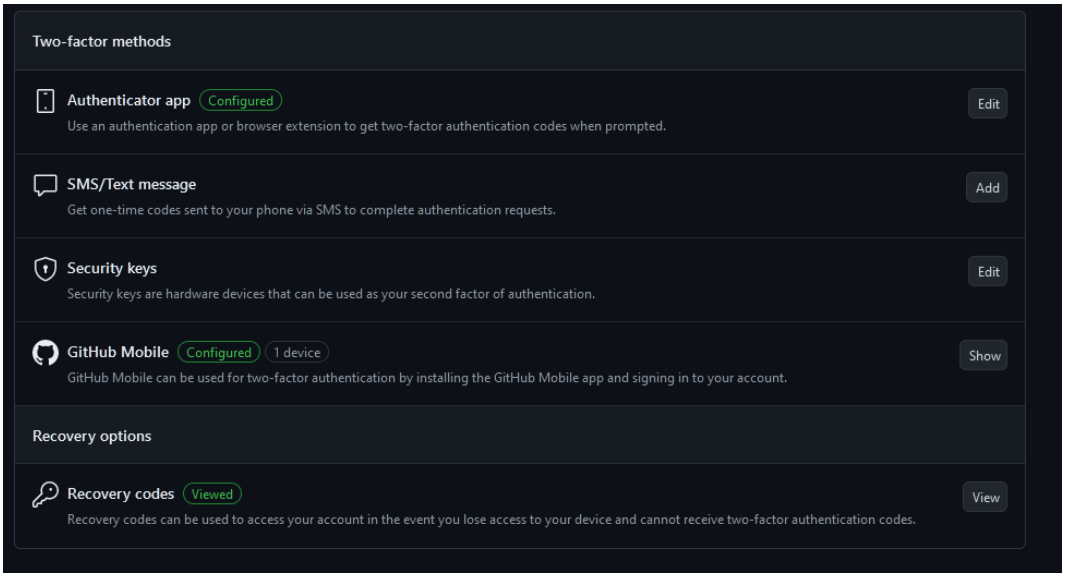
5. Ir al apartado “Password and authentication”

a. 

6. Scrollear hasta el apartado “Two-factor authentication” y en “Preferred 2FA method” seleccionar “Authenticator app”

a. 

7. Y en el apartado “Two-factor methods” configuramos “Authenticator app”, o agregamos este método si nunca lo hemos configurado.

a. 

8. Nos solicitará escanear un código QR que deberemos escanear con la aplicación Google Authenticator.
    a. Luego, nos solicitará el código que aparece en la aplicación.
        i. Si es correcta, nos mostrará códigos de recuperación que deberemos almacenar de manera segura.
9. Para verificar que este método fue correctamente implementado, podemos desconectarnos y probar ingresar nuevamente a GitHub con nuestro usuario y contraseña. Si todo el proceso fue exitoso, nos solicitará el código TOTP de la aplicación.

Conclusión Google Authenticator

Esta herramienta la recomiendo si se debe optar por una opción no open source. Varias empresas, tienen como política no utilizar herramientas open source, por algunas regulaciones que dejan en un “gris” ciertos incidentes que puedan ser origen por estos softwares.

Zero Trust

El enfoque llamado "Zero Trust" (Confianza Cero) se basa en la premisa de que las organizaciones no deben confiar en ninguna **entidad** dentro o fuera de su red de manera predeterminada. Esto significa que todas las solicitudes de acceso, ya sea desde dentro o fuera de la red, deben ser **verificadas** y **autenticadas** de manera exhaustiva antes de ser concedidas.

Los principios de Zero Trust que están estrechamente asociados a AAA son:

1. **Autenticación Continua**: la autenticación se realiza de forma continua y dinámica, en lugar de confiar en una única autenticación inicial. Se verifica la identidad del usuario o dispositivo en cada interacción.
2. **Autorización Basada en Políticas**: las decisiones de autorización se basan en políticas específicas y granulares que definen qué recursos pueden ser accedidos por quién y en qué circunstancias.
3. **Auditoría y Monitorización Continuas:** se realiza una monitorización constante de las actividades de los usuarios y dispositivos, y de los accesos a los recursos, para detectar comportamientos anómalos o potencialmente maliciosos.

Dichos principios ayudan a garantizar que las organizaciones puedan mantener un alto nivel de seguridad y mitigar el riesgo de violaciones de datos y otras amenazas cibernéticas.

ZTA: Zero Trust Architectures

Las arquitecturas Zero Trust, arquitectura de confianza cero, se basa en la separación de los servicios en microservicios. Se separa en capas dedicadas, de las cuales podemos mencionar el servicio de red que provee a los servicios de aplicación.

Generalmente, los servicios de instancia de red son desplegados para manejar un único clúster, donde múltiples clústeres separan múltiples sitios on-premises (posee y administra sus propios servidores) y muchas zonas de disponibilidad en diferentes clouds.

Requerimientos de ZTA para un control de acceso granular

Para implementar un control de acceso granular en una arquitectura Zero Trust (ZTA), es fundamental contar con una combinación de tecnologías y prácticas que permitan definir y aplicar políticas de acceso detalladas a recursos y datos. Aquí hay algunos requisitos clave para lograr un control de acceso granular efectivo:

1. **Política de Control de Acceso Basada en Atributos (ABAC)**:
    - Utilizar una política ABAC que tome decisiones de acceso basadas en múltiples atributos del sujeto, el recurso y el entorno. Esto permite una autorización más dinámica y adaptable.
2. **Autenticación y Autorización Contextual**:
    - Implementar mecanismos de autenticación y autorización contextual que consideren factores como la ubicación del usuario, la hora del día, el estado del dispositivo, etc., para adaptar las políticas de acceso según el contexto.
3. **Control de Acceso Dinámico**:
    - Permite la actualización dinámica de las políticas de acceso en función de los cambios en el entorno de la red, el estado del usuario o el riesgo percibido. Esto garantiza una respuesta ágil a las amenazas y cambios en el entorno.
4. **Gestión de Identidades y Accesos (IAM)**:
    - Implementar una solución IAM que permita la gestión centralizada de identidades, roles y privilegios de acceso. Esto garantiza la coherencia y la eficiencia en la aplicación de políticas de acceso granular.
5. **Segregación de Funciones (SoD)**:
    - Aplicar el principio de segregación de funciones para limitar los privilegios de acceso y reducir el riesgo de abuso o mal uso de recursos. Esto implica asignar roles y permisos de acceso de manera cuidadosa y controlada.
6. **Encriptación de Datos**:
    - Utilizar la encriptación para proteger los datos en reposo, en tránsito y en uso. Esto garantiza la confidencialidad e integridad de los datos, incluso en caso de acceso no autorizado.
7. **Auditoría y Registro de Acceso**:

   - Implementar mecanismos de auditoría y registro de acceso que registren todas las actividades de acceso a recursos y permitan la detección y respuesta rápida ante incidentes de seguridad.
8. **Interoperabilidad y Estándares Abiertos**:
   - Asegurar que las soluciones de control de acceso sean interoperables y basadas en estándares abiertos para facilitar la integración con otros sistemas de seguridad y herramientas de gestión.

Al cumplir con estos requisitos, podrás establecer un control de acceso granular efectivo en tu arquitectura Zero Trust, lo que ayudará a proteger tus activos digitales contra amenazas internas y externas.

Otras recomendaciones son:

1. **Autenticación Fuerte**: Utiliza métodos de autenticación multifactor (MFA) para verificar la identidad de los usuarios y dispositivos antes de permitir el acceso a recursos sensibles. Esto puede incluir la verificación biométrica, tokens de seguridad, códigos de un solo uso, entre otros.
2. **Autorización Basada en Políticas**: Define políticas de acceso detalladas que determinen quién puede acceder a qué recursos y en qué circunstancias. Estas políticas deben ser flexibles y adaptarse dinámicamente según el contexto del acceso, como la ubicación del usuario, el dispositivo utilizado y la sensibilidad de los datos.

Despliegue de Zero Trust Achitectures

El despliegue de arquitecturas Zero Trust (Confianza Cero) implica un enfoque de seguridad que elimina la confianza implícita en la red (no confiar) y requiere verificación explícita de cualquier entidad que intente acceder a recursos, ya sea dentro o fuera de la red corporativa.

1. **Inventario de Activos**: Identifica y clasifica todos los activos, incluyendo dispositivos, aplicaciones y datos, tanto dentro como fuera de la red corporativa.
2. **Mapeo de Flujos de Datos**: Comprende cómo fluyen los datos a través de la red y entre los activos. Esto te ayudará a identificar puntos de acceso y posibles vulnerabilidades.

3. **Segmentación de Red**: Divide la red en segmentos más pequeños y seguros. Esto reduce la superficie de ataque y limita la propagación de amenazas en caso de una violación de seguridad.
4. **Autenticación Multifactor (MFA)**: Implementa la autenticación multifactor para verificar la identidad de los usuarios y dispositivos antes de permitir el acceso a recursos sensibles.
5. **Control de Acceso Basado en Políticas**: Establece políticas granulares de control de acceso que determinen quién puede acceder a qué recursos y en qué circunstancias. Esto se puede lograr mediante soluciones de seguridad como firewalls de próxima generación, soluciones de acceso seguro a la nube (CASB) y soluciones de gestión de identidades y accesos (IAM).
6. **Monitoreo Continuo**: Implementa herramientas de monitoreo de seguridad para detectar y responder a amenazas en tiempo real. Esto incluye análisis de comportamiento de usuarios y dispositivos, así como detección de anomalías en el tráfico de red.
7. **Encriptación**: Utiliza la encriptación para proteger los datos en reposo, en tránsito y en uso, tanto dentro como fuera de la red corporativa.
8. **Actualizaciones y Parches**: Mantén todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad para mitigar vulnerabilidades conocidas.
9. **Concientización y Capacitación**: Educa a los empleados sobre las mejores prácticas de seguridad, como la identificación de correos electrónicos de phishing y el uso seguro de contraseñas.
10. **Pruebas de Penetración y Evaluaciones de Seguridad**: Realiza pruebas de penetración regulares y evaluaciones de seguridad para identificar y remediar posibles debilidades en la arquitectura Zero Trust.
11. **Adopción Gradual**: Implementa la arquitectura Zero Trust de manera gradual, comenzando con segmentos de red menos críticos y expandiéndola gradualmente a medida que adquieres experiencia y recursos.

Bajo este enfoque, cada aplicación es implementada, generalmente, como microservicio con un servicio en una instancia de red para cada clúster. Cada servicio tiene reglas estrictas de ingreso y salida para el tráfico de la red. El servicio de red es una infraestructura dedicada que proporciona todos los servicios de la aplicación, incluidos controles de seguridad como la comunicación segura y el control de acceso a nivel de aplicación.

Al seguir estos pasos adaptándose a las necesidades específicas de la organización, se logrará desplegar con éxito una arquitectura Zero Trust, lo cual, que mejorará significativamente la seguridad de tu infraestructura.

Análisis del diagrama de red

Controles de acceso que pueden implementarse

Seguridad de puertos:

- Limitar los puertos abiertos de las máquinas.
- Si no se utiliza, por ejemplo, la herramienta Portainer, que dichas máquinas no tenan acceso a este puerto.

En el diagrama de red no queda explícito quién tiene acceso a qué y a qué no:

- Definir accesos.
- Definir permisos y roles.

Red pública para invitados:

- Dicha red, deberá solicitar un ingreso con un usuario a cualquier persona que quiera acceder a la red. De esta manera, si se encuentra alguna anomalía, se puede saber el origen.

Red privada:

- Whitelist de los dispositivos permitidos, solo para uso de trabajo.
- Los dispositivos como celulares o notebooks personales no podrán utilizarse en esta red.

Autenticación:

- Todos los dispositivos deben tener claves fuertes.
- Todos los ordenadores y servidores deben contar con acceso por ssh como root desactivado. Tener activo el MFA por ssh y cualquier otra herramienta de la terminal que lo permita.

NextCloud:

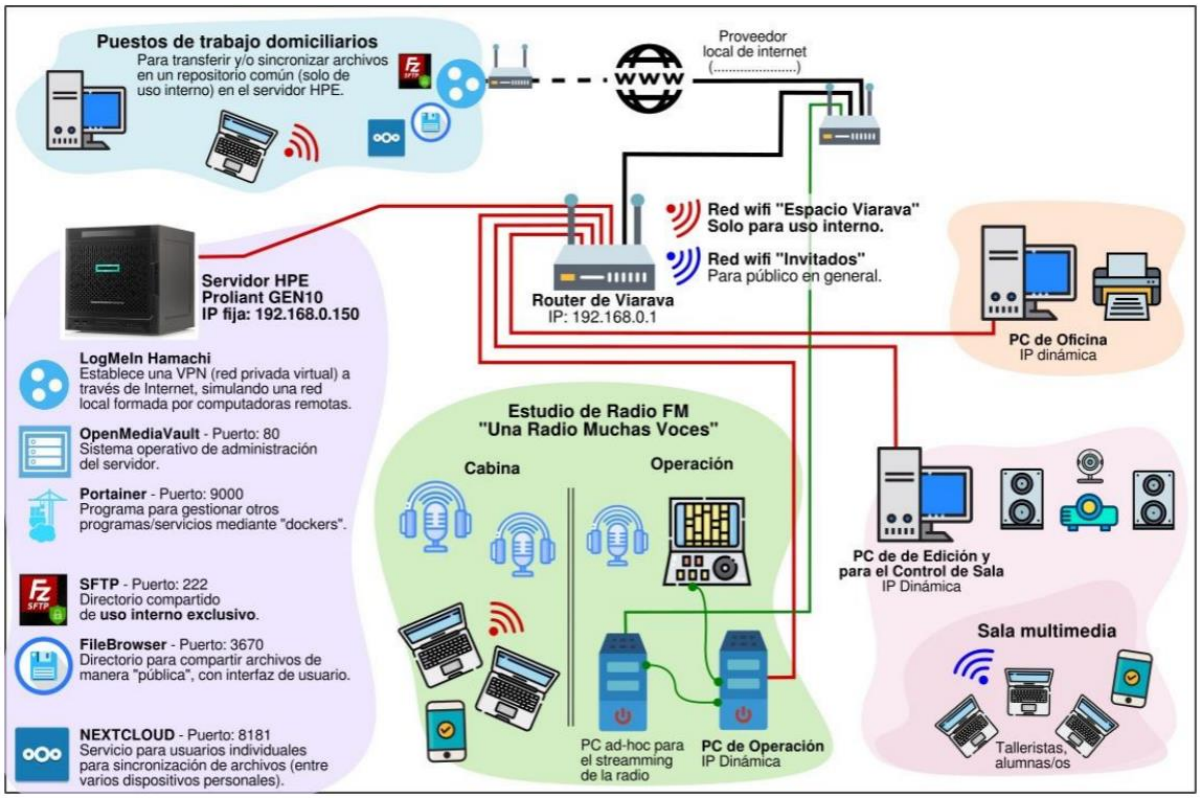
- Si se usa únicamente para uso personal, denegar el uso de la herramienta en dispositivos de trabajo.
- Si esta herramienta se utiliza para el trabajo, establecer limitaciones y restricciones de su uso.

Portainer:

- En el diagrama no se visualiza que se utilice en otro lugar diferente del servidor.
    - Si es el caso, restringir en todos los dispositivos.

Agregar un monitoreo del tráfico de la red:

- Esto permitirá saber qué está ocurriendo en la red.
- Establecer alertas ante anomalías.



La implementación puede ser realizada con herramientas open source.

Referencias

https://docs.github.com/en/authentication/securing-your-account-with-two-factor-authentication-2fa/accessing-github-using-two-factor-authentication

https://docs.github.com/en/authentication/securing-your-account-with-two-factor-authentication-2fa/configuring-two-factor-authentication#configuring-two-factor-authentication-using-a-totp-app