

GESTIÓN ACTIVA DE LA SEGURIDAD PARTE II

EL CONTROL DE ACCESO AL SISTEMA

La primera medida de protección de un sistema consiste en impedir el acceso físico al mismo. En los equipos de escritorio, esto es imposible puesto que los usuarios trabajan delante de los equipos físicos, por lo que en estos casos hay que habilitar medidas alternativas equivalentes.

En los servidores, la protección se hace más fácil (basta con que estén bajo llave o en un lugar reservado), pero también más necesaria por el grado de compromiso que se pone en entredicho en caso de ataque. En este caso, el acceso a las salas de servidores debe estar monitorizado y controlado mediante tarjetas de acceso o sistemas biométricos.

Para diseñar un buen sistema de acceso seguro a las instalaciones se puede reflexionar sobre las siguientes cuestiones o tecnologías:

- ¿Qué salas contienen sistemas críticos y deben ser protegidas?
- ¿Qué formas de acceso podrían utilizar los intrusos?
- Definición de los horarios de acceso permitidos para cada usuario.
- Instrucción de los empleados sobre el sistema de acceso.
- Métodos de autenticación permitidos en la organización.
- Chequeos periódicos del sistema de seguridad (auditoría).
- Cambio frecuente de contraseñas como parte de la política de seguridad.
- Creación de un plan de seguridad y de respuesta frente a brechas.

A partir de aquí debe diseñarse la seguridad lógica. La parte más importante de esta seguridad es una buena política de gestión de contraseñas. Parece mentira, pero este es uno de los puntos más débiles en la mayor parte de las organizaciones. Una buena política de contraseñas incrementa notablemente la seguridad de los sistemas.

Para crear una buena política de contraseñas podríamos considerar algunos o todos los factores siguientes en función de nuestras exigencias de seguridad:

- Longitud mínima de las contraseñas de las cuentas de usuario, especialmente si se trata de usuarios administradores o con ciertos privilegios.
- Caducidad de las contraseñas. Toda contraseña de usuario debe tener una fecha de caducidad de modo que si la pierde o se la roban sin su advertencia, el acceso estará comprometido solo durante el tiempo en que esa contraseña sea válida.
- No permitir que la renovación de una contraseña coincida con una anterior del mismo usuario.
- Exigir contraseñas complejas. Por ejemplo, que contenga caracteres alfabéticos en mayúsculas y minúsculas, símbolos y números.
- Combinar el uso de contraseñas (algo que el usuario sabe) con tarjetas de seguridad (algo que el usuario tiene).
- Auditar todos los accesos de usuario en el sistema, así como los cambios de contraseñas o las alteraciones de privilegios de las cuentas.

La seguridad en la BIOS y en los gestores de arranque

Algunas de las características básicas de los equipos se configuran en las BIOS del sistema, cuyo acceso siempre debe estar protegido con una contraseña (ver figura). Esta contraseña suele ser muy débil pero ya es una primera barrera. Algunas BIOS también pueden proteger mediante contraseña la posibilidad de arrancar de un disco o de otro, de modo que solo quien conozca esta contraseña podrá arrancar el sistema.

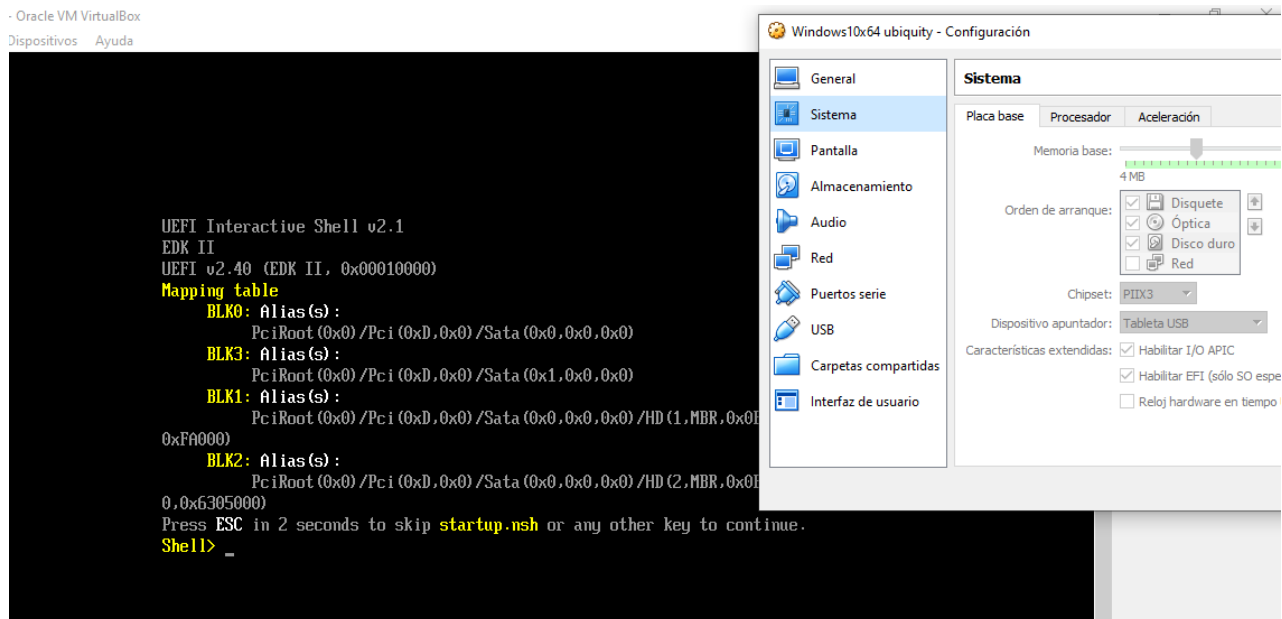
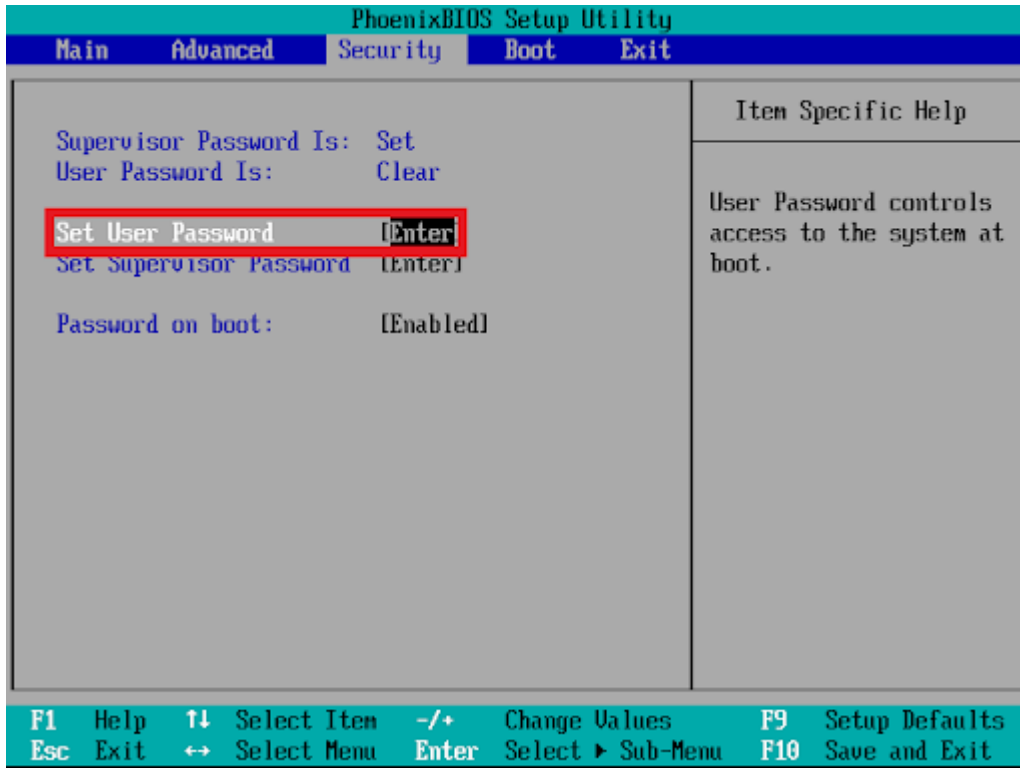


Figura: Acceso a la BIOS mediante contraseña o la UEFI en VB

La alteración o manipulación de la BIOS puede originar muchos problemas:

- **Ataques de denegación de servicio.** Por ejemplo, el equipo no arranca del disco adecuado y se impide el acceso al sistema contenido en él. También, desde la BIOS, se puede deshabilitar parte del hardware.
- **Ataques de suplantación.** Por ejemplo, se puede arrancar de un disco alternativo, que simula ser el original, pero que contiene software que compromete la privacidad del usuario que cree presentarse en su sistema habitual.
- **Pérdidas o fugas de información.** Como ejemplo, se puede arrancar de un LiveCD y se copian los datos del sistema objetivo o se formatean sus particiones. También se podrían suplantar las contraseñas de cuentas privilegiadas.

En cualquier caso, se necesita el acceso a la BIOS para indicarle que debe arrancar de un LiveCD, por eso nunca debe establecerse que un sistema arranque por defecto de un CD, un pendrive o un disco externo, ni dejar las BIOS sin protección de contraseña.

El control de acceso al sistema también se puede hacer mediante software a través de los gestores de arranque avanzados, por ejemplo, GRUB.

Actualización de sistemas y aplicaciones

La actualización de los sistemas y aplicaciones es una de las actividades más importantes que se pueden realizar para mejorar sustancialmente la seguridad de un sistema porque reduce sensiblemente el número de vulnerabilidades disminuyendo la superficie de ataque. Aun así, una actualización comporta algún riesgo: no debe hacerse nunca una actualización sin practicar previamente una copia de seguridad probada. Si algo saliera mal durante la actualización o el comportamiento del sistema después de la actualización fuera errático, podríamos volver atrás restaurando el backup realizado.

Pero, esta no es la única razón que aconseja actualizar el sistema y sus aplicaciones, aunque sí es la más relacionada con la seguridad. Otras razones son las siguientes:

- Eliminar vulnerabilidades detectadas por el desarrollador de la aplicación o del sistema operativo (bugs).
- Incorporación de mejoras en el software, por ejemplo, incrementando el rendimiento o la usabilidad.
- Adición de nuevas funcionalidades que mejoran la aplicación.
- Compatibilidad con nuevas plataformas tecnológicas de software de sistemas.
- Compatibilidad con novedades en el hardware.

Por otra parte, no solo se puede actualizar el software de aplicación o de sistemas. Otros elementos actualizables son el firmware de los distintos componentes de hardware, la BIOS, los controladores de dispositivos, etc.

Los desarrolladores suelen proveer parches o actualizaciones periódicamente para que los usuarios los descarguen y apliquen en sus sistemas, pero como esta operación no está exenta de riesgo ¿quién? ¿cuándo y de qué modo deben hacerse estas actualizaciones?

Algunas actualizaciones, que son de bajo o nulo riesgo, pueden ser realizadas directamente por los usuarios de las aplicaciones, sin embargo, los sistemas suelen defenderse impidiendo que los usuarios no administradores puedan realizar instalaciones o actualizaciones. La cuenta de usuario más indicada para cualquier actualización es la de administrador, superusuario o similar.

Precaución

Cuando se realizan operaciones delicadas como es una actualización, que puede colisionar con la operación del antivirus, es conveniente desactivar el antivirus del sistema para que no interfiera —mediante un falso positivo— con la instalación y esta se quede a medio realizar, lo que podría dejar al sistema en un estado inestable. Una vez realizada la actualización debe habilitarse de nuevo el antivirus. Obviamente, el parche o la actualización deben ser comprobados por un antivirus antes de su instalación en un equipo final. Además, conviene descargar parches exclusivamente de los sitios oficiales de los fabricantes o distribuidores, asegurándose de la compatibilidad del parche para el hardware y software operativo del sistema de destino.

Otra buena práctica es realizar la actualización previamente en un equipo de laboratorio para observar cómo se comporta el sistema después de la actualización. Para ello son muy útiles los entornos de laboratorio contruidos en torno a herramientas de virtualización.

¿Cuándo hacer las actualizaciones? Cuanto antes, mejor. Especialmente si se trata de sistemas muy amenazados como los que están en contacto directo con Internet (redes perimetrales) o redes hostiles.

En organizaciones de tipo medio o grande se acostumbra a confeccionar un plan periódico de actualizaciones que los administradores de sistemas deben seguir, sin perjuicio de que, si se descubre una vulnerabilidad crítica, y el fabricante confecciona el parche de seguridad que la corrige haya que saltarse este calendario para aplicar el parche inmediatamente. En la confección de este calendario deben tenerse en cuenta los ciclos de producción de la organización: por ejemplo, las actualizaciones podrían hacerse por la noche o en horas de baja producción ya que gran parte de estas actualizaciones requieren el reinicio del sistema.

En cuanto al modo de aplicación de las actualizaciones caben dos posibilidades básicas: manual o automáticamente. La mayor parte de los sistemas pueden actualizarse automáticamente de manera periódica desde los repositorios del fabricante o distribuidor. En otras ocasiones, para disponer de un mejor control sobre los parches lo que se hace es descargarlos manualmente y luego aplicarlos uno a uno en el orden recomendado por el fabricante. En caso de que se opte por una actualización manual, adquiere una relevante importancia fijarse específicamente si cada parche descargado se corresponde con el hardware y software para el que se destina.

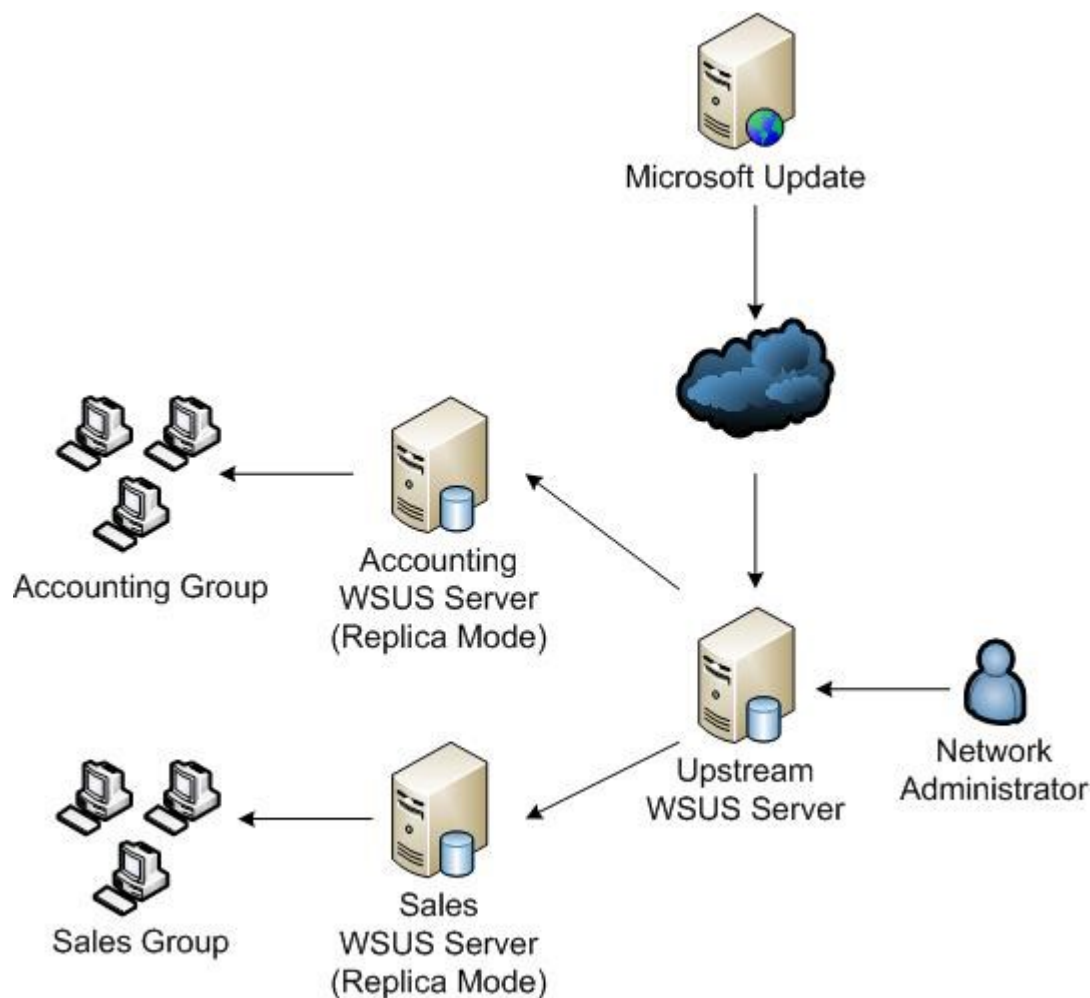
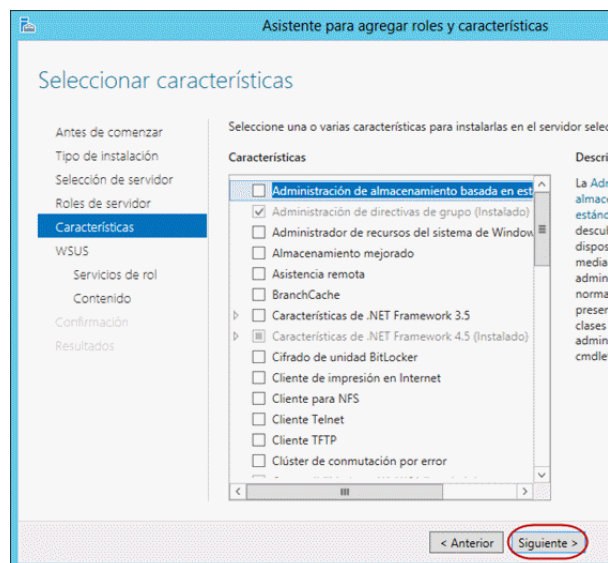
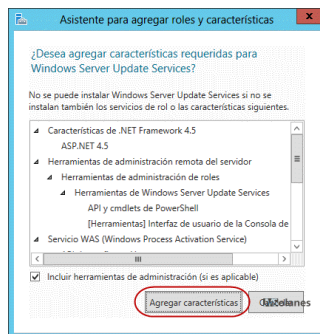
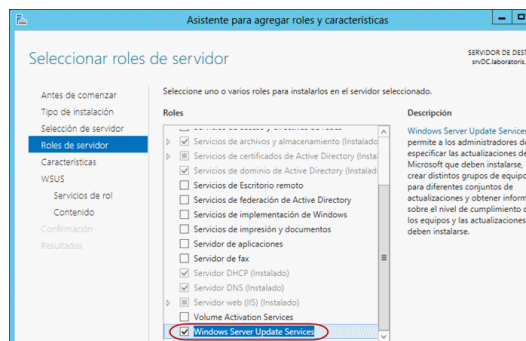


Figura: Arquitectura de un WSUS para una organización grande.

En La figura, se puede ver la arquitectura de un conjunto de servidores WSUS, específicos de sistemas Microsoft, para abastecer de actualizaciones a los sistemas de una organización grande. Un servidor WSUS básicamente es un servidor proxy de actualizaciones con algunas propiedades específicas. El servidor descarga las actualizaciones desde la sede web de Microsoft (servicio Microsoft Update) y las almacena localmente. Cuando un equipo final necesita hacer una actualización la solicita a un servidor WSUS de su organización y no es necesario que consuma ancho de banda por la descarga de Internet, puesto que el parche ya está en la red local.

Un WSUS puede alimentar a su vez a otros de menor nivel en la jerarquía. Además, el administrador puede aprobar o desaprobar cada parche descargado de modo que los hace visibles o no en su organización. Se puede conseguir más información sobre WSUS en <http://technet.microsoft.com/es-es/windowsserver/bb332157>



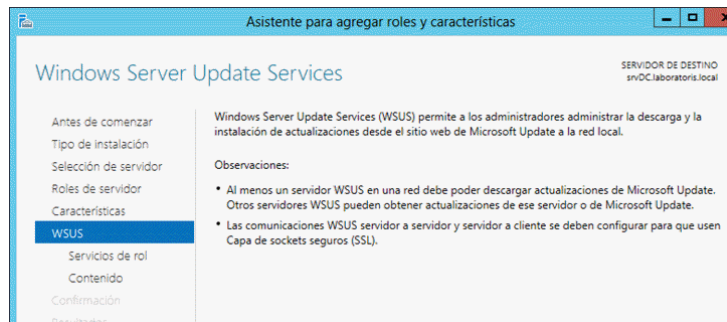


Figura: Arriba, Configuración de Windows Update. Abajo, fichas de configuración de actualizaciones de Ubuntu.

En La figura arriba, se puede ver la configuración de Windows Update, la utilidad que actualiza un sistema Windows. En el caso de los sistemas GNU/Linux, una vez configurados los repositorios de descarga se pueden configurar las condiciones en las que se aplicarán las actualizaciones (en La figura, abajo).

Además, hay que comprobar que el software que descargamos viene de donde dice provenir. Buena parte de los equipos domésticos se infectan porque sus usuarios descargan antivirus (falsos antivirus) que contienen troyanos o virus en su interior desde sitios no autorizados: al hacer la instalación de la falsa aplicación introducimos el malware en el sistema.

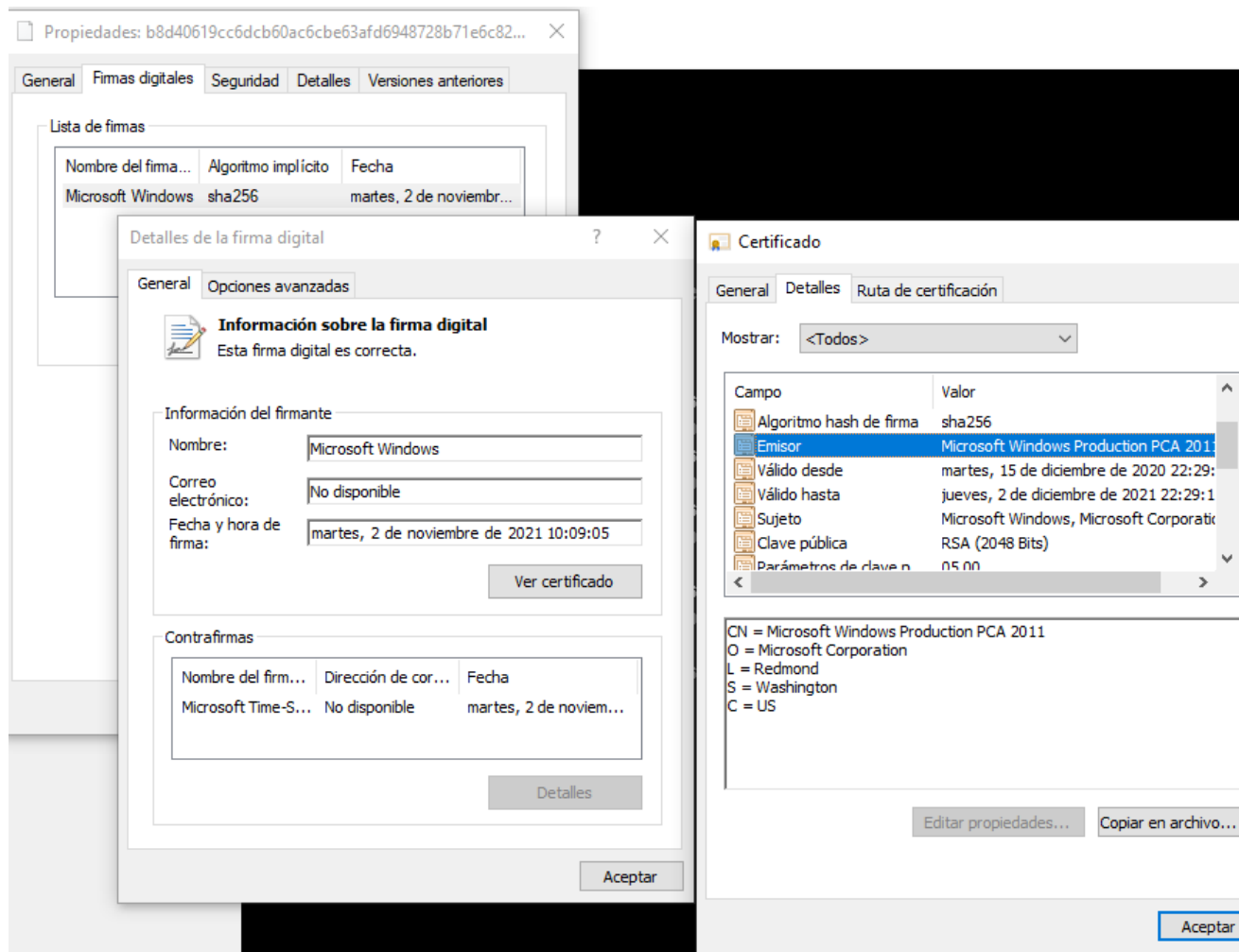


Figura: Secuencia de la vista del certificado de autenticidad de una actualización de seguridad de Microsoft.

Los fabricantes de software cuidadosos suelen firmar sus parches (y, en general, todo su código) mediante técnicas criptográficas, de modo que los sistemas de destino puedan reconocer la procedencia de cada parche como método de validación.

En La figura se puede ver las propiedades del fichero descargado que contiene una actualización de Microsoft. Si seguimos la secuencia de izquierda a derecha en la figura de referencia podemos ver la fecha de firma y el certificado con que se garantiza la autenticidad. En las dos ventanas de la derecha se puede ver quién firma (en este caso Microsoft Corporation) y la fecha de caducidad.

2.2.2. SEGURIDAD EN DISCOS Y FICHEROS

Otro nivel de seguridad en la defensa en profundidad se aplica a discos y ficheros. Efectivamente, si un atacante es capaz de acceder a un sistema, por ejemplo, por una puerta trasera (backdoor), se encontrará con otra barrera de protección cuando quiera acceder a los sistemas de ficheros.

Seguridad en el particionado de discos

Siempre deben elegirse cuidadosamente las configuraciones en que se van a particionar los discos, especialmente en servidores. Cada partición de disco debe llevar asociada una seguridad específica.

Errores en el diseño de las particiones de los discos originan ataques de denegación de servicios y vía de acceso libre al malware. Por ejemplo, si no dotamos a las particiones de disco del suficiente espacio, estas se pueden llenar y ocasionar discontinuidades en el servicio, lo que es un ataque de denegación de servicio en toda regla. Otro ejemplo: en una partición de disco formateada como FAT, cualquier usuario —puesto que FAT no admite seguridad de ficheros puede ejecutar cualquier herramienta al uso y deteriorar el sistema.

También deben cuidarse las conexiones de pendrives, discos conectables en caliente o unidades remotas de red, ya que contienen información que no ha podido controlar el sistema en el que se insertan en toda su historia anterior.

En sistemas GNU/Linux, especial consideración debe tenerse con particiones `/var`, `/var/log` y `/home`, que son las que se pueden llenar con más facilidad con el paso del tiempo. Es costumbre separar la partición raíz del sistema `/` de `/home`, que contiene los perfiles de los usuarios (salvo root). En una instalación más avanzada, también se podría separar `/usr` o los directorios en donde se instalasen las aplicaciones de usuarios.

En Windows hay que tener mucho cuidado con las particiones que alberguen ficheros de log o bases de datos de crecimiento ilimitado. También deben considerarse los tamaños de los ficheros `pagefile.sys` en el caso de Windows (ver figura) o la partición de swapping en GNU/Linux.

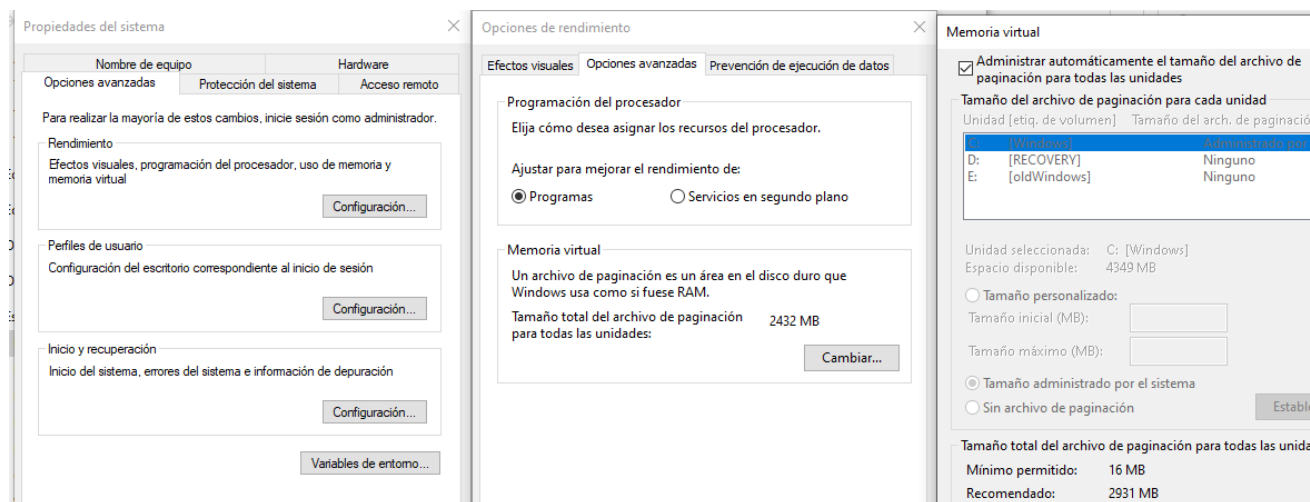


Figura: Configuración del tamaño de la paginación en Windows.

Seguridad en los sistemas de ficheros

Los ficheros que residen en el sistema de ficheros no están exentos de amenazas. Las más frecuentes apuntan a la corrupción o deterioro de los sistemas de ficheros en que residen. En este sentido, son más seguros los sistemas de ficheros transaccionales con journaling como son ext4 para GNU/Linux o NTFS para

Windows, en los que se garantizan que las operaciones de escritura no se quedarán a medias por un fallo de hardware o un corte de suministro eléctrico.

Otro vector de ataque para los ficheros proviene de los virus u otro tipo de malware. Un buen antivirus residente en memoria es una buena defensa, sin embargo, la operación de limpieza no puede nunca garantizar que el fichero desinfectado no quede dañado, bien por la acción malévola del virus o por la ejecución errónea del antivirus en la operación de desinfección.

Por otra parte, un fichero puede ser atacado violando sus permisos de acceso: usuarios que no debieran poder acceder al fichero, de hecho, acceden por usurpación de permisos que no les corresponden o por deficiencias en la seguridad del fichero que le ha asignado el administrador. Este tipo de ataque se combate mediante una correcta política de accesos controlados.

Por último, los ficheros deben estar protegidos contra el borrado o manipulación accidental. En este caso, un buen sistema de copias de seguridad puede atenuar el riesgo.

Listas de control de acceso, ACL

Una ACL es un objeto informático que describe el conjunto de entidades (usuarios, equipos, recursos) sobre el que se definirán una regla de acceso controlado.

Una vez definida la ACL se le asigna un derecho o permiso que básicamente es una denegación o una aceptación de operación o acceso. Todas las entidades descritas en la ACL podrán o no acceder al recurso sobre el que se establece la regla.

*Al conjunto de reglas que definen el acceso a un recurso se le **denomina política o directiva**.*

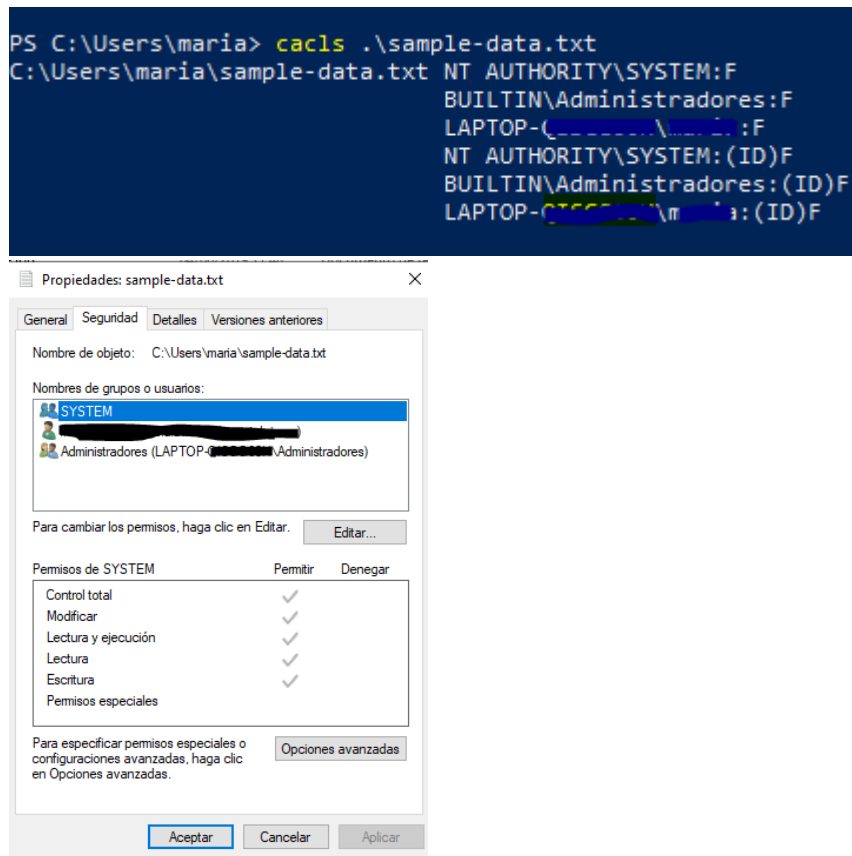
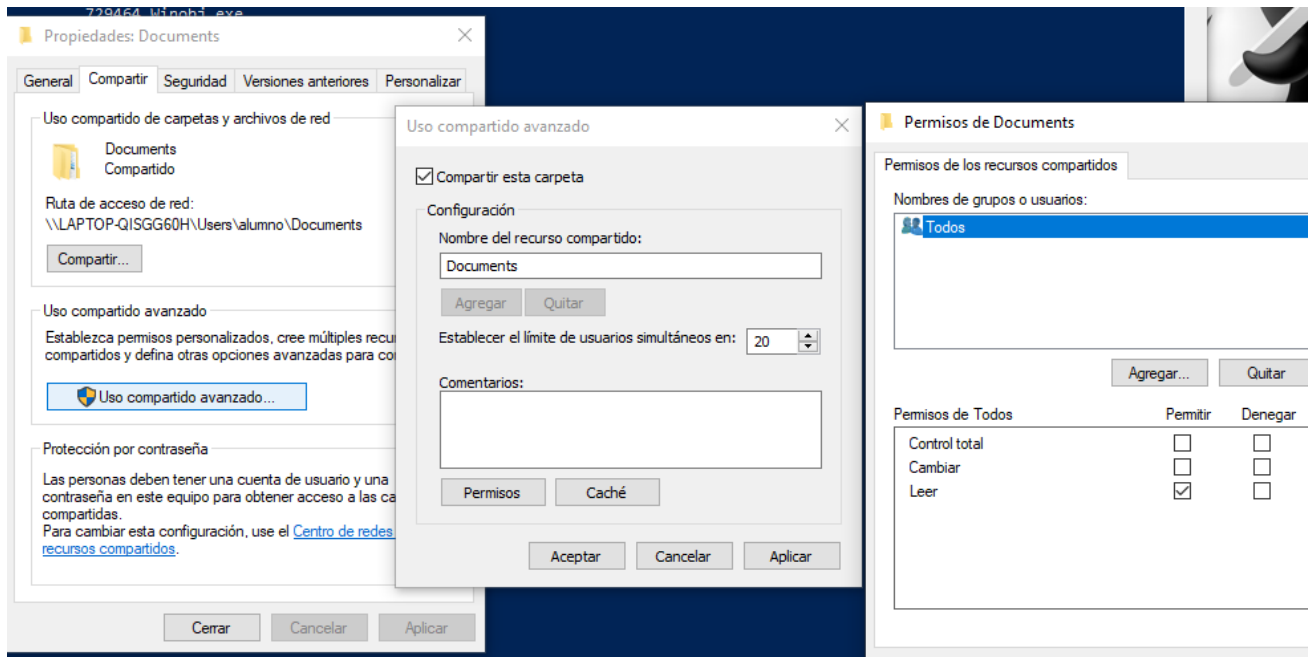


Figura: Utilización de cacls en Windows para asignación de permisos: vista de la línea de comandos y su representación en entorno gráfico.

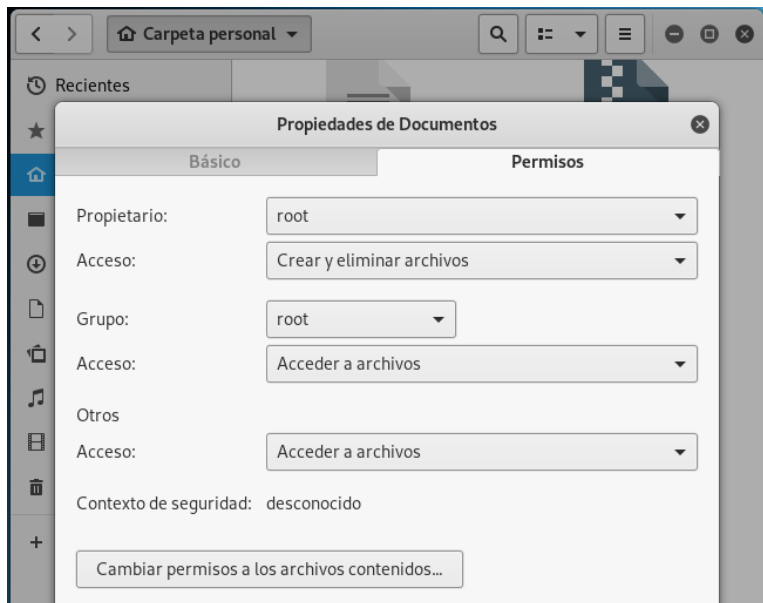
Un ejemplo de uso común de ACL se encuentra en los routers. Cuando se define una ACL en un router (RACL o Router ACL) este decide dejar pasar un paquete a su través o eliminarlo de la red en función de si cumple o no unas reglas. Estas reglas se establecen de acuerdo con variables tales como el protocolo de la capa de red del paquete (IP, ICMP), o de la capa de transporte (TCP, UDP), la dirección IP de origen y/o destino, el número de puerto de origen/destino, etc.

Recursos compartidos

Los recursos compartidos se comportan desde el punto de vista del acceso de los usuarios como si fueran ficheros o carpetas remotos. La conexión se realiza o no dependiendo de las reglas establecidas con ACL específicas para recursos de red: discos compartidos, impresoras de red, etc.



Configuración de un recurso compartido en windows



Configuración de un recurso

compartido en Linux

Si se desciende al nivel de ficheros, los sistemas operativos modernos disponen sistemas de permisos para asignar a cada fichero o carpeta las correspondientes reglas de seguridad. Como estos permisos no son compatibles de unos sistemas a otros, por ejemplo, los de Windows con respecto de los de GNU/Linux, esto supone una fuente de vulnerabilidades por deficiencias en la configuración cuando unos sistemas utilizan remotamente los recursos compartidos de otros.

2.2.3. LA AUTENTICACIÓN PARA EL ACCESO AL SISTEMA

Todo usuario que requiera el consumo de recursos en un sistema seguro debe poseer una cuenta de usuario que lo identifique ante el sistema. A esta cuenta se asociarán permisos y derechos que restrinjan las actividades del usuario para que se ciñan a lo que debe ser su función productiva. Los administradores deben considerar los siguientes elementos de seguridad relacionados con las cuentas de usuario:

Deshabilitar las cuentas conocidas

Los sistemas suelen crear por defecto algunas cuentas que deben renombrarse o deshabilitarse para que un intruso no pueda utilizarlas. Por ejemplo, en Windows la cuenta Administrador (Administrator en las versiones en Inglés) o la cuenta root en GNU/Linux. Otras cuentas a tener presentes son las de invitados (típicamente: invitado o guest).

Creación de una política de restricciones en el logon de los usuarios

Por ejemplo, se puede asignar un horario de uso de las cuentas de usuario. Si la jornada laboral es de lunes a viernes, nadie tiene que utilizar esa cuenta un fin de semana, por tanto, esa cuenta no podrá ser atacada cuando no se pueda usar.

También se puede contabilizar el tiempo total de sesión, de modo que al finalizar el tiempo previsto el sistema despida al usuario automáticamente. Esto impediría, por ejemplo, que si un usuario olvida despedirse quede la sesión abierta indefinidamente.

Otra restricción común es que ciertos servicios solo pueden ser consumidos desde sesiones establecidas por ciertas direcciones IP y no por otras, o desde la red interna, pero desde Internet.

Por último, se podría restringir el número de intentos fallidos de presentación de usuario, de manera que si se sobrepasa un límite, la cuenta utilizada en el intento de intrusión quede bloqueada por un tiempo o permanentemente hasta que un administrador del sistema la desbloquee. De este modo, combatiríamos los ataques de fuerza bruta para crackeo de contraseñas.

Políticas de contraseñas

Un acceso con contraseña se basa en algo que solo su propietario sabe (la contraseña), que se asocia a un nombre de usuario (el suyo). La política debe tener en cuenta que las contraseñas asociadas a las cuentas de usuario sean suficientemente largas y complejas. Además, puede ser conveniente que se tengan que cambiar frecuentemente, de modo que, si una contraseña es comprometida, lo será solo hasta que su propietario la cambie.

Algunas recomendaciones y elementos utilizados para confeccionar políticas o directivas de contraseñas son los siguientes:

1. Siempre hay que cambiar las contraseñas que los sistemas asocian a ciertas cuentas por defecto después de su instalación oficial.
2. No debe utilizarse información familiar o personal en la construcción de las contraseñas para evitar ataques de ingeniería social.

3. No utilizar palabras que puedan aparecer en un diccionario, sea cual fuere el idioma, para repeler ataques de diccionario.
4. Deben establecerse contraseñas largas, siempre por encima de 8 caracteres, que incluyan mayúsculas y minúsculas, cifras, letras y símbolos.
5. Nunca deben escribirse las contraseñas en papeles o documentos electrónicos no protegidos. Tampoco debe cederse nunca una contraseña. Una contraseña no debe ser compartida por varios usuarios. Si es necesario que varios usuarios compartan una función, debe crearse una cuenta para cada uno de ellos con los mismos derechos.
6. Cambiar la contraseña periódicamente, por ejemplo, cada 60 días o más frecuentemente si se protegen datos especialmente sensibles.
7. En lo posible, debe evitarse la reutilización de contraseñas que ya expiraron por si las anteriores estuvieron en algún momento comprometidas.
8. Deben utilizarse diferentes contraseñas para diferentes sistemas o aplicaciones.

Otros medios de control de acceso

El uso de tarjetas inteligentes establece la seguridad basada en algo que el usuario "tiene" (la tarjeta inteligente). Las hay de diversos tipos: tarjetas con banda magnética como las tarjetas de crédito, tarjetas con chip como el DNI electrónico o sencillamente un pendrive con un contenido específico y protegido (token). Todas estas tarjetas utilizan técnicas criptográficas.

Otro sistema de control de acceso son los sistemas biométricos, cuya seguridad se basa en algo que se "es": una huella dactilar, el iris ocular, un patrón facial, etc. En el caso en el que se requieran sistemas de muy alta seguridad se pueden combinar varios de estos sistemas de autenticación.

2.2.4. ATAQUES POR SOFTWARE MALICIOSO

Se entiende por malware o software malicioso todo procedimiento, programa, utilidad o aplicación que se construye con el fin de atacar un sistema o un proceso. Diariamente se vuelcan sobre Internet centenares de nuevos malware, lo que da una idea de la ingente tarea de las compañías que desarrollan suites de seguridad y del riesgo que se corre incluso teniendo actualizado el antivirus. En sistemas de alta seguridad suelen instalarse antivirus con varios motores de análisis, cada uno de un proveedor de seguridad distinto.

La naturaleza del malware es muy variada. A continuación, se expone una clasificación general:

- **Virus.** Se componen de una secuencia de instrucciones ejecutables con capacidad de autorréplica parasitando otras secuencias. Debe tenerse en cuenta que un virus no es un programa por sí solo: necesita el concurso de otro programa para llevar a cabo la infección. El principal objetivo de un virus es autorreplicarse, sin embargo, se le suele añadir otras funciones destructivas.
- **Gusanos o worms.** Son programas independientes con autonomía de funcionamiento, capacidad de autorréplica y que actúan en entornos de red explotando alguna vulnerabilidad de algún protocolo o servicio. Su propósito principal es expandirse por los sistemas de la red y causar un ataque de denegación de servicio.
- **Caballos de troya o troyanos.** Son fragmentos de código que se esconden en el interior de un archivo con apariencia inofensiva. Un troyano es incapaz de replicarse: para reproducirse requiere el concurso de la actividad de un usuario. Su funcionamiento se basa en la ejecución del programa

anfitrión, ejecutado por el usuario casi siempre por engaño, que activa el troyano. Un caso especial de troyano son las bombas lógicas que son utilizadas para el lanzamiento de un virus o un gusano preparado para atacar bajo ciertas condiciones como fechas determinadas.

- **Puertas falsas, traseras o backdoors.** Su objetivo es ofrecer un modo de acceso al sistema que esquiva las medidas de seguridad dejando puertos activos abiertos que actúan como servicios a las órdenes del atacante que actúa desde el otro lado de la red como un cliente de ese servicio.
- **Spyware.** Es un software que se infiltra en el sistema con objeto de espiar las actividades de los usuarios, lo que constituye una información muy valiosa para el atacante. Un caso especial de spyware son los keyloggers que son aplicaciones que recogen las pulsaciones en el teclado del usuario y las envía a un receptor situado en el exterior del sistema.
- **Adware.** Integra publicidad no deseada en las aplicaciones de los usuarios.
- **Spam.** Consiste en la recepción masiva de correo electrónico no deseado.

El malware establece su objetivo de ataque en el sistema en algunos lugares especialmente vulnerables (targets de ataque). Por ejemplo, en el sector de arranque de los discos de arranque del sistema o en los dispositivos extraíbles, en la shell o procesador de comandos del sistema, en las aplicaciones y utilidades y en los servicios residentes en memoria.

Las vulnerabilidades más buscadas por el malware son las que permiten escalar privilegios, las que permiten un ataque de denegación de servicio (DOS, Denial of Service) y las que otorgan privilegios de Administrador o root. Estas vulnerabilidades pueden originarse tanto en el sistema operativo como el software de aplicación.

El atacante explota la vulnerabilidad mediante un exploit. La mayor parte de los troyanos y otros malware generan vulnerabilidades en los sistemas por lo que incrementan los riesgos de ataque del sistema desde el exterior, con independencia de los daños que puedan causar sus propias actividades maliciosas.

2.2.5. SEGURIDAD EN LA CONEXIÓN DE REDES PÚBLICAS

Cuando un equipo realiza una conexión a una red pública aumenta el riesgo debido a que, aunque las vulnerabilidades permanecen inalteradas por el hecho de realizar la conexión, se incrementan notablemente las amenazas por el inmenso número de posibles atacantes.

- Los riesgos más comunes en las conexiones de redes públicas son los siguientes:
- El cortafuegos podría no estar configurado correctamente o puede que no proporcione suficiente protección.
- Las transmisiones de información sobre seguridad (nombres de usuarios y sus contraseñas) en texto plano (no cifrado).
- Las conexiones telnet o ftp, que no son cifradas.
- Los hackers pueden obtener información sensible en los foros, newsgroups, mailing-lists, etc.
- Sesiones abiertas en servidores de chat (IRC).
- Ataques de denegación de servicio.

Estos riesgos se atenúan integrando en el plan de seguridad contramedidas como las que se describen seguidamente y que se irán estudiando paulatinamente a lo largo de este libro.

- Disponer de un antivirus de calidad y actualizado. En servidores deben instalarse antivirus con varios motores de análisis.
- Tener siempre activado y bien configurado el cortafuegos.
- Integrar el antivirus en una suite de seguridad que provea otros servicios de seguridad como antiphishing, antispam y detección de vulnerabilidades.
- Proteger las conexiones mediante cifrado. Por ejemplo, utilizando IPSec, sustituyendo http por https o smtp por smtps.
- Utilización de redes privadas virtuales VPN.
- Validar las conexiones remotas realizadas mediante robustos sistemas de autenticación.

2.2.6. ESTRATEGIAS DE DEFENSA

Conviene conocer las técnicas de hacking para descubrir de qué amenazas hay que defenderse aglutinando una buena estrategia de defensa en profundidad. Las técnicas de hacking usuales incluyen la recolección y eliminación de huellas del ataque, el robo de información, el escaneo y análisis posterior de información robada, el escalado de privilegios, y la instalación de puertas traseras u otros tipos de malware.

Para cada vulnerabilidad susceptible de ataque se tendrá que adoptar una contramedida. Algunas de ellas son generales porque defienden de muchos posibles ataques, pero otras son muy específicas de cada ataque o del sistema sobre el que se aplican.

Estrategias de defensa por contramedidas generales

- Deshabilitar todos los servicios que no se usan ni se necesitan. Si se pueden desinstalar, mejor aún que deshabilitar.
- Utilizar una buena combinación de firewall y proxy.
- Permanecer constantemente informados de las últimas vulnerabilidades descubiertas sobre el software instalado, tanto de sistemas como de aplicación.
- Aplicar los parches y actualizaciones a las vulnerabilidades y agujeros de seguridad tan pronto como sea posible.
- Tener siempre instalado, activo y actualizado el antivirus o la suite de seguridad. ● Mantener una coherencia interna entre las distintas políticas de seguridad adoptadas, de modo que sean suficientes y no contradictorias.
- Realizar permanentemente tanto auditorías internas como test de penetración de intrusos.
- Adoptar una buena política de gestión de contraseñas.
- Llevar una eficiente política de copias de seguridad, comprobando la integridad de las copias y probando periódicamente los procedimientos de restauración.
- Controlar periódicamente los ficheros de log.
- Migrar los concentradores (hubs) a conmutadores (switches), para conseguir que el tráfico en cada puerto de red sea selectivo, lo que evita las escuchas no autorizadas. ● Usar protocolos cifrados en sustitución de los no cifrados, por ejemplo, utilizar ssh en vez de telnet.

Truco

Una buena forma de estar informados sobre vulnerabilidades es suscribirse a listas de correo sobre el tema, por ejemplo, la que se encuentra en www.securityfocus.com.

Contramedidas específicas para entornos GNU/Linux

- Seguir las sugerencias de los portales de seguridad para Linux.
- Utilizar herramientas como Nessus y COPS con cierta frecuencia para evaluar los niveles de seguridad de los sistemas.
- Como GNU/Linux es de código libre, hay mucha información publicada muy exhaustiva sobre seguridad en libros, artículos, blogs, etc., que debe ser conocida por los administradores de seguridad de estos sistemas para aplicar las soluciones que crean convenientes.

Contramedidas específicas para entornos Microsoft

Bloquear el acceso los puertos 135-139 tanto para TCP como para UDP, por los que Windows pone a escuchar a algunos servicios susceptibles de ataque.

- Desactivar el acceso anónimo deshabilitando la cuenta de invitado (Guest, en Inglés). ● Aplicar los service packs y cualquier parche recomendado por los boletines de seguridad de Microsoft.
- Renombrar la cuenta de Administrador (Administrator, en lengua inglesa) para que un posible atacante no conozca cuál es su nuevo identificador.
- Habilitar la encriptación de la SAM con SYSKEY.

2.3. SEGURIDAD EN LA RED CORPORATIVA

Asegurar un equipo es un logro importante que contribuye enormemente a la seguridad de una organización, pero no es suficiente. Los sistemas informáticos, cada vez más, son distribuidos de modo que las aplicaciones se encuentran repartidas entre varios sistemas conectados en red. Por tanto, la seguridad debe extenderse también a los protocolos de red y a los procedimientos de interconexión e intercambio de datos. Esto hace que haya elementos de seguridad específicos cuando se trata de proteger la red corporativa.

2.3.1 . LA SEGURIDAD Y LAS VULNERABILIDADES EN REDES TCP/IP

Las amenazas más frecuentes sobre los recursos de comunicaciones se agrupan en los siguientes cuatro tipos (ver figura):

- **Interrupción.** Integra los ataques de denegación de servicio, lo que produce una falta de disponibilidad.
- **Interceptación.** El atacante consigue hacer una copia de la información a la que no debería tener acceso, lo que produce falta de privacidad.
- **Modificación.** Una vez interceptado el mensaje, este puede ser modificado y reenviado al receptor suplantando al mensaje original, lo que ataca a la integridad,
- **Generación, creación o fabricación.** El atacante fabrica un mensaje que envía al receptor suplantándole, lo que agrede la autenticidad.

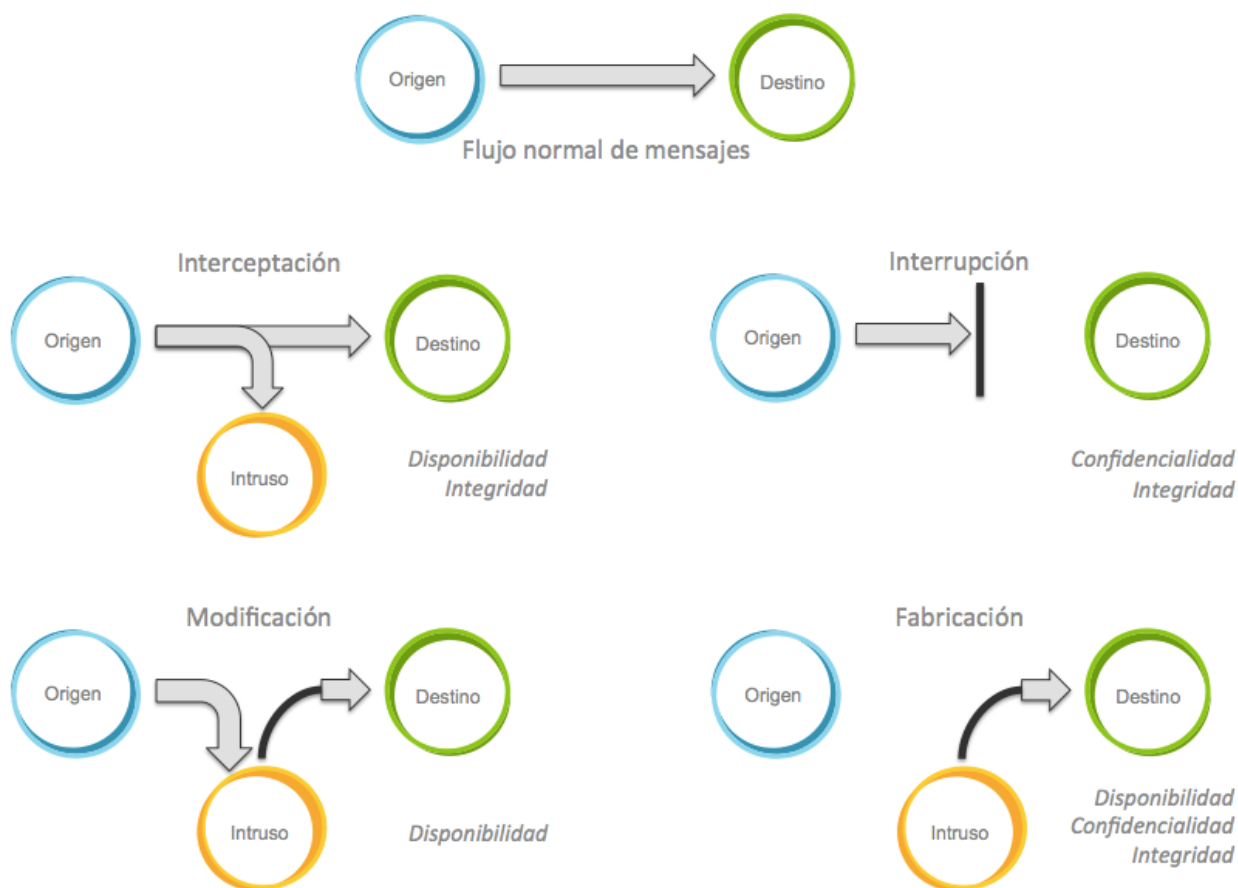


Figura: . Representación gráfica de las amenazas sobre los recursos de comunicaciones.

Vulnerabilidades de la capa de Red TCP/IP (niveles 1 y 2 de OSI)

En el nivel físico, la primera vulnerabilidad es la posibilidad de acceso físico al cuarto de telecomunicaciones, al cableado o a los equipos que intervienen en la comunicación, por ejemplo, ataques sobre los cables de datos, desvío del cableado o interceptación de las comunicaciones, lo que genera problemas asociados a la confidencialidad y al control de acceso.

Para asegurar la capa de Red se tiene que considerar:

- La confidencialidad: los datos solo han de estar disponibles para las personas autorizadas.
- La autenticidad: debe verificarse la identidad digital de los agentes.
- La integridad: debe comprobarse la exactitud de la información frente a alteraciones, pérdidas o destrucción de datos.

Por tanto, se generan problemas de suplantación de mensajes y de direcciones físicas, alteración del control de acceso al medio mediante sniffers no autorizados y posibilidad de ataque mediante exploits contra los adaptadores de red.

Vulnerabilidades de la capa de Internet TCP/IP (nivel 3 de OSI)

El principal problema en este nivel es el de las escuchas no autorizadas de paquetes de nivel 3 (paquetes IP).

Un segundo problema es el de la suplantación de direcciones IP, ya que IP carece de posibilidades de autenticación: para hacerlo requiere el concurso de protocolos de otras capas. Esto permite que se puedan robar sesiones de nivel superior, como TCP.

Un tercer ataque reside en el envenenamiento de las tablas de caché de ARP, que permiten la suplantación de las direcciones MAC utilizadas en el nivel 2.

Vulnerabilidades de la capa de Transporte TCP/IP (nivel 4 de OSI)

Los principales problemas en este nivel se asocian con la búsqueda e interceptación de puertos TCP y UDP.

La apertura de puertos indiscriminada o su falta de protección en el cortafuegos corporativo también puede producir la delación de los servicios ofrecidos que quedarán más expuestos al hacerlos públicos. La búsqueda de puertos abiertos suele hacerse mediante utilidades de escaneo de la red.

Aunque estos servicios estén protegidos mediante un mecanismo de autenticación, al hacerlos públicos, se prestan a ataques de fuerza bruta.

Vulnerabilidades de la capa de Aplicación TCP/IP (niveles 5 a 7 de OSI)

Los niveles superiores se prestan a problemas asociados a los servicios de red y a la autenticación de datos, por lo que su protección también exige herramientas de muy alto nivel. Entre los problemas más comunes se encuentran los siguientes:

- Deficiencias en el servicio de nombres de dominio.
- Envenenamiento de las cachés del DNS.
- Suplantación del servidor DNS.
- Inseguridad de protocolos no cifrados que transportan contraseñas, como telnet o ftp.
- Vulnerabilidades específicas del protocolo http, asociadas a la construcción de los URL, por ejemplo en los ataques de inyección de código.

2.3.2. EL ATAQUE A UNA RED TCP/IP

Se describen a continuación algunas características específicas de algunos de los ataques más comunes en redes TCP/IP.

Ataque de ingeniería social, web y whois

Un ataque de ingeniería social consiste en persuadir veladamente a los usuarios para que ejecuten acciones o revelen la información que el atacante necesita para comprometer la red. Sutilmente, el atacante puede deducir información sobre el acceso del usuario del target mediante la utilización de fechas, aniversarios, nombres de personas, etc. Por eso, estos elementos nunca deben constituirse o formar parte de contraseñas.

El análisis de una sede web puede proporcionar también mucha información a un atacante: direcciones de correo, organización corporativa, etc. El servicio whois también puede proporcionar información valiosa para el atacante (ver figura).




Whois Record for Marca.es	
Domain Profile	
Registrar Status	taken
Name Servers	DNS01.ELMUNDO.ES (has 166 domains) DNS02.ELMUNDO.ES (has 166 domains) NS.EL-MUNDO.NET (has 76 domains) NS.ELMUNDO.ES (has 166 domains)
Tech Contact	—
IP Address	193.110.128.199 - 23 other sites hosted on this server
IP Location	 - Madrid - Madrid - Unidad Editorial S.a.
ASN	 AS9052 Unidad Editorial, ES (registered Nov 06, 1998)
Website	
Website Title	 500 SSL negotiation failed:
Response Code	500
Terms	1,550 (Unique: 780, Linked: 990)
Images	61 (Alt tags missing: 2)
Links	257 (Internal: 251, Outbound: 5)
Whois Record (last updated on 2021-11-25)	
<pre>% NOTE: The registry for this domain name does not publish ownership % records (whois records) in the standard format. This data % represents the most likely status of the domain based on % information provided by the Internet's domain name servers (DNS) . domain: marca.es status: taken nameserver: dns01.elmundo.es nameserver: dns02.elmundo.es nameserver: ns.el-mundo.net nameserver: ns.elmundo.es % For more information, please visit http://www.nic.es/</pre>	

Figura: Información proporcionada por un servidor whois. <https://whois.domaintools.com>

Actividad

En la dirección <http://emailextractorpro.com/> puedes descargar Free Email Extractor, que es una aplicación gratuita para explorar información que reside en la web. Descárgalo y trata de obtener direcciones de correo electrónico que estén publicadas en la sede web de algunas organizaciones,

Por ejemplo, en la figura vemos la ejecución de un informe sobre la página web www.marca.es. El informe nos proporciona abundante información sobre la salud de la sede web: información que puede ser aprovechada por un hacker para diseñar la arquitectura de su ataque.

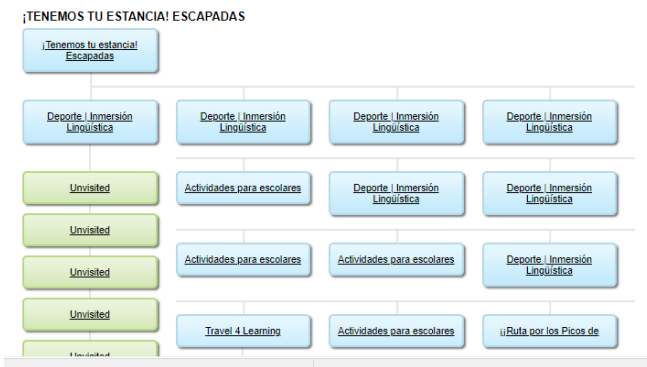
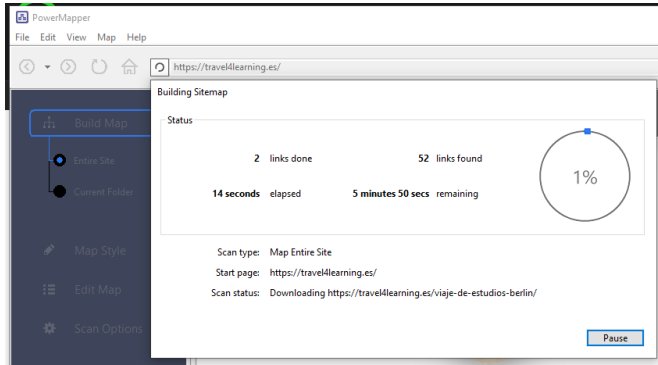


Figura: Búsqueda de vulnerabilidades y cumplimiento de estándares para una página web desde el webspider Powermapper.

Ataques de denegación de servicio

El objetivo principal de un ataque de denegación de servicio (DOS, Denial of Service) es impedir el uso legítimo del sistema atacado por parte de los usuarios autorizados. Suele producirse porque el atacante provoca un excesivo consumo de recursos del servidor, que impide que estos recursos lleguen a los usuarios legítimos (ver en la figura, a la izquierda).

Zombies

Atacado



Atacante

Usuario Normal

Figura. Representación de un ataque DDoS

Frecuentemente, el atacante no se esconde detrás de un único sistema, sino de detrás de toda una red de atacantes (botnet o red zombie) compuesta de sistemas infectados con troyanos especializados en el ataque y coordinados por el hacker que los dirige. En este caso, el ataque se denomina DDoS (Distributed Denial of Service) o ataque de denegación de servicio distribuido .

La defensa de un ataque DOS se realiza bloqueando la dirección IP del atacante, de modo que este no consuma recursos (ver en la figura, a la derecha). En el ataque DDoS esto ya no es tan fácil puesto que el número de sistemas que atacan simultáneamente es innumerable.

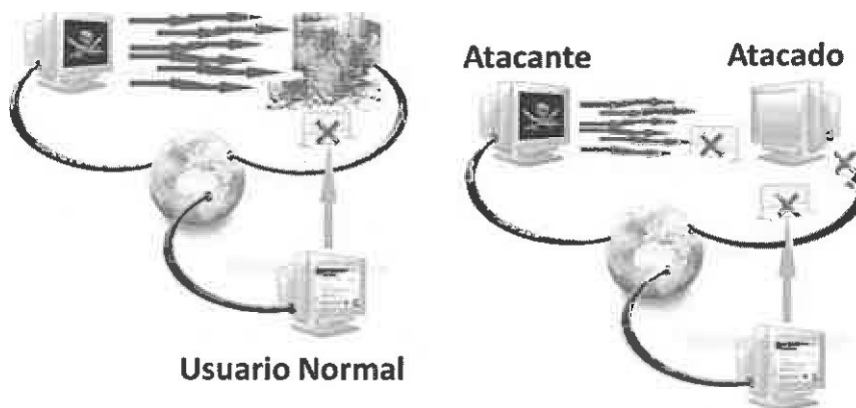


Figura: A la izquierda, ataque DOS. A la derecha, defensa contra un ataque DOS.

Un administrador de sistemas no debe concederle demasiada importancia a un ataque DOS puesto que su defensa no es complicada, pero debe temer mucho a los de DDoS pues la defensa contra ellos se organiza de acuerdo con su naturaleza, por ello conviene conocer cómo operan. Fundamentalmente los hay de tres tipos:

- **Net Flood.** Este ataque degrada la conectividad de una red mediante la saturación de sus enlaces de comunicación. Se organizan ataques masivos desde diferentes puntos de la red mediante zombies. Con la tecnología actual, contra este ataque se puede hacer muy poco.
- **Connection Flood.** Todo servicio de red orientado a la conexión tiene un límite máximo en el número de conexiones simultáneas que soporta. Cuando este número es alcanzado ya no se admitirán nuevas conexiones. Por tanto, el atacante intentará agotar con conexiones ilegítimas este máximo. Las conexiones TCP/IP se realizan mediante tres pasos, que en este caso se completan perfectamente, lo que proporciona a la máquina atacada la información de la identidad real del atacante. Esta información puede ser pasada al cortafuegos para que bloquee estas conexiones, sobre todo si el número de atacantes no es demasiado grande.
- **Syn Flood.** Se basa en la regla de conexión en tres pasos (handshake) para las conexiones TCP/IP. Si el paso final no llega a realizarse, la conexión queda en estado de semiabierto. El ataque consiste en agotar los recursos del sistema atacado mediante conexiones semiabierto. Si el sistema está actualizado, este ataque no suele suponer un problema significativo.

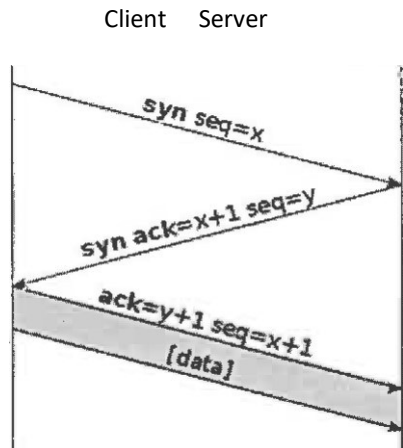


Figura: Creación de una conexión TCP con un handshake de tres pasos.

Comentario de figura:

El handshake de tres pasos consiste en que el cliente envía un paquete SYN hacia el servidor, quien le contesta con un acuse de recibo. Esto deja la conexión semiabierta, consumiendo recursos en el servidor. Una vez recibido en cliente el acuse de recibo (SYN ACK) el cliente valida la apertura de conexión en el servidor enviándole un ACK de respuesta. En este momento el servidor termina la apertura de conexión. A partir de este instante, cliente y servidor podrán intercambiar datos.

Cracking de contraseñas, mail bombing y spamming

Es el proceso por el que se descubre la contraseña de un usuario en un sistema atacado. El atacante tendrá mucho interés en que ese usuario precisamente sea privilegiado, típicamente Administrador o root. Esta es la razón por la que deshabilitar o renombrar estas cuentas levantará una barrera más al atacante, que tendrá que descubrir no solo la contraseña sino el identificador de la cuenta privilegiada.

Hay dos métodos fundamentales para el crackeo de contraseñas:

- **Ataque por diccionario.** Consiste en efectuar un ataque ordenado utilizando palabras de un diccionario hasta encontrar la contraseña buscada, lo que exige que esta esté contenida en el diccionario. Impidiendo que las contraseñas estén en cualquier diccionario, derribaremos el éxito de este ataque.
- **Ataque por fuerza bruta.** Se trata de realizar todas las combinaciones posibles de un conjunto de caracteres y de una longitud máxima, confiando en que la contraseña buscada se halle en alguna de estas combinaciones. Este ataque se dificulta en la medida en que se exija que las contraseñas sean suficientemente largas y tengan una gran variedad de símbolos (letras mayúsculas y minúsculas, números y caracteres especiales).
- Ejemplo
- Supongamos un sistema que es capaz de probar 100.000 claves por segundo. La figura muestra los tiempos necesarios para crackear la contraseña mediante fuerza bruta con este sistema en función de la longitud de la contraseña y del número de símbolos posibles para cada carácter

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

El ataque de **mail bombing** consiste en enviar muchas veces el mismo mensaje a un usuario provocando ataques DOS por desbordamiento del buzón. En cambio, el ataque de **mail spamming** se orienta a enviar mensajes no deseados a muchos buzones distintos, provocando no solo la pérdida de recursos en los buzones de destino sino también problemas en el servidor de correo que emite los mensajes.

Por tanto, el elemento más perjudicado con mail bombing es el cliente mientras que en el caso de mail spamming el más perjudicado es el servidor, aunque no sea este el objetivo primordial del spammer.

Escaneo de puertos y sniffers

El escaneo de puertos es un procedimiento ampliamente utilizado por los hackers para averiguar qué puertos están abiertos en el target objetivo de su ataque. Una vez conocidos los puertos abiertos, el hacker intentará buscar vulnerabilidades en los servicios que se hallan detrás de los puertos abiertos. Esta es la razón por la que conviene tener el sistema y las aplicaciones actualizadas y que, por tanto, tengan sus vulnerabilidades conocidas corregidas.

Algunos cortafuegos detectan las actividades de rastreo de los escáneres de puertos. Los cortafuegos más avanzados pueden, incluso, presentar resultados ficticios al escáner de puertos, de modo que este confunda al hacker que lo emplea.

Los sniffers o escuchadores de red operan activando la interfaz de red del sistema sobre el que se ejecutan en modo promiscuo. En este modo de configuración de la tarjeta de red, el sniffer almacenará en un fichero de log todo el tráfico que circule por el punto de red en el que se conecta el adaptador, sea él o no el destinatario del tráfico.

La utilización de un sniffer permite la obtención de una gran cantidad de Información sensible enviada sin cifrar: nombres de usuario, contraseñas, direcciones de correo electrónico, etc. El análisis de la información

transmitida permite a su vez extraer relaciones entre los equipos y así poder intuir una posible topología de la red, lo que es una información muy relevante para el atacante.

La condición necesaria para que un sniffer pueda recoger un tráfico amplio y variado es que este pase por el puerto de red del sistema en que se ejecute. Esto no ocurre en redes conmutadas ya que estas solo hacen pasar por el puerto el tráfico con origen y destino en el sistema. Sin embargo, si en vez de conmutadores se utilizan hubs, que son repetidores multipuertos, todos los puertos reciben todo el tráfico. Esta es la razón de que los hubs sean mucho más inseguros que los switches.

En el caso de las redes conmutadas, los switches suelen implementar una función de mirroring entre puertos por la que el tráfico destinado o con origen en un puerto concreto es copiado también a otro en el que se conecta el sniffer, de este modo el escuchador puede recoger el tráfico de la red por ese puerto.

Desbordamiento de buffer

Un desbordamiento de buffer (buffer overflow) aprovecha algunos errores de programación de una aplicación para alterar el funcionamiento de la pila de un proceso. Los desbordamientos se pueden producir por múltiples causas, los más conocidos son:

- **Overflow por combinaciones no esperadas.** Los programas suelen construirse formando capas de código que se instalan jerárquicamente encima del sistema operativo. Un mal diseño de una de las capas puede causar que entradas pertenecientes a una capa superior sea enviada directamente al sistema operativo y ejecutado de manera descontrolada.
- **Overflow por entrada anormal.** Los programas suelen utilizar parámetros o valores suministrados como entradas válidas. Si el programador no valida correctamente la entrada del usuario, se pueden producir daños en los datos que maneja la aplicación.
- **Overflow por concurrencia.** En este caso, dos o más procesos leen o escriben en un área de memoria compartida entre ambos, pero si no se tiene control, el resultado final dependerá de la secuencia temporal de ejecución de uno y otro proceso. En estos casos, la programación debe arbitrar estos accesos mediante semáforos.

Ataques internos en LAN conmutadas

En el caso de redes conmutadas los hackers disponen de unos ataques específicos que explotan vulnerabilidades relacionadas con las tecnologías de conmutación incorporadas en los switches.

- **Inundación de direcciones MAC (flooding).** El ataque intenta producir una sobrecarga de la tabla CAM (Content Addressable Memory) del conmutador hasta que produce su desbordamiento. Como esta tabla es la que consulta el conmutador para derivar cada paquete a su destino, una vez desbordada se producirá una denegación de servicio.
- **IRDP spoofing.** IRDP (ICMP Router Discovery Protocol) es un protocolo que extiende ICMP para que pueda descubrir enrutadores en el entorno de red. Con este ataque, el hacker simula ser un router, por lo que a partir de ese momento recibe un tratamiento como tal, lo que le proporciona amplias ventajas.
- **ARP poisoning.** Es un ataque de envenenamiento de la tabla ARP utilizada por los equipos para la resolución de direcciones IP en direcciones MAC.

Ejemplo: envenenamiento ARP

El atacante utilizará alguna herramienta como Caín, Ettercap, Nemesis o similares para realizar un ARP poisoning (también llamado AR_P spoofing) en una red conmutada. Este tipo de ataque no suele realizarse en redes de hubs, ya que en estas redes todos los sistemas escuchan todo el tráfico de la red y el sistema atacado se daría cuenta del ataque.

El atacante envenenará las tablas ARP de las víctimas enviando mensajes ARP engañándoles.

Por ejemplo, imaginemos que originalmente tenemos un sistema atacante y dos objetivos con direcciones IP y MAC siguientes:

Atacante: IP=10.0.0.5 MAC= AA:AA:AA:BB:BB:BB

Objetivo1: IP=10.0.0.1 MAC= CA:FE: CA:FE:CA:FE

Objetivo02: IP=10.0.0.1, MAC= CA:FE::FE:CA:CA:FE

El atacante, mediante paquetes ARP intentará modificar las tablas ARP de estos objetivos. Para ello, enviará paquetes a los objetivos con la siguiente información:

- Para la tabla de Objetivo 1 : Asociar 10.0.0.2 (IP de Objetivo 2) con la MAC .AA:AA:AA:BB:BB:BB (la del atacante).

Para la tabla de Objetivo 2: Asociar 10.0.0.1 (IP de Objetivo 1) con la MAC AA:AA:AA:BB:BB:BB .(la del atacante).

De este modo, si Objetivo1 quiere enviar un paquete a Objetivo02, confeccionará tramas con destino en AA:AA:AA:BB:BB:BB .que es el atacante, quien registrará el tráfico, De modo análogo, si Objetivo02 envía datos a Objetivo], también capturará su tráfico. Se ve fácilmente que el atacante ha podido capturar toda la secuencia de diálogo de red entre los dos objetivos,

En este ejemplo, se han producido dos ataques: uno de envenenamiento de tablas de AR_P, que es inocuo; pero sobre él se ha producido un ataque Man-In-The-Middle porque se ha derivado todo el tráfico a un tercer agente (el atacante) sin advertencia de los objetivos .

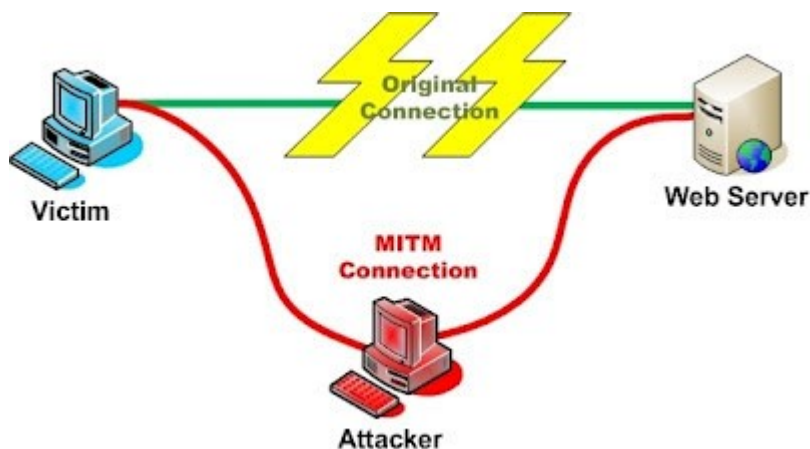


Figura: Arquitectura de un ataque MITM (Man-In-The-Middle).

En general, en función de las arquitecturas de red, se pueden utilizar unos ataques u otros. En Internet se puede conseguir abundante información sobre cada uno de ellos. Las dimensiones de este libro impiden detenernos en cada uno de ellos. Enumeramos aquí algunos de ellos para diversos escenarios y lo hacemos en inglés para facilitar mejor las voces de búsqueda:

Dentro de la LAN: ARP poisoning, DNS spoofing, STP mangling, Port stealing. ● En la red remota: DNS poisoning, Traffic tunneling, Route mangling.

Desde la LAN a una red remota a través de un gateway. ARP poisoning, DNS spoofing, DHCP spoofing, ICMP redirection, IRDP spoofing, Route mangling.

2.3.3. RIESGOS POTENCIALES EN LOS SERVICIOS DE RED

Los clientes consumen los recursos de red en forma de servicios. Cada servicio lleva asociado un software que le proporciona soporte sobre el sistema operativo, por tanto, las vulnerabilidades de ese software pueden producir riesgos para ese servicio de red. Por otra parte, si el servicio no está correctamente configurado puede dejar abiertas posibilidades al atacante. Otros posibles problemas pueden venir de la apertura de puertos TCP o UDP no controladas, por los servicios de red gestionados mediante puertas traseras o por otro malware.

Para hacer que un sistema sea más seguro hay que tender a que exhiba la "mínima superficie de exposición", que es un concepto que se acuña para describir que solo se deben instalar los servicios que realmente se utilicen. Ninguno más. Por ejemplo:

- En el cortafuegos solo deben estar abiertos los puertos de los servicios que estén activos.
- Solo deben activarse los servicios estrictamente necesarios.
- Únicamente deben instalarse los servicios que vayan a ser activados.
- Si hay posibilidad de elegir, es mejor utilizar un protocolo cifrado que su equivalente no cifrado.
- Si se puede elegir y el servicio se presta a ello, es mejor utilizar un protocolo autenticado que otro que no admita autenticación.

Los puertos de los servicios de red

En IPv4 un puerto se expresa con 16 bits por lo que solo es posible gestionar $2^{16}=65.536$ puertos, que se clasifican del siguiente modo:

- **Puerto 0.** Es un puerto reservado, aunque permitido si el emisor no admite respuestas del receptor, por lo que **no suele utilizarse**.
- **Puertos 1 a 1.023.** Son los llamados puertos **bien conocidos** porque son utilizados por los protocolos de aplicación más comunes en Internet. Para ser enlazados con un servicio se requieren permisos de superusuario, por lo que son puertos que suelen estar más protegidos de manera natural.
- **Puertos 1.024 a 49.151.** Son los llamados puertos **registrados**, que son de libre utilización por cualquier usuario del sistema. Por tanto, son puertos desprotegidos.
- **Puertos 49.152 a 65.535.** Son los llamados puertos efímeros o **temporales**, que son utilizados dinámicamente por las aplicaciones clientes de la red en sus conexiones a servidores.

En la página https://es.wikipedia.org/wiki/Anexo:Puertos_de_red se encuentran descritos los servicios habituales ofrecidos por cada uno de estos puertos.

Apertura de puertos de red

¿Qué significa la apertura de un puerto de red? La respuesta depende del escenario al que se aplique. En un sistema, abrir un puerto significa autorizar al cortafuegos para permitir las comunicaciones por ese puerto, tras el cual debe activarse un servicio que atienda las peticiones que los clientes de ese servicio hagan por ese puerto desde el exterior a través del cortafuegos..

Sin embargo, en el caso de un router, abrir un puerto significa redirigir el tráfico entrante por ese puerto hacia un destino caracterizado por su IP (función de encaminamiento) y por el mismo u otro puerto de destino (función de traducción de puertos, protocolo PAT). Esta redirección (también denominada publicación de puerto) solo puede hacerse hacia un único destino: no es posible la redirección desde un puerto a varios puertos.

Abrir un puerto conlleva riesgos. Si no se quieren asumir riesgos no hay que abrir puertos, pero entonces no se pueden proporcionar servicios, por lo que hay que llegar a una solución de compromiso de mínima exposición pero que permita proporcionar los servicios necesarios a la red.

Algunos riesgos asociados a la apertura de puertos son:

- Si el puerto es atendido por una aplicación y esta debe estar instalada en múltiples clientes, el router debe abrir un puerto por cada uno de los clientes, lo que multiplica los riesgos de ataque en el router. Por ejemplo, un router publica al exterior varios servidores web internos, lo que requiere un puerto en el router por cada web. Hay que asegurarse de que el puerto queda operativo tanto en el router como en el cortafuegos: de nada sirve asignar un puerto en el router si luego lo cierra el cortafuegos.
- Se pueden presentar problemas de asignación de puertos cuando los sistemas están configurados para aceptar direcciones IP procedentes de servidores DHCP, si estos sistemas tienen que publicar servicios en el router ya que la IP puede variar y no habrá manera de realizar asociaciones IP-puerto estables. Por ello, es recomendable utilizar IP estáticas en los sistemas que publican servicios. Por otro lado, en el router conviene diferenciar las reglas correspondientes a IP estáticas de las que controlan IP dinámicas.
- Los routers deben vigilarse para comprobar los puertos que están abiertos permanentemente. Por ejemplo, se podría comprobar que no se tienen abiertos permanentemente los puertos utilizados por el malware. En <http://www.adslzone.net/lista-de-puertos-troyanos.html> se puede encontrar un listado de los puertos utilizados por los troyanos más comunes.

Se pueden encontrar muchas aplicaciones online en Internet para escanear los puertos de los sistemas de red expuestos en Internet, por ejemplo, en <http://www.internautas.org/wscanonline.php>.

2.4. PROTOCOLOS DE SEGURIDAD

En general son protocolos que introducen una capa de seguridad en la pila de protocolos tradicionales para conseguir mejorar la gestión del riesgo. Algunos son muy fáciles de gestionar, pero otros requieren disponer de arquitecturas específicas para explotar su funcionalidad. Por ejemplo, con este tipo de protocolos podemos crear túneles cifrados, penetrar cortafuegos mediante port forwarding, codificar mensajes, utilizar técnicas de criptografía, etc.

SCP y SFTP

SCP (Secure CoPy) es una extensión de OpenSSH, una suite de utilidades seguras, que permite copiar ficheros con seguridad entre dispositivos de red que tienen instalado un servidor SSH, que es otro de los componentes de OpenSSH. Por ejemplo, para copiar un fichero desde un sitio remoto a uno local se podría ejecutar la orden

```
scp usuario@host-origen:fichero-origen fichero-destino
```

donde cada elemento es descriptivo de lo que significa.

SFTP (Secure FTP) es semejante a FTP pero utiliza conexiones seguras utilizando SSH como túnel de seguridad. De esta manera, se puede utilizar la tecnología FTP sin los inconvenientes de seguridad de la falta de cifrado: la capa de cifrado la pone SSH, que actúa desde dentro de SFTP

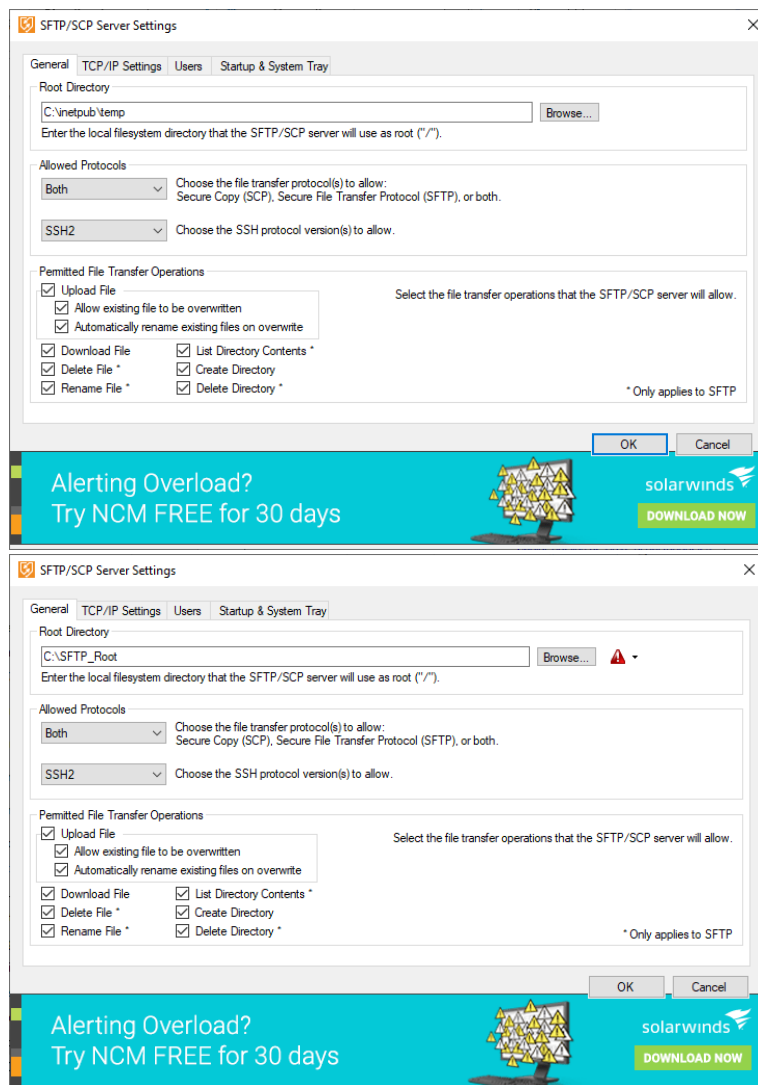
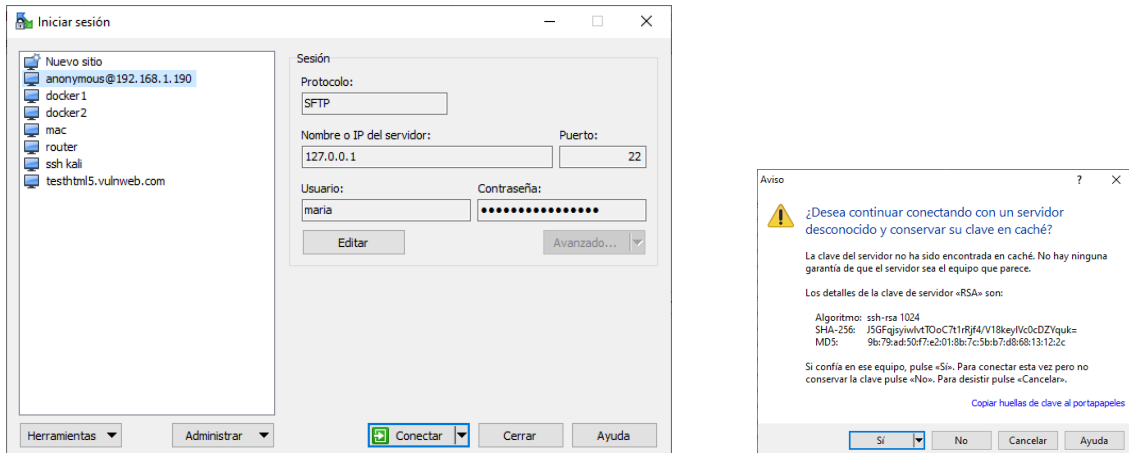


Figura. Configuración de un servidor SFTP/SCP de SolarWinds.

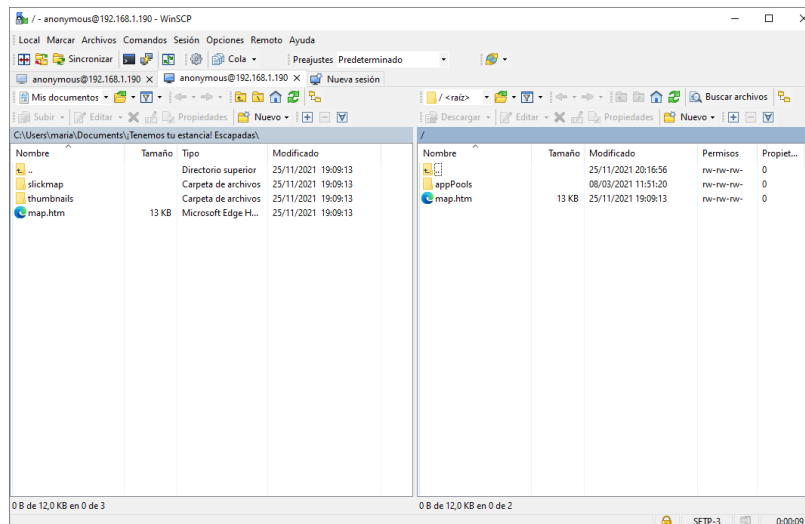
SCP y SFTP son herramientas cliente/servidor. Por tanto, los clientes SCP y SFTP requieren que los servidores a los que se conectan provean los servicios homólogos. Los sistemas operativos GNU/Linux proveen estos servicios de manera nativa (o través de OpenSSH o paquetes similares). Windows no provee estos servicios, aunque existen distribuidores de software que proveen estos servicios para su instalación sobre sistemas Windows.

En la figura se puede ver la configuración y el acceso a un servidor mediante SCP utilizando WinSCP una herramienta cliente open source para Windows. Como se puede apreciar, una vez realizada la conexión, la aplicación presenta dos ventanas: una de las cuales representa el sistema de ficheros local y la otra el sistema



de ficheros remoto.

Figura: Configuración y conexión de una sesión con WinSCP sobre Windows.



2.4. SEGURIDAD Y MONITORIZACIÓN

En este epígrafe nos centraremos en el ataque y su defensa. Tendremos que ponemos en las circunstancias tanto del atacante para radiografiar el ataque como en las del administrador de seguridad para prevenir o paliar el ataque.

La mayor parte de los conocimientos necesarios para desarrollar esta sección ya son conocidos de epígrafes anteriores: aquí solo haremos un uso coordinado de ellos.

2.4.1. HERRAMIENTAS PREVENTIVAS Y PALIATIVAS

Ya se ha estudiado anteriormente cómo entre las amenazas más comunes están las escuchas secretas (espionaje o eavesdropping) mediante sniffers, accesos no autorizados o ataques de denegación de servicio, tanto en su versión simple DOS como en su versión distribuida DDoS.

Lo que se hace común a todas ellas, desde el punto de vista del atacante, son las fases que este sigue ordenadamente para perpetrar el ataque informático a una organización.

Fase de investigación

Antes de realizar un ataque, el intruso estudiará profundamente su objetivo. Este estudio dará como resultado:

- Información de la empresa objetivo.
- Información del dominio objetivo: conociendo el nombre de la empresa se puede obtener su información de dominio a través de consultas tipo WHOIS.
- Información de los servidores: una vez que el intruso obtuvo el dominio, puede realizar consultas NSLOOKUP para conocer cuáles son los servidores que tiene la empresa.
- Identificación de la plataforma: uno de los principales datos que buscan de sus objetivos es la plataforma sobre la que trabajan (Windows, Linux, UNIX). Esto se puede realizar mediante la utilización de técnicas de OS fingerprint.

Identificación de los servicios: otra información importante que buscan obtener los atacantes son los servicios que ofrecen los servidores-objetivo. Esto se puede realizar mediante escaneadores de puertos (pofl-scanners)..

Algunas contramedidas útiles en la fase de investigación el ataque son restringir la información que se difundirá a través de los servicios DNS y whois. También se puede activar el filtrado de paquetes para evitar la detección de la plataforma atacada y de los servicios que provee. Un buen IDS también podría detectar cuándo se está produciendo un escaneo de puertos para alertar al administrador.

Fase de penetración

En esta fase el atacante intentará acceder al objetivo. Para dar este paso, utilizan diferentes técnicas:

- Explotación de vulnerabilidades: buscará algún producto instalado que permita la ejecución de código arbitrario.
- Exploración de la eventual debilidad de contraseñas: una contraseña débil puede permitir el ingreso de intrusos.
- Búsqueda de servicios mal configurados: un servicio que no esté adecuadamente configurado puede permitir que intrusos hagan uso abusivo del mismo, o incluso, que ejecuten código arbitrario.

Algunas contramedidas útiles en la fase de penetración serían la revisión de los ficheros de logs del filtrado de paquetes, la permanente actualización del software para subsanar las vulnerabilidades cuanto antes y la revisión permanente de la configuración de cada servicio de red, asegurándose de que no hay servicios activados, o mejor aún instalados, que no se utilizan.

Fase de persistencia

Una vez que un atacante ha logrado ingresar a un sistema, generalmente realiza actividades para evitar ser detectado y deja puertas traseras en el sistema para poder mantener un acceso permanente. Para evitar ser detectado, en general un atacante busca los archivos de auditoría o log del sistema, para borrarlos o modificarlos ocultando su acceso y sus actividades.

Para evitar que un intruso elimine los archivos de log, se puede optar por mantenerlos guardados fuera del lugar donde se generan. Es complicado evitar la copia de archivos, pero puede detectarse la modificación de ellos. Existen herramientas que crean un hash de los archivos de sistema, y avisan al administrador en caso de detectar una modificación.

Fase de expansión

Frecuentemente, el objetivo final de un ataque no es el primer sistema atacado, sino que se utilizan varios saltos intermedios para lograr realizar un ataque sin ser rastreados. Esto puede generar que nuestro sistema sea víctima y a la vez sea atacante.

Las contramedidas que impiden la expansión son también el filtrado de paquetes, los sistemas IDS, y el control periódico de los archivos de log.

Logro del objetivo

Llegados a este punto se podría decir que la tarea del intruso ha llegado a su objetivo. A partir de aquí, podemos esperar diferentes acciones por parte del intruso:

- Desaparecer sin dejar rastro.
- Avisar al administrador que se ha ingresado al sistema.
- Comentar los fallos de seguridad encontrados a sus colegas.
- Hacer públicos los fallos de seguridad.

2.4.2. EL ESCALADO DEL ATAQUE

Cuando el atacante tiene comprometido un equipo de la organización, intentará continuar su ataque desde allí para comprometer otros objetivos y adueñarse de toda la organización.

Reconocimiento

Lo primero que hará será un "reconocimiento" de la red, que es intentar un descubrimiento no autorizado de la topología de la red, sus sistemas, servicios y vulnerabilidades. Todo ello realizado desde el primer y, de momento, único sistema comprometido. Para realizar esta operación de reconocimiento dispone de herramientas que ya integran toda la secuencia de pasos: detectan los hosts alcanzables en la red, buscan los servicios y sus vulnerabilidades en cada uno de esos hosts. Por ejemplo, utilizando herramientas como nslookup y whois, un atacante puede determinar también el rango de direcciones IP asignados a una corporación.

La alternativa para evitar el descubrimiento es establecer filtros de tráfico que puedan actuar como barreras que impidan que paquetes ICMP echo puedan proporcionar la información de la fase de descubrimiento de nuevos equipos.

Interceptación o eavesdropping

La interceptación o EAVESDROPPING, es un proceso mediante el cual un agente capta información (en claro o cifrada) que no le iba dirigida. Lo más peligroso del eavesdropping es que resulta muy difícil de detectar mientras se produce.

Un medio de interceptación habitual es el sniffing, que como sabemos consiste en capturar tramas que circulan por la red mediante un software que corre en una máquina conectada al segmento de red. Otro punto a tener en cuenta es la imposibilidad de establecer límites concretos en redes inalámbricas.

Algunas medidas contra la interceptación serían no permitir la existencia de segmentos de red de fácil acceso, utilizar cifrado para realizar las comunicaciones o el almacenamiento de la información, no tener activadas tomas libres de red o realizar autenticación a nivel de la capa de enlace, por ejemplo, en WLAN puede utilizarse la norma IEEE 802.11i, que incluye a la 802.1x que realiza el acceso por puertos.

El ataque por acceso

Un ataque por acceso consiste en que un atacante obtiene los privilegios necesarios para acceder a los dispositivos o recursos de red en forma ilícita. Los métodos más utilizados son:

- **Explotar contraseñas triviales:** aplicar fuerza bruta, diccionarios o herramientas de crack.
- **Explotar servicios mal configurados** como TFTP, FTP anónimo y acceso remoto al registro.
- **Explotar fallas de aplicaciones:** desbordamientos de buffers.
- **Ingeniería social:** engañar a los usuarios con el fin de obtener información.

Algunos ejemplos de ataques por acceso son el ataque Man-in-the-middle, la explotación de las relaciones de confianza, la manipulación de datos, IP spoofing, la repetición de una sesión, los auto-rooters y las puertas traseras.

Ataques en routers y conmutadores

Tanto los switches de nivel 2 como los de nivel 3, así como los routers, tienen algunas consideraciones de seguridad adicionales que deben tenerse en cuenta. En ellos, los ataques más comunes son:

- La sobrecarga en la tabla CAM de los switches.
- El acceso a diferentes VLAN.
- La utilización de STP para modificar el árbol de expansión.
- La falsificación de direcciones MAC.
- La inundación y saturación del servidor DHCP.

2.4.3. EL ATAQUE DE DENEGACIÓN DE SERVICIO

Como ya se ha estudiado, los ataques de DOS intentan afectar negativamente el funcionamiento de un servicio ofrecido por algún sistema o dispositivo de red. Un ataque de DOS exitoso afectará al servicio de modo que lo volverá totalmente inalcanzable. Este tipo de ataques no involucran un acceso al sistema, sino que buscan la degradación del servicio.

Ataque y defensa DOS

Un ataque DOS se puede generar de varias maneras. Por ejemplo, por explotación de errores de las aplicaciones: se envían paquetes malformados que generan una caída de la aplicación, que a partir de ese momento impide el servicio que prestaba. Otro medio de ataque sería utilizando mensajes de control: se envían paquetes con mensajes de control para que los dispositivos interrumpen la operación de red, por ejemplo, ordenando desconexiones. La forma más común de DOS es el ataque por inundación (flooding), que intentará un consumo de recursos inundando al sistema con una gran cantidad de paquetes.

Algunos ataques conocidos que utilizan DOS son el ataque de ping de la muerte, syn flood, land attack y teardrop.

Para defenderse de los ataques DOS por explotación de vulnerabilidades, es aconsejable mantener los sistemas libres de estas vulnerabilidades mediante las últimas actualizaciones.

Para la defensa de ataques de DOS por mensajes de control, será necesaria la creación de filtros de paquetes apropiados.

Para defendernos de los ataques de DOS por inundación se utilizarán IDS (Intrusion Detection Systems). Otra alternativa es restringir la cantidad de conexiones simultáneas que atenderá un servidor.

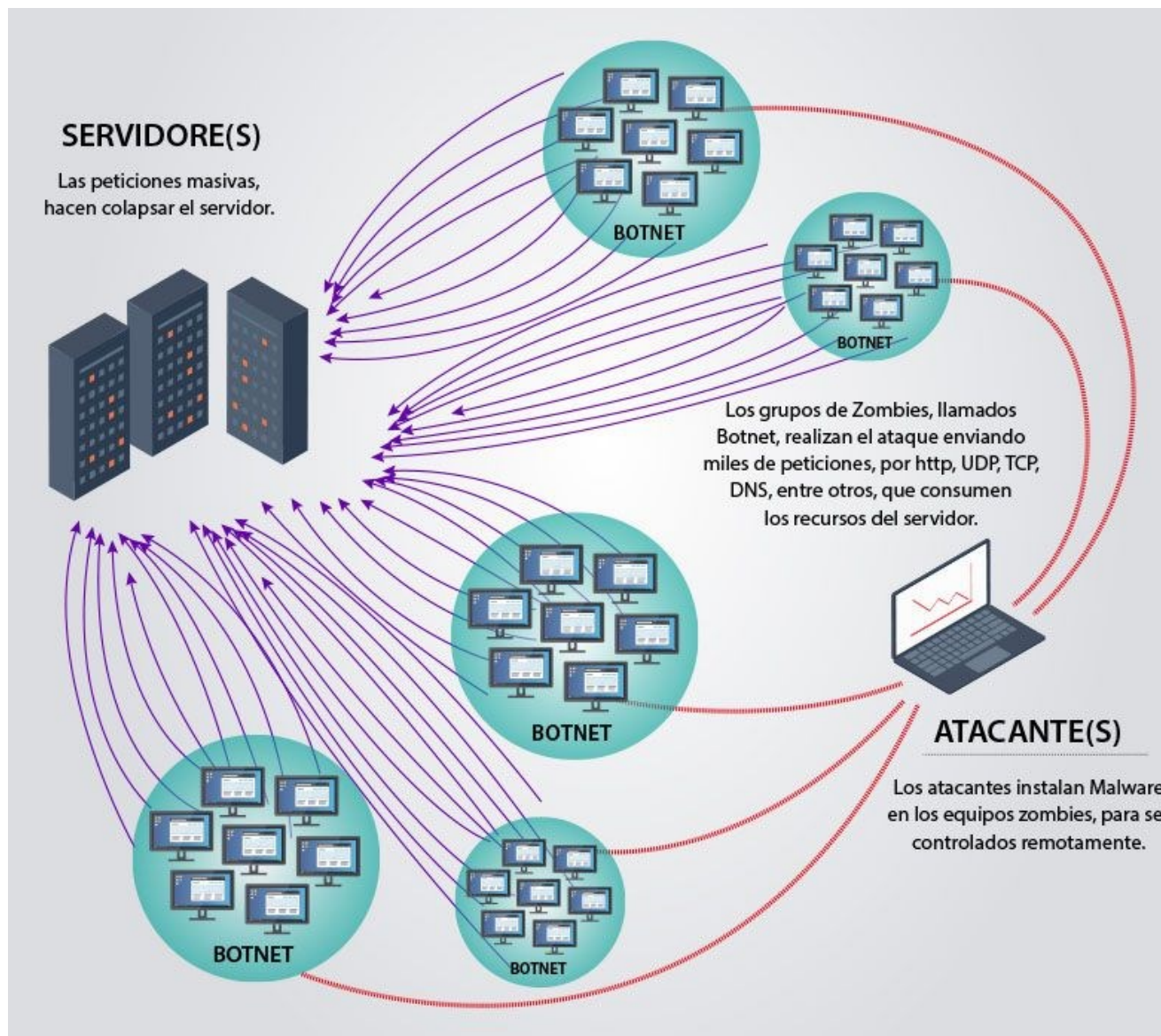


Figura: Anatomía de un ataque DDoS.

Ataque y defensa DDoS

Básicamente el DDoS es un ataque similar al DOS, donde se intenta consumir todos los recursos de una víctima hasta agotar su capacidad de procesamiento o llegar a un desborde. A diferencia del DOS, en este caso nos enfrentamos a múltiples atacantes, ocasionando así una avalancha mucho mayor de paquetes sobre el destino del ataque.

En los ataques por DDoS, el atacante se suele aprovechar de los hosts de usuarios domésticos que están conectados en forma permanente. Este tipo de hosts, generalmente, no están lo suficientemente protegidos, entonces un usuario malicioso podría cargar en miles de estos hosts un software de ataque.

El programa de ataque permanece latente en las computadoras hasta que reciben una señal del usuario malicioso. Esta señal, le indica a todos los hosts (comúnmente llamados zombies) en forma simultánea que deben comenzar el ataque hacia un destino determinado.

Los ataques DDoS más comunes son:

- **SMURF.** Este sistema de ataque se basa en transmitir a la red una trama ICMP correspondiente a una petición de ping. Esta trama lleva como dirección de origen la dirección IP de la víctima, y como dirección de destino la dirección broadcast de la red atacada.
- **TFN (Tribe Flood Network).** En este ataque, un usuario malicioso obtiene acceso privilegiado a múltiples hosts e instala un software que realice Syn Flood sobre un destino en particular al momento de recibir la orden del atacante.

Las contramedidas usuales contra ataques DDoS son complicadas y en algunos casos — lamentablemente— imposibles. Algunos servicios en los sistemas operativos permiten definir el número máximo de conexiones, pero otros no. En su caso, deben restringirse moderadamente de modo que puedan ofrecer su servicio, pero que no agoten los recursos del sistema. Este equilibrio es muy difícil porque dependerá del sistema, de la aplicación y de la carga del servicio.

Otra contramedida posible es configurar los routers de borde para que ajusten la velocidad de llegada de determinados tipos de paquetes (por ejemplo, limitar la velocidad de ICMP y TCP Syn).

2.4.4. INSTALACIÓN Y CONFIGURACIÓN BÁSICA DE UNA SUITE DE ATAQUE: KALI

En este epígrafe se expondrá la instalación y configuración básica de una de las herramientas de seguridad más conocidas y utilizadas actualmente: se trata de Kali Linux, que es una distribución GNU/Linux especialmente confeccionada como suite de ataque y análisis de seguridad.

Para usar Kali Linux no es necesario hacer una instalación en disco duro. Se pueden descargar la ova de la máquina virtual correspondiente a vmware o virtualbox, incluso el Docker.

En el ejemplo que aquí desarrollaremos utilizaremos la versión 2021.3 de KALI que está basada en la distribución Debian. Por tanto, la instalación en disco duro de Kali 2021.3 se inicia exactamente igual que un sistema Debian. Kali se puede descargar desde <https://www.kali.org/>.

Los pasos de instalación son los siguientes:

Inicio del LiveCD de instalación y elección de instalación sobre disco duro.

El sistema arrancará el LiveCD. Podremos entrar en él con la cuenta root/toor (usuario/contraseña) que es la que Kali trae por defecto. Una vez dentro, podremos disparar el interfaz gráfico ejecutando startx o seleccionar la opción de instalación gráfica.

Una vez arrancado el interfaz gráfico, podremos hacer la instalación desde la aplicación "Install Kali" que aparecerá en el escritorio. El proceso de instalación sigue un proceso similar a un sistema Debian.

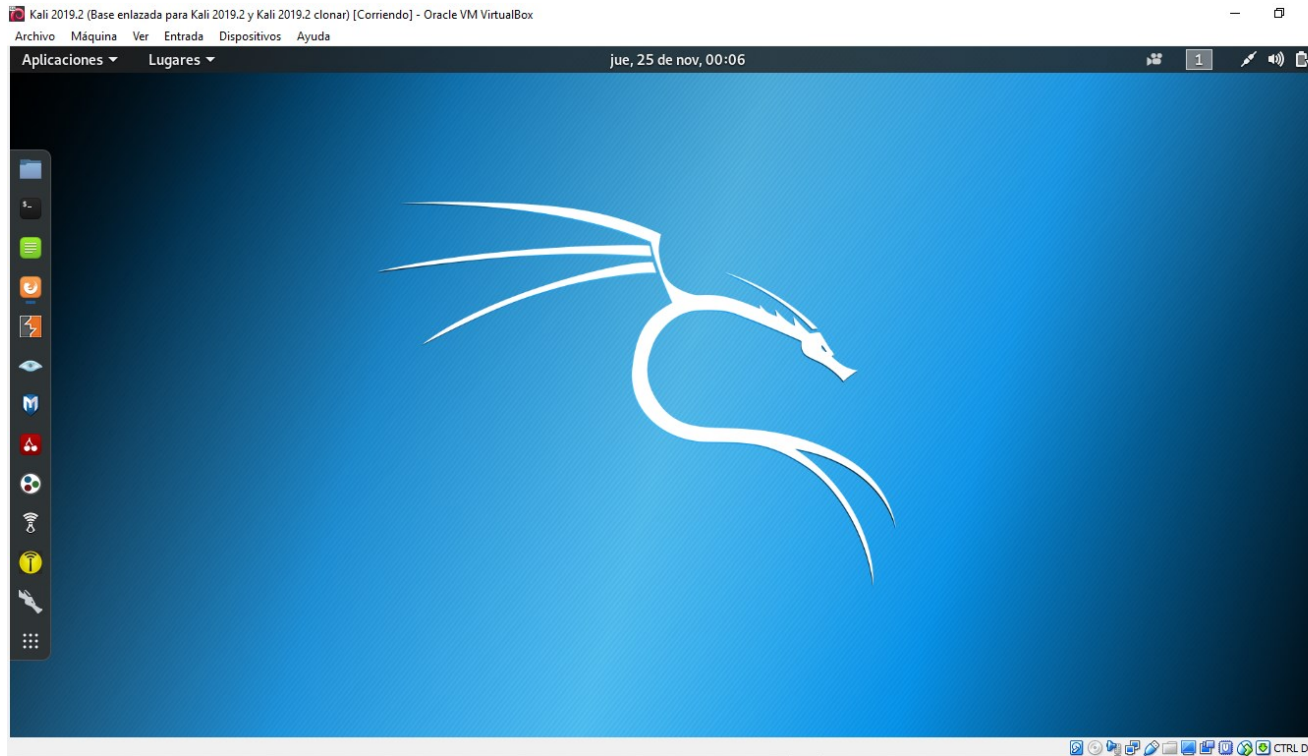
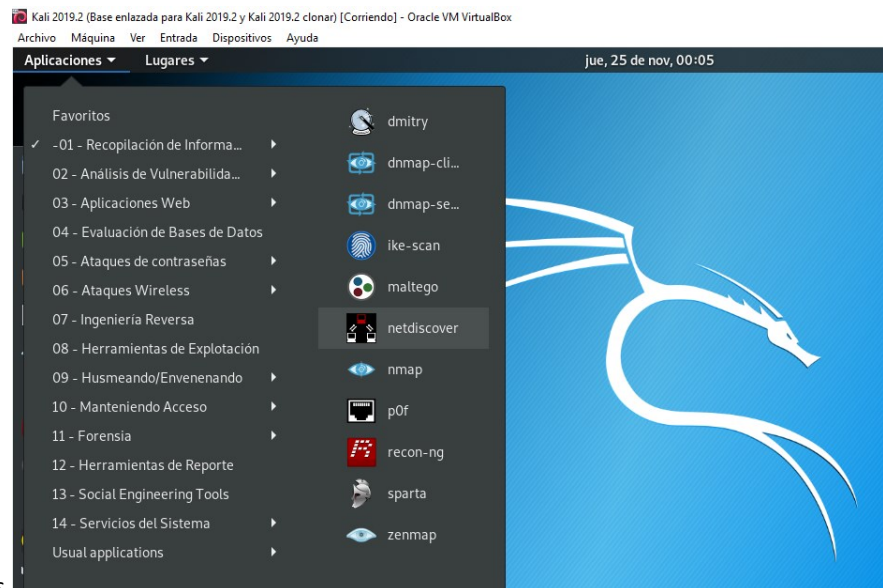


Figura. inicio de instalación de KALI

Una vez instalado el sistema, deberemos arrancar el sistema y se nos proporcionará una consola de texto sobre la que podremos disparar el interfaz gráfico para gestionar el sistema.

Desde ese momento podremos arrancar las diferentes herramientas de que se compone el sistema, que son



muchas y muy variadas.

Figura: Vista general de los menús de herramientas de KALI 2019.2

ESCANEO DE UN NODO DE LA RED CON WEBSHAG

A modo de ejemplo vamos a utilizar la herramienta webshag, para explorar un nodo desde el otro lado de la red. En primer lugar, arrancaremos webshag y teclearemos la dirección IP del nodo que queremos escanear. El resultado de la operación, después de unos segundos, será una lista de puertos abiertos en el sistema explorado. En La figura, a la izquierda, se ve que solo hay un puerto abierto que es el 5327. La razón de que no haya más que un puerto abierto es porque el sistema de destino (192.168.88.133) tiene su firewall activado de un modo muy restrictivo.

Si el target desactiva su firewall y exploramos de nuevo con webshag podremos ver que aparecen muchos nuevos puertos que nos proporcionarán información sobre los servicios disponibles en el nodo, ahora accesibles sin barreras puesto que el firewall los ha desprotegido (ver figura a la derecha).

```
webshag_cli.py: error: bad module or target missing
root@kali:~/Descargas/webshag-master# ./webshag_cli.py scanme.nmap.org
#####
% webshag 1.10
% Module: uscan
% Host(s): scanme.nmap.org
% Port(s): 80
% Root(s): /
#####

scanme.nmap.org / 80
#####

% BANNER %      Apache/2.4.7 (Ubuntu) => apache
% INFO %       FP(/) => 200#text/html#8c6f3ef75fd5b6b7c79bd67d71af043e#5bcc23934c5fa317f41902dbfcfaabda
% INFO %       FP(/liIJ6z8T) => 404#text/html#36dc86ab8b2d5e13543ed05c4e5abea8#6596e0bfbf82d6d3fe35239a191a3ff7
% INFO %       FP(/index.php) => 404#text/html#36dc86ab8b2d5e13543ed05c4e5abea8#6596e0bfbf82d6d3fe35239a191a3ff7
```

Figura: Ejecución de webshag con firewall activado en el destino (izquierda), sin firewall (derecha).

Webshag provee múltiples funcionalidades de exploración. Por ejemplo, vamos a explorar el servidor web que brinda por el puerto 80 el nodo scanme.nmap.org (Figura). Podemos ver que la utilidad explora la web y nos proporciona información detallada sobre sus páginas, direcciones de correo que ha sido capaz de localizar y enlaces externos a los que se enlazan las páginas de la sede web.

ESCANEO DE NODOS CON ZENMAP

Zenmap es básicamente un interfaz gráfico para la ejecución de nmap, uno de los escáneres de red más utilizados, que está incluido en la suite KALI. En La figura podemos ver la ejecución de nmap sobre un sitio web del que tenemos permiso para hacerlo, por ejemplo scanme.org, el objetivo es explorar este nodo para averiguar información sobre él.

Podemos ver que el nodo scanme.org, tiene la dirección pública 45.33.32.156 y 4 puertos abiertos. Tiene el puerto 80 abierto, lo que indica que soporta un servidor web público. También hemos averiguado que este nodo no tiene abierto el puerto 443 utilizado por https, por lo que ya podríamos descartar todas las vulnerabilidades posibles por ese puerto. En cambio, por el puerto 80 tenemos al alcance un servidor Apache de versión 2.4.7, que no es la última versión y podría tener alguna vulnerabilidad.

Un hacker experimentado, buscará rápidamente información sobre las vulnerabilidades conocidas de esa versión de Apache y tratará de averiguar si son aplicables al nodo para iniciar desde allí el ataque al nodo y, posteriormente, comprometer toda la red.

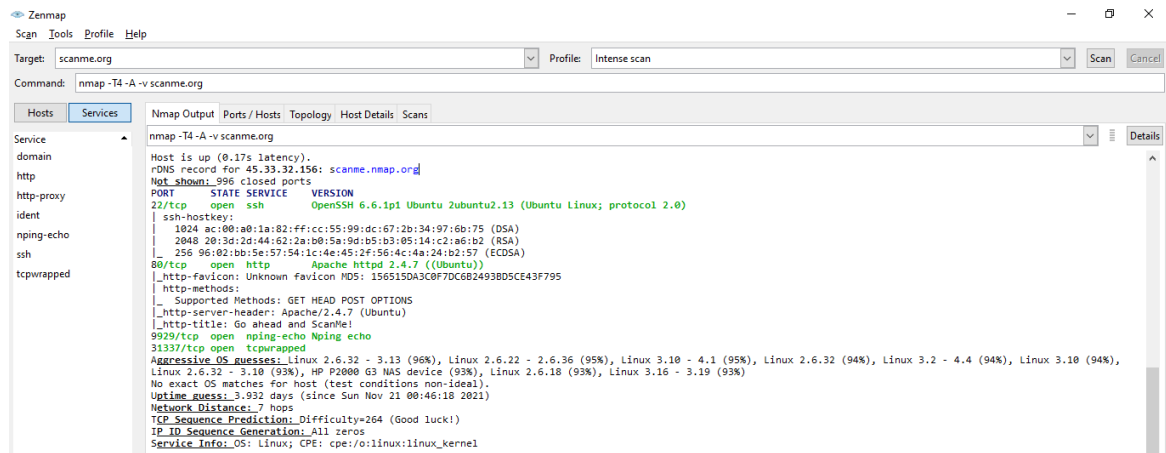


Figura. Escaneo de scanme.org con Zenmap.

Si ahora examinamos la información proporcionada por Zenmap en la ficha de detalles de host (host details), en el escaneo del propio KALI, vemos que el sistema operativo sobre el que se soporta es de tipo Linux (Figura inferior). Probablemente, sea uno de los sistemas listados, pero no ha encontrado un match 100%, aunque el sistema explorado le presenta a Zenmap este patrón de sistema operativo. Es posible, solo scanme lo sabrá, que el firewall que protege al equipo al reconocer la operación de escaneo haya engañado a Zenmap para que este no descubra realmente qué sistema operativo se está ejecutando.

El sistema tiene cerrados 996 puertos de los 1000 explorados: solo están accesibles el 80, 22, 9929 y el 31337, aunque ya hemos visto que el 443 no está activo, mientras que en el 80 reside el servidor web scanme.nmap.org.

Figura. Detalles de un host Kali 2019.2 escaneado por Zenmap.

