**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Hacking Ético en Sistemas y Redes |
| --- | --- |

| COMPETENCIA | 220501111- Controlar sistema de seguridad de la información de acuerdo con los procedimientos y la normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-3. Emplear herramientas especializadas para la solución de problemas de ciberseguridad y seguridad informática en sistemas y redes. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF003 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Vulnerabilidades y Ataques en el Hacking Ético |
| BREVE DESCRIPCIÓN | La seguridad informática se ha convertido hoy en día en una preocupación para empresas y organizaciones en medio del mundo digital, es por ello que es importante conocer y aplicar diferentes herramientas digitales para ciberseguridad y conocer las vulnerabilidades y ataques a los cuales están expuestos los sistemas y redes y así protegerlos de cibercriminales. |
| PALABRAS CLAVE | Ataque, Escaneo, Redes, Vulnerabilidad, Virus |

| ÁREA OCUPACIONAL | 2 - CIENCIAS NATURALES, APLICADAS Y RELACIONADAS |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDO:**

**Introducción**

1. **Análisis de vulnerabilidades**
   1. Herramientas
   2. Falsos positivos
2. **Escalamiento de privilegios**
   1. Escalamiento horizontal y vertical
   2. Contramedidas
3. **Ataques a dispositivos**
   1. Conceptos y tipo de ataques
   2. Herramientas y técnicas de ataques
   3. Contramedidas
4. **Ataques a redes cableadas**
   1. Conceptos y generalidades
   2. Modelo de redes OSI
   3. Herramientas de ataque
   4. Contramedidas
5. **Ataques con virus y malware**
   1. Conceptos y generalidades
   2. Tipos de virus y malware
   3. Protección con antivirus y evasiones

**B. DESARROLLO DE CONTENIDO:**

**Introducción**

En el mundo digital de hoy, se encuentra con gran cantidad de información al alcance de su mano, la cual se ha convertido en uno de los activos más importantes para una persona u organización. Con el uso de las tecnologías de información y comunicación y su avance tan vertiginoso, aparecen agentes tanto internos como externos que pueden poner en riesgo los sistemas de información y los datos que se pueden almacenar al igual que la infraestructura tecnológica donde se encuentran, es por ello que el hacking ético se ha convertido en una herramienta de gestión para poder salvaguardar los datos. Observe el siguiente recurso que amplía esta introducción. Bienvenido.



1. **Análisis de vulnerabilidades**

Las vulnerabilidades en el *software*, son una de las principales puertas de entrada para los cibercriminales, pero también, es un vector de ataque, una mala configuración de nuestros servicios, e incluso la exposición de puerto TCP/UDP a Internet sin ningún tipo de filtrado. Los piratas informáticos están buscando constantemente nuevas formas de atacar cualquier ordenador, servidor o red a través de estos fallos de seguridad, por este motivo, los propios ingenieros de las compañías, los investigadores de seguridad y los hackers éticos están constantemente analizando los diferentes programas en busca de fallos de seguridad y reportándose para que se solucione, la herramienta imprescindible para esta tarea con los escáneres de vulnerabilidades.





En el siguiente gráfico, puede observar la diferencia entre los escaneos de vulnerabilidad y las pruebas de penetración.

**Figura 1**

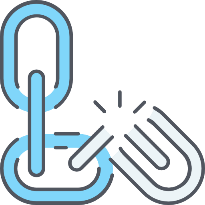
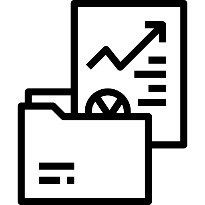
*Escaneos de vulnerabilidad y pruebas de penetración*



















Existen varias formas de realizar análisis de vulnerabilidades, pero una de las más comunes es a través de un *software* de exploración de vulnerabilidades automatizado, estas herramientas utilizan bases de datos de vulnerabilidades conocidas para identificar posibles fallos en sus redes, aplicaciones, contenedores, sistemas, datos, hardware y más, la herramienta de análisis de vulnerabilidades escaneará exhaustivamente cada aspecto de su tecnología, una vez que se completen los escaneos, la herramienta informará sobre todos los problemas descubiertos y sugerirá acciones para eliminar las amenazas

Las herramientas más completas pueden ofrecer una visión de la seguridad y el impacto operativo de la reparación de un riesgo, en comparación con la aceptación del riesgo, los datos de escaneo de vulnerabilidades también pueden ser integrados en un SIEM junto con otros datos para un análisis de amenazas aún más holístico.

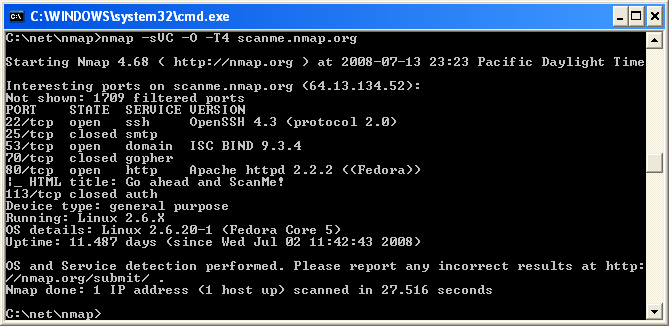
* 1. **Herramientas**

Un escáner de vulnerabilidades es un *software* diseñado para realizar análisis automáticos de cualquier aplicación, sistema o red en busca de cualquier posible vulnerabilidad que exista, aunque estas aplicaciones no son capaces de detectar la vulnerabilidad con total precisión, sí son capaces de detectar ciertos elementos que podrían desencadenar en una vulnerabilidad, facilitando enormemente el trabajo a los investigadores e ingenieros.

Hay varios tipos de escáneres de vulnerabilidades, autenticados, en los que se realizan pruebas y ataques potenciales desde la propia red, y no autenticados, en los que el investigador o hacker ético se intenta hacer pasar por un pirata informático simulando un ataque desde fuera para ver hasta dónde es capaz de llegar analizando posibles vulnerabilidades.

Existe un gran número de herramientas de este tipo, tanto comerciales como de código abierto, y todas estas herramientas tienen sus propios puntos fuertes y débiles, si está interesado en la eficacia de las herramientas DAST, consulte el proyecto OWASP *Benchmark*, que mide científicamente la eficacia de todos los tipos de herramientas de detección de vulnerabilidades, incluidas las DAST.

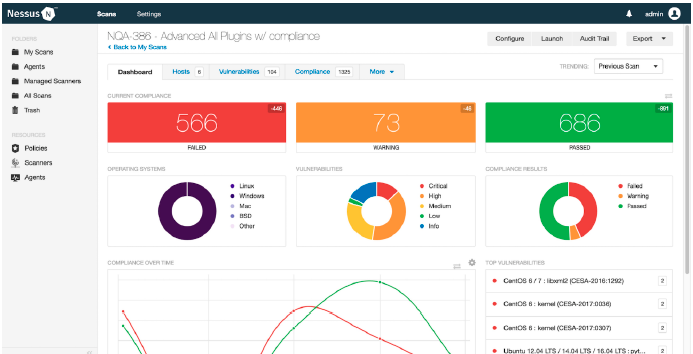
* **Herramienta Nmap**

*Network Mapped* (Nmap) es una herramienta de escaneo de red y detección de host que es muy útil durante varios pasos de las pruebas de penetración. Nmap no se limita a la mera recopilación de información y enumeración, sino que también es una poderosa utilidad que puede utilizarse como detector de vulnerabilidades o escáner de seguridad. Así que Nmap es una herramienta multipropósito, y puede ser ejecutada en muchos sistemas operativos diferentes, incluyendo *Windows*, *Linux*, *BSD* y *Mac*. 

Nmap es una herramienta muy común y poderosa, y está disponible tanto para la interfaz de línea de comandos como para la interfaz gráfica de usuario. Puede utilizarse para:

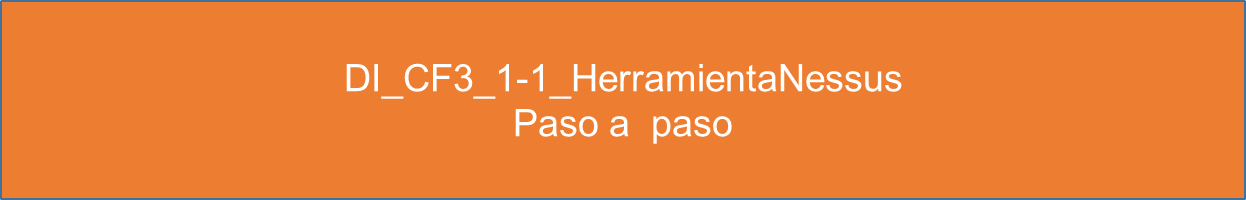
* Detectar el anfitrión vivo en la red (descubrimiento de anfitrión)
* Detectar los puertos abiertos en el host (descubrimiento o enumeración de puertos)
* Detectar el software y la versión del puerto respectivo (descubrimiento de servicio)
* Detectar el sistema operativo, la dirección del hardware y la versión del *software*.
* Detectar la vulnerabilidad y los agujeros de seguridad (scripts Nmap)

* **Herramienta Nessus**

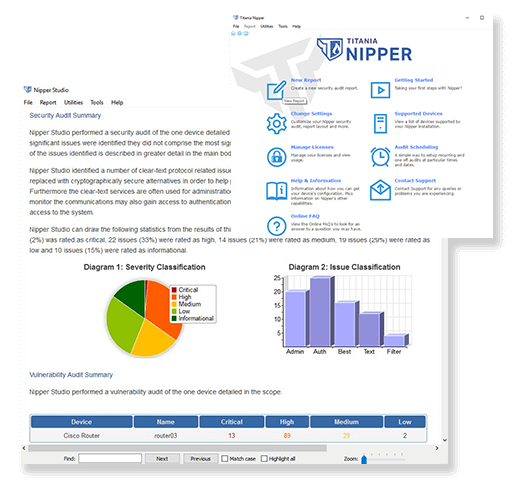
Nessus es una herramienta de escaneo de seguridad remota, que escanea un ordenador y emite una alerta si descubre alguna vulnerabilidad que los hackers maliciosos podrían utilizar para obtener acceso a cualquier ordenador que se haya conectado a una red, todo esto lo logra ejecutando más de 1200 chequeos en una computadora dada, probando para ver si alguno de estos ataques podría ser usado para irrumpir en la computadora o dañarla de alguna manera.



Lo invitamos a ver el siguiente recurso, para aprender cómo funcionan Nessus y otras herramientas de seguridad de escaneo de puertos.



Nessus es llamado un "scanner remoto" porque no necesita ser instalado en una computadora para que pueda probar esa computadora, en su lugar, puede instalarlo en un solo ordenador y probar tantos ordenadores como desee.



* **Herramienta Nipper**

Titania Nipper Studio tiene una tasa de éxito incomparable y una reputación muy marcada en el campo de la auditoría de configuración de cortafuegos, conmutadores y enrutadores, Nipper identifica rápidamente las vulnerabilidades no descubiertas en los *firewalls, switches y routers*, priorizando automáticamente los riesgos de acuerdo con su empresa. Nuestro modelado virtual reduce los falsos positivos a un índice insignificante e identifica las correcciones exactas para ayudarte a mantener tu empresa segura y en cumplimiento con las normas.

Nipper Studio ofrece las siguientes soluciones como parte de su experiencia de producto:

**Remediación precisa con arreglos técnicos exactos**

Nipper Studio ofrece una identificación exacta de las amenazas y riesgos en toda su infraestructura de red y proporciona soluciones de remediación completas, incluyendo, pero no limitado a, correcciones en la línea de comandos, el uso de Nipper ha documentado que los equipos de auditoría pueden ahorrar hasta una enorme cantidad de 3-4 horas por dispositivo. Incluso le permite personalizar las auditorías de las mejores prácticas del mercado o utilizar estándares de cumplimiento de la industria "listos para usar" (como los puntos de referencia STIG y CIS).

**Le da características críticas que otros escáneres no tienen**

Auditoría sin tráfico de red, configuración de autenticación, configuración de autorización, traducción de direcciones de red, protocolos de red, opciones específicas de dispositivos, sincronización de tiempo, etc. Nipper Studio hace innumerables cosas para el bienestar cibernético de su empresa que otros productos no le ofrecen.

**Configuración crucial y análisis de construcción**

Puede elevar aún más sus sistemas de seguridad utilizando herramientas de análisis de configuración y construcción automática, que sirven como una ventaja significativa para un SOC o NOC, utilizar estas herramientas para analizar la configuración de su sistema, en detalle y a velocidad - implica que puede encontrar y cerrar las vulnerabilidades explotables que las soluciones basadas en la monitorización o el análisis se perderían.

En la siguiente infografía se puede revisar el proceso de análisis de vulnerabilidades a través de la herramienta Nipper.



La información proporcionada por un análisis de vulnerabilidad ayuda a los equipos de TI, así como a las herramientas automatizadas de terceros (es decir, la gestión de parches), a priorizar las vulnerabilidades y a trazar el camino para la acción, lo que a menudo significa la reparación. Sin embargo, a veces las organizaciones optan por aceptar la continuidad del riesgo.

Por ejemplo, si la vulnerabilidad descubierta tiene un impacto potencial bajo y una probabilidad baja, pero, por otra parte, su reparación requeriría un tiempo de inactividad o la posible ruptura de otros sistemas, la tecnología de la información puede determinar que el riesgo de vulnerabilidad es menor que el riesgo que plantean las operaciones de tecnología de la información en curso, así es como los análisis de vulnerabilidad se inscriben en un marco general de gestión de los riesgos de la tecnología de la información.

* 1. **Falsos positivos**

Comúnmente, los falsos positivos en la exploración de vulnerabilidades ocurren cuando el explorador puede acceder solo a un subconjunto de la información requerida, lo que le impide determinar con precisión si existe una vulnerabilidad. Para ayudar a reducir el número de falsos positivos, se deben configurar sus escáneres con las credenciales adecuadas, estos necesitan acceder a toda la información requerida de los activos para que pueda determinar con precisión si existe una vulnerabilidad, tanto si se utiliza una herramienta de exploración de vulnerabilidades como si se utiliza otra forma de identificación de vulnerabilidades. Existen dos tipos de errores que hay que tener en cuenta:

**Error de tipo I - falso positivo**, un resultado que indica que una vulnerabilidad está presente cuando no lo está, esto crea ruido y resulta en un trabajo de remediación innecesario.

**Error de tipo II - falso negativo**, donde una vulnerabilidad está presente pero no está identificada.

A continuación, se explica cuándo ocurre un falso positivo.



Si las primeras 20 variantes son falsos positivos, el probador de penetración asume que todas las demás son falsos positivos e ignora todas las demás; al hacerlo, hay posibilidades que las vulnerabilidades reales de las aplicaciones web no sean detectadas, por eso es crucial comprobar cada vulnerabilidad y tratar cada falso positivo por separado para asegurar los falsos positivos.

La mayoría de los proveedores de escáneres dedican un esfuerzo considerable a mejorar continuamente la calidad de sus algoritmos de comparación y a añadir nuevas capas de comprobaciones cruzadas que buscan mejorar el nivel de certeza de cualquier informe de vulnerabilidad, aunque este enfoque proporciona ganancias incrementales en la precisión de los informes, no aborda el problema subyacente que una vulnerabilidad de seguridad solo puede confirmarse absolutamente si se explota con éxito. Cualquier cantidad de retoques en las firmas y algoritmos de concordancia es, en efecto, un mero adorno, ya que el único mecanismo 100 fiable para confirmar una vulnerabilidad es la explotación.

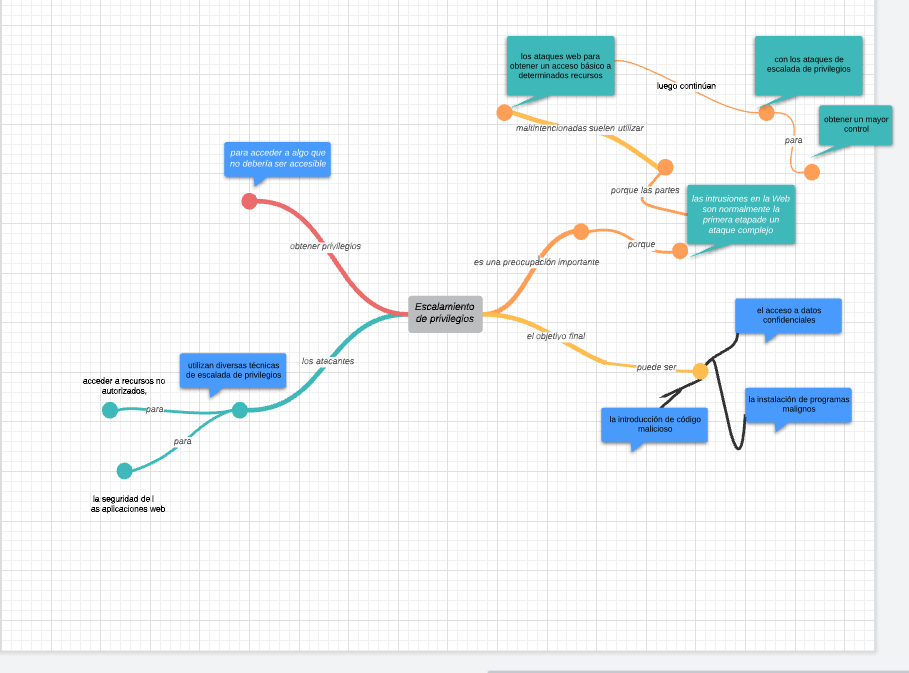
1. **Escalamiento de privilegios**

La escalada de privilegios es la explotación de un error de programación, una vulnerabilidad, un fallo de diseño, la supervisión de la configuración o el control de acceso en un sistema operativo o una aplicación para obtener un acceso no autorizado a recursos que suelen estar restringidos de la aplicación o el usuario.

Esto da lugar a que la aplicación o el usuario tenga más privilegios de los previstos por el desarrollador o el administrador del sistema, lo que permite a los atacantes acceder a datos confidenciales, instalar programas malignos y lanzar otros ataques cibernéticos. En palabras simples, significa obtener privilegios para acceder a algo que no debería ser accesible, como se muestra en la siguiente figura.

**Figura 2**

*Escalamiento de privilegios*



* 1. **Escalamiento horizontal y vertical**

Existen dos tipos de escalada de privilegios:

**Escalamiento de privilegios horizontal**

El término escalada de privilegios horizontales se aplica a todas las situaciones en que un atacante actúa como un usuario específico y obtiene acceso a los recursos pertenecientes a otro usuario con un nivel de acceso similar. Por ejemplo, si un atacante se hace pasar por un usuario y obtiene acceso no autorizado a su cuenta bancaria, éste es un ejemplo de escalada horizontal de privilegios

Muchas vulnerabilidades de la web pueden dar lugar a una escalada horizontal de privilegios, por ejemplo, los ataques de Cross Site Scripting (pueden permitir al atacante robar las cookies de sesión del usuario para acceder a su cuenta de usuario Los ataques CSRF también son ejemplos de escalada de privilegios horizontales.

**Escalamiento de privilegios vertical**

Un atacante intenta obtener mayores privilegios o acceso con una cuenta existente que ha comprometido. Por ejemplo, un atacante se hace cargo de una cuenta de usuario normal en una red e intenta obtener privilegios administrativos, normalmente el administrador o el usuario del sistema en Microsoft Windows, o el root en los sistemas Unix y Linux, una vez que obtienen privilegios elevados, los atacantes pueden robar datos confidenciales sobre un usuario específico, instalar software de rescate, spyware u otros tipos de malware, ejecutar código malicioso y dañar la postura de seguridad de su organización.

Se suele denominar elevación de privilegios, se aplica a todas las situaciones en las que el atacante obtiene privilegios más altos, la mayoría de las veces privilegios de raíz (privilegios administrativos) la elevación de privilegios es, en la mayoría de los casos, el segundo paso de un ataque, si el ataque se dirige directamente al servidor web, el usuario malicioso a menudo tiene como objetivo primero obtener cualquier tipo de sistema de archivos y/o acceso a la consola; después de obtener acceso al servidor web, puede intentar utilizar otras técnicas para obtener acceso a una cuenta con privilegios, en la mayoría de los casos el administrador del sistema.



* 1. **Contramedidas**

Las vulnerabilidades de la escalada de privilegios pueden surgir por diferentes razones, como lo puede revisar en la siguiente figura.

**Figura 3**

*Contramedidas*



**Para prevenir los ataques de escalada de privilegios,** los atacantes utilizan muchas técnicas de escalada de privilegios y así lograr sus objetivos. La buena noticia es que, si puedes detectar rápidamente los ataques de escalada de privilegios exitosos o intentados, tienes una buena oportunidad de detener a los intrusos antes de que puedan lanzar su ataque principal.

Para intentar la escalada de privilegios, en primer lugar, los atacantes normalmente necesitan acceder a una cuenta menos privilegiada. Esto significa que las cuentas de usuarios regulares son su primera línea de defensa, asegúrese de invertir en un fuerte control de acceso:

**Aplicar políticas de contraseñas**

Una de las formas más simples de mejorar la seguridad es hacer cumplir las contraseñas seguras. No reutilice las contraseñas, ya que pueden quedar expuestas en grandes violaciones de datos. Consulte nuestra guía sobre cómo crear contraseñas seguras e invierta en una herramienta para controlar continuamente las credenciales filtradas.

**Crear usuarios y grupos especializados con los mínimos privilegios necesarios y acceso a los archivos**

El principio del mínimo privilegio en un contexto de seguridad se refiere a proporcionar a los usuarios normales solo el conjunto de privilegios que necesitan para hacer su trabajo y nada más. Lea nuestra guía sobre control de acceso para más información. Aunque es conveniente dar a cada usuario el mismo nivel de acceso a todos los recursos, proporciona a los atacantes un único punto de entrada a su organización, es mucho más seguro emplear la defensa en profundidad a través de sus esfuerzos de seguridad de datos, seguridad de la información y seguridad de la red.

**Invierta en formación de concienciación sobre ciberseguridad**

Incluso si su organización tiene una política de contraseñas sólida y aplicada, los ataques de ingeniería social como el *phishing* y el *spear phishing* pueden hacer que los ciberdelincuentes accedan a sus sistemas sensibles. Eduque a sus empleados y a los proveedores de terceros sobre las amenazas cibernéticas comunes y cómo evitarlas. Habilite la DMARC para evitar el *spoofing* de correo electrónico y comprar posibles dominios de tipografía.

1. **Ataques a dispositivos**

En los últimos tiempos, donde el mundo digital se ha acrecentado de manera exponencial, los ataques a dispositivos son cada vez más frecuentes, la tendencia es que tanto la adquisición como su uso de duplique en poco tiempo, es por ello que los ciberdelincuentes aprovechan esto para poder realizar ataques de diferente índole, es por ello que es perentorio conocer dentro del hacking ético las diferentes formas de ataques que se pueden realizar para poder salvaguardar su información.

* 1. **Conceptos y tipo de ataques**

Existen diferentes tipos de ataques dentro del *Hacking* ético, los más utilizados son los denominados ataques activos en línea, donde el atacante realiza el descifrado de contraseñas comunicándose directamente con la máquina víctima.

**Ataque del diccionario**

Revise a continuación en qué consiste este tipo de ataque, el cual es muy común.



**Ataque de fuerza bruta**

Un ataque de fuerza bruta utiliza el método de prueba y error para adivinar la información de acceso, las claves de cifrado o encontrar una página *web* oculta, los *hackers* trabajan con todas las combinaciones posibles esperando adivinar correctamente.

Estos ataques se realizan mediante "fuerza bruta", lo que significa que utilizan intentos excesivamente fuertes para intentar "forzar" su entrada en su(s) cuenta(s) privada(s)

Este es un método de ataque antiguo, pero aún es efectivo y popular entre los hackers, porque, dependiendo de la longitud y complejidad de la contraseña, su crackeo puede llevar desde unos pocos segundos hasta muchos años. Es así como los ciberdelincuentes se benefician de los ataques de fuerza bruta:

* Beneficiándose de los anuncios o recolectando datos de actividad.
* Robo de datos personales y objetos de valor.
* Difundir malware para causar interrupciones.
* Secuestro de su sistema para actividades maliciosas.
* Arruinar la reputación de un sitio web.

Tipos de ataques de fuerza bruta

Cada ataque de fuerza bruta puede utilizar diferentes métodos para descubrir sus datos sensibles. Puede estar expuesto a cualquiera de los siguientes métodos populares de fuerza bruta:

**Ataques simples de fuerza bruta**

Los ciberdelincuentes intentan adivinar lógicamente sus credenciales, sin ayuda de herramientas de software u otros medios, estos pueden revelar contraseñas y PINs extremadamente simples. Por ejemplo, una contraseña que se establece como "SENA12345".

**Ataques de diccionario**

Es un ataque estándar, un ciberdelincuente elige un objetivo y ejecuta posibles contraseñas contra ese nombre de usuario (como lo vimos en anteriormente), estos son conocidos como ataques de diccionario, los ataques de diccionario son la herramienta más básica en los ataques de fuerza bruta, aunque no son necesariamente ataques de fuerza bruta en sí mismos, a menudo se utilizan como un componente importante para descifrar contraseñas; algunos ciberdelincuentes recorren los diccionarios completos y aumentan las palabras con caracteres y números especiales o utilizan diccionarios especiales de palabras, pero este tipo de ataque secuencial es engorroso.

**Ataques de fuerza bruta híbridos**

Estos ciberdelincuentes mezclan medios externos con sus conjeturas lógicas para intentar un allanamiento, un ataque híbrido suele mezclar los ataques de diccionario y de fuerza bruta, estos ataques se utilizan para descifrar contraseñas compuestas que mezclan palabras comunes con caracteres aleatorios. Un ejemplo de ataque de fuerza bruta de esta naturaleza incluiría contraseñas como Sena1993 o SeNa1234.

**Ataques de fuerza bruta inversa**

Tal y como su nombre indica, un ataque de fuerza bruta inversa invierte la estrategia de ataque empezando con una contraseña conocida, luego los ciberdelincuentes buscan millones de nombres de usuario hasta que encuentran una coincidencia, muchos de estos criminales empiezan con contraseñas filtradas que están disponibles en línea a partir de brechas de datos existentes.

**Relleno de credenciales**

Si un ciberdelincuente tiene una combinación de nombre de usuario y contraseña que funciona para un sitio web, también lo intentará en muchos otros, como se sabe que los usuarios reutilizan la información de inicio de sesión en muchos sitios web, son el objetivo exclusivo de un ataque como este.

**Ataques basados en reglas**

Observe el siguiente video, el cual lo introduce a este tipo de ataques.



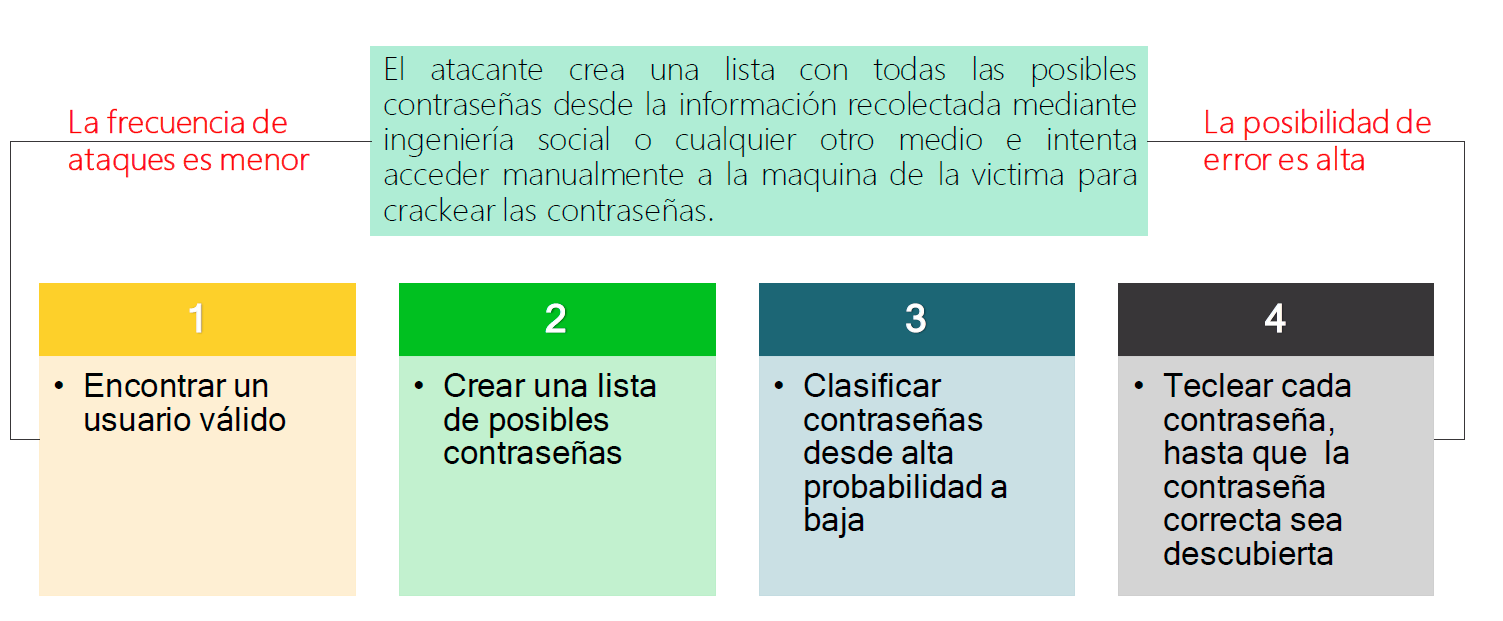
Existen malas prácticas de administración que facilitan mucho el trabajo a la hora de intentar acceder a un sistema Las contraseñas por defecto, son las contraseñas suministradas por los fabricantes cuando instalan un dispositivo o un servicio y que muchas veces los administradores de TI olvidan cambiar. Existen herramientas en línea que pueden utilizarse para buscar las contraseñas por defecto las cuales le pueden servir para realizar esta práctica:

* <https://cirt.net/passwords>
* <http://default-password.info>
* <http://www.defaultpassword.us>
* <http://www.passwordsdatabase.com>
* <https://open-sez.me>
* <http://www.routerpasswords.com>

**Adivinación de contraseña**

Suponga que no tiene ningún bloqueo en las cuentas. ¿Hay alguna manera de lidiar con los ataques de fuerza bruta sin un bloqueo? Una política de contraseñas débil puede dar lugar a que entre en el sitio en tan solo 18 días si ya conoce el nombre de usuario de la cuenta.

Primero, considere endurecer la política de contraseñas, supongamos que tiene una política de contraseñas que requiere 12 caracteres en mayúsculas y minúsculas que deben incluir tanto letras como números, los hackers tienen una probabilidad de 50:50 de entrar dentro de 6211 intentos, eso se traduce en unos 52 millones de millones de intentos.



**Contraseña por defecto**

Una contraseña por defecto es una contraseña estándar preconfigurada para un dispositivo, estas contraseñas son la configuración predeterminada de muchos dispositivos y, si no se modifican, representan un grave riesgo para la seguridad.

lLos ejemplos típicos de contraseñas predeterminadas incluyen admin password e guest, además, un proveedor suele utilizar una sola contraseña predeterminada, que puede encontrarse fácilmente en línea mediante la búsqueda o en sitios web que ofrecen listas compiladas, las contraseñas predeterminadas se utilizan comúnmente para los enrutadores, puntos de acceso, conmutadores y cortafuegos.



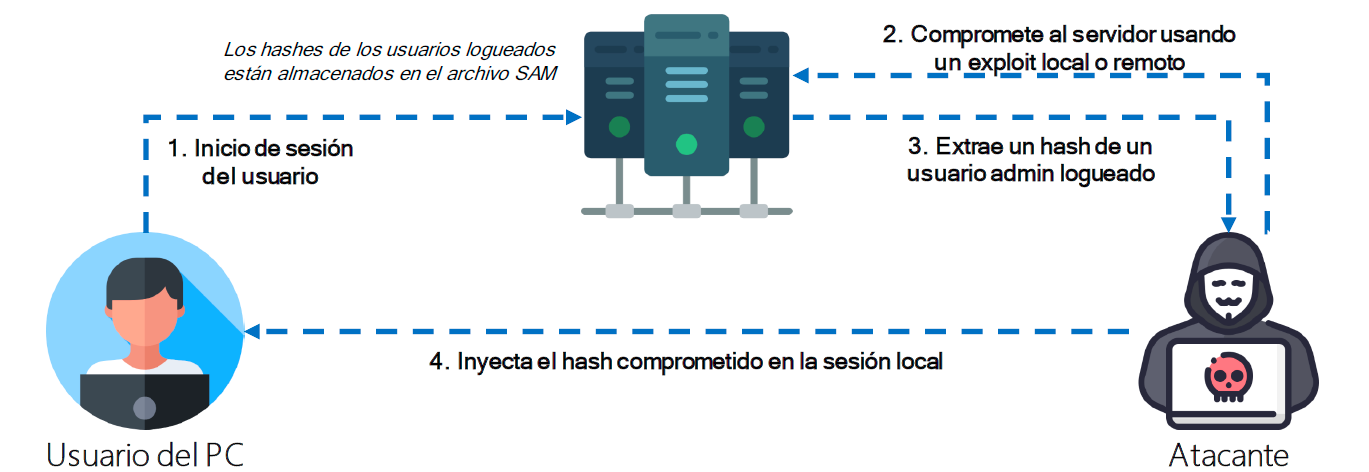
También son comunes en los sistemas empotrados, los sistemas de control industrial (y las interfaces de terminales remotas como Telnet y SSH). Si no se modifican, las contraseñas por defecto proporcionan un fácil vector de ataque para el equipo de la red doméstica si el propietario también se conecta a una red corporativa, ese riesgo se extiende también a la empresa, un atacante que se conecta con éxito a un dispositivo es probable que tenga acceso a nivel administrativo.

Una contraseña por defecto es una contraseña (normalmente "123", "admin", "root", "password", "<blank>", "secret" o "access") asignada a un programa o dispositivo de hardware por el desarrollador o fabricante, aunque las contraseñas predeterminadas pueden ayudar a protegerse de algunos usuarios, cualquiera que sepa lo que está haciendo puede adivinar una contraseña predeterminada.



**Ataque de inyección de *hash***

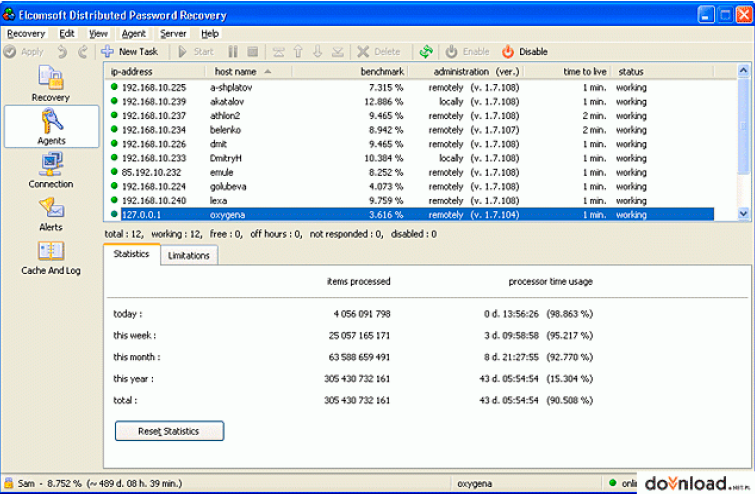
Un ataque de inyección de *hash* permite a un atacante inyectar un hash comprometido en una sesión local y usar el hash para validar los recursos de la red, donde el atacante encuentra y extrae un hash de la cuenta de administración del dominio y usa el hash extraído para buscar en el controlador de dominio.



Con esta técnica, un atacante captura el *hash* de una contraseña (en contraposición a los caracteres de la contraseña) y luego simplemente la pasa para autenticarse y tener un acceso potencialmente lateral a otros sistemas en red, el actor de la amenaza no necesita desencriptar el hash para obtener una contraseña en texto plano, los ataques PtH explotan el protocolo de autenticación, ya que el hash de las contraseñas permanece estático en cada sesión hasta que la contraseña se rota (cambia de posición). Los atacantes comúnmente obtienen el hash raspando la memoria activa de un sistema y otras técnicas.

* 1. **Herramientas y técnicas de ataques**

El mundo del hacking ético tiene múltiples posibilidades en el uso de herramientas, las cuales ayudan al atacante a encontrar contraseñas y explotar vulnerabilidades.

**Herramientas para la recuperación de contraseñas**

Están diseñadas para expertos forenses y organizaciones gubernamentales, servicios y corporaciones para la recuperación de datos. Está diseñada para descifrar las contraseñas más complejas y las claves de cifrado sólidas en plazos más cortos.

Es una herramienta para la recuperación de contraseñas a docenas de formatos de archivo, documentos, claves y certificados en grupos de ordenadoras combinadas en una sola red de ordenadoras distribuida *Elcomsoft Distributed Password Recovery,* ofrece escalabilidad y es compatible con la aceleración por GPU para la recuperación más rápida.

**Autenticación Microsoft SAM**

Se sabe que las computadoras de Windows pueden ser configuradas para estar en un grupo de trabajo o unidas a un dominio. En un grupo de trabajo, cada computadora tiene su propio SAM que contiene información sobre todas sus cuentas locales de usuario y de grupo, las contraseñas asociadas con cada una de estas cuentas se guardan en el SAM; el hash de las contraseñas ofrece cierta medida de seguridad y minimiza los riesgos de un ataque, la autoridad de seguridad local (LSA) valida el intento de inicio de sesión de un usuario verificando sus credenciales con los datos almacenados en el SAM El intento de inicio de sesión de un usuario sólo tiene éxito cuando la contraseña introducida coincide con la contraseña almacenada en el SAM local.

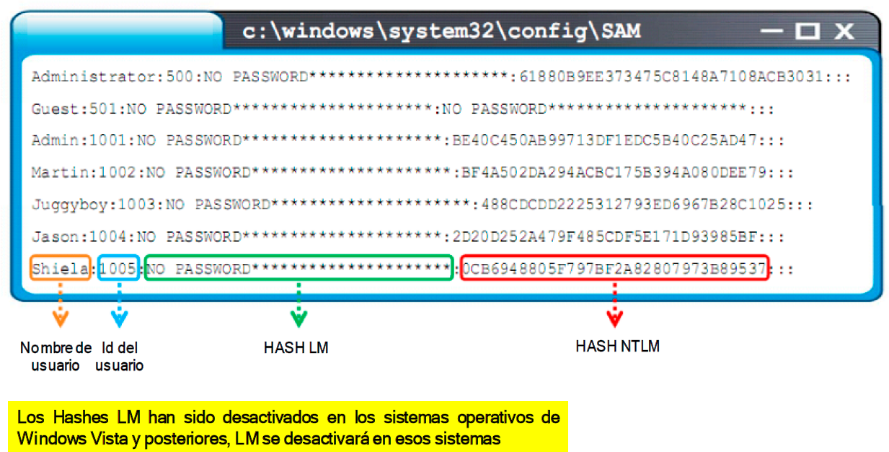
Revise en el siguiente recurso para conocer cómo se lleva a cabo la autenticación Microsoft SAM.



**¿Qué es SAM (Security Account Manager Database)?**

La base de datos SAM es la base de datos de información de cuentas de usuario y de grupo almacenada en un controlador de dominio en una red basada en Microsoft Windows Server.



La base de datos SAM ocupa una parte del registro del sistema operativo Windows Server. Todas las cuentas de usuario, las cuentas de grupo y las definiciones de recursos como acciones e impresoras tienen sus principios de seguridad definidos en la base de datos SAM. Debido a que toda la base de datos SAM debe residir en la memoria RAM de un controlador de dominio, no puede exceder de unos 40 MB en Windows NT, lo que equivale a unas 40.000 cuentas de usuario, o 26.000 usuarios y estaciones de trabajo de Windows NT combinadas. 

La gráfica anterior muestra la enumeración del tamaño de los objetos comunes en una base de datos SAM.

En una base de datos SAM:

* La copia maestra de la base de datos SAM se almacena en el controlador de dominio primario (PDC)
* La sincronización periódica de directorios asegura que los controladores de dominio de respaldo (CDP) tengan una réplica exacta de esta base de datos maestra.
* La réplica de los CDP también puede utilizarse para los inicios de sesión y para la autenticación de paso de los usuarios que intentan acceder a los recursos de la red.
* SAM utiliza medidas criptográficas para evitar que usuarios no autenticados accedan al sistema.
* Las contraseñas de los usuarios se almacenan en un formato de hash en una colmena de registro, ya sea como hash LM o como hash NTLM. Este archivo se encuentra en %SystemRoot%/system32/config/SAM y está montado en HKLM/SAM.

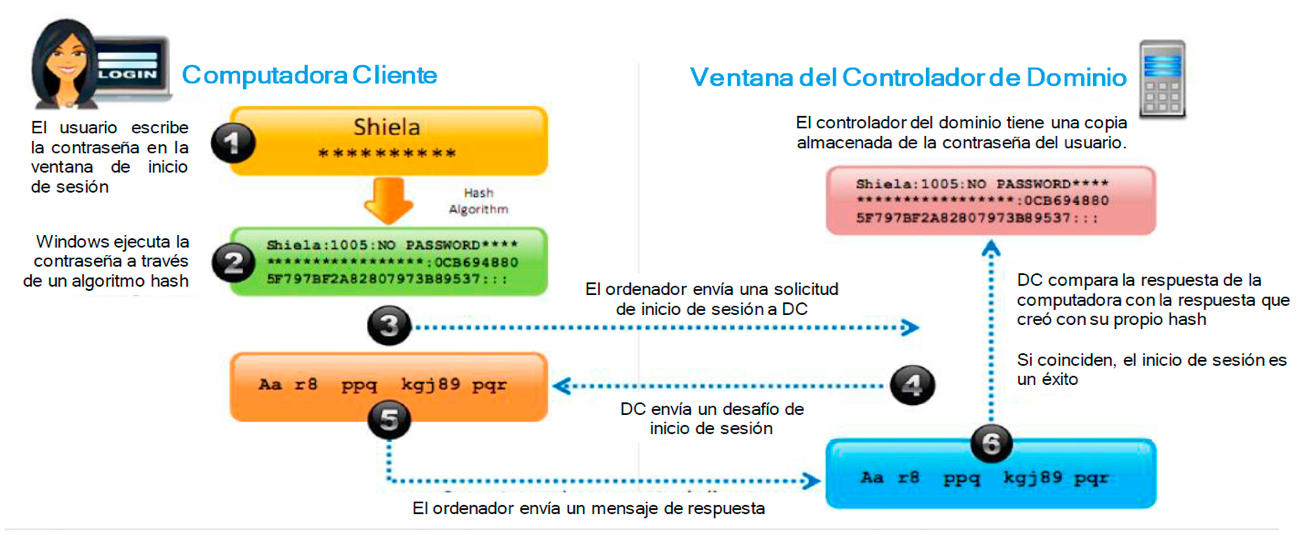
**Autenticación Microsoft NTLM**

NTLM consiste en una serie de protocolos de autenticación del desarrollador de software Microsoft. Al principio, solo se utilizaba como protocolo propietario, aunque ahora la autenticación NTLM (en inglés, NTLM authentication) también está disponible para otros sistemas además de Windows. NT LAN Manager permite que diferentes ordenadores y servidores se verifiquen entre sí. Una de las prioridades de la mayoría de las redes es evitar el acceso de participantes no autorizados, por lo que deben implementar un procedimiento de verificación: el cliente solo puede entrar en la red o utilizar sus servicios si ha sido autorizado.

El protocolo NTLM estipula que el cliente se autentique con un nombre de usuario y la contraseña correspondiente. Para ello, se genera un intercambio entre el dispositivo del usuario y un servidor. Este último conoce los datos de inicio de sesión, por lo que puede comprobar la solicitud de acceso y, a continuación, permitirlo.

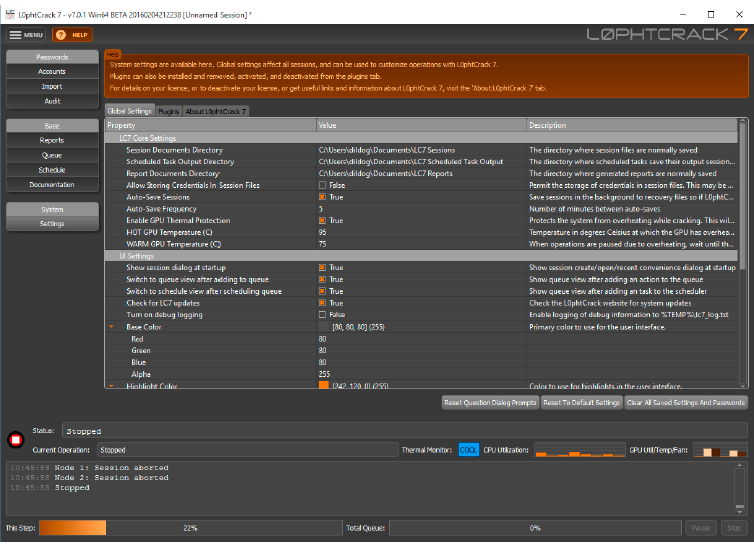
**Figura 4**

*Protocolo NTLM*



La autenticación NTLM es una familia de protocolos de autenticación que se engloban en el Msv 1 0 dll de Windows Los protocolos de autenticación NTLM incluyen LAN Manager versión 1 y 2 y NTLM versión 1 y 2 Los protocolos de autenticación NTLM autentican a los usuarios y a las computadoras sobre la base de un mecanismo de desafío/respuesta que demuestra a un servidor o a un controlador de dominio que un usuario conoce la contraseña asociada a una cuenta Cuando se utiliza el protocolo NTLM, un servidor de recursos debe realizar una de las siguientes acciones para verificar la identidad de una computadora o usuario siempre que se necesite un nuevo token de acceso:

* Ponerse en contacto con un servicio de autenticación de dominio en el controlador de dominio para el dominio de la cuenta de la computadora o del usuario, si la cuenta es una cuenta de dominio.
* Busque la cuenta de la computadora o del usuario en la base de datos de cuentas locales, si la cuenta es una cuenta local.

**Herramienta para crackear contraseñas L0 phtCrack**

L0phtCrack es una aplicación de auditoría y recuperación de contraseñas. Utiliza múltiples métodos de evaluación para ayudar a los administradores a reducir los riesgos de seguridad. L0phtCrack ayuda a identificar y remediar las vulnerabilidades de seguridad que resultan del uso de contraseñas débiles o fáciles de adivinar y a recuperar las contraseñas de las cuentas de Windows y Unix para acceder a las cuentas de usuarios y administradores cuyas contraseñas se han perdido o para agilizar la migración de los usuarios a otro sistema de autenticación.

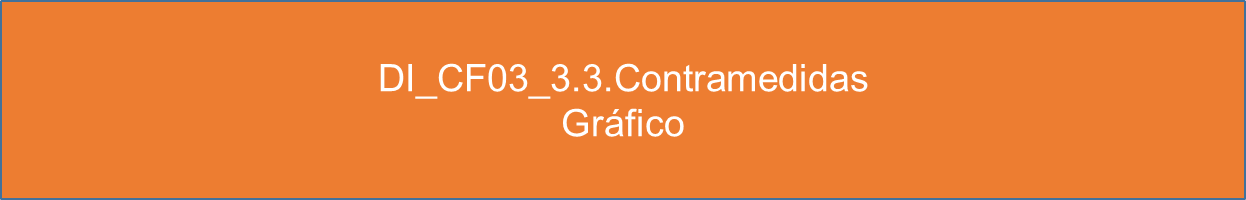


* 1. **Contramedidas**

Dentro de las contramedidas para poder defenderse del crackeo de contraseñas, se debe de tener en cuenta las siguientes consideraciones:

* Habilitar la auditoría de seguridad de información para monitorear y rastrear ataques a contraseñas.
* No usar la misma contraseña durante una actualización de contraseña.
* No compartir las contraseñas.
* No usar contraseñas que puedan ser usadas en un diccionario.
* No usar protocolos con un cifrado débil.
* Aplicar una política de cambio de contraseña cada 30 días.
* Evitar almacenar contraseñas en ubicaciones inseguras y no usar ningún sistema con contraseñas por defecto.

Las contramedidas en este caso, se refieren a:



1. **Ataques a redes cableadas**

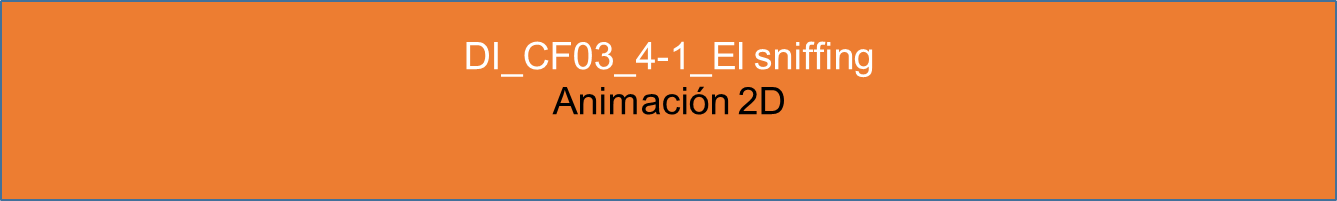
Al igual que los dispositivos e infraestructuras de los diferentes sistemas, la interconexión de redes es cada vez más versátil, el uso de canales digitales hace que piratas informáticos estén al acecho de realizar ataques. Existen diferentes técnicas que pueden servir para identificar las vulnerabilidades de las redes y poder tomar las medidas necesarias para protegerlas; apropiarse de estos conocimientos logrará que la infraestructura sea menos vulnerable y esté seguro de la información que por las redes circula.

* 1. **Conceptos y generalidades**

A continuación, se estudiarán algunos conceptos generales sobre el ataque a redes cableadas.

**El sniffing**

Este es un proceso de monitorizar y capturar todos los paquetes que pasan a través de una red dada usando herramientas de sniffing.





**¿Cómo utilizan los administradores de redes el software de sniffing?**

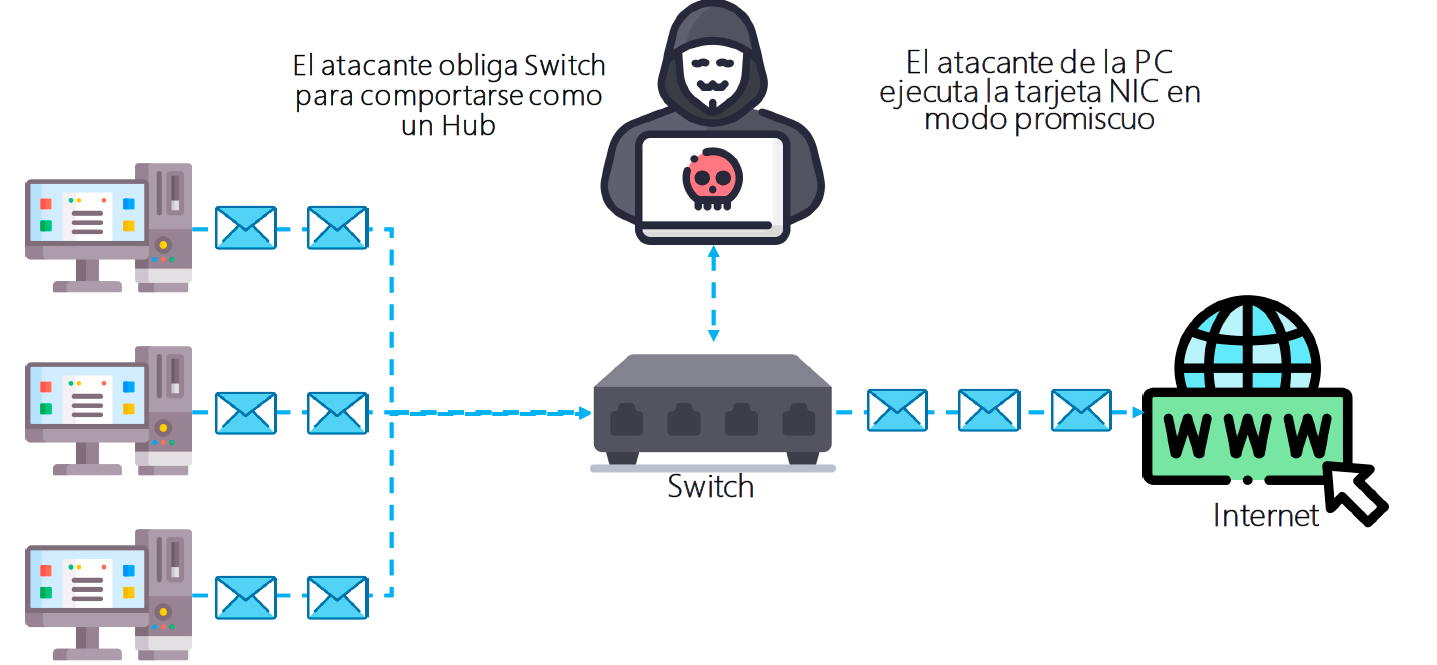
En primer lugar, es importante comprender cómo funciona generalmente el tráfico de Internet en una red, en la mayoría de los casos, la computadora solo investigará los paquetes que le han sido dirigidos específicamente. En la metáfora de los "coches que circulan por una carretera", podemos imaginarnos el ordenador como una casa en esa carretera, no inspeccionará todos los coches que pasan por su casa, pero si alguien aparca en su entrada, probablemente abriría la puerta para ver quién es, así es como su ordenador trata la mayoría de los paquetes de datos: ignora los que van por la red a otros destinos mientras inspecciona los paquetes que se le envían.

El software de "sniffing" ajusta la configuración de la red de un ordenador para que "huela" cada paquete - en lugar de solo los que se le envían - y los copia todos para su posterior investigación, en lugar de abrir la puerta sólo cuando alguien viene de visita, el sniffer se pega a la ventana, observando todos los coches mientras pasan.

El sniffer de la ventana puede monitorear obsesivamente cada auto, o puede elegir investigar sólo los camiones, o los autos rojos, o los autos con al menos tres ocupantes, o tal vez solo las motocicletas, en otras palabras, una persona que usa un sniffer en modo no filtrado puede recoger todo el tráfico de la red, o puede configurar el sniffer para filtrar paquetes que contengan un tipo específico de datos.

**Figura 5**

*Sniffing*



* 1. **Modelo de redes OSI**

OSI significa Interconexión de Sistemas Abiertos. Ha sido desarrollado por la ISO - 'Organización Internacional de Normalización', en el año 1984, es una arquitectura de 7 capas, cada una de las cuales tiene una funcionalidad específica que realizar y todas estas 7 capas trabajan en colaboración para transmitir los datos de una persona a otra en todo el mundo.

**Capa física (Capa 1)**

La capa más baja del modelo de referencia de OSI es la capa física, es responsable de la conexión física real entre los dispositivos, la capa física contiene información en forma de bits, es responsable de transmitir los bits individuales de un nodo al siguiente, al recibir los datos, esta capa obtendrá la señal recibida y la convertirá en 0 y 1 y la enviará a la capa de enlace de datos, que volverá a unir el marco.

**Capa enlace de datos (Capa 2)**

La capa de enlace de datos es donde operan los interruptores y proporciona un enlace fiable entre dos nodos directamente conectados, la capa de enlace de datos también es responsable de detectar y posiblemente arreglar cualquier error de paquetes que se pueda formar en la capa física.

La capa de enlace de datos se divide en dos capas separadas, las capas de Control de Acceso a los Medios (MAC) y Control de Enlace Lógico (LLC), la capa MAC es responsable de controlar cómo los dispositivos conectados a la red obtienen acceso, la capa LLC controla la comprobación de errores, las posibles correcciones y la sincronización de paquetes.

**Capa red (Capa 3)**

La capa de red sirve para la transmisión de datos de un host a otro ubicado en diferentes redes. También se encarga del enrutamiento de los paquetes, es decir, de la selección del camino más corto para transmitir el paquete, a partir del número de rutas disponibles. La capa de red coloca en el encabezamiento la dirección IP del emisor y del receptor.

**Capa transporte (Capa 4)**

La capa de transporte proporciona servicios a la capa de aplicación y toma servicios de la capa de red. Los datos de la capa de transporte se denominan segmentos. Es responsable de la entrega de extremo a extremo del mensaje completo. La capa de transporte también proporciona el reconocimiento de la transmisión de datos exitosa y retransmite los datos si se encuentra un error.

**Capa Sesión (Capa 5)**

La capa de sesión se encarga de crear y mantener sesiones entre el sistema operativo de la capa de presentación y otras máquinas de terceros, Por ejemplo, cuando un usuario navega por Internet, está interactuando con la capa de aplicación, la capa de aplicación está interactuando con la capa de presentación y la capa de sesión permite que el sistema operativo interactúe con el servidor web.

**Capa Presentación (Capa 6)**

La capa de presentación es donde se encuentra el sistema operativo, este sistema operativo podría ser Windows, OS X, un sistema operativo basado en Unix o uno de los muchos otros disponibles donde el usuario humano interactúa con la capa de aplicación descrita anteriormente, la capa de aplicación interactúa con la capa de presentación, esto puede hacerse directamente, o a través de un entorno de ejecución como el Java Runtime Environment (JRE). Su función principal es homogeneizar los formatos de representación de los datos entre equipos de la red Para homogeneizar la representación de datos (textos, sonidos, imágenes, valores numéricos, instrucciones), la Capa de presentación interpreta las estructuras de las informaciones intercambiadas por los procesos de la aplicación y las transforma convenientemente.

**Capa de aplicación (Capa 7)**

En la parte superior de la pila de capas del Modelo de Referencia OSI, encuentras la capa de Aplicación que es implementada por las aplicaciones de la red, estas aplicaciones producen los datos, que deben ser transferidos a través de la red, esta capa también sirve como ventana para que los servicios de aplicación accedan a la red y para mostrar la información recibida al usuario, la capa de aplicaciones también se llama capa de escritorio. Ejemplo: Aplicación - Navegadores, Skype Messenger, etc.



* 1. **Herramientas de ataque**

Hay tantas herramientas disponibles para realizar el sniffing en una red, y todas tienen sus propias características para ayudar a un hacker a analizar el tráfico y diseccionar la información, las herramientas de sniffing son aplicaciones extremadamente comunes. A continuación se presentan algunas de las más interesantes.

**Bettercap:** hay mucho material en línea, especialmente del sitio web oficial de Bettercap, que documenta cómo se utiliza la herramienta y algunas de las mejoras que se han hecho a lo largo de los años. Se puede clonar el repositorio de bettercap en github.com para utilizar la versión de desarrollo.

**Figura 6**

*Bettercap*



**Wireshark:** es un analizador de protocolo de red, o una aplicación que captura paquetes de una conexión de red, como por ejemplo de su ordenador a su oficina en casa o a Internet, paquete es el nombre que se da a una unidad discreta de datos en una red Ethernet típica.

Wireshark es el rastreador de paquetes más utilizado en el mundo. Como cualquier otro rastreador de paquetes, Wireshark hace tres cosas:

* Captura de paquetes: Wireshark escucha una conexión de red en tiempo real y luego capta flujos enteros de tráfico, muy posiblemente decenas de miles de paquetes a la vez.
* Filtrando: Wireshark es capaz de cortar y trocear todos estos datos aleatorios en vivo usando filtros. Aplicando un filtro, puedes obtener solo la información que necesitas ver.
* Visualización: Wireshark, como cualquier buen olfateador de paquetes, te permite sumergirte justo en el centro de un paquete de red. También te permite visualizar conversaciones enteras y flujos de red.



* 1. **Contramedidas**

A veces usted se centra más en el lado inalámbrico de la red cuando se trata de la seguridad porque el WiFi no tiene barreras físicas. Después de todo, un War driver detectar su SSID y lanzar un ataque mientras está sentado en el estacionamiento, pero en un mundo de amenazas internas, ataques dirigidos desde el exterior, así como hackers que utilizan la ingeniería social para obtener acceso físico a las redes corporativas, la seguridad de la parte cableada de la red también debería ser lo más importante, por lo tanto, presentamos algunas precauciones de seguridad básicas que puede tomar para la parte conectada de la red, tanto si es una pequeña empresa como una gran empresa.

**Ejecutar auditorías y mapear la red**

Tenga siempre una comprensión clara de toda la infraestructura de la red, por ejemplo, el proveedor/modelo, la ubicación y la configuración básica de los cortafuegos, los enrutadores, los conmutadores, el cableado y los puertos Ethernet y los puntos de acceso inalámbricos, además, sepa exactamente qué servidores, computadoras, impresoras y cualquier otro dispositivo están conectados, dónde están conectados y su ruta de conectividad a través de la red.

Durante la auditoría y el mapeo, es posible que encuentre vulnerabilidades de seguridad específicas o formas de aumentar la seguridad, el rendimiento y la fiabilidad Tal vez se encuentre con un firewall mal configurado o tal vez con amenazas físicas a la seguridad, si está trabajando con una red pequeña con solo unos pocos componentes de red y una docena o menos de estaciones de trabajo, podría realizar la auditoría manualmente y crear un mapa visual en una hoja de papel Para redes más grandes, los programas de auditoría y mapeo pueden ser útiles, pueden escanear la red y comenzar a producir un mapa o diagrama de la red

**Mantener actualizada la red**

* Una vez que tenga una auditoría básica de la red y el mapeo completo, considere la posibilidad de profundizar en el tema, compruebe si hay actualizaciones de firmware o software en todos los componentes de la infraestructura de la red.
* Inicie sesión en los componentes para asegurarse de que se han cambiado las contraseñas predeterminadas, revise los ajustes para cualquier configuración insegura y busque cualquier otra característica o funcionalidad de seguridad que no esté utilizando actualmente.
* A continuación, eche un vistazo a todos los ordenadores y dispositivos conectados a la red Asegúrese de que se han cuidado los aspectos básicos, como las actualizaciones del sistema operativo y de los controladores, que el cortafuegos personal está activo, que el antivirus se ejecuta y actualiza y que se establecen las contraseñas.

**Asegurar físicamente la red**

Aunque a menudo se pasa por alto o se minimiza, la seguridad física de la red puede ser tan crucial como, por ejemplo, el firewall de cara a Internet, así como necesita protegerse contra los delincuentes, los *bots* y los virus, también necesita protegerse contra las amenazas locales Sin una fuerte seguridad física de su edificio y su red, un pirata informático cercano o incluso un empleado podría aprovecharse de ello.



Asegúrese de tener un buen plan de seguridad para el edificio, para intentar evitar que entren personas ajenas, luego asegúrese que todos los armarios de cableado y/u otros lugares donde se colocan los componentes de la infraestructura de la red estén físicamente protegidos tanto del público como de los empleados, utilice cerraduras de puertas y gabinetes y verifique que el cableado Ethernet esté fuera de la vista y no sea fácilmente accesible lo mismo con los puntos de acceso inalámbrico. Desconecte los puertos Ethernet no utilizados, físicamente o mediante la configuración de un conmutador/enrutador, especialmente los que se encuentran en las zonas públicas del edificio.

**Considere el filtrado de direcciones MAC**

Un importante problema de seguridad del lado cableado de la red es la falta de un método de autenticación y/o cifrado rápido y fácil la gente puede simplemente conectarse y utilizar la red En el lado inalámbrico tienes al menos WPA 2 Personal (PSK) que es fácil de desplegar.



Aunque el filtrado de direcciones MAC puede ser evitado por un pirata informático determinado, puede servir como la primera capa de seguridad, no detendrá completamente a un pirata informático, pero puede ayudarle a evitar que un empleado, por ejemplo, cause un agujero de seguridad potencialmente grave, como permitir que un huésped se conecte a la red privada También puede darle más control sobre qué dispositivos están en la red, pero no permita que le dé una falsa sensación de seguridad, y esté preparado para mantener actualizada la lista de direcciones MAC aprobadas

**Usar VPNs para cifrar ciertos PCs o servidores**

* Si realmente busca asegurar el tráfico de la red, considere el uso de la encriptación, recuerde que incluso con las VLAN y la autenticación 802 1 X, alguien puede escuchar a escondidas la red (para capturar el tráfico sin cifrar que podría incluir contraseñas, correos electrónicos y documentos.
* Aunque pueda encriptar todo el tráfico, primero analice su red, podría tener más sentido solo encriptar algunas comunicaciones que considere más sensibles que no estén ya encriptadas, como por ejemplo a través de SSL/HTTPS Puedes pasar el tráfico sensible a través de una VPN estándar en el cliente, que podría ser usada solo durante la comunicación sensible o forzada a ser usada todo el tiempo.



**Cifrar toda la red**

También puede cifrar una red entera, una opción es IPsec Un servidor Windows puede servir como servidor IPsec y la capacidad del cliente es soportada nativamente por Windows también, sin embargo, el proceso de encriptación puede ser una carga bastante pesada para la red las tasas de rendimiento efectivas pueden caer dramáticamente.

También existen soluciones de encriptación de red patentadas de los proveedores de redes, muchos de los cuales utilizan un enfoque de Capa 2 en lugar de la Capa 3 como el IPsec para ayudar a reducir la latencia y los gastos generales.

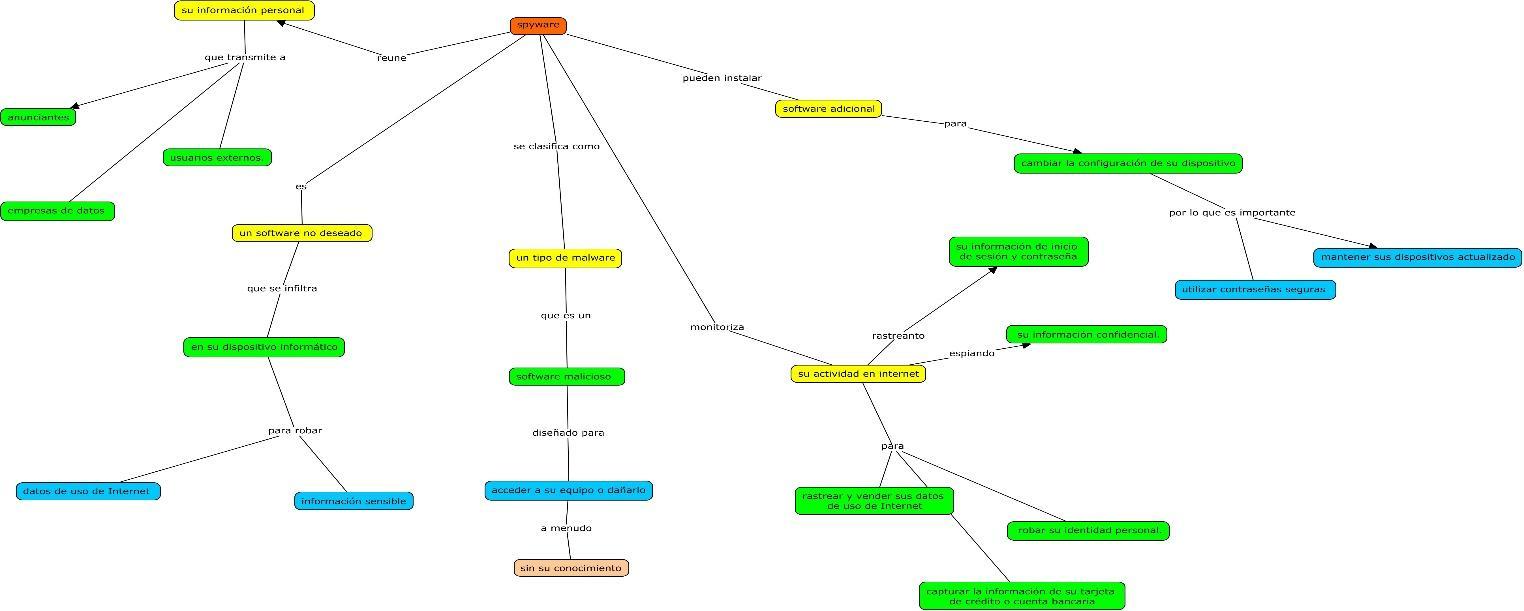


1. **Ataques con virus y malware**

Los ataques con virus y *malware*, más allá de convertirse en un serio problema, muchas veces son estrategias de los ciberdelincuentes para generar secuestro o pérdida de información, son de los más comunes que se observa en el mundo digital, estos se disfrazan de archivos que el sistema los cree nativos de sus sistema operativo y no son detectados, es así que debe de saber cómo operan y cuál es su cadena operativa para poder evitar que incurran en robo o pérdida de información importante para una organización.

* 1. **Conceptos y generalidades**

Dentro de los conceptos que se deben abordar con respecto a Ataques con Virus y malware, es el spyware, conozca acerca del mismo en el siguiente mapa:





* 1. **Tipos de virus y malware**

El software espía es una de las amenazas más comunes en Internet. Puede infectar fácilmente su dispositivo y puede ser difícil de identificar. El spyware es una amenaza para las empresas y los usuarios individuales, ya que puede robar información confidencial y dañar su red.

Existen cuatro tipos principales de spyware y cada uno utiliza tácticas únicas para rastrearlo.



El *spyware* puede afectar a PC, Mac y dispositivos iOS o Android. aunque los sistemas operativos de *Windows* pueden ser más susceptibles de ser atacados, los atacantes también están mejorando para infiltrarse en los sistemas operativos de *Apple*, algunas de las formas más comunes en que su computadora puede infectarse con *spyware,* son las siguientes:

* Aceptar un aviso o una ventana emergente sin leerlo primero.
* Descargar software de una fuente no fiable.
* Abrir los archivos adjuntos de los correos electrónicos de remitentes desconocidos.
* Piratear medios como películas, música o juegos.

Propagación de Spyware



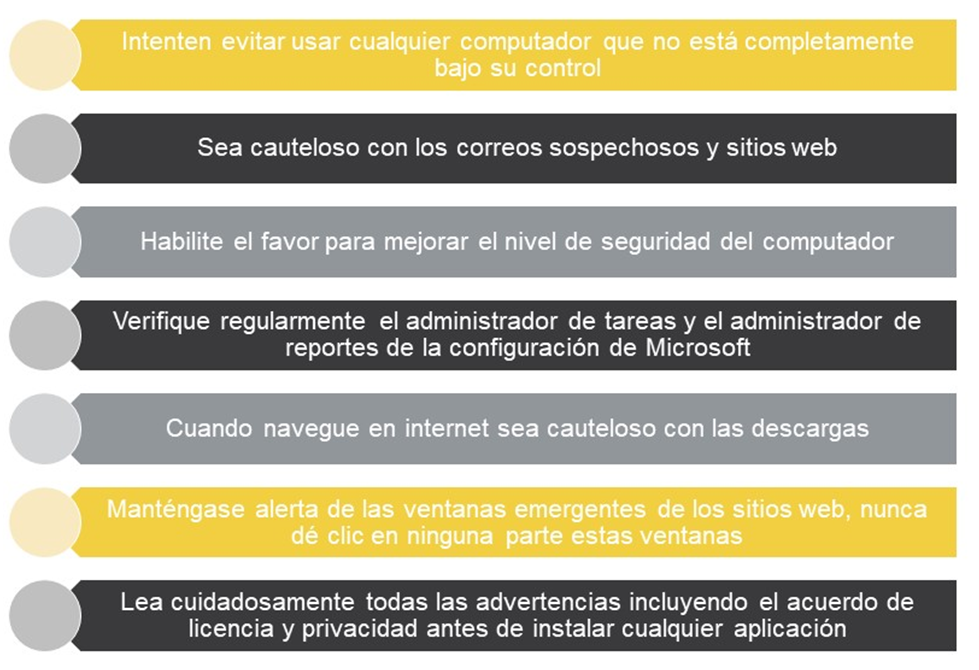


* 1. **Protección con antivirus y evasiones**

Si cree que su dispositivo está infectado con spyware, realice un análisis con su software de seguridad actual para asegurarse de que ha limpiado todo lo que puede. A continuación, descargue y ejecute una herramienta de eliminación de virus, como el Norton Power Eraser gratuito.

También existen otras herramientas de eliminación de software espía de buena reputación. Algunas de ellas sólo funcionan cuando se inicia manualmente el análisis. Otras supervisan continuamente el equipo para asegurarse de que el spyware no pueda modificar o supervisar su información

A continuación, revise cómo defenderse de un *Spyware*.

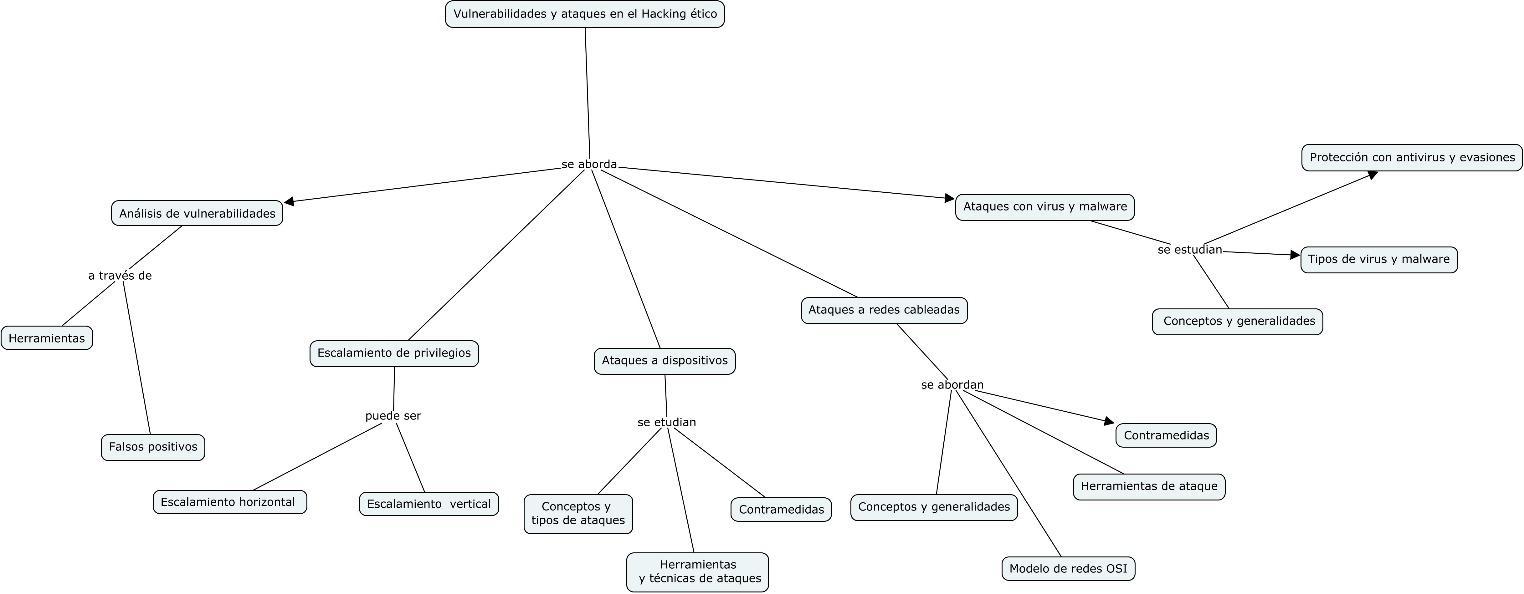
****

Estos son los cuatro pasos principales para ayudar a prevenir el *spyware*.

* No abra los correos electrónicos de remitentes desconocidos.
* No descargue archivos de fuentes no fiables.
* No haga clic en anuncios emergentes.
* Utilice un *software* antivirus de confianza.



**C. SÍNTESIS**

****

**D. ACTIVIDADES DIDÁCTICAS**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la actividad | Emparejamiento entre término y definición |
| Objetivo de la actividad | Afianzar algunos de los conceptos más importantes de las vulnerabilidades de un sistema, que debemos de tener en cuenta al hacer uso de herramientas de hacking ético y prevención de ataques . |
| Tipo de actividad sugerida | Arrastrar y soltar el término con la definición que corresponde |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexo \_Actividad didáctica 1 |

**E. MATERIAL COMPLEMENTARIO**

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del recurso o  archivo del documento o material |
| --- | --- | --- | --- |
| Herramientas | UNIR. (2018). *Las mejores herramientas de ciberseguridad* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=tG1OarXj4DU> | Videoconferencia | <https://www.youtube.com/watch?v=tG1OarXj4DU> |
| Tipos de virus y malware | Departamento UAEM. (2021). *Tipos de ataques informáticos* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=-b7NZRM3x_Q> | Video | <https://www.youtube.com/watch?v=-b7NZRM3x_Q> |

**F. GLOSARIO**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Cifrado | Esconder información, la cual se utiliza con el fin de proteger la estructura de los datos e información de una empresa o persona |
| Footprinting | Proceso de creación de un plano o mapa de la red y los sistemas de una organización |
| Nmap | Es una herramienta informática opensource (programa de código abierto) que se utiliza para escanear puertos de un sistema |
| OSINT | (Open Source INTelligence), que significa inteligencia de código abierto, que se refiere a cualquier información que pueda ser legalmente obtenida de fuentes públicas y gratuitas |
| Pentesting | Son pruebas de penetración, que consiste en atacar un sistema para encontrar vulnerabilidades y poder contrarrestarlas, las hay de caja blanca, negra y gris |
| Proxy | Programa que hace de intermediario entre los servicios y recursos de la red, trabaja bajo peticiones |

**G. REFERENCIAS BIBLIOGRÁFICAS:**

Borges, E. (12 de febrero de 2019). Servidor FTP., <https://blog.infranetworking.com/servidor-ftp/>.

Borges, S. (04 de enero de 2019). Servidor web, <https://blog.infranetworking.com/servidor-web/>.

Caballero Quezada, Alonso Eduardo. (17 de noviembre de 2015). Introducción a OSSTMM (Open Source Security Testing Methodology Manual)., <http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual>.

Castillo, J. A. (15 de diciembre de 2018). Active Directory que es y para que sirve. Obtenido de <https://www.profesionalreview.com/2018/12/15/active-directory/>.

Echeverry Parada, J. S. (mayo de 2009). Metodologia para el diagnóstico continuo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada. <https://pdfs.semanticscholar.org/60c7/dbe2abab31a25422c92ead74085fd7093715.pdf>.

Gaviria Valencia, R. A. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM V2.1 y la guía OWASP V3.0. [http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GUÍA%20PRÁCTICA%20PARA%20PRUEBAS.pdf?sequence=1](http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1).

INCIBE. (20 de marzo de 2017). Amenaza vs vulnerabilidad, ¿sabes en qué se diferencia? Obtenido de <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>.

Martinez Ferrel, E. (2018). Las diferentes amenazas de seguridad informática, <https://sites.google.com/site/lasamenazaslainformatica/>.

Zuluaga Mateus, A. D. (Noviembre de 2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia, <https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf>

**H. CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Pedro Javier Lozada Villota | Experto temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Diciembre de 2021 |
| Alix Cecilia Chinchilla Rueda | Diseñadora instruccional | Regional Distrito Capital – Centro de Gestión Industrial | Diciembre de 2021 |
| Ana Catalina Córdoba Sus | Revisora metodológica y pedagógica | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica. | Diciembre 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor pedagógico | Regional Santander - Centro Industrial del Diseño y la Manufactura. | Diciembre 2021 |
| Sandra Patricia Hoyos Sepúlveda | Revisión y corrección de estilo | Centro para la Industria de la Comunicación Gráfica - Distrito capital | diciembre 2021 |

**J. CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | Nombre | Cargo | Dependencia | Fecha | Razón del cambio |
| --- | --- | --- | --- | --- | --- |
| Autor (es) |  |  |  |  |  |