Colegio Tecnológico en Informática

Facultad de Bachillerato Industrial y Perito en Computación con Orientación en Desarrollo de Aplicaciones Web y Móvil

Chun Icuté Gerbin Adolfo

Programación II

Grado Quinto

Sección A

Investigación Individual de Diferentes Temas y Ejercicios Prácticos

Ariel Fernando Saucedo De León

Clave 27

Puntuación /20

12/03/2023

INDICE

Introducción

En el mundo actual, donde la tecnología avanza a un ritmo vertiginoso, la seguridad informática se ha convertido en un tema de vital importancia. La protección de la información y los sistemas es esencial para salvaguardar la integridad, confidencialidad y disponibilidad de los recursos digitales. En este trabajo, exploraremos varios aspectos claves de la seguridad informática, centrándonos en seis temas fundamentales: Firewall o Cortafuegos, Software Antivirus, Infraestructura de clave pública o PKI, Servicios MDF, Pentesting, Stego y Técnicas de Cifrados Actuales.

La seguridad informática y la ciberseguridad son fundamentales para proteger la información y los recursos en un mundo cada vez más conectado y dependiente de la tecnología. Mantener la seguridad en línea es un desafío constante

Objetivos

1. Firewall o cortafuegos

- Evaluar la efectividad de diferentes tipos de firewalls en la protección de una red contra amenazas externas.
- Investigar nuevas técnicas de detección y prevención de intrusiones en firewalls.
- Analizar el impacto de los firewalls en el rendimiento de la red y proponer mejoras para minimizar la degradación.
- Investigar la integración de tecnologías de inteligencia artificial y aprendizaje automático en los firewalls para mejorar la detección de amenazas.

2. Software antivirus

- Evaluar y comparar la eficacia de diferentes soluciones antivirus en la detección y eliminación de malware.
- Investigar las técnicas de detección de malware más avanzadas utilizadas en los software antivirus.
- Analizar la evolución de las amenazas y los desafíos actuales que enfrentan los antivirus, como el malware oculto o las técnicas de evasión.
- Evaluar el impacto del software antivirus en el rendimiento del sistema y proponer estrategias de optimización.

3. Infraestructura de clave pública o PKI

- Investigar los desafíos de seguridad asociados con la implementación de una infraestructura de clave pública.
- Evaluar y comparar los diferentes protocolos y algoritmos criptográficos utilizados en la PKI.
- Analizar las vulnerabilidades y amenazas comunes en la PKI y proponer estrategias de mitigación.
- Investigar nuevas tecnologías y enfoques para mejorar la escalabilidad, la eficiencia y la seguridad de la PKI.

4. Servicios MDF (Managed Detection and Response)

- Investigar las mejores prácticas y estrategias para implementar servicios de MDF efectivos.
- Evaluar la eficacia de diferentes herramientas y soluciones de MDF en la detección y respuesta a incidentes de seguridad.
- Analizar las técnicas y metodologías utilizadas en los servicios de MDF para la identificación temprana de amenazas y la respuesta efectiva.
- Investigar el impacto de los servicios de MDF en la reducción del tiempo de detección y respuesta a incidentes.

5. Pentesting (Pruebas de penetración)

- Investigar las metodologías y técnicas más actuales en pruebas de penetración.
- Evaluar las herramientas y enfoques utilizados en el pentesting y su efectividad en la identificación de vulnerabilidades.

- Analizar los desafíos éticos y legales asociados con el pentesting y proponer pautas para una conducta ética en estas pruebas.
- Investigar nuevas técnicas de evasión y detección de pentesting por parte de sistemas de seguridad.

6. Steganografía y técnicas de cifrado actuales

- Investigar las técnicas de esteganografía más recientes y su aplicación en la ocultación de información.
- Evaluar la seguridad de los algoritmos y protocolos de cifrado actuales.
- Analizar las vulnerabilidades y debilidades conocidas en las técnicas de cifrado y proponer mejoras.
- Investigar nuevos enfoques en la esteganografía y el cifrado, como el uso de aprendizaje automático o criptografía cuántica.

Firewall o Cortafuegos

¿Qué es el firewall o Cortafuegos?

El firewall cortafuegos es una barrera entre una red interna segura y una red que no sea de confianza, como Internet.

La mayoría de las compañías utilizan un cortafuegos para conectar sin peligro la red interna segura a Internet, aunque el cortafuegos también sirve para proteger una red interna frente a otra.

El firewall o cortafuegos proporciona un único punto de contacto controlado (llamado *punto de estrangulamiento*) entre la red interna segura y la red que no es de confianza. Las funciones del cortafuegos son:

- Permitir a los usuarios de la red interna utilizar los recursos situados fuera de la red.
- Impedir que los usuarios no autorizados de la red externa puedan utilizar los recursos de la red interna.

Cuando se utiliza un firewall o cortafuegos como pasarela a Internet (o a otras redes), se reduce el riesgo de la red interna. El uso del cortafuegos también facilita la administración de la seguridad de la red, ya que sus funciones llevan a cabo muchas de las directivas de la política de seguridad.

¿Cómo funciona un Firewall o Cortafuego?

Un firewall sirve para bloquear el trafico no autorizado a nuestra red LAN. Es efectivo al 100% para tráfico restringido pero no cubre cualquier tipo de ataque informático, ni mucho menos, pero resulta una medida de bajo coste que se encuentra implementada en sistemas operativos y routers, entre otros. Hay que aclarar que un firewall no protege del tráfico de datos que no pase por él, porque no puede controlarlo siquiera. Esto significa que nuestros dispositivos se pueden infectar fácilmente mediante pendrives o cualquier otro tipo de almacenamiento externo. Ataques informáticos hay muchos y de diversos tipos, si un virus entra mediante el USB, por medio de cualquier almacenamiento externo, el firewall no lo detectará.

Un firewall no es algo suplementario a un antivirus, sino complementario. Ambos métodos de seguridad son altamente recomendables en cualquier equipo informático, tenga o no conexión a internet. Un antivirus específico protege de aquellos virus que el cortafuegos, por lo general, no puede detectar, así que se complementan a la perfección.

Los firewalls suelen tener dos políticas de acción, una restrictiva y otra permisiva. La primera bloquea todo el tráfico no consentido mientras que la segunda admite todo el tráfico salvo el que esté denegado. Esto se puede hacer fácilmente desde la configuración del firewall de Windows, por ejemplo.

Un virus informático puede tener como fin muchos objetivos, desde obtener información personal, tarjetas de crédito, archivos… Una vez entre en el sistema, el virus puede mandar información hacia la WAN (generalmente internet) con todos los datos recopilados, lo que puede hacer que tu conexión a internet se vea bastante afectada, aunque ese sería el menor de tus problemas. Puedes evaluar la velocidad de tu conexión a internet desde este test de velocidad en apenas 1 minuto, pero cabe destacar que el hecho de que el resultado del test no

sea el esperado no quiere decir que tengas un virus, para ello complementa el firewall con un antivirus.

Componentes del Firewall o Cortafuegos

El cortafuegos es un conjunto de piezas de hardware y aplicaciones de software que, utilizadas conjuntamente, impiden el acceso no autorizado a una parte de la red. El cortafuegos está formado por los siguientes componentes:

- **Hardware**

  El hardware del cortafuegos suele constar de una máquina independiente o un dispositivo dedicado para ejecutar las funciones del software del cortafuegos.

- **Software**

  El software del cortafuegos proporciona una amplia variedad de aplicaciones. En términos de seguridad de la red, el cortafuegos proporciona, mediante diversas tecnologías, estos controles de seguridad:

  - filtrado de paquetes de protocolo de Internet (IP)
  - Servicios de conversión de direcciones de red (NAT)
  - Servidor SOCKS
  - Servidores proxy para distintos servicios, como HTTP, Telnet, FTP, etcétera
  - Servicios de retransmisión de correo
  - Sistema de nombres de dominio (DNS) dividido
  - Archivos de anotaciones

- Supervisión en tiempo real

Utilización de las tecnologías de Firewall o Cortafuegos

Los servidores proxy de cortafuegos, los servidores SOCKS o las reglas NAT permiten proporcionar a los usuarios internos un acceso seguro a los servicios de Internet. Los servidores proxy y SOCKS desglosan las conexiones TCP/IP en el cortafuegos para ocultar información de la red interna a la red que no es de confianza. Los servidores también proporcionan funciones adicionales de archivos de anotaciones.

Puede utilizar NAT para ofrecer a los usuarios de Internet un acceso fácil al sistema público situado detrás del cortafuegos. El cortafuegos aún protege la red, porque NAT oculta las direcciones IP internas.

El cortafuegos también puede proteger información interna si utiliza un servidor DNS. De hecho, tiene dos servidores DNS: uno que se utiliza para los datos relacionados con la red interna y otro, situado en el cortafuegos, para los datos relacionados con las redes externas y el propio cortafuegos. Esto le permite controlar el acceso externo a la información relacionada con los sistemas internos.

Cuando define una estrategia de cortafuegos, tal vez piense que es suficiente con prohibir todo aquello que represente un riesgo para la organización y permitir todo lo demás. Sin embargo, como los delincuentes informáticos están creando constantemente nuevos métodos de ataque, conviene que se anticipe a ellos para impedir que se salgan con la suya. Al igual que en el ejemplo del edificio, también necesitará supervisar en busca de signos que indiquen que alguien, de alguna

manera, ha burlado las defensas. Normalmente, es mucho más perjudicial y costoso recuperar el sistema ante una invasión que prevenirla.

En el caso del cortafuegos, la mejor estrategia es permitir solo aquellas aplicaciones que hayan sido comprobadas y que sean de confianza. Si sigue esta estrategia, deberá definir de modo exhaustivo la lista de servicios que desea ejecutar en el cortafuegos. Puede caracterizar cada servicio con la dirección de la conexión (de dentro a fuera o de fuera a dentro). También debe crear una lista con los usuarios a los que autorizará a utilizar cada servicio y las máquinas que pueden emitir una conexión para el servicio.

¿Qué puede hacer un firewall o cortafuego para proteger la red?

El cortafuegos se instala entre la red y el punto de conexión a Internet (o a otra red que no sea de confianza). Luego podrá limitar los puntos de entrada a la red. El cortafuegos proporciona un único punto de contacto (llamado punto de estrangulamiento) entre la red e Internet. El hecho de tener un solo punto de contacto le da más control sobre qué tráfico puede entrar y salir de la red.

El cortafuegos aparece como una dirección única a la vista del público. Proporciona acceso a la red que no es de confianza mediante los servidores proxy o SOCKS o mediante la conversión de direcciones de red (NAT), a la vez que oculta las direcciones de la red interna. De esta forma, el cortafuegos mantiene la privacidad de la red interna. El mantenimiento de la privacidad de la información de la red es uno de los métodos que utiliza el cortafuegos para disminuir la probabilidad de que se lleven a cabo ataques de imitación (usurpación).

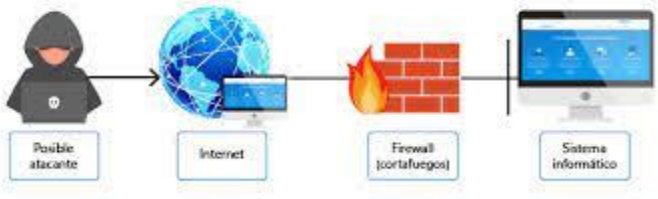
Un cortafuegos permite controlar el tráfico hacia dentro y hacia fuera de la red para minimizar el riesgo de ataques. Filtra de forma segura todo el tráfico que entra en la red, para que solo puedan

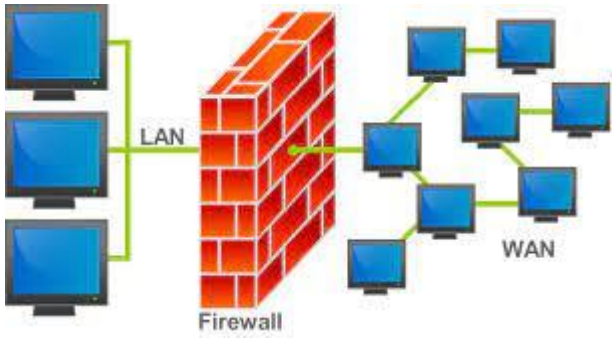
entrar tipos determinados de tráfico con destinos específicos. Así se minimiza el riesgo de que se utilice Telnet o el protocolo de transferencia de archivos (FTP) para acceder a los sistemas internos.

¿Qué es lo que no puede hacer un firewall o cortafuego para proteger la red?

El cortafuegos, si bien proporciona una gran protección contra algunos tipos de ataques, solo es una parte de la solución total de seguridad. Por ejemplo, el cortafuegos no necesariamente podrá proteger los datos que se envíen por Internet mediante aplicaciones como las de correo de protocolo simple de transferencia de correo (SMTP), FTP y Telnet. A menos que opte por cifrar esos datos, cualquier persona podrá acceder a ellos desde Internet mientras viajan a su destino.

Imágenes





Software Antivirus

¿Qué es un software antivirus?

Un programa antivirus es un software que protege tu ordenador, portátil, tableta, teléfono u otros dispositivos conectados a Internet contra el malware. El software antivirus identifica virus y a continuación los detiene y elimina.

A lo largo de los años, el malware ha cambiado y aumentado. Los programas maliciosos son ahora más diversos y listos. Por supuesto, las empresas que crean software antivirus están a la zaga de estos cambios. Este es el motivo por el cual, actualmente, los antivirus son programas sofisticados que funcionan en distintos niveles y de varias formas. Hablaremos sobre ello más adelante.

¿Por qué necesitas un antivirus?

Al usar un programa antivirus mantienes seguro tu dispositivo. Los virus informáticos, y muchos otros peligros en línea, son detenidos por los antivirus. Esto reduce enormemente la posibilidad de que tu dispositivo se vuelva inutilizable o de que tus datos caigan en las manos equivocadas.

Internet está lleno de malware y virus. Pueden ser, por ejemplo, un virus informático «normal», un gusano informático, un troyano, un keylogger o incluso un spyware o ransomware. Una vez tu ordenador está infectado, es extremadamente complicado conseguir tener de nuevo completamente «limpio» tu sistema. A menudo, algún que otro código malicioso continúa merodeando por algún lugar de tu dispositivo, aunque hayas eliminado todos los archivos infectados. Como resultado, nunca puedes estar al 100 % seguro de que el virus o malware se haya eliminado por completo.

Para protegerte contra este tipo de amenazas, necesitas un antivirus apropiado. El software antivirus escanea los archivos antes de que los abras, así un virus no tiene la oportunidad de infectar tu sistema. Los antivirus más avanzados también detectan el malware menos tradicional. Este tipo de malware no necesita necesariamente ser «activado» para causar daños, por ejemplo, abriendo un archivo. Ejemplos de este tipo de malware son los adware y los spyware.

¿Cómo funciona un antivirus?

El objetivo de un antivirus es proteger tu dispositivo de virus y otras clases de malware. Lo hace comparando cualquier amenaza que encuentra en una «lista negra», o blacklist. Todos los virus que conoce el programa antivirus se encuentran en esta lista negra.

Tan pronto como el antivirus encuentra algo que debe incorporarse a la lista negra, el programa detendrá el fichero e intentará borrarlo. Un programa antivirus analiza tu sistema de varias formas:

- **Análisis en tiempo real:** estos análisis ocurren cuando el programa antivirus se ejecuta en segundo plano. El software comprueba cada archivo y cada programa en el momento que clicas en él. Si el antivirus encuentra algo sospechoso, te lo hará saber. Debido a que el análisis se realiza antes de abrir el archivo, se detiene el virus antes de que pueda infectar tu sistema, manteniendo tu dispositivo a salvo.
- **Analizando todo tu sistema:** los análisis del sistema se hacen de una tirada y revisan todo tu dispositivo para ver si hay virus o malware. Los análisis completos no son a menudo necesarios, especialmente cuando está funcionando constantemente el análisis en tiempo real. Sin embargo, puede ser útil ejecutar un análisis de sistema cuando instalas un nuevo programa antivirus. Los análisis semanales que muchos antivirus ejecutan

automáticamente también son útiles debido a que hacen una doble revisión de tu sistema entero buscando los virus más recientes. En cualquier otro momento, el software antivirus se activará de inmediato, en tiempo real, tan pronto como hagas clic en un archivo con un virus oculto.

Técnicas de detección de virus

Para entender como funciona un antivirus, es necesario conocer las técnicas de detección de virus que existen.

Entre las técnicas de detección están:

Verificación de Firmas

Verificación Heurística

Bloqueo de Comportamiento

Técnicas de Verificación de Firmas

La verificación de Firmas determina las características que lleva un archivo a ser o no considerado un malware.

Se verifican características como: tamaño del archivo, secuencia de instrucciones binarias, entre otras.

Cuando un archivo es reconocido como un malware, recibe una identidad propia, con su respectiva firma. Estas firmas son las que determinan cada malware que forma parte de la lista de definición del antivirus.

Este tipo de detección puede no ser muy eficiente, pues no posibilita de nuevos tipos de malware, que aún no fueron incluidos en la base de datos del antivirus sean detectados, o sea, los nuevos

tipos de malwares no serán detectados antes de que el software antivirus tenga su lista de definición actualizada.

Técnica de Detección Heurística

La verificación Heurística es la capacidad que un antivirus posee de detectar un malware, sin poseer una vacuna especifica para él, o sea, la idea de la heurística es la de anticipar el descubrimiento de un malware.

Existen softwares antispam que trabajan con la misma filosofía. El gran problema de este tipo de método de detección está en la posibilidad de generar un número muy alto de falsos positivos.

Los falsos positivos son los archivos que poseen algunas características que puedan hacer parecer como un malware, aunque en realidad no los son.

Además de esto, esta técnica realiza la verificación más lentamente, pues el proceso de buscar archivos que posean determinadas características es diferente de buscar malwares ya reconocidos.

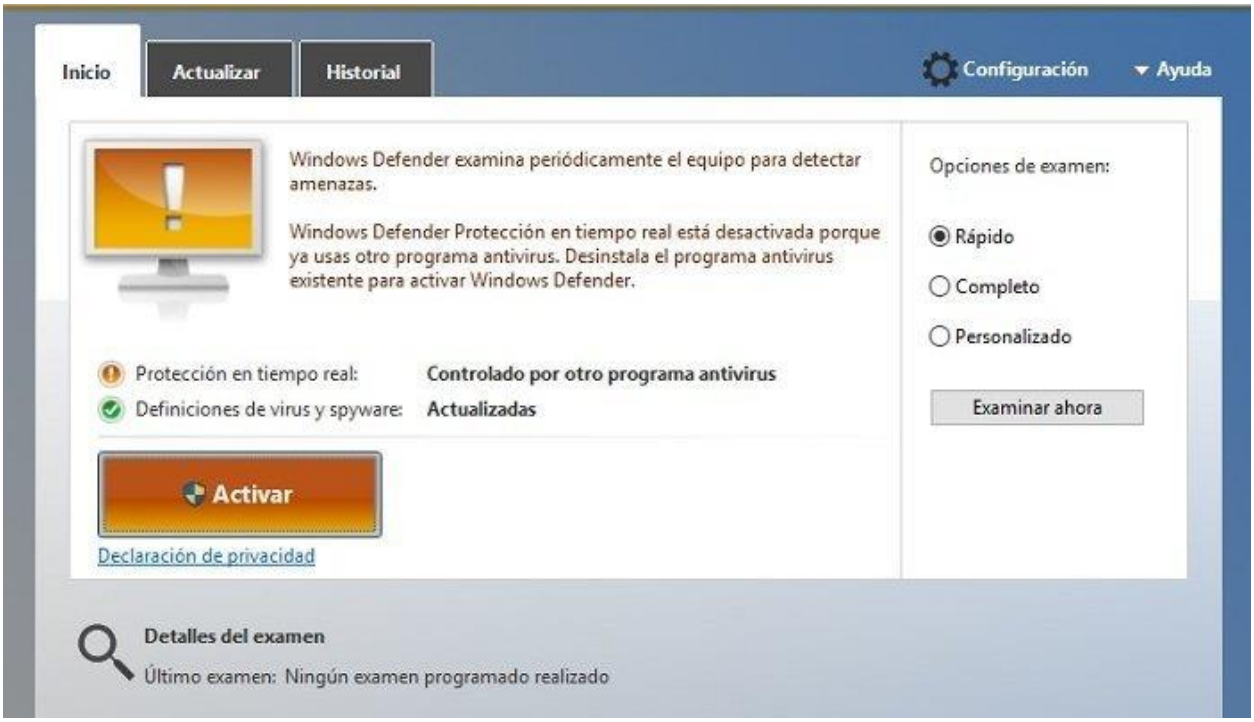
Esta técnica tampoco identificará nuevos malwares que posean características diferentes a la de los malwares ya conocidos, pues la heurística está preparada para detectar características comunes a otros malwares.

Técnica de Bloqueo de Comportamiento

El bloqueo de comportamiento es la técnica que analiza las acciones ejecutadas por los programas (acciones sospechosas), a fin de identificar posibles tentativas de invasiones o infecciones.

Conforme a las acciones realizadas por algún software, él podrá ser considerado un malware y no permitírsele su ejecución.

La mayoría de los softwares antivirus hacen una combinación de estas técnicas para detectar y remover los malwares.



La diferencia entre un antivirus y un firewall

La diferencia entre un programa antivirus y un firewall se encuentra en cuándo una amenaza de malware se detecta y cómo se neutraliza. Los programas antivirus escanean los archivos de tu ordenador en busca de malware, mientras que el firewall te protege del malware, cibercriminales y otras cosas maliciosas de Internet antes de que lleguen a tu ordenador. Puedes ver un firewall como una «pared» entre ti y el mundo en línea. Solo archivos e información considerados seguros pasan a través de esta pared. Un antivirus, por el otro lado, escanea todos los archivos que ya se encuentran en tu ordenador y los elimina, incluso si aún no han sido activados.

Muchos antivirus tienen su propio firewall integrado. Lo que quiere decir que instalas los dos a la vez.

Imágenes

Infraestructura de claves públicas (PKI)

¿Qué es la Infraestructura de Claves Públicas?

Una infraestructura de claves públicas (PKI) es un sistema de recursos, políticas y servicios que da soporte al uso del cifrado de claves públicas para autenticar a las partes que participan en una transacción.

No hay ningún estándar individual que defina los componentes de una Infraestructura de clave pública, pero normalmente un PKI consta de entidades emisoras de certificados (CA) y entidades emisoras de registro (RA). Las CA proporcionan los servicios siguientes:

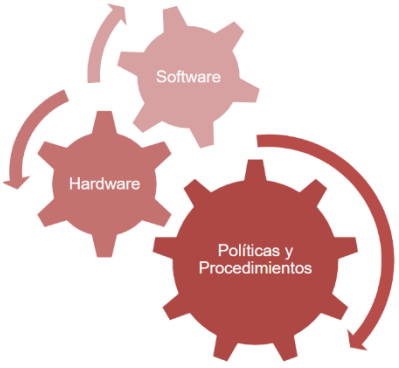
- Emisión de certificados digitales
- Validación de certificados digitales
- Revocación de certificados digitales
- Distribución de claves públicas

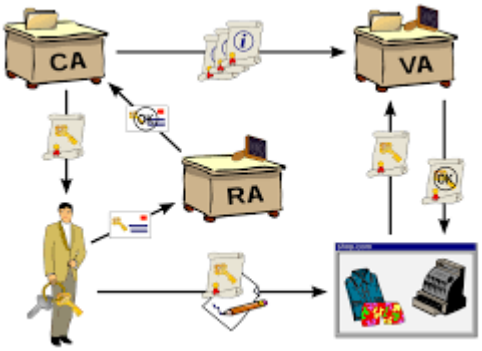
El estándar X.509 proporcionan la base para la industria estándar de la infraestructura Public Key Infrastructure.

Consulte Certificados digitales para obtener más información sobre los certificados digitales y las entidades emisoras de certificados (CA). Las RA verifican la información proporcionada cuando se solicitan certificados digitales. Si la RA verifica esta información, la CA puede emitir un certificado digital para el solicitante.

Una PKI también puede proporcionar las herramientas para gestionar los certificados digitales y las claves públicas. Una PKI se describe a veces como una *jerarquía fiable* para la gestión de certificados digitales, aunque la mayor parte de las definiciones incluyen servicios adicionales. Algunas definiciones incluyen servicios de cifrado y firma digital, pero estos servicios no son esenciales para el funcionamiento de una PKI.

Imágenes





Servicios MDF

¿Qué son los Servicios MDF?

El MDF (Main Distribution Frame) generalmente se denomina Main Distribution Frame, que es a decuado para usar con equipos de conmutación telefónica de gran capacidad para conectar líneas internas y externas. Generalmente, también tiene la función de cablear, probar y proteger los equi pos y la seguridad personal en el buró. MDF también se denomina armario de cableado principal en la red, también llamado marco de cableado integrado o marco de cableado del usuario. Es el c omponente más importante del subsistema de gestión y es el concentrador que realiza la conexión cruzada de los dos subsistemas, la línea troncal vertical y el cableado horizontal. Los paneles de c onexión generalmente se instalan en gabinetes o paredes. Mediante la instalación de accesorios, e l cuadro de distribución puede satisfacer las necesidades de UTP, STP, cable coaxial, fibra óptica , audio y video.

El Main Distribution Frame está compuesto por un rack, un bloque de cableado de seguridad, un bloque de cableado de prueba, una unidad de seguridad y otros accesorios. Tiene una buena funci ón de protección para evitar que la sobrecorriente y el sobrevoltaje causados por rayos y otras raz ones dañen el equipo de comunicación y el personal en la sala de computadoras. Todos los plástic os son plásticos de ingeniería ignífugos. La superficie de contacto adopta tecnología de oro, plata , níquel y tratamiento anticorrosión. Cuatro niveles de alarma: alarma de unidad, fila, columna y a larma total (sonido, luz). El marco tiene un sistema de puesta a tierra confiable.

Los MDF comunes son generalmente DF a presión de 120 ohmios (también hay MDF con conect ores L9 y BNC, pero son raros). Las leyendas comunes y los accesorios auxiliares son los siguien tes:

Figura 1.1 Diagrama esquemático general

Figura 1.2 Pantalla detallada

Figura 1.3 Accesorios auxiliares comunes (unidad de seguridad, cable de prueba y cortador de alambre)

Función de Main Distribution Frame de MDF

El Main Distribution Frame de MDF es uno de los equipos principales de la red de comunicación. Todas las líneas externas están conectadas al Main Distribution Frame, y luego el Main Distribution Frame está conectado al equipo relacionado. El cable externo no se puede conectar directamente al interruptor y debe pasar a través de una especie de equipo de traspaso, que es el Main Distribution Frame.

Las funciones básicas del repartidor principal son las siguientes:

1) Con la función de cableado, cualquier cable interno se puede conectar a cualquier cable externo a través de un puente.
2) Tiene un dispositivo de protección que, junto con las instalaciones de protección en la línea exterior y el interruptor, forma un sistema de protección para evitar que la sobretensión y la sobre corriente que ingresan desde la línea exterior causen daños y lesiones a los equipos y operadores en la oficina.
3) Tenga un lugar para probar los cables interior y exterior.
4) Tiene una función de alarma, que puede enviar señales audibles y visibles de la alarma, y puede detectar la acción de la unidad de seguridad a tiempo.

Reglas de Cableado para Cables Logarítmicos Grandes

5 colores principales: blanco, rojo, negro, amarillo y morado

5 colores: azul, naranja, verde, marrón y gris

- La secuencia de líneas cromatográficas de 10 pares de cables telefónicos es la siguiente:

1 par-Bailan 2 pares-blanco naranja 3 pares-blanco verde 4 pares-blanco marrón 5 pares-blanco gris

6 pares-rojo azul 7 pares-rojo naranja 8 pares-rojo y verde 9 pares-rojo marrón 10 pares-rojo gris

- 30 pares de secuencia de línea cromatográfica de cable telefónico

Nota: Preste atención a 30 pares de cables telefónicos. Hay 2 colores principales de blanco en 30 pares de cables de comunicación. ¡Si hay más de 25 pares, debe mirar la línea de identificación! ! ¡Una mano pequeña está envuelta con el logotipo "Bai Lan" y otros 5 pares están envueltos con el logotipo "Blanco Naranja"! Se pueden utilizar cables de más de 30 pares

(Nota: estos 25 pares están enredados con la línea de marcado del círculo de color "blanco azul")

1 par-Bailan 2 pares-blanco naranja 3 pares-blanco verde 4 pares-blanco marrón 5 pares-blanco gris

6 pares-rojo azul 7 pares-rojo naranja 8 pares-rojo y verde 9 pares-rojo marrón 10 pares-rojo gris

11 pares-orquídea negra 12 pares-negro naranja 13 pares-negro y verde 14 pares-negro y marrón 15 pares-negro y gris

16 pares-amarillo azul 17 pares-amarillo naranja 18 pares-amarillo verde 19 pares-amarillo marró n 20 pares-amarillo gris

21 pares-morado orquídea 22 pares-morado naranja 23 pares-morado verde 24 pares-morado mar rón 25 pares-morado gris

(Nota: estos 5 pares están enredados con el logo "naranja blanco")

21 pares-Bailan 22 pares-blanco naranja 23 pares-blanco verde 24 pares-blanco marrón 25 pares-blanco gris

Los cables con más de 30 pares se pueden deducir de la misma manera. Por ejemplo, hay 4 tipos de líneas de identificación en un cable telefónico de 100 pares, ¡y los primeros 25 pares están env ueltos con líneas de identificación "Branchi"! ! ¡Los segundos 25 pares están enredados con la lín ea de marcado "blanco naranja"! ¡Los terceros 25 pares están enredados con líneas de marcado "b lancas y verdes"! ¡Los cuartos 25 pares están enredados con la línea de marcado "blanco y marró n"!

Análisis de estado del Main Distribution Frame de MDF

La unidad de seguridad es un dispositivo de protección insertado en el bloque de cableado de seg uridad para evitar que el personal y el equipo sufran daños por sobretensión y sobrecorriente. Es u na parte importante del Main Distribution Frame. De acuerdo con el estándar internacional "Prop uesta CCIqTK.20" y la situación real del entorno de la línea, la unidad de seguridad instalada en e l Main Distribution Frame debe tener tres funciones, a saber, funciones anti-rayos, anti-inducción eléctrica fuerte y anti-CA. . En particular, la función de protección primaria de la unidad de segur idad de intercambio controlada por programa con protección secundaria pobre contra sobretensió n y sobrecorriente es más importante.

1) Impacto del rayo: se refiere a la sobretensión generada por el impacto del rayo. Tiene las carac terísticas de ocurrencia instantánea y finalización instantánea. Algunos voltajes son tan altos com o decenas de miles de voltios y miles de voltios, dependiendo de la distancia de ocurrencia.

2) Fuerte inducción eléctrica: cuando el cable pasa por algunos lugares especiales, como ferrocarr iles electrificados o subestaciones o centrales eléctricas, a veces se generan corrientes inducidas d ebido a campos electromagnéticos. De acuerdo con la distancia de la corriente inducida, hay indu cción de línea larga e inducción de línea corta, que generalmente se pueden resumir de la siguient e manera: la inducción de línea larga tiene las características de alto voltaje y, en consecuencia, c orriente pequeña; La inducción de línea corta tiene las características de alto voltaje y alta corrien te.

3) Contacto con la línea eléctrica: En cuanto a la instalación de cables, la situación actual en mi p aís es que los cables telefónicos y los cables de red o de tranvía se instalan en paralelo o entrecruz ados en el aire. Debido al viento, la lluvia y el sol, los rayos, los daños causados por animales y e l envejecimiento de los cables, etc., los golpes en las líneas eléctricas siguen ocurriendo con más f recuencia.

Las tres situaciones anteriores pueden hacer que se quemen llamas abiertas y quemar los módulos del marco de distribución o las placas de circuito de usuario de los interruptores. La unidad de se guridad de MDF puede proteger el suelo de la intrusión de electricidad externa, lo que puede dese mpeñar un cierto papel de protección y función de alarma. Aquí hay un breve análisis de la siguie nte manera.

- Método de protección contra cortocircuitos

La idea básica del diseño actual de MDF es cortocircuitar la sobretensión intrusiva y la sobrecorri ente a tierra.

- Todos los niveles de puesta a tierra del Main Distribution Frame de MDF

La unidad de seguridad se inserta en el bloque de cableado de seguridad, y cuando la línea de co municación es atacada por electricidad fuerte, alto voltaje, corriente sumergida, alta corriente, etc ., juega un papel protector. Cuando el bloque de cableado de seguridad no está insertado en la uni dad de seguridad, las líneas internas y externas están desconectadas. Después de enchufar la unid

ad de seguridad, se conectan las líneas internas y externas. Cuando la unidad de seguridad se inse rta en el bloque de cableado de seguridad, la clavija de conexión a tierra de la unidad de segurida d pasa a través del orificio de conexión a tierra del bloque de cableado de seguridad para conectar se a la barra de conexión a tierra. La barra de conexión a tierra de cada bloque de cableado de seg uridad está conectada al marco conectado a tierra para formar todo el cableado. El sistema de con exión a tierra del marco.

En resumen, como dispositivo de protección para la protección de interruptores, el Main Distribu tion Frame de MDF juega un papel importante en la prevención de sobretensiones de rayos, sobre tensiones inducidas por frecuencia de potencia y sobrecorriente de contacto de frecuencia de pote ncia. Como protección principal de los interruptores de comunicación, el Main Distribution Fram e juega un papel vital para garantizar la seguridad de las operaciones de comunicación.

Pentesting

¿Qué es Pentesting?

Debido a los fraudes y ataques cibernéticos sufridos por las entidades, se ha puesto en marcha el pentesting o testeador de penetración. El **pentesting o test de penetración** consiste en atacar diferentes entornos o sistemas con el objetivo de **detectar y prevenir posibles fallos**. Se trata de una técnica para encontrar aquellos errores en el sistema. Es una de las prácticas más demandadas actualmente, ya que gracias a este tipo de exámenes las empresas pueden poner remedio a sus debilidades antes de que lo hagan los ciberdelincuentes.

Un **pentester** es un auditor de seguridad informática. Se dividen en dos, el **red team**, que es la parte más ofensiva, y el **blue team** que es la parte defensiva de los pentester.

Se trata de un método para **evaluar la seguridad de una empresa**, un ataque real simulado. Intentan atacar una organización con el objetivo de hacer un informe con el que la empresa obtenga toda la información que necesita y pueda mejor sus vulnerabilidades. Evalúa la seguridad de un sistema al intentar romper y acceder a este.

En resumen, los pentesting o test de penetración son útiles por las siguientes razones: para **determinar qué posibilidad de éxito podría tener un ciberataque**, qué vulnerabilidades de mayor y menor riesgo tiene la empresa, cuáles de ellas pueden poner en riesgo a la organización y cuáles son casi imposibles de detectar. Por último, también comprobar la capacidad y la eficiencia de los informáticos a la hora de responder a posibles ataques.

Tipos de Pentesting

Por otro lado, los pentesting se clasifican según el tipo de información de la que disponga el profesional de la seguridad informática antes de elaborar el test. Podemos encontrar tres tipos:

White box o Caja Blanca

Black box o Caja Negra

Grey box o Caja Gris

White Box o Caja Blanca

El pentester **conoce todos los datos del sistema** y suele formar parte del equipo técnico de la empresa. Tiene toda la información sobre la estructura, datos, IP, logings, contraseñas, firewords, etc. Es el más completo y forma parte de un análisis integral de la estructura. Con estos datos preliminares la prueba es suficientemente certera a la hora de descubrir los fallos y las medidas que se deben tomar.

Black Box o Caja Negra

Es la segunda mejor opción a la hora de contratar un pentesting. El auditor **no tiene ningún dato de la organización** y parte desde cero, como si fuera un ciberdelincuente real. Esto ayuda a que el simulacro sea lo más verídico posible. **Es una prueba a ciegas de la estructura de la red**. Dadas estas características se trata de una gran experiencia para la empresa, ya que es un buen método para reconocer las fragilidades del sistema informático de un negocio.

Grey Box o Caja Gris

Sería una mezcla de la Caja negra y la Caja blanca. Los pentesters **tienen cierta información para realizar esta prueba** de intrusión. No van a ciegas como la opción anterior y tienen una cantidad baja de información. Dada esta forma, el auditor invertirá tiempo y recursos para identificar las

debilidades y amenazas basándose en la cantidad de información que ya dispone. Es el pentest más recomendado a la hora de contratar alguno de estos servicios.

Auditoría→Fases del Pentesting

El proceso a la hora de llevar a cabo una auditoría se divide en cinco etapas:

Reconocimiento

La primera etapa es la de planificación y el reconocimiento. Se trata de definir el alcance y los objetivos de la prueba, incluidos los sistemas que se abordarán y los métodos de prueba que se utilizarán. Además, también se aprovecha para recopilar toda la información posible, como los nombres del dominio y de red, el software, correos electrónicos, etc. para comprender mejor cómo funciona la empresa y sus potenciales debilidades.

Análisis de vulnerabilidades

El segundo paso es entender cómo responderá el sistema al que se está intentando penetrar a varios intentos de intrusión. Empezamos a interactuar con el objetivo y se analiza el sistema de forma manual o automática para identificar posibles debilidades. Se define el ámbito y el alcance del test de intrusión y se consulta con el cliente la profundidad de las pruebas que se van a realizar y la permisividad de los ataques.

Modelado de amenazas

Una vez ya tenemos toda la información, hay que elaborar una **representación estructurada de toda la información que afecta a la seguridad de una aplicación**. Es el proceso de capturar,

organizar y analizar todos los datos desde una vista a través de expertos en seguridad. Permite tomar decisiones sobre los riesgos y producir un modelo de amenazas típico o una lista priorizada de mejorar de seguridad informática.

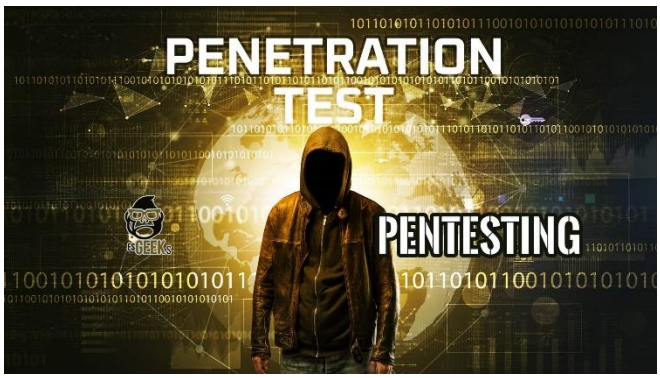
Explotación

El modelo nos ayuda a ver de qué forma atacaremos el sistema, por qué puerto acceder. Si la intrusión se ha llevado con éxito, esta fase consta de la recolección de información privada, como archivos alojados en un servidor o sistema. La finalidad es demostrar al cliente que si un ciberdelincuente atacara el sistema podría acceder a el y robar la información.

Elaboración de informes

Por último, como nos podemos imaginar, se trata de redactar todo los fallos y mejoras en seguridad detectadas. Se realizan dos tipos de reportes. Por un lado, uno técnico para los administradores del sistema, que se escribe con las terminologías apropiadas junto a las soluciones detalladas. Por otro lado, un reporte ejecutivo dirigido a la mesa directiva para que las personas que no se dedican al mundo de la informática lo entienda.

Imágenes



Stego y Técnicas de Cifrados Actuales

¿Qué es la esteganografía?

La esteganografía es la práctica de **ocultar un mensaje secreto** dentro (o incluso encima) de algo que no es secreto. Ese algo puede ser casi cualquier cosa que quieras. En estos días, muchos **ejemplos de esteganografía** implican incrustar un texto secreto dentro de una imagen. O esconder un mensaje secreto o un script dentro de un documento de Word o Excel.

El propósito de la esteganografía es ocultar y engañar. Es una forma de **comunicación encubierta** y puede implicar el uso de cualquier medio para **ocultar mensajes**. No es una forma de criptografía, porque no implica codificar datos o usar una clave. En cambio, es una forma de ocultar datos y se puede ejecutar de manera inteligente. Mientras que la criptografía es una ciencia que permite en gran medida la privacidad, la esteganografía es una práctica que permite el secreto y el engaño.

La ocultación de información está relacionada con dos campos, la esteganografía y la marca de agua.

Hay tres aspectos principales para el ocultamiento de la información, la capacidad, la seguridad y la solidez. La capacidad significa la cantidad de información que se puede ocultar, la seguridad se refiere a la incapacidad de un fisgón para detectar información oculta y la solidez a la cantidad de modificación que el medio de cobertura puede resistir antes de que la información oculta se corrompa. En general, la ocultación de información pasa por estos procesos:

- Identificación de bits redundantes en un medio de cobertura. Los bits redundantes son aquellos que se pueden editar sin tener en cuenta la calidad del medio de cobertura.

- Luego, seleccionamos un subconjunto de los bits redundantes para ser reemplazados con datos de un mensaje privado. El medio de la etapa se crea reemplazando los bits redundantes seleccionados con bits de mensaje.

La modificación de bits redundantes puede cambiar las propiedades estadísticas del medio de cobertura. Como resultado, el análisis estadístico puede revelar el contenido oculto.

¿Cómo funciona la esteganografía digital?

La **esteganografía digital** funciona ocultando información de una manera que no despierte sospechas. Una de las técnicas más populares es la esteganografía de bits menos significativos (LSB). En este tipo de esteganografía, el ocultador de información incrusta la información secreta en los bits menos significativos de un archivo multimedia.

Por ejemplo, en un **archivo de imagen**, cada píxel se compone de tres bytes de datos correspondientes a los colores rojo, verde y azul (algunos formatos de imagen asignan un cuarto byte adicional a la transparencia, o 'alfa').

La esteganografía LSB cambia el último bit de cada uno de esos bytes para ocultar un bit de datos. Entonces, para ocultar un megabyte de datos usando este método, necesitarás un archivo de imagen de ocho megabytes.

Dado que la modificación del último bit del valor de píxel no da como resultado un cambio visualmente perceptible en la imagen, una persona que vea el original y las imágenes modificadas esteganográficamente no podrá notar la diferencia.

El mismo esquema se puede aplicar a otros medios digitales (audio y video), donde los datos se ocultan en partes del archivo que dan como resultado el menor cambio en la salida audible o visual.

Otra técnica de esteganografía menos popular es el uso de **sustitución de palabras o letras**. Aquí, el remitente del mensaje secreto oculta el texto distribuyéndolo dentro de un texto mucho más grande, colocando las palabras en intervalos específicos.

Si bien este método de sustitución es fácil de usar, también puede hacer que el texto parezca extraño y fuera de lugar, ya que las palabras secretas pueden no encajar particularmente bien en sus oraciones objetivo.

Hay otros tipos de esteganografía, como ocultar una partición completa en un disco duro o incrustar datos en la sección de encabezado de archivos y paquetes de red. La eficacia de estos métodos depende de la cantidad de datos que puedan ocultar y de lo fáciles que sean de detectar.

Tipos de esteganografía

Los principales tipos de esteganografía son:

Pura

La **esteganografía pura** no requiere el intercambio de un cifrado como un stego-key. Se asume que ninguna otra parte tiene conocimiento de la comunicación.

De clave secreta

Aquí la clave secreta (stego) se intercambia antes de la comunicación. Esto es más susceptible a la interceptación. La **esteganografía de clave secreta** toma un mensaje de cobertura e incrusta el

mensaje secreto dentro de él mediante el uso de una clave secreta (stego-key). Solo las partes que conocen la clave secreta pueden revertir el proceso y leer el mensaje secreto.

De clave pública

En este caso se utiliza una clave pública y una clave privada para una comunicación segura. El remitente utilizará la clave pública durante el proceso de codificación y solo la clave privada, que tiene una relación matemática directa con la clave pública, puede descifrar el mensaje secreto.

Diferencia entre esteganografía y criptografía

La esteganografía se centra en ocultar la presencia de información, mientras que la criptografía (**ver artículo sobre el cifrado César*) se preocupa más por asegurarse de que no se pueda acceder a la información. Cuando la esteganografía se usa correctamente, nadie, aparte de los destinatarios previstos, debería poder decir que se está produciendo una comunicación oculta. Esto la convierte en una técnica útil para situaciones en las que el contacto obvio no es seguro.

Por el contrario, la **criptografía** tiende a usarse en situaciones en las que los participantes no están preocupados si alguien descubre que se está comunicando, pero necesitan que el mensaje en sí esté oculto e inaccesible para terceros.

Repasemos algunos ejemplos para comprender las diferencias. Si eres un activista político que has sido encarcelado y necesitas comunicarte con tu organización, la logística puede ser un desafío. Las autoridades pueden monitorizar todo lo que entra y sale de tu celda, por lo que probablemente tendrás que ocultar cualquier comunicación que tenga lugar .

En este tipo de situación, la esteganografía sería una buena opción. Puede ser un desafío con los recursos que tienes a mano, pero podrías escribir una carta que suene sencilla con un mensaje oculto con diferentes tipos de fuentes u otras técnicas esteganográficas.

Alternativamente, digamos que eres un diplomático que discutes detalles secretos con tu país de origen. Es normal que los diplomáticos hablen con funcionarios de su propia nación para que las comunicaciones en sí mismas no levanten sospechas. Sin embargo, dado que el contenido de la conversación es de alto secreto, el diplomático puede querer usar criptografía y hablar por una línea encriptada.

Si los espías o atacantes intentan interceptar la conversación, solo tendrán acceso al texto cifrado, y no a lo que las dos partes realmente estén diciendo .

Si el activista político usó criptografía para comunicarse con su organización, lo más probable es que las autoridades la hubieran interceptado.

Los funcionarios verían el texto cifrado y sabrían que el activista estaba tratando de enviar mensajes codificados, entonces lo más probable es que detuvieran su entrega e interrogarían al activista al respecto. Es por eso que la esteganografía sería más adecuada en tal escenario.

Por el contrario, los diplomáticos a menudo son monitorizados por sus países anfitriones. Si un diplomático intentara enviar mensajes ocultos esteganográficamente a su país, podrían ser interceptados, analizados y el contenido podría ser descubierto. En esta situación, la criptografía es más adecuada, porque aunque los interceptores sabrán que se está comunicando, no podrán averiguar de qué se trata.

Técnicas esteganográficas

Existen muchas técnicas para ocultar información. A continuación explicamos las más habituales.

Enmascaramiento

En este caso la información se oculta dentro de una imagen digital usando marcas de agua donde se introduce información, como el derecho de autor, la propiedad o licencias. El objetivo es diferente de la esteganografía tradicional, lo que se pretende es añadir un atributo a la imagen que actúa como cubierta. De este modo se amplía la cantidad de información presentada.

Algoritmos de la compresión de datos

Esta técnica oculta datos basados en funciones matemáticas que se utilizan a menudo en algoritmos de la compresión de datos. La idea de este método es ocultar el mensaje en los bits de datos menos importantes.

Métodos de sustitución

Una de las formas más comunes de hacer esto es alterando el bit menos significativo (LSB). En archivos de imagen, audio y otros, los últimos bits de información en un byte no son necesariamente tan importantes como los iniciales. Por ejemplo, 10010010 podría ser un tono de azul. Si solo cambiamos los dos últimos bits a 10010001, podría ser un tono de azul que es casi exactamente igual. Esto significa que podemos ocultar nuestros datos secretos en los dos últimos bits de cada píxel de una imagen, sin cambiar la imagen de forma notable. Si cambiamos los primeros bits, lo alteraría significativamente.

El método del LSB funciona mejor en los archivos de imágenes que tienen una alta resolución y usan gran cantidad de colores. En caso de archivos de audio, favorecen aquellos que tienen muchos y diferentes sonidos que poseen una alta tasa de bits.

Además este método no altera en absoluto el tamaño del archivo portador o cubierta (por eso es «una técnica de sustitución»). Posee la desventaja de que el tamaño del archivo portador debe ser mayor al mensaje a embeber; se necesitan 8 bytes de imagen por cada byte de mensaje a ocultar; es decir, la capacidad máxima de una imagen para almacenar un mensaje oculto es de su 12,5%. Si se pretende emplear una mayor porción de bits de la imagen (por ejemplo, no solo el último, sino los dos últimos), puede comenzar a ser percibible al ojo humano la alteración general provocada.

Esteganografía según el medio

Dependiendo de la naturaleza del objeto de cobertura (objeto real en el que se incrustan datos secretos), la esteganografía se puede dividir en varios tipos. Exploremos cada uno de ellos.

Documentos

La **esteganografía de texto** oculta información dentro de los archivos de texto. Implica cosas como cambiar el formato de texto existente, cambiar palabras dentro de un texto, generar secuencias de caracteres aleatorias o usar gramáticas libres de contexto para generar textos legibles. Varias técnicas utilizadas para ocultar los datos en el texto son:

- Método basado en formato
- Generación estadística y aleatoria

- Método lingüístico

Imágenes

Ocultar los datos tomando el objeto de portada como imagen se conoce como **esteganografía de imagen**. En la esteganografía digital, las imágenes son una fuente de cobertura ampliamente utilizada porque hay una gran cantidad de bits presentes en la representación digital de una imagen. Hay muchas formas de ocultar información dentro de una imagen. Los enfoques comunes incluyen:

- Inserción de bits menos significativa
- Enmascaramiento y filtrado
- Codificación de patrón redundante
- Cifrar y dispersar
- Codificación y transformación del coseno

Vídeo

En la **esteganografía de video** puede ocultar tipos de datos en formato de video digital. La ventaja de este tipo es que se puede ocultar una gran cantidad de datos en su interior y el hecho de que es un flujo de imágenes y sonidos en movimiento. Puedes pensar en esto como la combinación de esteganografía de imagen y esteganografía de audio. Dos clases principales de video esteganografía incluyen:

- Incrustar datos en video sin comprimir y comprimirlos más tarde
- Incrustar datos directamente en el flujo de datos comprimidos

Audio

En la **esteganografía de audio**, el mensaje secreto está incrustado en una señal de audio que altera la secuencia binaria del archivo de audio correspondiente. Ocultar mensaje secretos en digital es un proceso mucho más dificil en comparación con otros, como la esteganografía de imágenes. Los diferentes métodos de esteganografía de audio incluyen:

- Codificación de bits menos significativos
- Codificación de paridad
- Codificación de fase
- Espectro ensanchado

Este método oculta los datos en archivos de sonido WAV, AU e incluso MP3.

Otros archivos

Uno de los métodos más fáciles de implementar es el de inyección o agregado de bytes al final del archivo. Esta técnica consiste, esencialmente, en agregar o adosar al final de un archivo, de cualquier tipo, otro archivo que será el contenedor del «mensaje a ocultar», también de cualquier tipo. Esta metodología es la más versátil, pues permite usar cualquier tipo de archivo como

portador (documentos, imágenes, audio, vídeos, ejecutables, etc) y añadir al final del archivo contenedor el «paquete enviado», que es otro archivo, también de cualquier tipo.

Esteganografía en internet y redes sociales

Hoy en día todos (o casi) utilizamos al menos, una red social, como Twitter, Facebook o Instagram, entre otras muchas. Esto convierte a estos canales de comunicación en los transportes ideales de todo tipo de información, un medio de interconexión fácil de usar y con capacidad de llegada a múltiples destinatarios, a cualquier parte del mundo.

A través de las redes sociales también es posible enviar información de forma completamente inadvertida. Esto es: utilizando **esteganografía informática**. No es fácil hacerlo, pues tienen sus propios algoritmos de detección de código oculto, amén de otras técnicas de inserción, como el cambio de resoluciones de imágenes, una vez subidas a la plataforma, etc. Pero esto no quiere decir que sea imposible conseguirlo.

Otros usos: espías ilegales, terrorismo y más

Hoy en día, los atacantes utilizan scripts de **PowerShell** y **BASH** para automatizar los ataques. También lo son los probadores de lápiz. Por ejemplo, los atacantes han incrustado scripts reales en documentos de Excel y Word habilitados para macros. Una vez que una víctima abre el documento de Excel o Word, activa la secuencia de comandos secreta incrustada.

El atacante no necesita engañar al usuario para que use aplicaciones como **Steghide**. El atacante está utilizando una aplicación esteganográfica para aprovechar las funciones y aplicaciones comunes de Windows, como Excel y PowerShell. Todo lo que la víctima debe hacer es leer el documento y comienza a ocurrir una serie de eventos desafortunados.

- Primero, la víctima hace clic en un documento de Excel que un atacante ha modificado usando esteganografía.

- Ese clic libera un script de PowerShell oculto.

- Este script luego instala una aplicación de instalación en la computadora con Windows. Esta aplicación de instalación se mueve rápidamente y es tan sutil que las aplicaciones antivirus típicas no lo notan.

- Este descargador luego sale a Internet y toma versiones actualizadas de malware como URLZone (o herramientas más recientes) que luego comprometen la computadora de la víctima.

A lo largo de los años, los atacantes han utilizado el procedimiento anterior para entregar ransomware como Snatch. Los piratas informáticos han instalado malware sofisticado que es un cable de registro de teclas, alistando computadoras en redes de bots DDoS o instalando troyanos, como las últimas variantes de Rovnix y Pillowmint.

Estegoanálisis o detección de mensajes ocultos

El **estegoanálisis** es una disciplina de investigación relativamente nueva con pocos artículos que aparecieron antes de finales de la década de 1990. El estegoanálisis es el proceso de detectar la esteganografía al observar las variaciones entre los patrones de bits y los tamaños de archivo inusualmente grandes. Es el arte de descubrir y transmitir mensajes encubiertos inútiles.

El objetivo del estegoanálisis es identificar los flujos de información sospechosos, determinar si tienen mensajes ocultos codificados en ellos y, si es posible, recuperar la información oculta.

El hecho de que la esteganografía no se pueda detectar en todo momento hace que el estegoanálisis sea un área de investigación en curso. Las limitaciones se magnifican debido al hecho de que la esteganografía no es una técnica exacta.

Los **programas esteganográficos** actuales pueden ocultar cualquier tipo de datos binarios en varios tipos de medios de cobertura. Para empezar, nunca se puede predecir si hay un mensaje secreto; Es probable que el uso de la esteganografía por terroristas y delincuentes aumente en el futuro, lo que plantea un problema para las fuerzas del orden. El estegoanálisis debe desarrollarse aún más para ayudar a contrarrestar el terrorismo de alta tecnología y los casos de espionaje industrial.

Herramientas para descifrar esteganografía online

Veamos las principales herramientas para descifrar esteganografía online.

Stegdetect

Es una herramienta de esteganálisis común. Stegdetect puede encontrar información oculta en imágenes JPEG utilizando esquemas de esteganografía como F5, Invisible Secrets, JPHide y JSteg. También tiene una interfaz gráfica llamada Xsteg.

Stego Suite

Se compone de tres productos. Stego Watch es una herramienta de esteganografía que busca contenido oculto en archivos de imagen o audio digitales. Stego Analyst es un analizador de archivos de imagen y audio que se integra con Stego Watch para proporcionar un análisis más

detallado de los archivos sospechosos y Stego Break es un descifrador de contraseñas diseñado para obtener la contraseña de un archivo que contiene esteganografía.

ILook Investigator

Es una herramienta de análisis forense utilizada por miles de laboratorios de aplicación e investigadores de todo el mundo para la investigación de imágenes forenses creadas por diferentes utilidades de imágenes.

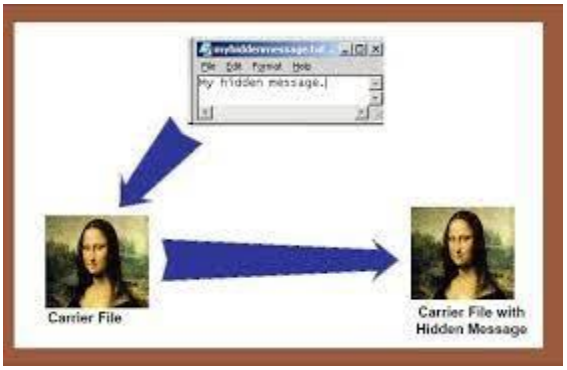
EnCase

EnCase cuenta con una guía intuitiva que permite a los examinadores gestionar fácilmente grandes volúmenes de pruebas informáticas y ver todos los archivos relevantes, incluidos los archivos «eliminados», la holgura del archivo y el espacio no asignado.
La solución automatiza eficazmente los procedimientos de investigación básicos, reemplazando procesos y herramientas arcaicos, que requieren mucho tiempo y costes.

En EnCase, los investigadores deben identificar y hacer coincidir el valor hash MD5 de cada archivo sospechoso. Deben importar o construir una biblioteca de conjuntos hash (en este caso, un software de esteganografía) con la función de biblioteca en EnCase. El hash identificará coincidencias de archivos stego.

Además, los investigadores deben tener cuidado al crear conjuntos de hash para descubrir esteganografía, para prevenir falsos positivos. Por ejemplo, los investigadores deben utilizar conjuntos de hash seguros para filtrar archivos inofensivos de su investigación.

Imágenes


File Edit Format Help
My hidden message.
Carrier File
Carrier File with
Hidden Message


Encriptación o cifrado
10100110 1

Conclusión

En conclusión, el trabajo de ciberseguridad y seguridad informática es de vital importancia en la era digital actual. La protección de la información y la prevención de ataques cibernéticos se han convertido en prioridades para individuos, empresas y organizaciones en todo el mundo.

A lo largo de este trabajo, hemos explorado diversos aspectos clave de la ciberseguridad y seguridad informática, como firewalls, software antivirus, infraestructura de clave pública (PKI), servicios de detección y respuesta gestionados (MDF), pruebas de penetración (pentesting), esteganografía y técnicas de cifrado.

Hemos aprendido que la implementación de medidas de seguridad efectivas, como firewalls y software antivirus, es fundamental para proteger los sistemas y redes contra amenazas cibernéticas. Además, la utilización de PKI garantiza la confianza en entornos digitales y facilita la autenticación y el cifrado de datos.

También hemos explorado la importancia de los servicios MDF, que brindan una respuesta proactiva y continua ante incidentes de seguridad, y las pruebas de penetración, que ayudan a identificar y solucionar vulnerabilidades en sistemas y aplicaciones.

Por último, hemos analizado la esteganografía y las técnicas de cifrado como herramientas para ocultar información y proteger la confidencialidad de los datos.

En resumen, la ciberseguridad y la seguridad informática son campos en constante evolución, donde la comprensión y aplicación de medidas adecuadas son fundamentales para garantizar la integridad, confidencialidad y disponibilidad de la información. La implementación de un enfoque holístico de seguridad, combinando medidas técnicas, procesos y educación, es esencial para protegerse de las amenazas cibernéticas en curso y mantener la seguridad en el entorno digital actual.

Bibliografía

https://www.ibm.com/docs/es/i/7.1?topic=options-firewalls

https://www.geeknetic.es/Firewall/que-es-y-para-que-sirve

https://vpnoverview.com/es/antivirus-informacion/que-es-un-antivirus/

https://www.tecnologia-informatica.com/que-es-un-antivirus-como-funciona/

https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009900--htm

https://forum.huawei.com/enterprise/es/%C2%BFqu%C3%A9-es-mdf/thread/667227925411414016-667212890693840896

https://www.iebschool.com/blog/que-es-pentesting-tecnologia/

https://ayudaleyprotecciondatos.es/2021/03/17/esteganografia/#Que_es_la_esteganografia