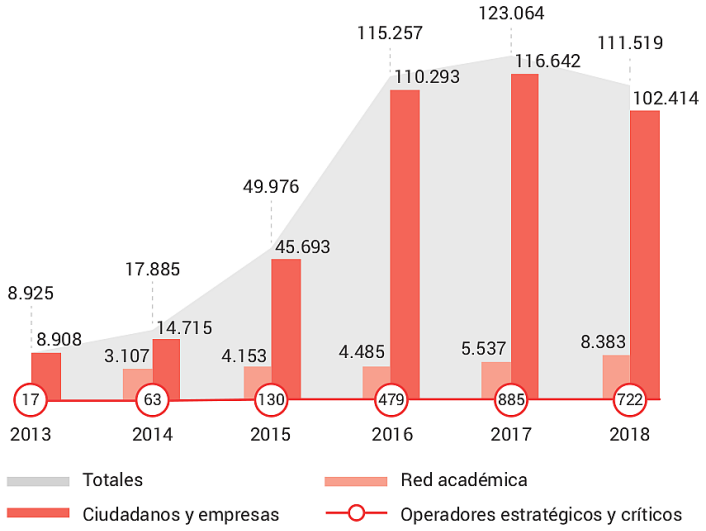
1. Introducción

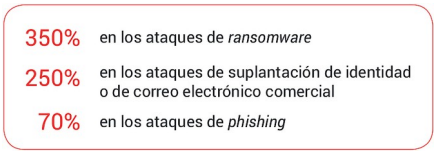
Los motivos por los que la seguridad debe formar parte de la agenda de cualquier organización, independientemente de su sector económico o de su tamaño, son muchos y variados, algunos de los cuales se pueden leer en la prensa con mucha frecuencia: fraudes electrónicos, casos de phishing en la banca, filtraciones no deseadas de información o de datos personales, cortes en las comunicaciones, etc. Los perjuicios que ocasionan los incidentes de seguridad son, cuando menos, incómodos y en muchos casos económicamente gravosos: paradas de producción, pérdidas de clientes, pérdida de reputación, etc.

Desde hace unos años INCIBE[1] realiza estudios sobre el sector de la seguridad TIC en España donde se puede comprobar una tendencia al alza en incidencias de seguridad. Principalmente son ataques de ransomware, secuestro de sistemas, fugas de información, ciberestafas y técnicas de engaño como el phishing.



Fuente: INCIBE

En un estudio similar realizado por Google en 2018, se estimó que el coste medio de un ciberataque a una pyme es de unos 35.000€ y que el 60% de las pymes cierra 6 meses después del haber sufrido el ciberataque. Ese mismo año el porcentaje de ataques a nivel mundial aumentó:



2. Seguridad de la Información

En el mundo IT, al analizar que se hace cuando se protege un ordenador, un iPAD, un teléfono móvil, una infraestructura de comunicaciones o un servicio se llega a la conclusión que lo que en realidad se está haciendo, es proteger la información almacenada, enviada, transmitida y modificada en dichos servicios, infraestructuras o dispositivos.

La información es un activo; es decir, un **elemento que tiene valor** para las empresas. En torno a ella se crean y desarrollan procesos y tareas; sin la información, esas tareas y procesos no sirven para nada o no pueden llevarse a cabo adecuadamente. En muchos casos, la información y su seguridad están directamente relacionadas con la supervivencia del negocio o el aseguramiento de ingresos:

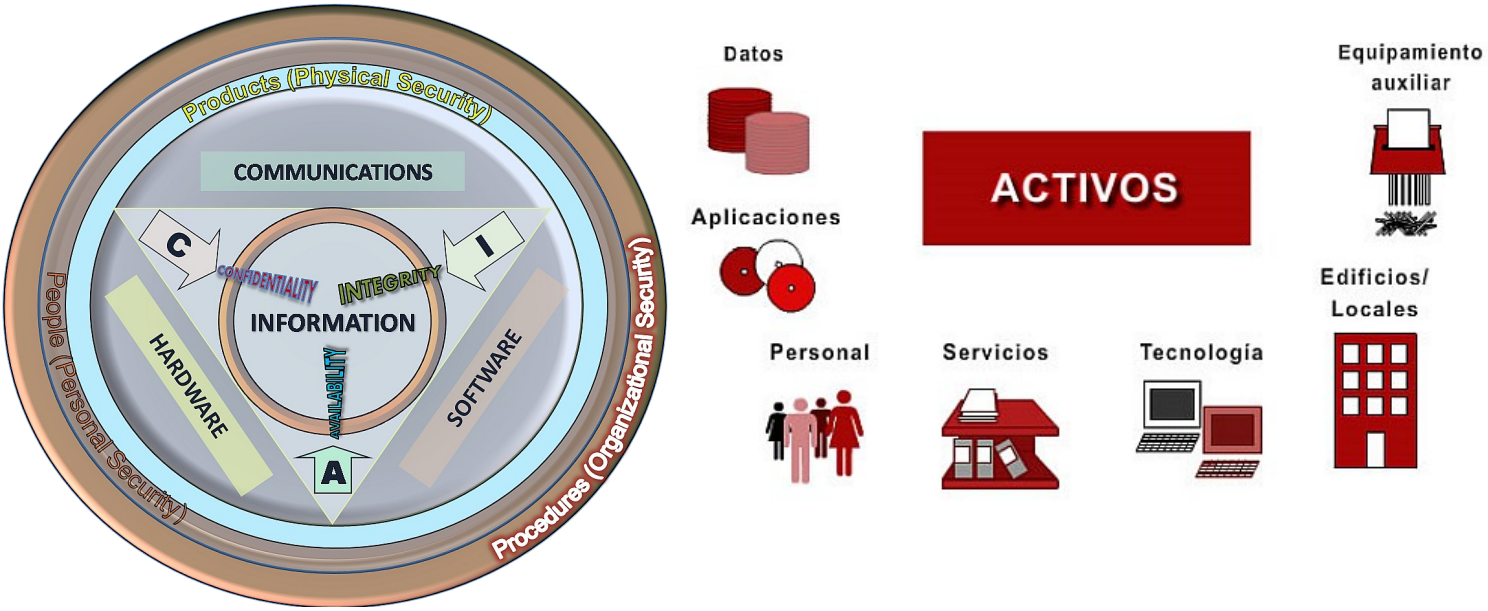
- Fallos de energía eléctrica que imposibiliten acceder a la información.
- Robo o extravío de equipamiento con información (portátiles, PDAs, etc.).
- Venta de información interna a competidores.
- Ataque a sistemas informáticos con robo de información sobre clientes, con posible repercusión mediática y violación de legislación o normativa.
- Incendios donde se destruyan equipamiento, oficinas, etc.

Debido a su importancia, se busca la protección de la información, independientemente de su formato, localización, naturaleza, etc. Al hablar de Seguridad de la Información no hay por qué referirse a incidentes

[1]INCIBE: Insituto Nacional de Ciberseguridad - https://www.incibe.es/

relacionados con el malware, el robo de información u otros incidentes de tipo tecnológico, sino que la información puede verse afectada también por un incendio, una inundación, un empleado descontento, etc.

La Seguridad de la Información se puede definir como la **protección de la confidencialidad, integridad y disponibilidad** de los activos de información[2] según sea necesario para alcanzar los objetivos de negocio de la organización.



Es lo que se conoce como la triada C.I.A. por sus siglas en inglés: Confidentiality-Integrity-Availavility. Estos tres parámetros básicos de la seguridad se definen como:

- **Confidencialidad (*confidentiality*):**
  - A la información únicamente pueden acceder las personas autorizadas para ello.
  - La información se revela exclusivamente a los usuarios autorizados.
  - Para garantizar la confidencialidad hay que prevenir la divulgación de información a personas/sistemas no autorizadas.
  - Si accediera a ella alguien de la competencia podría utilizarla para conseguir beneficios económicos, o bien denunciar a la organización ante la Agencia de Protección de Datos para que se le impusiera una multa si se demuestra que se vulneró la Ley de Protección de Datos de Carácter Personal, o publicarla en la prensa para dañar la imagen de la organización.

La Unión de Consumidores expone que el día 22/12/2008 el denunciante accedió a la página web de Vodafone y que, al acceder a la opción "Mi Vodafone" para acceder a sus cuentas de teléfono, pudo visualizar en la pantalla datos de otros clientes de la operadora, que variaban cada vez que accedía a la citada opción. Preocupado por la posibilidad de acceder a datos personales de terceros el denunciante llamó inmediatamente al Servicio de Atención al Cliente de la operadora para comunicarles la incidencia, sin que haya obtenido una respuesta de ésta.

Los datos a los que el denunciante tuvo acceso incluían el nombre y apellidos del titular de contrato, su DNI o NIF, número de pasaporte, sexo, fecha de nacimiento, nacionalidad, número de teléfono móvil, número de teléfono fijo, dirección postal completa y, en ocasiones, su dirección de correo electrónico.

El artículo 44.3.h) de la LOPD, considera infracción grave:

"*Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen*".

Como se ha expuesto anteriormente, Vodafone ha vulnerado el principio de seguridad de los datos, por lo que la operadora ha incurrido en la infracción grave descrita.

Fig. Partes de una sanción impuesta por la AEPD

[2] Activos de información: los datos, los equipos, las aplicaciones, las personas, que se utilizan para crear, gestionar, trasmitir y destruir la información

- **Integridad (*integrity*):**
  - La información ha de estar completa y correcta en todo momento.
  - Se mantienen los datos libres de modificaciones no autorizadas. La información se modificada sólo por personal autorizado.
  - La integridad garantiza la exactitud de la información contra la alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.
  - Si la información se corrompe, se podrían enviar cartas o facturas erróneas a los clientes, con la confusión y las quejas de los afectados que acarrearía, más el trabajo y el tiempo que habría que emplear para corregir los errores y restaurar a su estado correcto la información. Que la información permanezca íntegra en todo momento es más importante de lo que a primera vista pueda parecer.

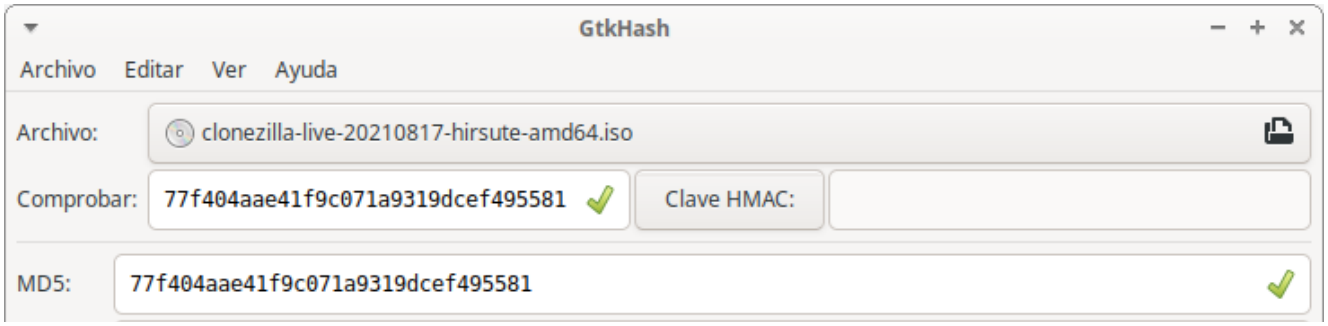


Fig. Comprobación de la integridad de un archivo usando MD5

- **Disponibilidad (*availability*):**
  - La información estará lista para acceder a ella o utilizarse cuando se necesita.
  - Las personas/sistemas/aplicaciones pueden acceder a la información.
  - Para garantizar la disponibilidad hay que lograr que la información sea utilizable cuándo y cómo lo requieran los usuarios autorizados.
  - Si el equipo en que reside esta información se estropea y no se puede acceder a ella, simplemente no se puede funcionar, no se puede dar servicio, lo que implica que se deja de ganar dinero y en casos extremos se puede perder, si el cliente decide marcharse y adquirir el servicio en otro proveedor. Un fallo de disponibilidad tiene siempre un impacto económico directo en la organización, por leve que sea, ya que se deja de trabajar, hay una parte de la organización que ha parado, por lo que ha dejado de generar beneficio.


Un ciberataque deja sin servicio a la UAB

14 octubre, 2021 Por Javier Aranda — Dejar un comentario

La madrugada del pasado lunes, la **Universitat Autònoma de Barcelona (UAB)** sufrió un ciberataque en su infraestructura digital, obligando a cancelar algunas clases clases virtuales.

ATAQUES INFORMÁTICOS >

Así ha afectado un ataque de 'ransomware' a una de las mayores aseguradoras de España

SegurCaixa Adeslas prevé volver por completo a la normalidad de su actividad el próximo viernes tras seis semanas intentado recuperarse de un apagón digital

Fig. Ataques de ransomware

Además de los anteriores también se habla de:

- **Autenticidad:**
  - La información es lo que dice ser o el transmisor de la información es quién dice ser.

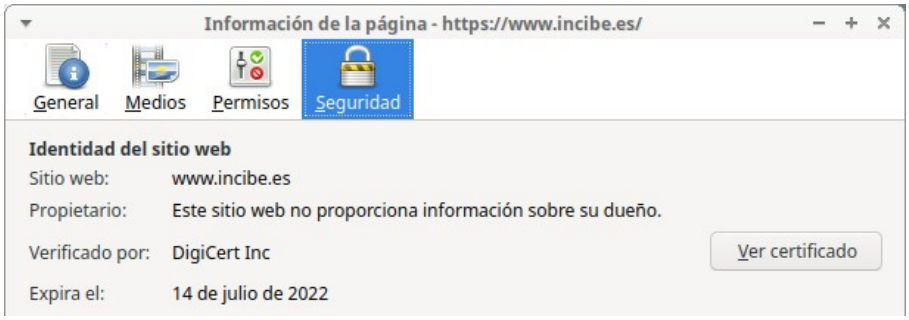


Fig. El uso de certificados digitales en https permite garantizar que el servidor es realmente el equipo con el que queremos hablar

- **Trazabilidad:**
  - Poder asegurar en todo momento quién hizo qué.
  - Poder asegurar en todo momento cuándo lo hizo.

```
/var/log/auth.log
Sep 20 12:40:39 x99 sudo:   manuel : TTY=pts/2 ; PWD=/home/manuel ; USER=root ; COMMAND=/usr/bin/apt update
Sep 20 12:40:39 x99 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 20 12:40:48 x99 sudo: pam_unix(sudo:session): session closed for user root
Sep 20 12:55:06 x99 sudo:   manuel : TTY=pts/2 ; PWD=/home/manuel ; USER=root ; COMMAND=/usr/bin/apt full-upgrade
Sep 20 12:55:06 x99 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 20 12:55:07 x99 sudo: pam_unix(sudo:session): session closed for user root
```

Fig. Líneas del fichero de log `/var/auth/log` donde se registran los comandos ejecutados con `sudo`

Como asegura el Centro Criptológico Nacional[3], la seguridad absoluta es imposible de alcanzar ya que las medidas de seguridad a implementar deben ser proporcionales a los riesgos. Es necesario adoptar un compromiso entre el nivel de seguridad, los recursos disponibles y la funcionalidad deseada.

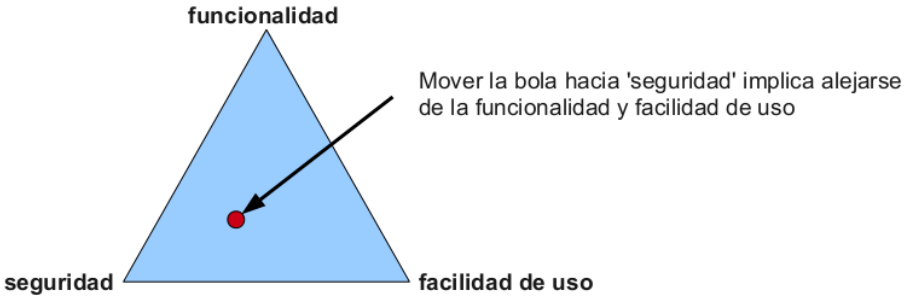


Fig. Seguridad frente a facilidad de uso y funcionalidades

Un planteamiento defensivo consistirá en alguno de los siguientes puntos:

- Segmentación de la red creando una o varias redes en la organización en función de los requisitos de seguridad de sus equipos (p.e. DMZ interna, DMZ externa, …).
- Seguridad perimetral implantando políticas de tráfico con firewalls/Proxys, IDS/IPS, ...
- EDR (Endpoint Detection Response), Antivirus, antispam, ...
- Filtros de contenidos
- Sistemas de monitorización
- Cifrado.
- Análisis de integridad.
- Actualizaciones, parches, …
- Securización S.O.
- Políticas de contraseñas, backups
- etc.

Es lo que se conoce como **Seguridad Defensiva**.

3. Ciberataque: Cyber Kill Chain

[3]CCN-Cert: Centro Criptológico Nacional - Organismo dependiente del Ministerio de Defensa - https://www.ccn-cert.cni.es/

La Cyber Kill Chain es la adaptación hecha por Lockheed Martin Corporation al mundo de seguridad de la información del concepto de Kill Chain militar (identificación del objetivo, decisión y orden de ataque y finalmente destrucción del objetivo).

En ella se describen los pasos a seguir por un adversario o actor malicioso para lanzar un ciberataque a un objetivo y es especialmente buena para representar un escenario de ransomware o de ataques dirigidos por grupos APT (*Advanced Persistent Threats*):

1. ***Reconnaissance*** (Reconocimiento)
   - Se recopila información sobre el objetivo usando fuentes abiertas (OSINT), whois, dns, network scanning, port scanning, enumeración de servicios, ...
   - En esta fase se busca obtener toda la información posible del objetivo como ubicaciones, presencia web (dominios, hosting, ...), empleados, direcciones de email, servidores (dns, web, correo, ftp, ...), topología de red, tecnologías empleadas, bloques de direcciones IP, ...
2. ***Weaponization*** (Preparación/Armamento)
   - En base al análisis de la información recopilada en la fase anterior, se prepara el ataque contra el objetivo.
   - Dependiendo del tipo de objetivo se escogen las herramientas a usar; por ejemplo:
     - se puede crear un documento de Office con una macro maliciosa o VBA scripts para remitir por email a un determinado usuario
     - se puede crear un payload malicioso en un pendrive que luego se distribuirá.
     - se puede preparar un exploit para aprovechar una vulnerabilidad de un sistema como la MS17-010 que permite la ejecución remota de código.
3. ***Delivery*** (Distribución/Entrega)
   - Se produce la transmisión del ataque; por ejemplo creando y enviando un email con el documento malicioso adjunto o con un enlace al documento para que el destinatario pinche en él y lo descargue.

- Ejemplos:
  - phishing emails.
  - distribución de pendrives infectados.
  - *watering hole attack* donde se compromete un sitio web que visitan habitulamente los objetivos y cuando lo visitan se les redirige a un sitio malicioso controlado por el atacante.

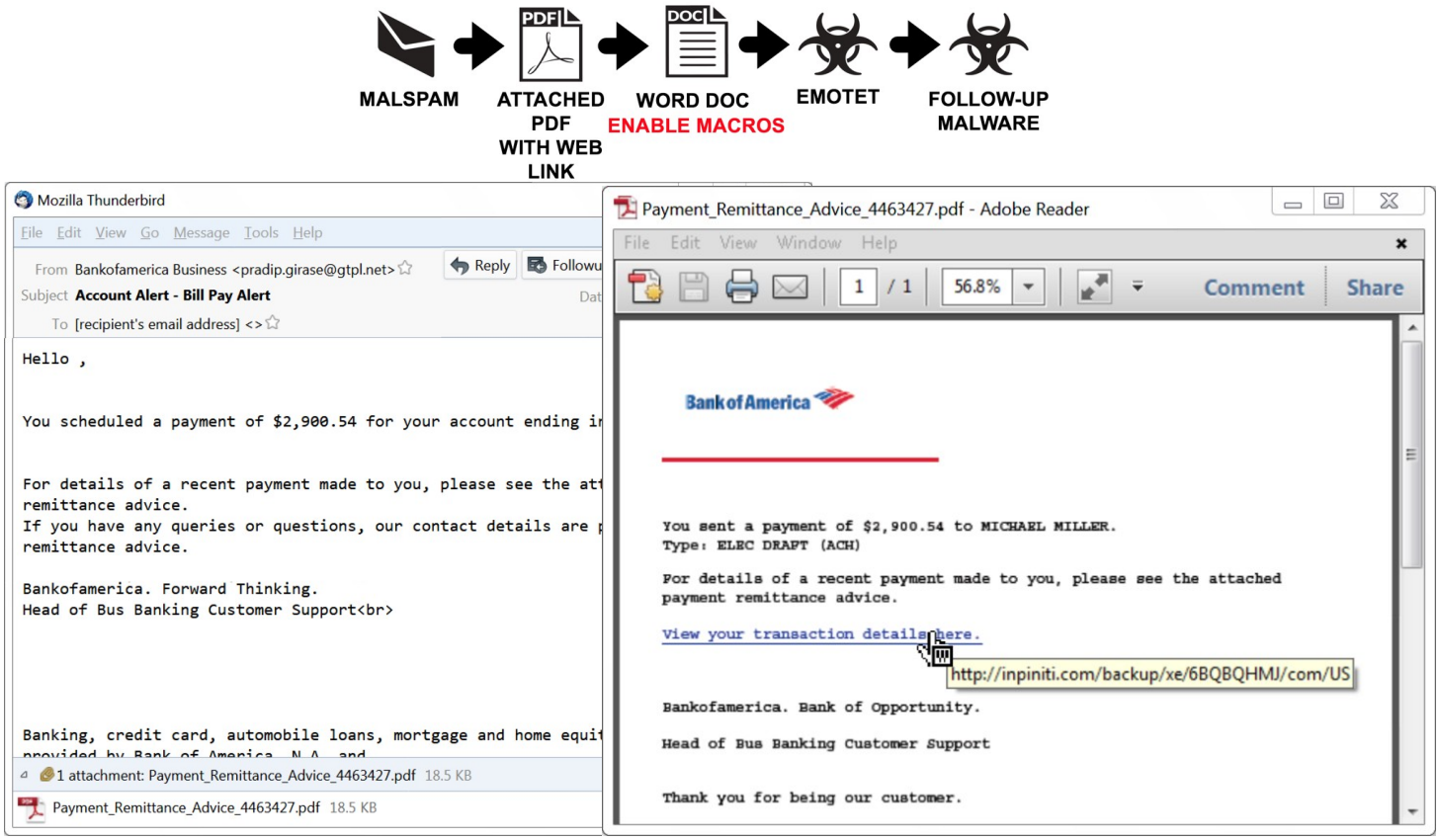
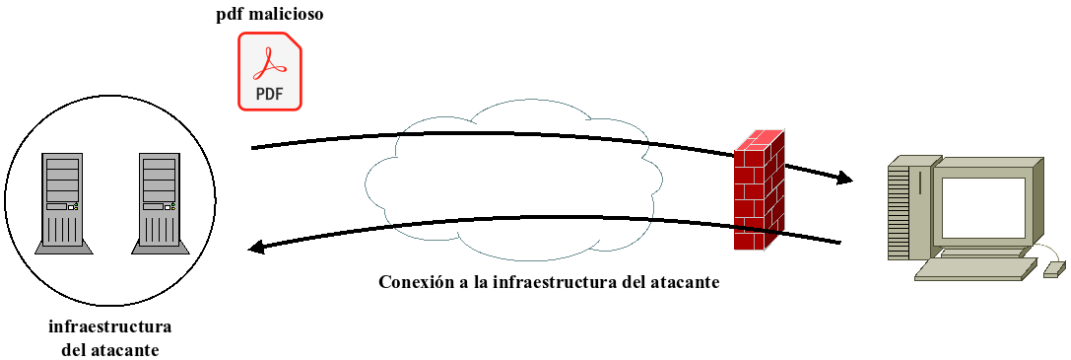


Fig. Cadena de infección del malware Emotet y ejemplo de mensaje y pdf con enlace a documento infectado

4. ***Exploitation*** (Explotación)
   - Es el momento en el que se aprovecha una vulnerabilidad del sistema objetivo para asaltarlo y obtener el primer acceso. El resultado puede ser por ejemplo que se envía una *shell* a un equipo del atacante, desde la que podrá ejecutar comandos.



5. ***Installation*** (Instalación)
   - En esta fase se busca la permanencia en el equipo atacado vía registro, tareas programadas, ..., para garantizar acceso futuros. Se suben/instalan más herramientas para tener vías alternativas de acceso y parar continuar el proceso de intrusión.
   - Ejemplos para conseguir la persistencia:
     - instalación de *web shells*.
     - instalación de puertas traseras (*backdoors*).
     - creación/modificación de servicios Windows.

- añadir entradas en el registro de Windows o en las carpetas de arranque.
- crear cuentas de usuario.

6. ***Command & Control*** (C2, C&C, Mando y control)
   - A través de canales C2 se controlan los sistemas atacados y en función del objetivo perseguido se les puede dar instrucciones para llevar acciones como ataques DoS.
   - Mediante canales dns, icmp, sitios web, redes sociales, ..., se envían órdenes al equipo comprometido para indicarle qué hacer.
7. ***Actions on objectives*** (Acciones sobre objetivos): se centra en lograr los objetivos del atacante como:
   - exfiltrar información y/o secuestrar datos (*ransomware*)
   - robar credenciales
   - identificar nuevos objetivos internos de la organización y expandirse, …
   - escalar privilegios para acceder a información reservada o nuevos sistemas
   - dañar o destruir activos

Una vez alcanzado el último paso y afectado un equipo dentro de la organización, el proceso se puede repetir para con más reconocimientos y movimientos laterales en el interior de la organización. Aunque la Cyber Kill Chain se representa como una línea hay que verla como un **proceso cíclico**.

El estar dentro de una organización hace que los privilegios y las posibilidades de acceso a los recursos sea diferente que desde el exterior, por lo que el atacante puede usar nuevas técnicas y procedimientos. Esto ha hecho que algunas organización trabajen con versiones ampliadas como la *Expanded Cyber Kill Chain* o el *Targeted Attack Lifecycle* de Mandiant :

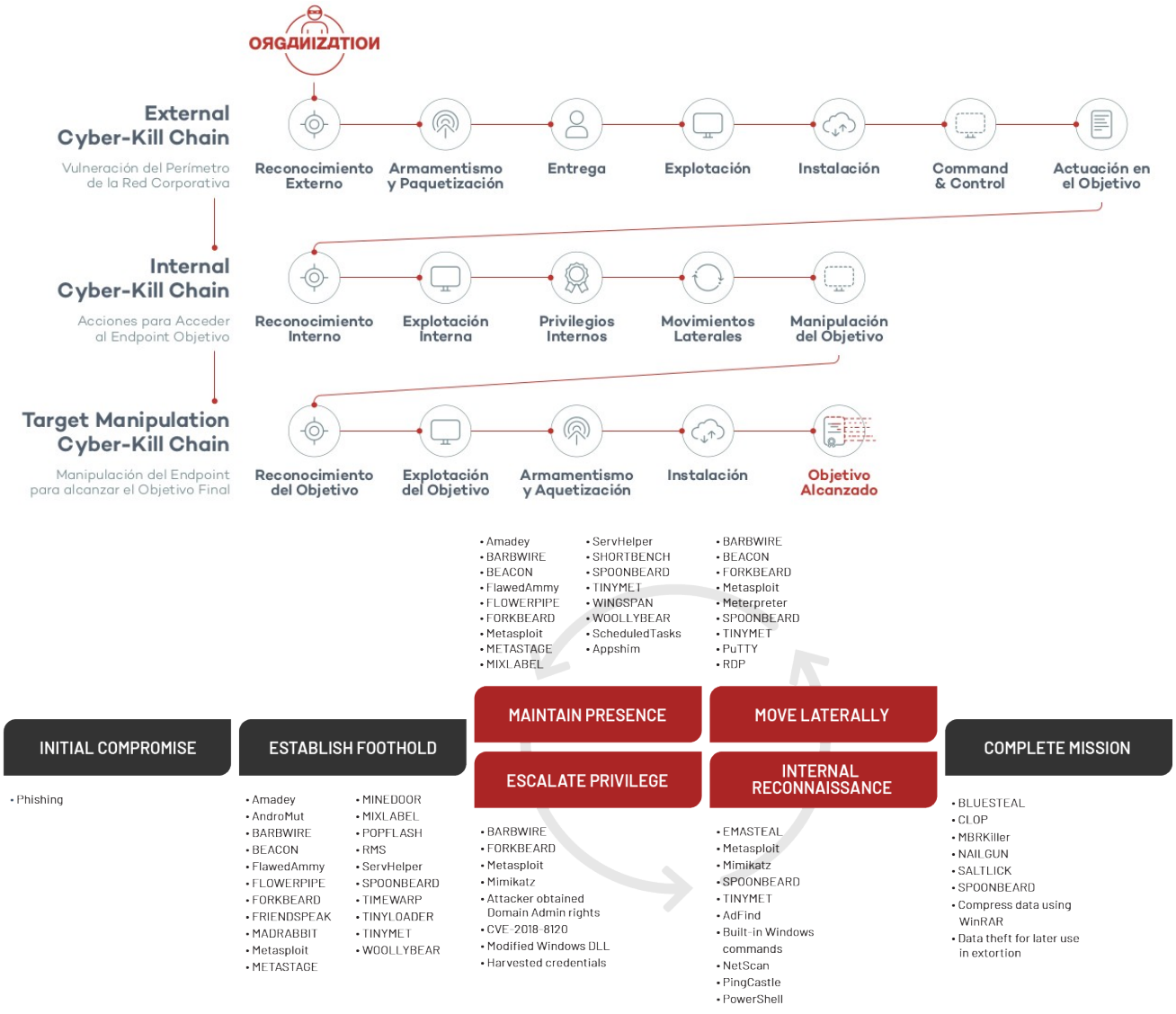


Fig. Cyber Kill Chain de Mandiant

4. Mitre ATT&CK

MITRE presentó en 2013 ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) que viene siendo una base de datos con información sobre tácticas y técnicas conocidas que usan los grupos de atacantes cuando están perpetrando una intrusión contra plataformas concretas (p.e. windows, linux, ...).

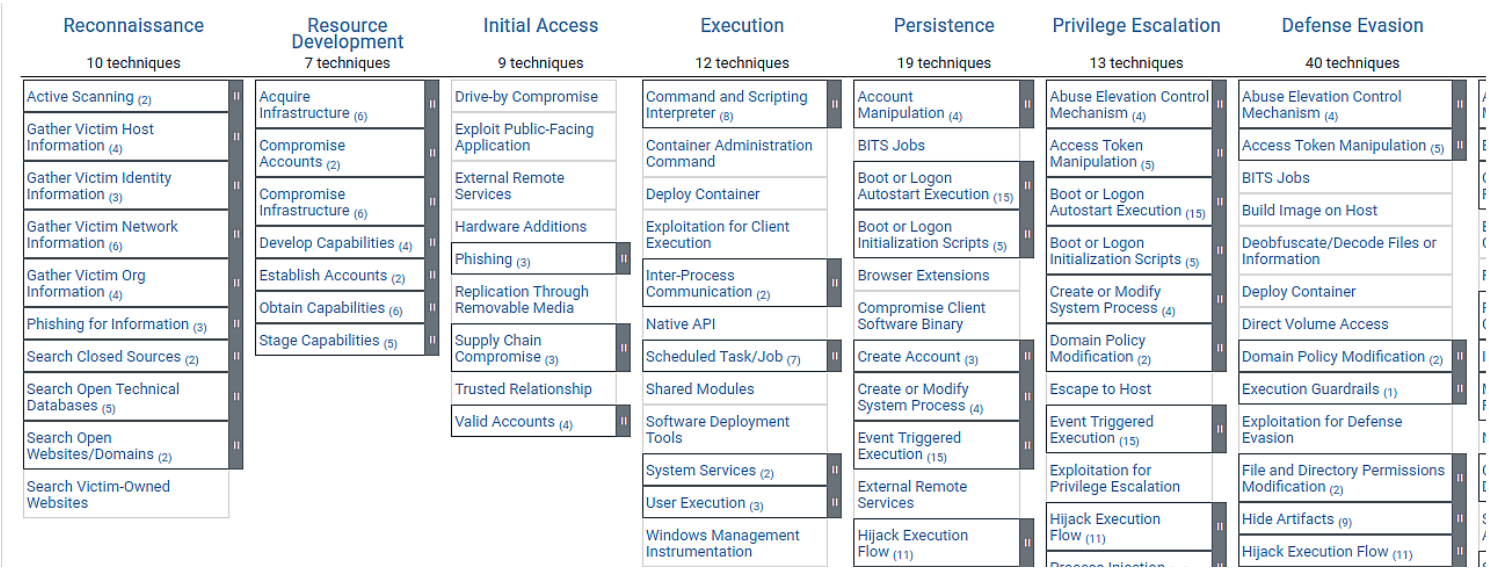
ATT&CK tiene algunos aspectos que lo hacen muy interesante y cada vez más presente en la industria:

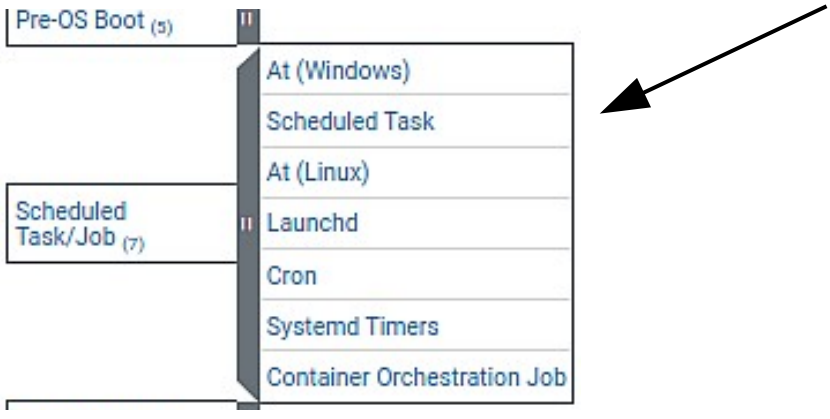
- **Comportamiento del adversario**: se centra en tácticas y técnicas usadas por los atacantes y no es indicadores como direcciones IP, nombres de archivo, herramientas, ..., que pueden cambiar fácilmente.
- **Aplicable a entornos reales**: las tácticas, técnicas y procedimientos (TTP) que recoge ATT&CK están basadas en incidentes observados y medibles.
- **Taxonomía común**: las TTP deben ser comparables entre diferentes tipos de grupos de adversarios utilizando la misma terminología.

Para ATT&CK:

- Las **tácticas** son *el qué* está tratando de conseguir un adversario en un momento dado de la intrusión. Es el objetivo del atacante para desarrollar una acción; por ejemplo, lograr la persistencia en un equipo.
- Las **técnicas** son *el cómo* se logra el objetivo. Por ejemplo, para lograr la persistencia se aprovecha la funcionalidad del sistema operativo de tareas programas.

Cómo hay muchas formas (técnicas) de que el atacante logre sus objetivos tácticos, hay múltiples técnicas en cada categoría táctica; por ejemplo, bajo la táctica Persistencia (*Persistence*) aparecen 19 técnicas que a su vez pueden tener subcategorías:





Para facilitar el uso de todo esta información MITRE ha creado tres matrices:

- ATT&CK Enterprise: centrada en el comportamiento de los adversario en entornos Windows, Linux, Mac, Cloud (Office 365, Azure, ...) y entornos de red..
- ATT&CK Mobile: para entornos Android e IOS.

- ATT&CK ICS (Indutrial Control Systems): para entornos industriales.

En la ATT&CK Enterprise se han definido las siguientes categorías (*tácticas*):

1. ***Reconnaissance***: técnicas para recopilar información sobre la organización para futuras acciones.

2. ***Resource Development***: preparación de recursos para dar soporte a las operaciones, como comprar de dominios, alquiler de VPS, ...

3. ***Initial Access***: técnicas que usa el adversario para tratar de entrar en la red, por ejemplo usando *spear phishing*, cuentas válidas, servicios de acceso remoto, medios de almacenamiento removibles, ...

4. ***Execution****:* técnicas para ejecutar código malicioso, por ejemplo comandos o scripts linux o powershell, ejecución por parte del usuario (URL, ficheros maliciosos, …), …

5. ***Persistence***: técnicas para mantenerse en el sistema, por ejemplo con tareas programadas, creando cuentas de usuario, ejecución de programas al inicio, ...

6. ***Privilege Escalation***: técnicas para obtener más privilegios en el sistema, por ejemplo aprovechando malas configuraciones o vulnerabilidades, cuentas de usuario (credenciales robadas por phishing, cuentas por defectos, credenciales '*hardcoded*', …), ...

7. ***Defense Evasion***: técnicas para evitar ser detectado, por ejemplo desactivando software de seguridad, ofuscando ficheros, borrando el historial/logs, ...

8. ***Credential Access***: técnicas para robar credenciales como usuario/contraseña, por ejemplo mediante keylogging, sniffing, fuerza bruta, ...

9. ***Discovery***: técnicas para descubrir el entorno, por ejemplo analizando los recursos compartidos, sniffing, ...

10. ***Lateral Movement***: ténicas para moverse a través de tu organización, por ejemplo usando servicios de acceso remoto como sshh o VNC, spearphishing interno , ...

11. ***Collection***: técnicas para localizar y recopilar información que le pueda servir para sus intereses, por ejemplo accediendo a audios, vídeos, emails, portapapeles, ...

12. ***Command and Control***: técnicas para comunicarse con los sistemas comprometidos para controlarlos, por ejemplo usando protocolos como http o túneles ICMP o DNS, puertos no estándar, ...

13. ***Exfiltration***: técnicas para robar información desde sistemas comprometidos sin ser detectados, por ejemplo subiéndola a una cuenta en la nube, exfiltración usando el canal C2, exfiltración a un repositorio de código usando http/https, ...

14. ***Impact***: acciones para manipular, interrumpir o destruir sistemas e información, por ejemplo impidiendo el acceso a usuarios (borrado de cuentas o cambio de contraseñas), modificando la página web de la empresa (*defacement*), cifrando la información (ransomware), ...

Además podremos acceder a información sobre mecanismos de mitigación y detección así como a datos de los grupos de adversarios (APT29, APT37, ...).

Hay dos diferencias fundamentales entre Mitre ATT&CK y la Cyber Kill Chain de Lockheed Martin:

- ATT&CK profundiza en cómo se desarrolla cada etapa del ataque especificando tácticas y técnicas.
- ATT&CK se actualiza regularmente en base a los nuevos incidentes informados desde las empresas, de forma que los defensores pueden conocer las últimas tácticas/técnicas empleadas por los adversarios. Esta actualización es especialmente relevante en sectores no contemplados originalmente por la Cyber Kill Chain como los entornos Cloud (donde acciones como el envío de malware no es tan relevante y es uno de los pilares de la Cyber Kill Chain).

5. Seguridad ofensiva: análisis de penetración

La seguridad ofensiva es una rama de la ciberseguridad donde se usan herramientas y metodologías como las que emplean los atacantes con el objetivo de localizar los puntos vulnerables de una organización, para posteriormente tomar las medidas oportunas.

Cuando se habla de análisis de penetración (*penetration test* o *pentest*) se habla de realizar una prueba de intrusión en una organización de manera controlada, emulando las acciones que realizaría un atacante. El objetivo de un pentest es acceder a un sistema logrando unos objetivos previamente pactados con el cliente.

Se pueden distinguir tres fases en un pentest:

- Fase I: Planificación, preparación y consentimiento.

- Fase II: Evaluación.
- Fase III: Informe, limpieza y destrucción de artefactos.

El consentimiento y el informe indicando los fallos encontrados es lo que diferencia a un atacante (*black hat*) de un hacker ético (*white hat*).

Fase I: Planificación, preparación y consentimiento

En esta fase, previa a la evaluación, se deben:

- Identificar los contactos de ambas partes, plazos temporales, …
- Acordar los objetivos, el tipo, la metodología y las limitaciones. Estas restricciones pueden limitar o impedir el uso de determinadas técnicas como Dos, instalación de rootkits, ...

El resultado de esta fase debe ser un acuerdo de auditoría (*assessment agreement*) donde se recogen:

- Consentimiento para realizar la auditoría.
- Objetivos, alcance y limitaciones de la auditoría.
- Obligaciones del cliente.
- Período de realización.
- Cláusulas de confidencialidad.
- Términos de pago.
- Limitaciones de responsabilidad.
- Causas de cancelación.
- Etc.

La importancia de este acuerdo se ve rápidamente revisando el código penal español:

"El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años".

Fase 2: Evaluación (*assessment*)

Existen diferentes formas de abordar esta fase y básicamente se trata de emular las acciones que realizaría un atacante:

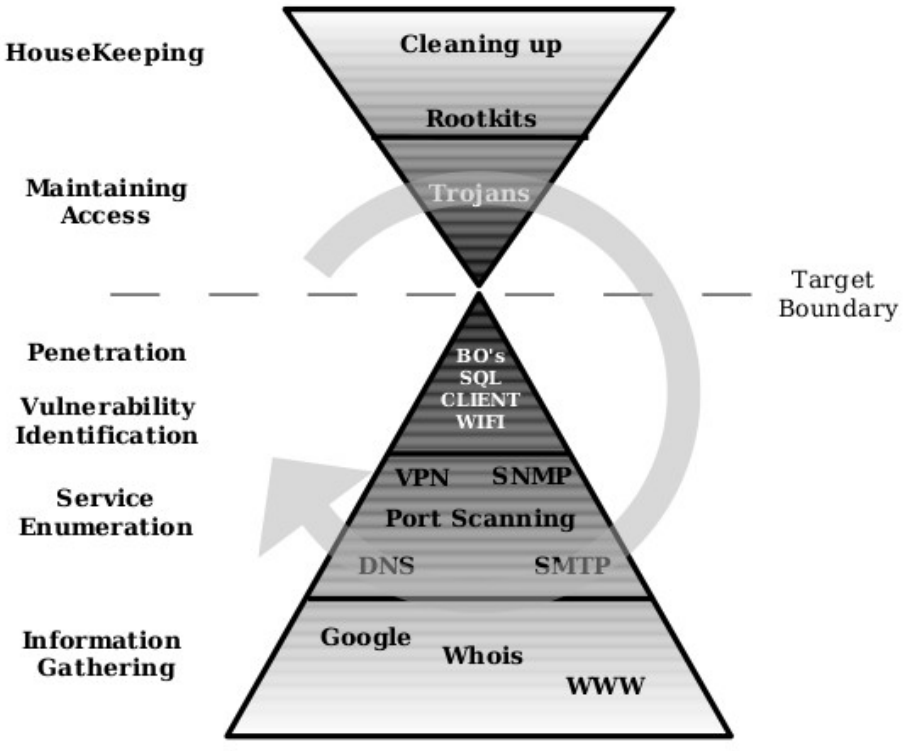


Fig. Fases de un pentest según Offensive Security

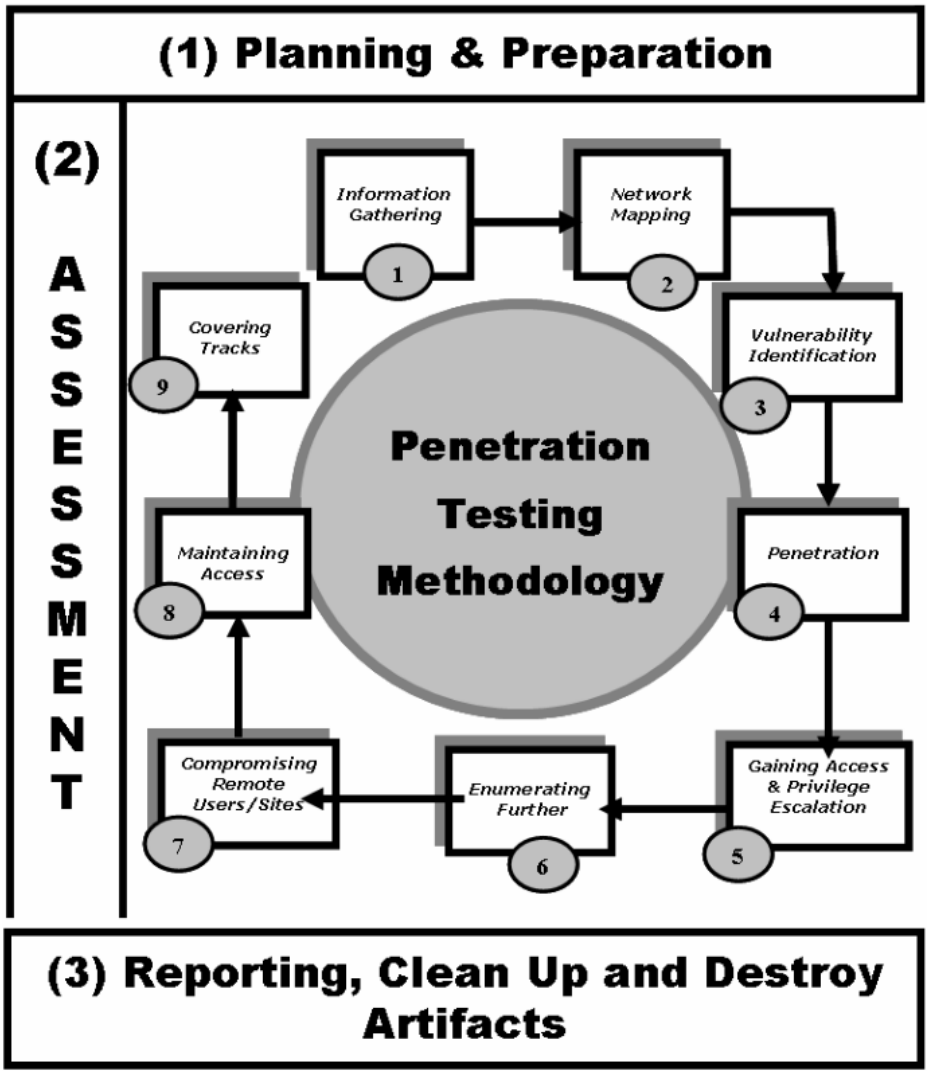


Fig. Fases de un pentest según ISSAF (Information Systems Security Assessment Framework)

Las fases se podrían resumir en:

1. Recopilación de información.
2. Enumeración de servicios.
3. Análisis de vulnerabilidades.
4. Explotación y mantenimiento de acceso (persistencia).
5. Postexplotación.
6. Ocultación.

Detallando los objetivos buscados en cada fase:

1. Recopilación de información (*information gathering*): obtener información sobre el objetivo.
   - Identificar presencia en internet usando motores de búsqueda (Google, Bing, ...).
   - Nombres de dominio (DNS), bloques de IPs, ..
   - Buscar el objetivo en bases de datos de spam, sitios web de estadísticas, sitios underground, …
   - Búsquedas en sitios de noticias y listas de correo.
   - Buscar sitios web personales de empleados, bases de datos de empleos, currículums, ...
   - Metadatos a partir de documentos de la organización.
   - Email: enumeración de cuentas, análisis de cabeceras de email, ...
   - Descarga del sitio web para análisis offline.
   - *Dumpster Diving* (rebuscar en la basura).
   - Etc.

   Esta fase es de vital importancia y de la cantidad y calidad de la información obtenida, puede depender el éxito o el fracaso de la auditoría.

2. Enumeración de servicios (*service enumeration*): la información sobre la red obtenida en la fase anterior se trata de ampliar y concretar para obtener una imagen de la topología del objetivo:
    - Encontrar equipos funcionando.
    - Identificar puertos abiertos y aplicaciones corriendo en ellos.
    - Identificar sistemas operativos.
    - Mapeo del perímetro de la red (routers, firewalls, ...).
3. Análisis de vulnerabilidades (*vulnerability identification*): del punto anterior, el auditor habrá seleccionado objetivos específicos en los que tratará de encontrar puntos vulnerables:
    - Identificar servicios vulnerables en base a banners.
    - Escaneo de vulnerabilidades manual apoyándose en bases de datos de vulnerabilidades y/o anuncios de fabricantes y CERTs.
    - Escaneo de vulnerabilidades usando herramientas automatizadas
    - Estimar el impacto de las vulnerabilidades encontradas.
    - Localizar puntos de acceso explotables.
4. Explotación y mantenimiento de acceso (persistencia) (*exploitation and persistence*):
    - El auditor trata de ganar acceso no autorizado al sistema aprovechando algunas de las vulnerabilidades encontradas saltándose las medidas de protección de la organización (firewalls, antivirus, IDS, ...). Se usarán herramientas, poc (*proof of concept*), …
    - Una vez dentro del sistema, se tratará de lograr la persistencia; es decir, mantener el acceso a pesar de reinicios, cambios de credenciales y otras interrupciones que podrían cortar el acceso.
5. Postexplotación (*postexploitation*): en la fase de postexplotación se pueden realizar acciones como:
    - Escalada de privilegios para obtener acceso como root/SYSTEM, cuentas de usuario con acceso a sistemas concretos o que realizan funciones específicas, ...
    - Robo de credenciales como usuarios/contraseña, claves digitales, ...
    - Establecimiento de sistemas de *command and control* (C&C o C2).
    - Exfiltración de información.
    - Descubrimiento para ganar conocimiento de la infraestructura interna y realizar movimientos laterales (*pivoting)*.
    - Etc.
6. Ocultación (*cover tracks*): normalmente en los pentest se trabaja *al descubierto* (salvo que lo pida el cliente) quedando registradas todas las actividades. En caso de pedirlo, se pueden utilizar técnicas de ocultación como:
    - Ocultar ficheros/herramientas.
    - Limpieza de logs para eliminar las entradas asociadas con las actividades del auditor.

Fase 3: Informe, limpieza y destrucción de artefactos

Una vez completadas todas las pruebas pactadas, debe generarse un informe que detalle cada una de las acciones ejecutadas y los resultados. Debe haber dos informes o en caso de un único informe contendrá dos partes:

- **Informe ejecutivo**: destinado a ejecutivos o directivos que no tienen porque tener amplios conocimientos técnicos, por lo que debe servir para informar de los resultados y que los directivos entiendan los riesgos existentes pero sin entrar en detalles técnicos concretos.
- **Informe técnico**: informe destinado a un público técnico donde se detallan:
    - todas y cada una de las acciones efectuadas.
    - herramientas utilizadas y capturas de pantalla de los resultados.
    - fechas y horas de las pruebas.
    - lista de vulnerabilidades encontradas, indicando la gravedad de la misma y con recomendaciones de como resolverlas.

Toda la información que se creó y/o almacenó en los sistemas testados debe borrarse; y en caso de no poder hacerse de forma remota, todos esos archivos con su localización deben mencionarse en el informe técnico para que el cliente pueda borrarlos.

En función de la cantidad de información de partida que recibe el auditor podemos hablar de auditorías de:

- **Caja blanca (*white box*)**: el auditor tiene acceso completo a la información sobre la red, sistema e infraestructura que está auditando (diagramas de red, código fuente, usuarios,, ...). Está pensada para simular una amenaza interna, como un administrador disgustado.
- **Caja negra (*black box*)**: el auditor no tiene ningún conocimiento sobre el objetivo a auditar. Está pensada para simular una amenaza externa.
- **Caja gris (*gray box*)**: el auditor tiene acceso a cierta información sobre el objetivo. A diferencia de la auditoría de caja blanca, en las de caja gris se asume que el auditor va a ser un *insider* pero sin llegar a tener un nivel de administrador.

6. Evaluación de vulnerabilidades, Red Team y Auditorías

Existen varios conceptos que aunque parecidos y que a veces se usan como sinónimos de pentest, tienen ciertas diferencias:

- **Evaluación de vulnerabilidades (*vulnerability assessment*)**: pensado para identificar y cuantificar las vulnerabilidades de un sistema priorizando su solución. Adecuado para organizaciones con un nivel bajo-medio de seguridad donde lo importante es descubrir que está mal y arreglar todo lo que se pueda de la forma más eficiente posible.

  Para distinguirlo del pentest: pensemos en la evaluación de vulnerabilidades como la búsqueda de problemas de seguridad cuando sabemos/asumimos que existen; y en cambio, el pentest se usa para validar una configuración cuando creemos que es segura.
- **Red Team**: el objetivo de un *red team* no es encontrar en un tiempo dado todas las posibles vulnerabilidades y explotarlas (*pentest*), sino poner a prueba las capacidades de detección y respuesta de la organización. Un *red team* tratará de acceder a información sensible de cualquier manera y tan sigiloso como sea posible, como si fuese un APT (*Advanced Persistent Threat*). No busca encontrar y explotar todas las vulnerabilidades posibles, pero sí encontrar y explotar aquella que le permita alcanzar su objetivo.

  Las campañas de red team suelen durar más tiempo, 3-4 semanas (o más) frente a 1-2 semanas de un *pentest,* e implicar a más personal. Aunque comparten muchas técnicas con los *pentest* también emplean otras como la ingeniería social y las campañas de phishing.
- **Auditoría**: sirven para determinar si una organización cumple con las medidas indicadas en un estándar. Por norma general no verifican la seguridad de la organización y sí el grado de cumplimiento del estándar. Ejemplo, auditorías para comprobar el cumplimiento del estándar PCI SSC (Payment Card Industry Security Standards Council).