TEMA

Tema 6. Software Antimalware

Administración de sistemas informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Linkia FP

Tema 6: Software Antimalware

¿Qué aprenderás?

- Identificar la gran variedad de ataques informáticos que podemos sufrir
- Reconocer qué medidas preventivas y correctivas podemos tomar
- Identificar qué es un Malware
- Identificar qué es la Ingeniería Social

¿Sabías que…?

- El Malware que roba contraseñas ha afectado en 2019 a 940.000 usuarios

5.1. Introducción

Antes de entrar en temática vamos a realizar una revisión de todas las amenazas que podemos tener en un sistema informático y de qué tipo pueden ser. De esta manera nos será más fácil conocer las medidas a tomar.

Las **amenazas de seguridad** se pueden clasificar en:

- Interrupción (Ataque a la Disponibilidad). El elemento atacado es destruido o deja de estar disponible. Por ejemplo, el borrado de información
- Interceptación (Ataque a la Confidencialidad). Un extraño al sistema consigue el acceso a un recurso. Por ejemplo, escuchar los datos de una comunicación
- Modificación (Ataque a la Integridad). Un extraño al sistema modifica un recurso de este. Por ejemplo, modificar el contenido de un mensaje
- Fabricación. Un extraño al sistema inserta objetos. En este caso estamos hablando de correo basura, por ejemplo

De la misma manera, podemos clasificar los ataques en:

- **Pasivos**: Ataques en los que el objetivo no es modificar la comunicación, sino que solo se monitoriza para obtener información. Esto se realiza:
  - Obteniendo el origen y destino de la comunicación mediante la lectura de las cabeceras de los paquetes monitorizados
  - Controlando el volumen de tráfico entre las entidades que monitorizamos
  - Controlando las horas habituales de actividad entre las entidades que monitorizamos

  Lo mejor que podemos hacer para evitar este tipo de ataques es Cifrar la información.

- **Activos**: Ataques que implican la modificación en el flujo de datos transmitidos o la inserción de información falsa en el flujo de datos. Esto se puede realizar:
  - Suplantando la identidad. Robando la contraseña de acceso, por ejemplo.
  - Reactuación. Se capturan varios mensajes válidos y se utilizan con fines malintencionados. Por ejemplo, el mensaje de ingreso de dinero en una cuenta bancaria se envía varias veces
  - Modificación. Se captura un mensaje y se modifica parte de este. Por ejemplo, cambiar la cantidad de dinero a ingresar en una cuenta determinada
  - Degradación. Interrumpir el funcionamiento normal del sistema. Por ejemplo, inundar el sistema de correo basura, ataque de denegación de servicio…

En la siguiente tabla realizamos un resumen a los ataques más comunes que podemos sufrir en nuestro sistema informático:

Nombre ataque	Descripción sencilla	Medidas a tomar
Ataque de Denegación de Servicio DoS	Bloquear servicios para que los usuarios no los puedan usar	Eliminar paquetes con direcciones falsas, limitar recursos del servicio
Ataque Fuerza Bruta o Diccionario	Obtención contraseña mediante prueba y error o mediante el uso de listados	Información cifrada y Firma digital
Bugs de Software	Vulnerabilidades de los programas	Actualizar software y testearlo periódicamente
Crack	Software que permite romper la protección de una aplicación comercial	Comprar software legal
Fuzzer	Ataque con datos aleatorios para detectar en un servidor fallos	Actualizar software, cortafuegos, infraestructura
Hijacking	Robar conexión a un usuario autenticado en el sistema	Encriptar protocolo, filtrar paquetes
Inyección SQL	Modificar consultas SQL de un servidor para entrar en él o ejecutar SQL	Configuración de servidor con medidas preventivas, mejorar el software para no permitir la inserción de ese código
Ingeniería Social	Convencer a un usuario para que desvele su información	Autenticación, información al usuario, políticas de contraseña
Keylogger	Software o hardware que registra las pulsaciones de teclado que se realizan	Revisar procesos, antivirus, cortafuegos
LFI, RFI	Ejecutar un script que está alojado en el servidor (LFI) o en un host remoto (RFI)	Configuración de servidor, mejorar el software para no permitir la ejecución
MiTM (Man in The Middle)	Situarse en medio de una comunicación para hacer más ataques	Cifrar protocolo, configurar dispositivos de red correctamente
Navegación anónima (TOR, Deep Web, DarkNet)	No es ataque, pero se usa para camuflar IP del atacante pasando por varios proxys.	
Phising, Stealer	Engañar al usuario mediante mensajes y sitios web fraudulentos para robo de datos	Información al usuario y evitar la autenticación en esos sitios

RansomWare	Crear amenaza al ordenador para intentar sacar dinero al dueño	Actualizar software, antivirus, cortafuego, abrir mensajes o webs conocidos
Reenvío de paquetes	Retransmitir paquetes para engañar o duplicar un mensaje (transferencia)	Rechazar paquetes duplicados, usar marcas de tiempo, nº de secuencia
Rootkit	Software que se instala en un sistema y oculta toda la actividad de un atacante	Revisar procesos del sistema para detectarlo, instalar antirootkit, cortafuegos.
Rubber-hosse	Usar soborno o tortura para obtener información	Defensa personal o jurídica
Sniffing (hub, switch)	Escuchar los datos que circulan por la red	Cifrar datos, usar contraseñas no reutilizables
Spoofing (IP, ARP, DNS)	Los paquetes de red se envían a una dirección falsa	Cifrar protocolo, configurar dispositivos de red correctamente
Troyano y/o Backdoor	Software que se instala camuflado en otro software para normalmente acceder a los recursos del equipo	Firma digital, verificar software, filtrar paquetes
Virus, gusanos, páginas JavaScript	Ataques dirigidos a sistemas en concreto	Antivirus, Firma Digital, Información cifrada
VLAN Hopping	Tener acceso al tráfico de red de otra VLAN inaccesible	Configurar dispositivos de red correctamente
XSS	Engañar al servidor web para que ejecute un script en el navegador del cliente	Configuración de servidor, mejorar el software para no permitir la ejecución

5.2. Software Malicioso

Definiremos Software malicioso (Malware) como todo programa diseñado para entrar en un sistema informático sin permiso.

¿Por qué alguien va a querer entrar en mi sistema informático?

Imagen. Malware

Vamos a hablar de dos posibles motivaciones:

5.2.1. Reconocimiento.

Aquí podríamos hablar largo y tendido sobre la diferencia entre “hackers” y “crackers”.

Un **Hacker** es una persona que por sus avanzados conocimientos en el área de la informática tiene la capacidad elevada en el tema y es capaz de realizar actividades que otros usuarios no puede realizar. Esencialmente son informáticos con muchas ganas de aprender y aplicar sus conocimientos, por eso necesitan retos para ponerse a prueba.

Dentro de los Hackers podemos definir los **White Hat** Hackers como los responsables de la seguridad de los sistemas informáticos. También tenemos los **Gray Hat** Hackers. A estos les encanta traspasar los niveles de seguridad que están implantados y luego ofrecer sus servicios para corregir dichos errores. Para terminar esta distribución tenemos a los **Black Hat** Hackers, que vulneran la seguridad de los sistemas para extraer información restringida con un fin económico. Son los creadores de virus, spyware y malwares.

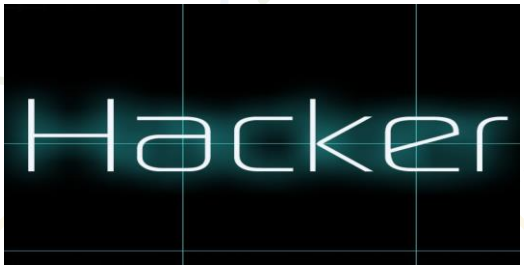


Imagen. Hacker

Y si hay “hackers”, tenemos la cara opuesta de la moneda, los “**crackers**”. Estos los definiremos como miembros de Black Hat pero que además modifican el software original generando KeyGen y distribución de software de pago.

En los últimos años, con la irrupción de la telefonica móvil, han aparecido los Phreaker, que se encargan de inspeccionar, monitorear, modificar comunicaciones.

Imagen. Crackers

Y, para acabar, el que todos conocemos, el que dice que es “hacker” y solo ha leído dos tutoriales. ¿A qué todos conocéis uno? Si, si… el **Newbie**, el Novato. Ha visto dos tutoriales de cómo se hace algo, visita sitios hacking, se viste con camisetas negras y … ya es un Hacker.

Pues toda esta gente, lo que busca es darse a conocer inicialmente, lo que después muchos se pasan al lado oscuro.

Os adjunto un listado de personajes conocidos:

- Black Hat Hackers
  - Jonathan James
  - Adrian Lamo
  - Kevin Mitnick
  - Kevin Poulsen
  - Robert Tappan Morris

- White Hat Hackers
  - Stephen Wozniak
  - Tim Berners-Lee
  - Linus Torvals
  - Richard Stalman
  - Tsutomu Shimomura

Imagen. Kevin Mitnick

Imagen. Steve Woozniak

Imagen. Richard Stallman

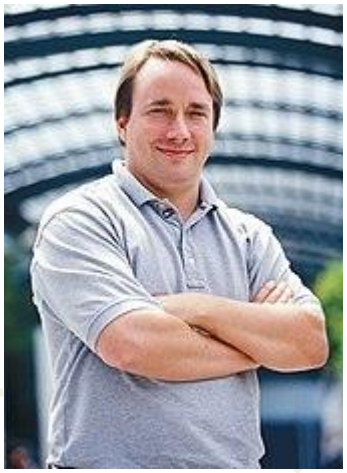


Imagen. Linus Torvalds

5.2.2. Interés económico

¿Cómo van a ganar dinero? Robando información sensible de usuarios y vendiéndola al mejor postor. Estamos hablando de listas de datos personales de usuarios, cuentas de servidores web, claves bancarias… El motivo como podéis deducir es claramente económico.

Veamos las técnicas que se utilizan:

- **Infectar ordenadores.**

Aquí vamos a tratar varios conceptos que tienen relación con esta técnica.

5.2.2.1. Spam

Término que agrupa a todos los correos electrónicos que recibimos cada dia y que no son solicitados. Estos correos se caracterizan porque no solo los recibimos nosotros, sino un gran número de personas.

El emisor suele comprar o generar una lista de direcciones e-mail a las cuales lo envía. Como la legislación no permite enviar una comunicación comercial sin permiso del usuario, el origen de los mensajes suele estar falsificado.

A continuación, vamos a detallar varios conceptos de este mundo:

- Llamamos **Spam User** a la persona que realiza el spam a un listado de destinatarios desconocidos.
- A la persona que vende ese listado sin la autorización de los componentes de ese listado, lo llamaremos **E-mail Dealer**.
- Al que vende sus servicios de spam usando sus propias listas, le denominamos Spam Dealer.
- Por otra parte, se define **Harvesting** a la obtención automática de direcciones de e-mail de los sitios de internet a través de programas denominados "**e-mail collectors**".
- También denominaremos como **Bulk Mailer** a los programas que realizan el envió automático de un gran número de menajes y que permiten el uso de servidores abiertos.

Imagen. Spam

A continuación, detallaré algunos de los ataques más comunes que se realiza usando el spam:

- **E-mail Spoofing**. Enmascarar los datos reales del remitente colocando un nombre y dirección falsa en el remitente. Si lo marcamos como Spam ya no recibimos mails de él.
- **Revenge Spam**: Es un ataque para denigrar la imagen del titular de la dirección electrónica.
- **Joe-Job**: El objetivo es que le lleguen al remitente del mensaje todos los mensajes devueltos por direcciones erróneas.

Podemos clasificar los tipos de Spam como:

- Rumores o bulos (**hoax**)
- Cadenas (**chain** letters): mensajes del tipo "si se lo envías a 10 más, la felicidad llegará a tu vida"
- **Propaganda**. Te ofrecen una oferta por un producto y un enlace que al pulsarlo te llevará a una web donde se te puede descargar de todo
- Estafas (**Scam**). Ofertas laborales falsas, prestamos financieros fantásticos…
- Timos (**Phising**): Está relacionado con la Ingeniería Social. Este es el que más está evolucionando con el tiempo.
    - Un Spammer crea un e-mail que tus datos a tu "banco" han cambiado
    - Te pide que pulses en un enlace para actualizarlo
    - En una página nueva, te aparece un formulario para que introducir tus datos como comprobación
    - Una vez acabas, vuelves a la página de tu banco.

5.2.2.2. Redes Zombies Botnets

Con estas redes, un criminal puede tomar el control de miles de ordenadores de forma remota sin que los usuarios tengan conocimiento de ello.

Nuestro ordenador puede ser utilizando para el robo de datos a otros usuarios, envío de spam o ataques a otros ordenadores. Activan nuestra webcam y graban nuestra intimidad.

Si estamos dentro de una red zombie, cualquier dato que utilicemos en nuestro sistema puede ser robado.

Todos los datos obtenidos se venden en foros de internet y los ciberdelincuentes pagan por ellos, por ejemplo, listados de tarjetas de crédito.

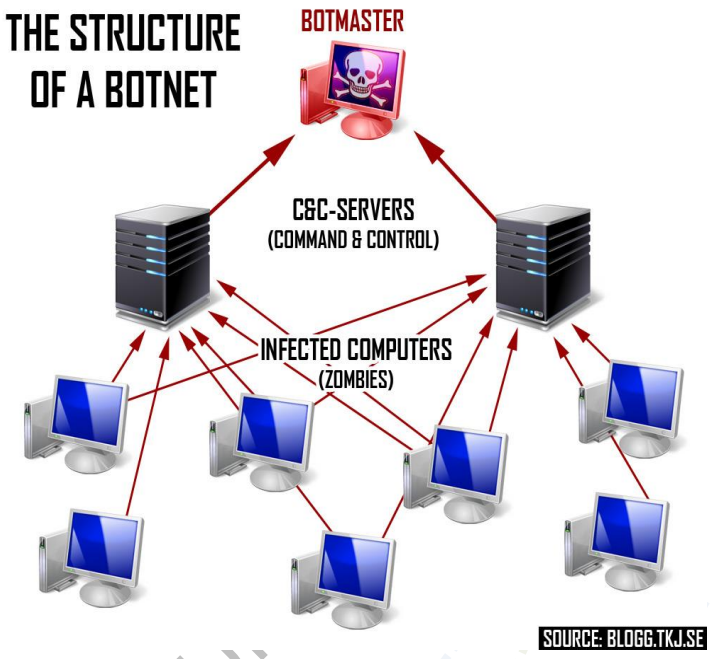


Imagen. La estructura de BOTNET

¿Pero cómo funcionan estas Botnet?

1. El creador de la botnet (botmaster) diseña la red que quiere crear: objetivos, medios y el sistema de control
2. Necesita de un malware que se aloje en los equipos. Lo denominaremos bot. Este bot se puede comprar a un hacker dedicado a programarlos
3. El bot es distribuido por cualquier medio: spam, webs con vulnerabilidades, ingeniería social…
4. El virus se descarga en el sistema y lo conecta a la red de ordenadores zombie
5. En poco tiempo, el botmaster tiene cientos de ordenadores infectados.

¿Qué podemos hacer?

- Una buena solución antivirus
- Tener instalado CONAN Mobile, una aplicación gratuita que nos ayuda a proteger el móvil
- Tener instalado el servicio AntiBotnet del Incibe. Es un servicio que te informa si tu conexión de internet se ha encontrado involucrada dentro de una red zombie.

5.2.2.3. Ataque denegación de servicio (DoS)

Este **Ataque DoS (Denial of Service)** consiste en provocar que un servicio o recurso sea inaccesible a los usuarios de este, mediante la pérdida de la conectividad con la red por el elevado consumo de ancho de banda o la sobrecarga de los recursos del sistema atacado.

Un ejemplo sencillo sería un cracker que es contratado por una empresa para que la web de la competencia deje de funcionar durante un día. Para ello desde su equipo informático realiza una cantidad masiva de peticiones. Como los servidores web poseen una capacidad de limitada de resolución de peticiones simultáneamente, se va ralentizando hasta bloquearse o desconectarse de la red.

Una versión mejorada de esto es el **DDoS (Distributed Denial of Service**), una aplicación de las botnets. En la misma situación anterior, el botmaster realiza las mismas peticiones, pero ahora desde todos sus ordenadores zombies de la botnet. Lógicamente, el número es superior y la capacidad de bloqueo mucho más rápida.

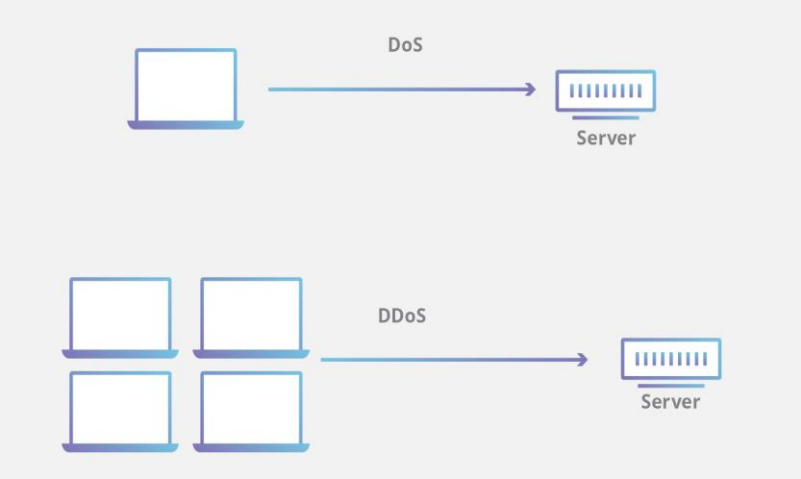


Imagen. Ataque denegación de servicio (DoS)

¿Cómo nos podemos proteger?

Como usuarios, nuestros ISP (Internet Solution Provider) debe estar actualizado y preparado para contrarrestarlos.

Como empresa, debemos configurar correctamente nuestros routers y firewalls con:

- Lista de IP Bloqueadas: Listas negras con IP críticas y el descarte de paquetes
- Filtros: Definir límites en la cantidad de datos procesados
- Balanceo de Carga: Extender el servicio entre varias máquinas para que el ataque nunca nos bloquee y nos dé tiempo a tomar medidas

5.2.2.4. Vender falsas soluciones de seguridad (RogueWare)

Estamos ante una de las formas más comunes en Internet para distribuir virus y malware.

Un **RogueWare** es una aplicación que intenta asemejarse a otra, ya sea por su nombre o apariencia, con la única finalidad de engañar y timar al usuario.

La forma más actualizada es la de ofrecer la descarga gratuita de programas antivirus, antispam, adware, que al ser instalados realizan un análisis del sistema y cuyo resultado es que tenemos el sistema infectado. Para desinfectar el sistema tenemos que comprar la versión completa.

Una vez instalada la versión completa, el equipo se infecta con el software malicioso. Esto no implica que la máquina vaya peor, o que nos aparezca más publicidad. Hay casos en los que realmente "limpia" el equipo de "competidores" para tener todos los recursos de la máquina a su disposición.

Imagen. Pantalla ejemplo RogueWare

Un ejemplo de RogueWare lo encontramos en el E-SET Antivirus 2011, un falso antivirus que se confundía con la popular y galardonada solución de seguridad ESET NOD32 Antivirus.

5.2.2.5. Cifrar el disco duro para pedir un rescate (RansomWare)

Seguro que conocemos gente que ha sufrido este ataque. Este ataque es una variante de Phishing, un engaño, pero que en lugar de robarnos información personal el atacante nos cifra la información de nuestros equipos y de los equipos que tengamos conectados.

Al rato de haberse producido el cifrado de la información, nos aparecerá una amable pantalla en la que nos exigirán un rescate para desencriptarnos la información: JAMAS HAY QUE PAGAR. Si lo hacemos, nos lo volverán a hacer y nadie nos asegura que lo descifren. Hay que denunciar el hecho ya que es un delito.

Imagen. Cifrado

La mejor medida de seguridad para evitar estos ataques es la prevención:

- No abrir correos que no conocemos su remitente
- No abrir adjuntos y no pulsar en enlaces
- Disponer de copias de seguridad periódicas para restaurar la información después de eliminar el malware

¿Qué haremos cuando nos ocurra?

Es complicado recuperar la información. Las empresas de antivirus generan dia a dia soluciones y parches para ello. También tenemos el proyecto **No More Ransom**, del Incibe, que recomienda el uso de la herramienta Crypto-Sheriff. Esta herramienta nos ayuda a saber qué variante de RansomWare nos está afectando y nos indica qué podemos hacer.

Siempre podemos ir a una empresa especialista donde con técnica de ingeniería inversa, intentaran recuperar la información.

Pero sobretodo, tener las copias de seguridad de la información al día.

A parte de todo el software malicioso que hemos comentado nos podemos encontrar también con:

5.2.2.6. Virus

Un **Virus** es un programa informático que se autoejecuta en el sistema informático en el que se encuentra y se propaga realizando copias de sí mismo en otros archivos de este (infección). Si copiamos o movemos ese archivo a otro equipo, nos estamos llevando el virus por lo que la infección se extiende.

Hay que destacar que el efecto del virus no tiene porqué ser inmediato, ya que a veces nos encontramos con lo que denominamos **Bombas**. El virus puede autoejecutarse en una fecha determinada o después de que el sistema realice una acción determinada.

Imagen. Virus

5.2.2.7. Gusanos

Un **gusano** es un programa que se reproduce por sí mismo, que viaja a través de una red y que no necesita un software o hardware para difundirse.

¿Cómo funciona un gusano? Es bastante lógico:

1. El gusano entra en un equipo por un cliente de correo a través de un adjunto
2. Recolecta todas las direcciones de correo electrónico de la libreta de direcciones
3. Se reenvía a todos los destinatarios

¿Cómo podemos detectar un gusano? Todos sabemos que, en Windows, por defecto, está habilitada la opción Ocultar extensiones en las Opciones de Carpeta—Ver. Si esto es así, un archivo llamado Contrato.txt.vbs será visto como Contrato.txt y al intentar abrirlo no lo abrirá el Bloc de Notas.

Os adjunto un listado de extensiones “peligrosas”:

386, ACE, ACM, ACV, ARC, ARJ, ASD, ASP, AVB, AX, BAT, BIN, BOO, BTM, CAB, CLA, CLASS, CDR, CHM, CMD, CNV, COM, CPL, CPT, CSC, CSS, DLL, DOC, DOT DRV, DVB, DWG, EML, EXE, FON, GMS, GVB, HLP, HTA, HTM, HTML, HTA, HTT, INF, INI, JS, JSE, LNK, MDB, MHT, MHTM, MHTML, MPD, MPP, MPT, MSG, MSI, MSO, NWS, OBD, OBJ, OBT, OBZ, OCX, OFT, OV?, PCI, PIF, PL, PPT, PWZ, POT, PRC, QPW, RAR, SCR, SBF, SH, SHB, SHS, SHTML, SHW, SMM, SYS, TAR.GZ, TD0, TGZ, TT6, TLB, TSK, TSP, VBE, VBS, VBX, VOM, VS?, VWP, VXE, VXD, WBK, WBT, WIZ, WK?, WPC, WPD, WML, WSH, WSC, XML, XLS, XLT, ZIP

¿Qué hacer si ya estamos infectados?

Hay que confiar en la solución antivirus que tengamos instalada.

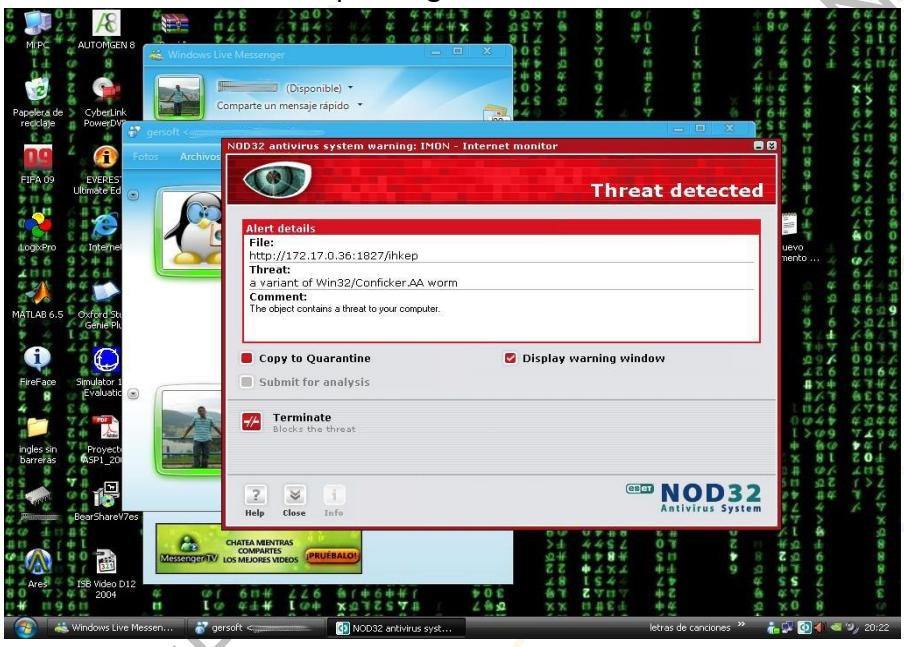


Imagen. Solución antivirus

5.2.2.8. Troyanos

Inicialmente el **Troyano** aparente ser un programa útil, pero que después nos va a dañar el sistema. El tema es que cuando lo abrimos nos damos cuenta de su objetivo.

Algunos troyanos solo son molestos (cambian iconos, agregan iconos, agregan barras de tareas, fondos de escritorios…) pero otros borran información del sistema.

Una variante de los troyanos son los **Backdoors** o Puertas Traseras, ya que permiten el acceso al sistema de usuarios no autorizados para controlar la máquina o acceder a la información de este.

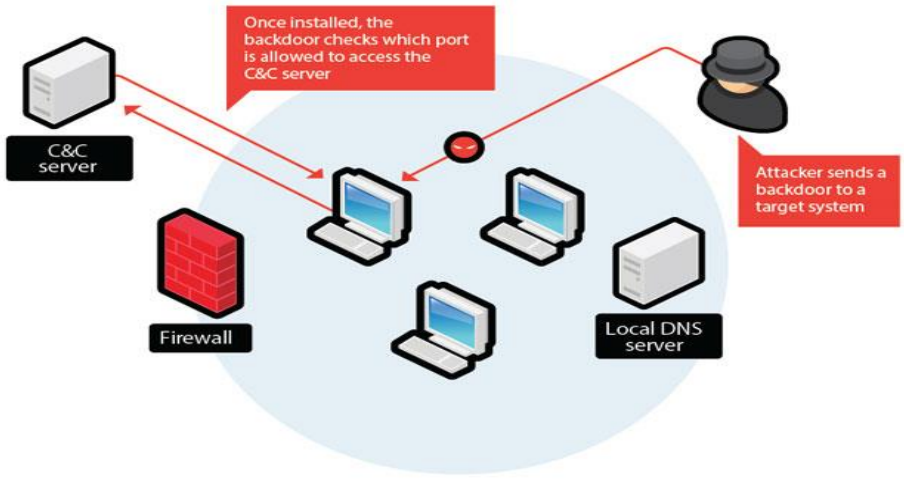


Imagen. Backdoors

5.2.2.9. SpyWare

Denominamos Spyware al software malicioso que infecta tu ordenador o dispositivo móvil, y recopila tu información personal, por donde has navegado y el uso habitual de internet. A parte de esta información, puede registrar capturas de pantalla, pulsaciones de teclas, credenciales de autentificación, dirección de correo electrónico, datos de formularios y números de tarjetas de crédito.

Los tipos de Spyware más común son:

1. Ladrones de contraseñas (**PasswordStealers**)
2. Troyanos bancarios
3. Ladrones de información (**InfoStealers**)
4. Registradores de pulsaciones del teclado (**KeyLoggers**)

Imagen. Ardamax Keylogger

5.2.2.10. Adware

El **Adware** es un tipo de software gratuito patrocinado mediante publicidad que aparece en ventanas emergentes o en una barra de herramientas. Es bastante molesto. Tiene como función recopilar información nuestra y realizar su seguimiento de los sitios web que visitamos.

Imagen. Adware

5.3. Medidas preventivas

En estos casos hay dos niveles de protección: el nivel personal y las herramientas de protección.

A nivel personal, el correo electrónico es el método más popular de propagación. Desconfía de los correos electrónicos en los que se solicita datos o partes de la contraseña o del teléfono o del número de cuenta. También desconfía de los que parecen que te los ha enviado un amigo, pero solo te dice “visita este sitio”.

Además, hay que utilizar contraseñas seguras, crear copias de seguridad regularmente, revisar los dispositivos de almacenamiento, actualizar los navegadores y los parches de seguridad del sistema.

En el segundo nivel, un buen paquete de software antivirus es el componente principal de la defensa tecnológica a nivel personal y empresarial.

Un buen antivirus se caracteriza por varias cosas:

- Comprueba todos los programas que se descargan de que no contienen malware
- Analiza el ordenador periódicamente para detectar y eliminar el malware
- Se actualiza con regularidad para detectar las amenazas más recientes
- Detecta amenazas de malware desconocidas y nos alerta de ellas
- Detecta sitios web sospechosos
- Tiene que ser fácil de descargar e instalar
- Tiene protección específicamente para tus finanzas (compras on-line)
- No entra en conflicto con otro programa del equipo, provocando problemas usabilidad

- Es fácil de usar
- Debe contener protección para el correo electrónico

Pero ¿cómo se detecta el malware con un antivirus? Hay varias técnicas:

- Comparando las firmas: Se comparan unos archivos que son sospechosos con una base de datos con las firmas de todo el software
- Métodos heurísticos: Como no se pueden tener todas las firmas utilizamos otras vías alternativas:
  - Firmas genéricas: No buscar una coincidencia 100% pero si similitudes con la original para detectar mutaciones del virus
  - Desensamblado: Estudia el código del virus en lenguaje ensamblador y se estudia el código
  - Desempaquetado: Detecta virus en archivos empaquetados y comprimido, los descomprime y desempaqueta y los analizan
  - Por comportamiento: qué hace un fichero cuando se ejecuta. Se aplican reglas en el caso de conexión con algunos sitios web
  - Bloqueando vulnerabilidades conocidas.
  - Reputación de un fichero. Si es de Microsoft Office365, te puede fiar.
  - **SandBox**. Son cajas o entornos controlados de software, en los que el Antivirus ejecuta el archivo. Como son aislados del sistema, este no sufre sus efectos y avisa en caso de sospecha.
  - Ejecución del malware en la memoria.
  - Antimalware en la nube (cloud). Ejecutar programas on-line.
  - En caso de botnets, bloquea tu máquina para que no colabore con la red

En mi caso particular, trabajo con soluciones de la empresa ESET que cumple los puntos que acabo de comentar.

5.4. Medidas correctivas

Vamos a ver qué vamos a hacer una vez estamos infectados y lo hemos detectado.

Lo vamos a realizar por fases de mejor a peor:

1. Ejecutar un programa antivirus que limpie los archivos, recuperando una copia anterior de los mismos, eliminando el código malicioso, borrando los archivos maliciosos o poniendo en cuarentena este
2. Recuperar un Punto de Restauración. Un Punto de Restauración es un sistema utilizado en sistemas operativos Windows. Consiste en que el sistema operativo realiza una imagen del sistema y sus programas en el momento en que lo creamos. Esto nos permite volver a ese momento en caso de fallo del sistema. Como es lógico, podemos ir

realizando puntos de restauración a posteriori. En las opciones de recuperación de Windows tenemos la posibilidad de recuperar el sistema desde un punto de restauración determinado.

3. Formatear la máquina y recuperar información de la copia de seguridad

5.5. Ingeniería social

He querido dedicar un apartado a este "mundo" que se ha vuelto fundamental en la seguridad informática y que está dando tantos quebraderos de cabeza a los expertos en seguridad.

Hemos comentado que la primera barrera de seguridad somos nosotros y nuestro "sentido común", pero está comprobado que no es suficiente ante los expertos en "**ingeniería social**".

Definiremos Ingeniería Social a todas las técnicas de manipulación psicológica de las personas para extraer información de ellas. Estas técnicas se usan constantemente para realizar fraudes a los que estamos expuestos porque somo humanos.

¿Y qué técnicas psicológicas utilizan para hacernos caer?

1- Si alguien nos ofrece algo, tendemos a ofrecerle también algo nosotros.
2- La urgencia nos provoca el tomar decisiones precipitadas: "Tienes 24 horas para responder…" "Quedan solo tres móviles en stock…"
3- Somos animales de costumbres. Solo hay que hacer cuatro cosas normales para que no nos paremos a pensar en que la quinta es rara.
4- Si un jefe nos pide una información, por si acaso, se la damos
5- Si en una conversación supuestamente grupal, se nos pide algún dato, no queremos ser el bicho raro.

¿Cómo funcionan estos ataques?

La mecánica es simple. Se diseña un escenario completamente inventado en el que se persuade a una persona para entregar información:

"Buenos días, le estamos llamando de su compañía de cable para informarle que hubo un problema con su tarjeta de crédito al cancelar la factura de este mes, ¿podría ser tan amable de confirmarnos sus datos para intentar realizar el pago nuevamente?"

Imagen. Proceso de los ataques

Un ejemplo de estos ataques lo encontramos en el Phishing, una técnica de ingeniería social que se aplica en el correo electrónico o en redes sociales. En este entorno recibimos un correo electrónico con un diseño "perfecto" que nos hace confiar que es del remitente, normalmente un banco, y en el

que nos solicitan información por correo. También se usa mucho en la venta por Internet. Lugares de envío de paquetes que no existen. Páginas web de entidades donde realizar los pagos o recibirlos que parecen reales. La verdad, es un mundo que ha mejorado en calidad mucho en los últimos años.

Siendo sincero, todos somos susceptibles de ser víctimas de un ataque. Sí, sí, lo digo por experiencia.

5.6. Conexión en redes públicas

Desde que tenemos dispositivos móviles, se nos ha generado la necesidad de estar permanentemente conectados. Lo normal es llegar a cualquier lugar comercial, bar, cafetería, restaurante, centro comercial, biblioteca… y comprobar si tenemos conexión inalámbrica.

Todas estas redes se caracterizan por permitirnos conectarnos a internet de manera cómoda y rápida. A todo caso, nos aparece una página web donde nos dejan conectarnos a cambio de información comercial.

El tema principal es que pidan contraseña o no, la información que se transmite entre ellas no está cifrada, por lo que un usuario malintencionado puede monitorizar el tráfico de la red y obtener la información que más le interese.

Imagen. Wifi

Por lo tanto, si podemos evitarlas mejor. Pero como no lo vamos a hacer, os recomiendo lo siguiente:

- Si podemos elegir entre varias redes públicas, elijamos la que disponga de seguridad WPA o WPA2, pues la seguridad WEP es totalmente insegura
- Detener cualquier proceso de sincronización de nuestros programas con la nube
- A parte del equipo actualizado y tener un antivirus instalado, nos vendrá muy bien un cortafuegos que impida los intentos de acceso al sistema
- Navega por página web seguras, que empiecen por HTTPS
- No te autentifiques en ninguna web ni servicio, Nada de bancos ni compras on-line
- Elimina los datos de la red abierta que tengas memorizados en el navegador

5.7. Ataque DoS (Un punto de vista técnico)

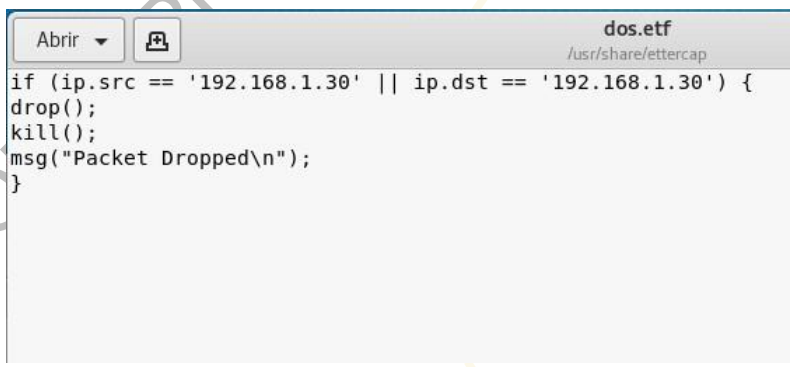
5.7.1. Pasos a realizar

En esta práctica realizaremos un ataque DoS contra un equipo de nuestra LAN con la herramienta Ettercap. Para tal fin, realizaremos un filtro de Ettercap lo compilaremos y lo ejecutaremos contra una máquina de nuestra red.

Ettercap tiene muchas herramientas integradas para permitir todo tipo de actividad de la red desde realizar Sniffing hasta realizar ARP Spoofing. También tiene la capacidad de utilizar filtros para centrar su actividad. Por ejemplo, queremos bloquear un host de la red, la forma más sencilla de hacerlo es no permitir que los paquetes sean enviados hacia el host que desea bloquear. Los filtros de Ettercap nos permitirán hacer precisamente eso.

Abriremos cualquier editor de texto y escribimos este script reemplazando el texto Target IP por la dirección IP del equipo que queremos bloquear.

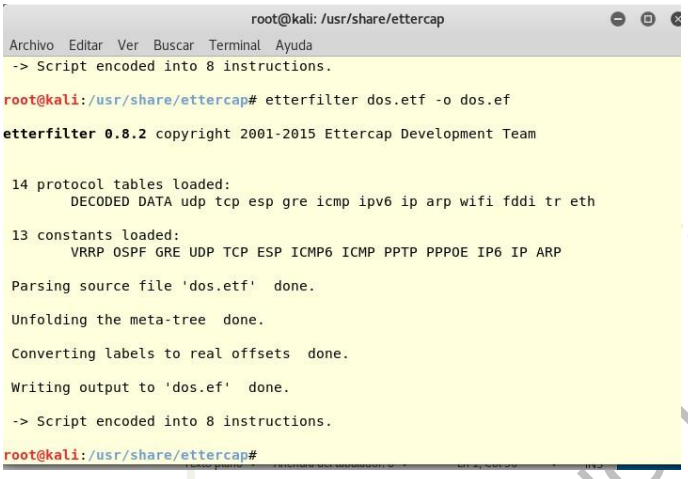
```
if (ip.src == 'Target IP' || ip.dst == 'Target IP') {
drop();
kill();
msg("Packet Dropped\n");
}
```



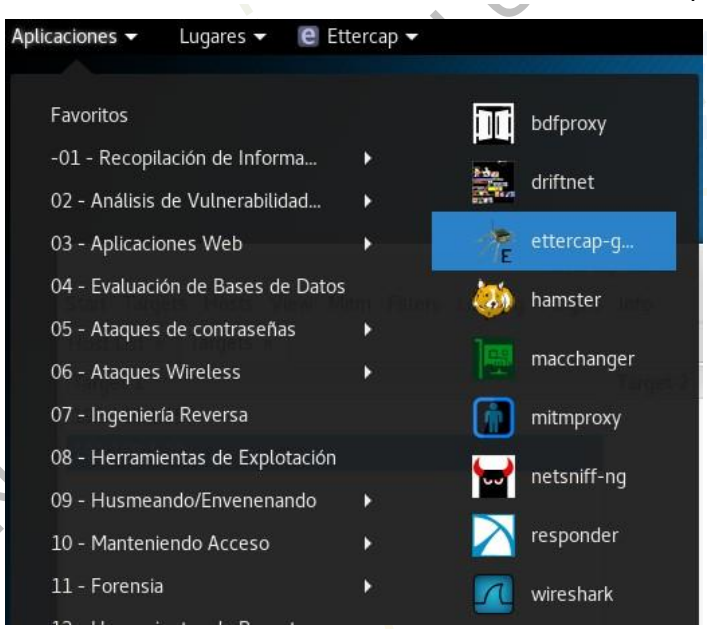
Lo guardaremos con el nombre **dos.eft** en la carpeta de filtros Ettercap ***/usr/local/share/ettercap*** *o en* ***/etc/ettercap***

Ahora tendremos que compilar un script para que lo podamos seleccionar con el Ettercap. Tendremos que escribir para consola:

etterfilter dos.eft -o dos.ef

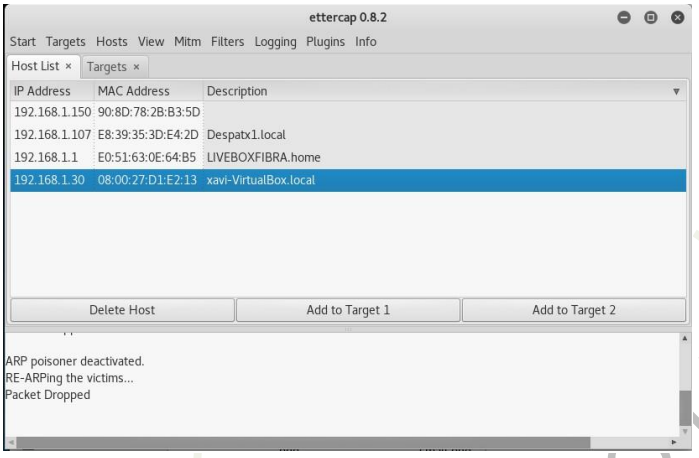


Una vez compilado, ya podemos inicializar la herramienta Ettercap. Para hacerlo tendremos que dirigir hacia Kali Linux, 'Aplicaciones', 'Husmeando/Envenenando' y 'Ettercap'



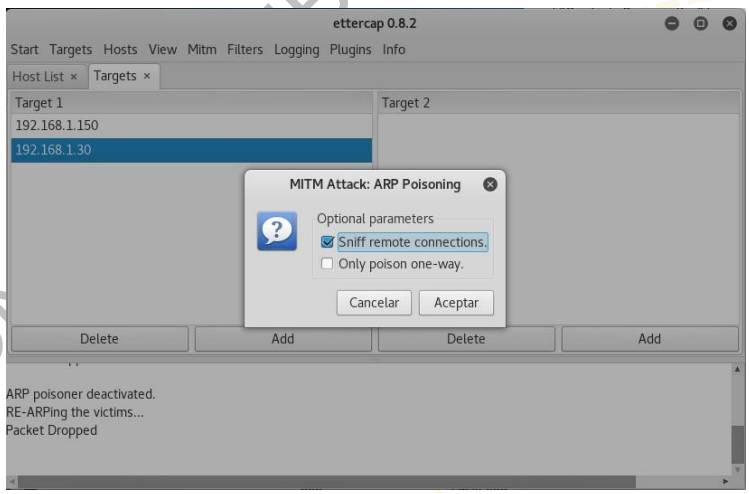
Una vez con el Ettercap hacemos clic en *'Sniff'* y justo después *'Unified Sniffing'*. Además, seleccionaremos la interface de red que tengamos configurada.

Ahora deberemos encontrar los hosts que tenemos accesibles, y lo haremos desde el menú *Host* y seleccionando ***Scan for Hosts***. Después vemos el listado de host en ***Host→Host List***.

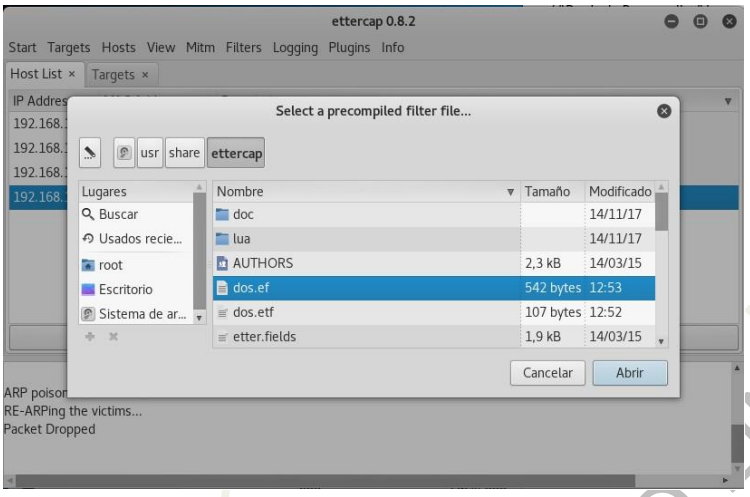


Una vez encontrados todos los hosts de la LAN, seleccionaremos 'Targets' y luego 'Targets List' y 'Add Target' bajo la ventana de Target 1. Aquí insertaremos la dirección IP de nuestra víctima.

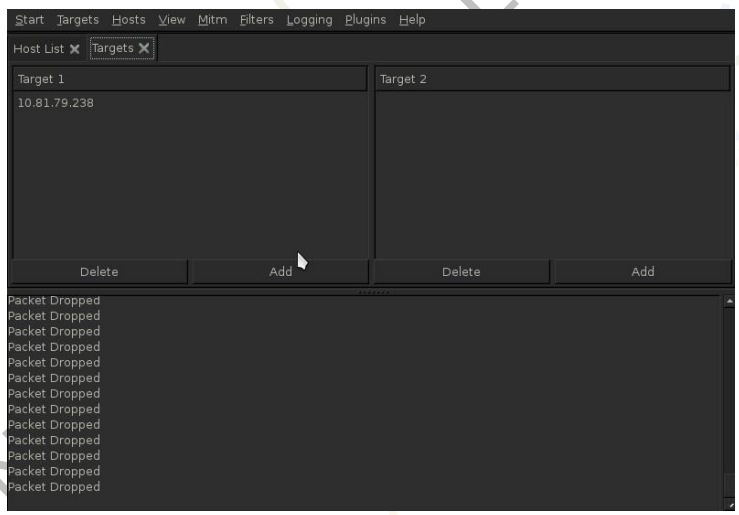
Una vez hemos hecho esto, ya podemos comenzar a realizar el ataque MiTM y después "ARP Poisoning".



Ahora tendremos que cargar nuestro filtro. Para ello nos dirigiremos a 'Filters' y luego 'Load Filter' y seleccionaremos *dos.ef* de la carpeta donde hemos dejado el filtro (/usr /share/ettercap/)



Una vez realizado esto, ya podremos ver como todos los paquetes que encuentra el Ettercap de nuestra víctima son descartados.



Ahora, si vamos a la máquina atacada y realizamos un ping a una web, por ejemplo, notaremos los efectos.

Otra herramienta que nos puede servir para realizar un DoS en una LAN puede ser hping3. El pedido que utilizaríamos sería:

#hping3 –a IPvictima –flood Ipbroadcast

Con este comando todas las máquinas de la red recibirán una petición ping de parte de la Ip de la víctima y las responderán. En este tipo de ataque, cuando mayor sea la red y por lo tanto más equipos envíen pings contra nuestra víctima más fácil y rápidamente caer.

Recursos y enlaces

Antivitus Linux. Claim

Objetivo: Instalar el software antivirus Claim en un entorno Linux y ejecutar un análisis del sistema.

- https://youtu.be/jJyi3bWpjFA

Antivitus Windows. ESET

Objetivo: En esta práctica instalaremos la solución antivirus NOD32 de la empresa ESET y la probaremos con un virus de prueba.

- https://youtu.be/8pK_Ggqx2mA

Windows Sysinternals. Utilidades Gráficas

Objetivo: En esta práctica vamos a conocer las herramientas de entorno gráfico que trae la caja de herramientas Microsoft que es la Suite Susinternals. La poéis descargar de: https://docs.microsoft.com/en-us/sysinternals/downloads/

- https://youtu.be/P9cAZFraa4k

- ¿Cómo funciona un antivirus? https://binged.it/31p96KS

- Black Hat https://www.blackhat.com/

- Laboratorios DragonJar https://www.dragonjar.org/laboratorios-de-seguridad-informatica.xhtml

- ESET SysInspector https://www.eset.com/es/soporte/sysinspector/

- X1red+segura https://www.x1redmassegura.com/

- Grupo Delitos Telemáticos Guardia Civil https://www.gdt.guardiacivil.es/webgdt/

- La historia secreta de los piratas informáticos https://www.youtube.com/watch?v=7KreXtq0QoA

- Los piratas de Silicon Valley https://www.filmaffinity.com/es/film399662.html

Test de autoevaluación

El Malware que crea una amenaza y después pide un dinero al usuario para eliminarla, se denomina:

a) Rootkit
b) RansomWare
c) ShareWare
d) RogueWare

A las redes de equipos informáticos, destinadas a realizar acciones maliciosas, se les denomina:

a) Botnet
b) Spyder
c) Crawler
d) Dealer

A los sistemas aislados, destinados a ejecutar aplicaciones sin afectar al resto del sistema, se les denomina:

a) Hybervante
b) HotSpot
c) Crawler
d) SandBox

Al Malware que se instala en el ordenador y se encarga de capturar las pulsaciones del teclado del usuario, se le denomina

a) PasswordStealer
b) InforStealer
c) KeyLogger
d) BackDoor

SOLUCIONARIOS

Test de autoevaluación

El Malware que crea una amenaza y después pide un dinero al usuario para eliminarla, se denomina:

a) Rootkit

b) RansomWare

c) ShareWare

d) RogueWare

A las redes de equipos informáticos, destinadas a realizar acciones maliciosas, se les denomina:

a) Botnet

b) Spyder

c) Crawler

d) Dealer

A los sistemas aislados, destinados a ejecutar aplicaciones sin afectar al resto del sistema, se les denomina:

a) Hybervante

b) HotSpot

c) Crawler

d) SandBox

Al Malware que se instala en el ordenador y se encarga de capturar las pulsaciones del teclado del usuario, se le denomina

a) PasswordStealer

b) InforStealer

c) **KeyLogger**

d) BackDoor