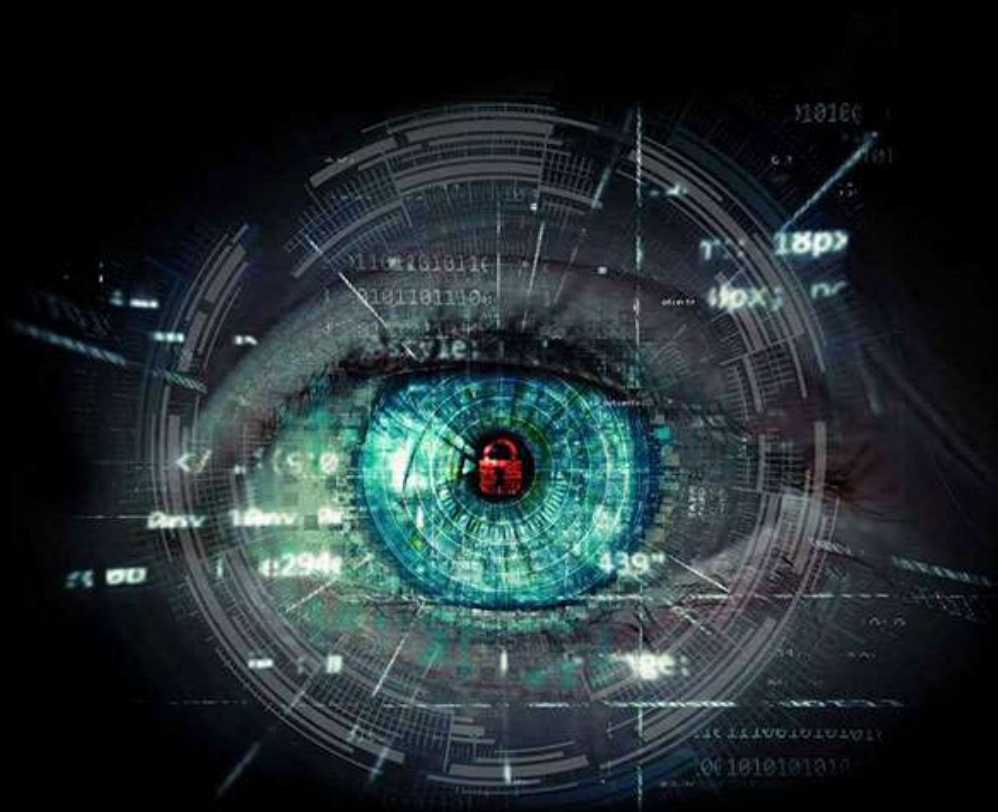




Fraudes Informáticos y Robos de Información

Por: Amairanis Saldaña
Rosmery

Concept



Fraude Informatico

01

Cualquier actividad ilegal que utiliza un sistema informático como herramienta principal para cometer el delito. Esto incluye el robo de información, la manipulación de datos, el acceso no autorizado a sistemas y la distribución de malware.

Robo de Información

02

Es la adquisición ilegal de información confidencial, personal o valiosa, almacenada en formato digital o físico, sin el consentimiento o conocimiento del propietario.

Características de Los Fraudes Informáticos y Robo de Identidad



✚ **Uso de tecnología avanzada:** Los ciberdelincuentes emplean software especializado, malware y técnicas como phishing o ataques de fuerza bruta para acceder a sistemas y obtener información confidencial.



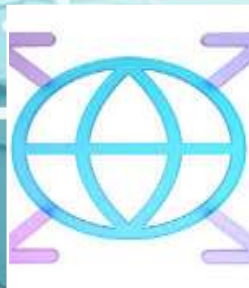
✚ **Dificultad para rastrear:** Los fraudes informáticos suelen ser difíciles de rastrear debido a la facilidad con la que los atacantes pueden ocultar su identidad, utilizando técnicas como el enmascaramiento de IP, redes VPN o el uso de la "dark web".



✚ **Acceso no autorizado a datos:** El objetivo principal de estos fraudes es obtener información sensible, como datos financieros, credenciales de acceso o propiedad intelectual, que luego puede ser utilizada para beneficio económico o chantaje.



✚ **Ingeniería social:** Muchas veces, los ataques no dependen únicamente de vulnerabilidades técnicas, sino también de manipular emocionalmente a las personas para que revelen información importante, como contraseñas o números de tarjetas de crédito.



✚ **Alcance global:** Los fraudes informáticos pueden dirigirse a cualquier persona o empresa en cualquier parte del mundo, haciendo que sean amenazas globales difíciles de combatir.

Importancia

Impacto económico:



Genera pérdidas millonarias a individuos, empresas y gobiernos.

Daño a la reputación:



Afecta la confianza en las instituciones y empresas.

Violación de la privacidad:



Expone datos personales y sensibles de las personas



Amenazas



Phishing: Engaño a través de correos electrónicos o sitios web falsos para obtener información confidencial.

Malware: Software malicioso que infecta sistemas para robar datos o causar daños.

Ransomware: Cifrado de datos con el objetivo de extorsionar a las víctimas.



Amenaza

Ataques de denegación de servicio (DoS): Sobrecarga de un sistema para que deje de funcionar.

Ingeniería social: Manipulación psicológica para obtener información o acceso a sistemas.

Prevención



Contraseñas seguras: Utilizar contraseñas robustas y únicas para cada cuenta.

Software de seguridad: Instalar antivirus, antimalware y firewall.

Actualizaciones: Mantener el software y los sistemas operativos actualizados.

Conciencia y educación: Capacitarse sobre las amenazas y cómo protegerse.

Precaución en línea: No hacer clic en enlaces sospechosos ni descargar archivos de fuentes desconocidas.

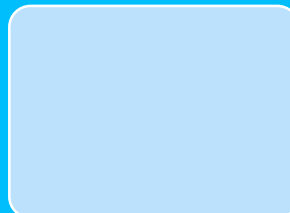
Ventajas del uso de la tecnología para la prevención:



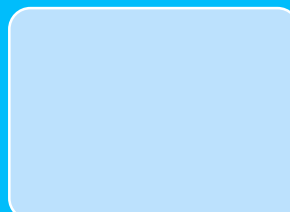
Automatización: Detección y respuesta a amenazas en tiempo real.



Escalabilidad: Protección de grandes volúmenes de datos y sistemas.



Análisis de datos: Identificación de patrones y anomalías para prevenir ataques.



Actualización constante: Adaptación a las nuevas amenazas y vulnerabilidades.



Costos: Implementación y mantenimiento de soluciones de seguridad.



Complejidad: Configuración y gestión de sistemas de seguridad.
Dependencia tecnológica:
Vulnerabilidad ante fallos o ataques a los sistemas de seguridad.



Falsos positivos: Bloqueo de actividades legítimas por error.

**Desventajas
del uso de la
tecnología
para la
prevención:**

Conclusiones

El fraude informático y el robo de información son amenazas crecientes en la era digital.

La prevención requiere una combinación de medidas tecnológicas, organizativas y de concienciación.

La educación y la capacitación son fundamentales para protegerse de estas amenazas.

Es importante mantenerse actualizado sobre las nuevas tendencias y técnicas de los delincuentes.



Recomendaciones



Implementar un plan de seguridad integral:
Incluye medidas de prevención, detección y respuesta a incidentes.

Realizar copias de seguridad: Almacenar copias de seguridad de la información importante en un lugar seguro.

Reportar incidentes:
Informar a las autoridades competentes en caso de ser víctima de un delito informático.

Promover la cultura de seguridad: Fomentar la conciencia y la responsabilidad en el uso de la tecnología.



Video

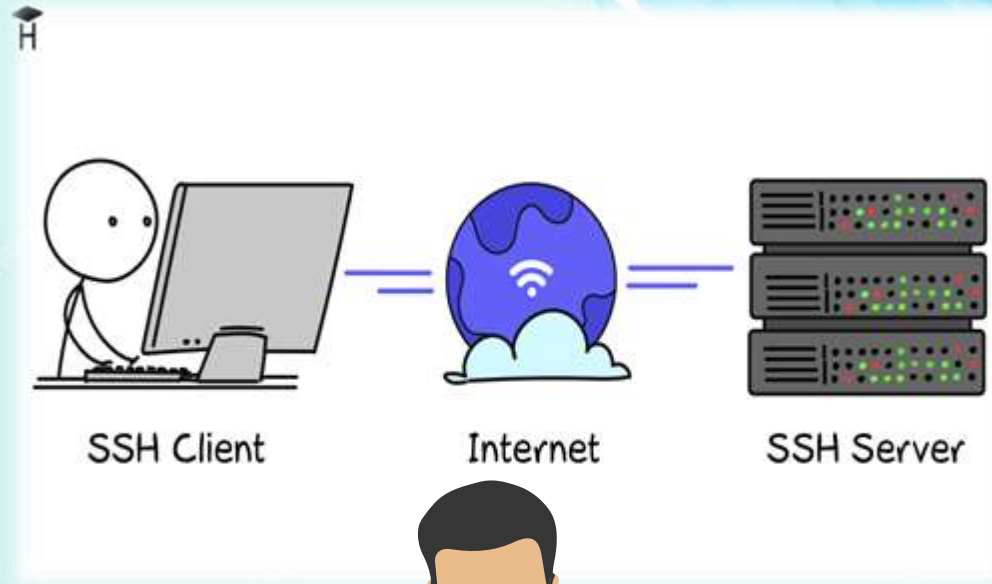


Security

Protocollo SSH

Concepto

SSH (Secure Shell): Es un protocolo de red criptográfico que permite a dos computadoras comunicarse de forma segura a través de una red insegura. Se utiliza principalmente para acceder a máquinas remotas y ejecutar comandos, pero también puede usarse para transferir archivos y tunelizar otros protocolos.



Conexión segura: SSH establece un canal encriptado entre dos dispositivos, protegiendo la información que se transmite de ser interceptada o modificada por terceros.

Autenticación: SSH utiliza mecanismos de autenticación para verificar la identidad del usuario que intenta conectarse, como contraseñas o claves públicas/privadas.



Características

Cifrado de Datos

SSH emplea técnicas de cifrado avanzadas para proteger la información transmitida, asegurando que las credenciales y datos no puedan ser interceptados o leídos por terceros..

Tuneles Seguros

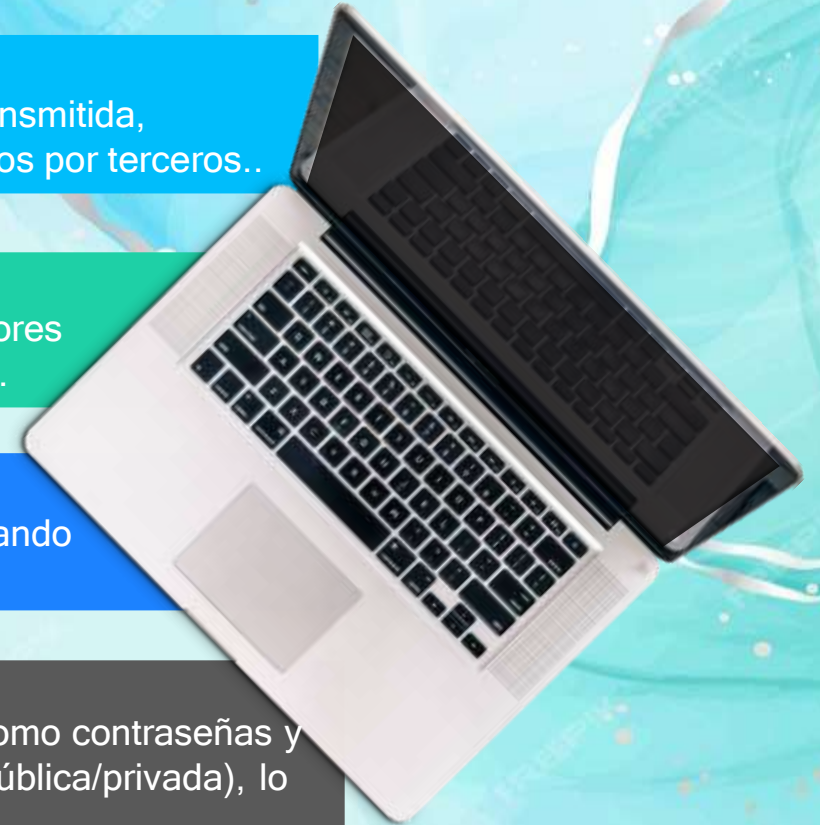
Permite crear túneles cifrados para ejecutar comandos en servidores remotos, transferir archivos o reenviar puertos de manera segura.

Integridad de Datos

Verifica la integridad de los datos transmitidos, garantizando que no han sido modificados durante la transmisión.

Autenticación Segura

SSH utiliza varios métodos de autenticación, como contraseñas y claves criptográficas (autenticación por clave pública/privada), lo que añade una capa extra de seguridad..



Importancia

Acceso remoto seguro:

Permite a los administradores acceder y gestionar servidores remotos de forma segura, sin exponer las credenciales de acceso.



Protección de datos:

Asegura la confidencialidad e integridad de la información que se transmite durante la conexión.



Gestión eficiente:

Facilita la administración de sistemas remotos al permitir la ejecución de comandos y la transferencia de archivos de forma segura.



Amenazas



Amenazas



Ataques de fuerza bruta:
Intentos repetidos de adivinar la contraseña para acceder al sistema.



Ataques de intermediario (Man-in-the-middle):
Intercepción del tráfico de datos para robar información o modificar la comunicación.



Explotación de vulnerabilidades:
Aprovechamiento de fallos de seguridad en el software SSH para obtener acceso no autorizado.

Prevención

Medidas de Prevención

Utilizar contraseñas fuertes: Crear contraseñas largas y complejas, o utilizar frases de contraseña.

Implementar claves públicas/privadas: Utilizar la autenticación basada en claves para mayor seguridad.

Mantener el software actualizado: Instalar las últimas actualizaciones de seguridad para el servidor SSH y el cliente.

Desactivar el acceso root: Restringir el acceso directo al usuario root para minimizar el impacto de un posible ataque.

Configurar el firewall: Bloquear el acceso SSH desde direcciones IP no autorizadas.

Security



Ventajas de SSH



Desventajas

Complejidad de configuración

Para usuarios inexpertos, la configuración inicial de SSH puede ser complicada, especialmente cuando se trabaja con autenticación de claves públicas y privadas.

Riesgo de uso indebido:

Si se configuran contraseñas débiles o claves mal protegidas, un atacante podría aprovechar vulnerabilidades de seguridad, como el robo de credenciales.


Acceso total:

SSH permite acceso completo al sistema remoto, lo que significa que si un atacante logra vulnerarlo, puede comprometer seriamente el sistema.

Dificultad en la gestión de claves:

La gestión y distribución de claves públicas y privadas puede volverse complicada, especialmente en entornos con muchos usuarios y dispositivos.

Conclusión



SSH es un protocolo fundamental para la seguridad en el acceso remoto y la gestión de sistemas.
Su uso es esencial para proteger la información sensible y prevenir ataques informáticos.
La correcta configuración e implementación de SSH son cruciales para garantizar la seguridad.

Recomendaciones

Utilizar SSH siempre que sea posible
Priorizar el acceso remoto a través de SSH en lugar de protocolos inseguros como Telnet..

Implementar las mejores prácticas de seguridad:
Utilizar contraseñas fuertes, claves públicas/privadas y mantener el software actualizado.

Monitorear la actividad SSH
Registrar y analizar la actividad SSH para detectar posibles anomalías o intentos de intrusión.