MARÍA ÁNGELES CABALLERO
DIEGO CILLEROS SERRANO

EL LIBRO DEL HACKER

EDICIÓN 2022

ANAYA MULTIMEDIA

Índice de contenidos

Algunos de los filmes más conocidos que muestran esta imagen del hacker son *La Red* (1995), *La Jungla 4.0* (2007), *Hackers* (1995), *Operación Swordfish* (2001), *23. Nada es lo que parece* (1998), *Firewall* (2006), *Blackhat: amenaza en la red* (2015) y *Juegos de guerra* (1983) y series destacadas como *Mr. Robot* (2015). Cabe destacar que en una película tan futurística como *Matrix Revolutions* (2003) se muestra una imagen más cercana a la realidad que en otras muchas, ya que, en una de las escenas, Trinity realiza un ataque SCADA a una central eléctrica, haciendo uso de la herramienta Nmap para el escaneo de puertos y explotando una vulnerabilidad a continuación en el servidor SSH, vulnerabilidades descubiertas en el 2001. En otras películas como en *The Listening* (2006) o *Battle Royale* (1999) se puede ver también parte del código de Nmap.

FIGURA 1.13. El mundo *hacker* es un tema recurrente en la literatura y en el cine.

Dejando a un lado los motivos y estudiando las técnicas que utilizan, el *hacking* es una metodología poco ortodoxa que se basa en resolver problemas. La mentalidad que desarrollan los *hackers* es una mentalidad completamente analítica, con determinados *skills*: análisis de información, resolución de problemas y toma de decisiones. Estas fortalezas les permiten incrementar su probabilidad de éxito y productividad a la hora de enfrentarse a los retos. Además, requiere de cierta creatividad para detectar vulnerabilidades y fallos de seguridad en los datos, programas, infraestructuras, etc. A menudo los *hackers* deben de tener un pensamiento *out of the box* para encontrar las soluciones. ¡Te animamos a que te enfrentes a algún reto *hacking* tipo *capture the flag* o *hackaton*, para que lo experimentes en primera persona! Algunos sitios web para practicar CTF son CTF365, OverTheWire o Hacking-Lab. Te recomendamos que visites esta página web si quieres descubrir más: `https://www.quora.com/What-are-the-best-online-hacking-and-CTF-websites`.

FIGURA 1.14. CTF365. Security Training Platform.

El término "*hacker*" se comenzó a gestar en los años 60 gracias a las computadoras del MIT (Massachusetts Institute of Technology) como alguien que es experto con los ordenadores, con muy buenas habilidades de programación y que hace uso de estas habilidades para ganar conocimiento junto a otros. Un *hacker* en origen no entra en sistemas ajenos con propósito malicioso o para beneficio personal. Debido a esta confusión mediática, la palabra *hacker* se ha ido desvirtuando, y es por lo que ha ido surgiendo la diferenciación entre *white hats*, *grey hats* y *black hats*, así como la creación de otras clasificaciones o tipologías como son los *insiders, script kiddies o phreakers*.

White hat, *sneaker* o hacker ético

White hat o ***hacker* de sombrero blanco** son términos que entran dentro de la definición original de *hacker* y, en ocasiones, se les llama ***hackers* éticos** o ***sneakers***. Estos términos se refieren a un *hacker* o experto en seguridad informática que está especializado en realizar test de intrusión o evaluaciones de seguridad, con ánimo de garantizar la seguridad de la información de los sistemas de una empresa. El término fue acuñado en origen por IBM. Algunos de los *hackers* éticos trabajan en equipos llamados ***red teams*** o ***tiger teams***.

Ataques famosos: Twitter

En julio de 2020 Twitter recibió un ataque muy sonado, en el cual se utilizaron cuentas de personajes famosos reales como Elon Musk, Barack Obama, Bill Gates o Joe Biden, y algunas empresas como Apple o Uber. Estas cuentas solicitaban una donación en bitcoins a un supuesto proyecto del sector sanitario. El objetivo fue el de recaudar 117.000 dólares en bitcoins, cifra que lograron obtener los atacantes.

FIGURA 2.2. Cuentas afectadas y número de seguidores.

Según la investigación de Twitter, parecía que se trataba de un ataque de ingeniería social a empleados internos de la compañía con acceso a sistemas internos que permitieron el control de estas cuentas. La respuesta de Twitter fue bloquear las cuentas afectadas, se borraron los mensajes y se limitó el acceso y las funcionalidades de las mismas a todas las cuentas verificadas de manera temporal.

Cómo protegernos

La mejor manera de protegernos del *phishing* es mediante el sentido común y tener unos mínimos conocimientos técnicos y de psicología social. Respecto a la parte técnica, en el siguiente capítulo veremos un ejemplo de APT donde podemos analizar un correo electrónico y ver si viene de una persona legítima y, respecto a la parte social, la clave está en conocer cuáles son los trucos que utilizan los tipos malos. Por supuesto, se recomienda encarecidamente que siempre se disponga de, al menos, doble factor de autenticación como medida para proteger la identidad digital.

FIGURA 2.3. Cuenta oficial de Twitter.

Respecto a los "trucos", se trata de jugar con la mente y comportamientos humanos para así atraer la atención de la víctima.

- **Inmediatez:** Se utiliza la inmediatez para que la persona no tenga tiempo de pensar dos veces si realmente tiene sentido lo que le están pidiendo a la víctima.
- **Temas generalistas:** Los temas que se tratan son generalistas, tareas que realizamos todos como pago de impuestos, mantenimientos, accesos a la banca electrónica, facturas, envío de paquetes, alertar que algo va mal, etc. Además, utilizan temas de actualidad, como comentábamos, en el 2020, el tema más utilizado fue el "Covid-19".
- **Empresas conocidas:** Además de los temas, las empresas son muy conocidas y prácticamente todos somos o hemos sido clientes de las mismas.
- **Recompensa suculenta y gratuita:** Se suele ofrecer una recompensa suculenta, no desmesurada, pero lo suficientemente buena como para que a la persona le llame la atención. Además, la recompensa suele ser gratuita o requerirá muy poco esfuerzo obtener el premio, bien porque han sido agraciados por un sorteo u otros motivos.
- **Respecto a la autoridad:** Cuando el mensaje viene de una autoridad, como pueden ser la policía o la guardia civil, tendemos a prestar más atención. De ahí que al *ransomware* que utiliza técnicas de ingeniería social fue inicialmente conocido como "el virus de la policía".
- **Aceptación social:** Se trata de una manera de ciberextorsión. Los atacantes suelen amenazar a la víctima con hacer pública cierta información que conocen de ella, como, por ejemplo, difundir un vídeo privado.

No obstante, muchos ataques de *phishing* pueden ser bastante sofisticados. Para evitar caer en cualquier estafa, os dejamos algunos consejos que podrán ayudaros:

4 | Hacker mindset

Término *hacker*

Lo primero que nos gustaría detallar en este capítulo es la acepción del término *hacker*. En su origen hace alusión a una persona con grandes habilidades en el manejo de sistemas que es capaz de encontrar fallos y buscar técnicas para mejorar dicho sistema. No obstante, si buscamos en la RAE el término, también está aceptado utilizarlo como "pirata informático", es decir, una "persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta". En nuestro caso, no dejamos de ser unos nostálgicos y en contadas ocasiones nos veréis utilizar dicho término en su significado de pirata informático, preferimos usar términos más adecuados como cibercriminal, ciberatacante o ciberdelincuente, pero bien es cierto que nos parecía acertado titular este capítulo como "Hacker *mindset*" o "Mentalidad del criminal" para el buen entendimiento del lector general y simplificar dicho título.

Introducción

Para poder protegernos de las más avanzadas técnicas de ataque necesitamos conocer cómo piensan los tipos malos, cuáles son sus motivaciones, por qué atacan, de qué manera lo hacen y cómo podemos protegernos. El conocer mejor la mentalidad del atacante nos puede ayudar, primero, a entender el porqué y el para qué de estos ataques y, segundo, nos ayudará a anticiparnos a estos ataques. Para ello hemos querido dividir este capítulo en dos partes:

Tamaulipas y Sinaloa. Según *El Universal*, se documentaron 849 cuentas falsas en total que recibieron uno 500 millones de pesos (unos 21 millones de euros aproximadamente). Aunque fueron 7 personas las detenidas como cabecillas del ataque, se cree que participaron en él alrededor de 700 personas, teniendo en cuenta las personas que acudieron a retirar el dinero de los cajeros.

Hacktivistas

Hacktivistas o *hackers* motivados ideológicamente están motivados por política, social o ideología y se dirigen a sus víctimas para lograr un cambio en las mismas a través de sus ataques. Sin duda, el grupo más conocido es Anonymous.

El término hacktivismo está compuesto por *hacker* y activismo, y fue acuñado por el crítico cultural y autor Jason Sack en un artículo sobre la artista de medio Shul Lea Cheand, publicado en *InfoNation* en 1995. Normalmente, estos actores tratan de reivindicar posturas políticas y sociales usando la tecnología e Internet de forma no violenta. Habitualmente, los ataques están dirigidos a gobiernos, instituciones públicas o grandes empresas.

Los ataques más comunes son los ataques de DDoS a sitios web para inhabilitarlos o *defacement* de webs, ambos con un propósito de hacer un daño reputacional. También se pueden dar otros ataques como suplantación de identidad o exfiltración de información.

Motivación: ideológica

Las motivaciones sociopolíticas son el principal conductor dentro de los grupos hacktivistas. Los ataques con motivaciones sociopolíticas se producen desde la mitad de los años 90, cuando muchos grupos de activistas que venían haciendo protestas desde los años 70 se trasladaron al ámbito digital. Muchas de las actuaciones estaban asociadas con protestas a grandes organizaciones, defensa de los derechos humanos y del medio ambiente, críticas a acciones internacionales sobre determinadas políticas o protestas contra acciones de guerra. En definitiva, es una forma de protestar frente a cambios sociales y políticos. Entre otras motivaciones, podemos destacar la de que el conocimiento sea libre, la promoción de la libertad de información haciendo uso de software libre y plataformas descentralizadas, así como mayor igualdad económica-social.

El hacktivismo supone un conjunto de emociones para la persona. Podríamos decir que se trata de una mezcla de enfado o ira, asco y desprecio. Los hacktivistas creen en la causa. Estas emociones se convierten en sentimientos de descontento con determinadas instituciones sociales, indignación y resentimiento.

También en ocasiones se da un sentimiento de patriotismo y toman más relevancia protestas de la esfera política ligado a conflictos internacionales o locales donde hay algún tipo de confrontación política.

El grupo organizado hacktivista más famoso sin duda es **Anonymous**. Es un grupo internacional descentralizado y muy conocido por los diferentes ataques contra gobiernos, instituciones y agencias gubernamentales, así como determinadas corporaciones. Este grupo se creó en 2003 en el *imageboard 4chan* y del foro Hackers, como un movimiento que nació por diversión. Las motivaciones de Anonymous son la libertad de expresión, el acceso libre a la información, la independencia de Internet y en contra de diversas organizaciones entre las que se encuentran el Daesh, la iglesia de la Cienciología, los servicios públicos, consorcios con presencia global, sociedades de derechos de autor y, en general, sistemas de censura gubernamentales. Los miembros de Anonymous (conocidos como *Anos*) son conocidos por llevar máscaras de Guy Fawkes, como se ha podido ver en algunas películas y series de televisión, quizás la más conocida *V de Vendetta*. Guy Fawkes fue unos de los integrantes del grupo de católicos ingleses que intentó asesinar al rey Jacobo I en la fallida conspiración de la pólvora. En ella se intentó volar la Cámara de los Lores en Londres en 1605. El uso de la máscara de Guy Fawkes como efigie tiene largas raíces como parte de las celebraciones de la Noche de Guy Fawkes.

FIGURA 4.9. Máscara de Anonymus.

- *Spanning Tree Protocol* (STP).
- *Cisco Discovery Protocol* (CDP).
- *Dynamic Trunking Protocol* (DTP).
- *Dynamic Host Configuration Protocol* (DHCP).
- *Hot Standby Router Protocol* (HSRP).
- IEEE 802.1Q.
- IEEE 802.1X.
- *Inter-Switch Link Protocol* (ISL).
- *VLAN Trunking Protocol* (VTP).

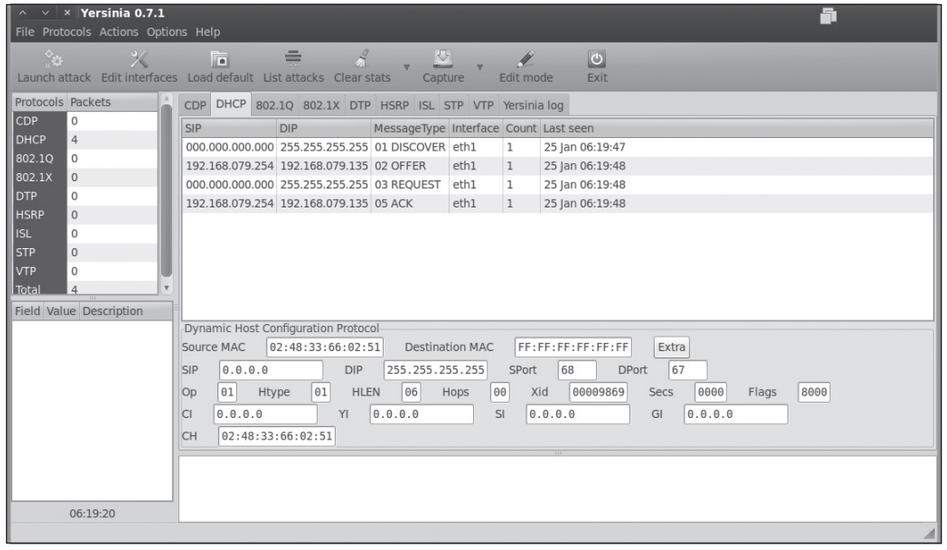

FIGURA 5.8. Interfaz gráfica de Yersinia.

Hardware de red

En esta sección se identifican algunos de los elementos hardware que se pueden encontrar en las redes LAN. Desplegarlos en la red depende de qué tipo de red tengamos y la conectividad que queramos.

El más común de los elementos hardware de red son los adaptadores Ethernet. En cualquier PC y en cualquier sistema que necesite conectividad, tendrá uno o más adaptadores de Ethernet. Estos adaptadores suelen presentarse en forma de módulos o tarjetas que se acoplan al hardware del equipo. Aunque estos adaptadores son de equipo final, para que exista conectividad dentro de una red LAN y conectividad con Internet, son necesarios múltiples equipos desplegados en la infraestructura.

En algunos casos suelen denominar hardware de red a elementos tales como teléfonos móviles, *tablet* o incluso a las televisiones inteligentes.

Repetidor

Un **repetidor** es un elemento con una funcionalidad muy básica, se ubican *inline* recibiendo todo el tráfico de una red y lo devuelven amplificado. Estos elementos funcionan en la capa física (nivel 1), por lo que no disponen de capacidad de conmutación o enrutamiento ni capacidad de control del *broadcast* o de los dominios de colisión.

Existe una regla que se debe aplicar en redes que utilizan repetidores, la regla del "**5-4-3**". Lo que nos viene a decir es que la ruta entre dos *host* de la red no debe ser mayor que 5 segmentos y 4 repetidores, además como mucho debe haber 3 de esos 5 segmentos con dispositivos conectados que no sean los propios *host*.

Bridge

Un ***bridge*** o **puente** conecta dos segmentos de una red. Estos dispositivos funcionan en la capa de enlace pudiendo analizar las tramas Ethernet, controlando los dominios de colisión. Almacenan las direcciones MAC de los equipos de los segmentos conectados para poder saber por cuál interfaz les deben reenviar los paquetes. También almacenan las tramas completas para verificar el CRC (*Cyclic Redundancy Check*, comprobación de redundancia cíclica), pudiendo descartar tramas si encuentra un error.

Switch

Los ***switches*** son una evolución de los *bridges*, trabaja en la capa de enlace (capa 2) y añade más funcionalidades de las que disponen los *bridges*. Cada puerto de un *switch* define un dominio de colisión, pero son parte del mismo dominio de *broadcast*. Dependiendo del tipo de direccionamiento de tramas tenemos:

- ***Store-and-Forward*:** Este es el tipo de direccionamiento que aplican los *bridges*, almacenando las tramas y comprobando que no tienen ningún tipo de error.
- ***Cut-Through*:** Este tipo de direccionamiento tiene menos latencia, pero puede propagar más errores, ya que reenvía la trama comprobando solo una parte (6 bytes) de la trama.
- ***Adaptative Cut-Through*:** El *switch* funciona en los dos modos anteriores. Puede seleccionar el modo el administrador o puede disponer de inteligencia para escoger un modo u otro basándose en el número de tramas con errores que hayan sido reenviadas.

Herramientas completas

Hasta ahora hemos visto algunos ataques y algunas herramientas que puedan ayudar a probar dichos ataques, pero existen soluciones más completas que aglutinan diferentes herramientas para ofrecer, de forma automatizada, diferentes ataques usando combinación de la mayoría de herramientas comentadas hasta ahora.

WiFiSlax no es una herramienta de *hacking*, directamente es una distribución Linux especializada en el análisis de redes Wireless que ya tiene instaladas todas las herramientas necesarias para llevar a cabo los análisis que se necesiten. Comparte muchas herramientas con Kali Linux, pero, al estar especializada en algo en concreto como es WiFi, tiene más herramientas, así como diccionarios y otros elementos que complementan.

FIGURA 5.29. Categorías de herramientas en WiFiSlax. Fuente: `wifislax.com`.

La distribución puede descargarse desde su página web (`https://www.wifislax.com`) y seguir el proceso de grabado ISO que prefiera el lector; en la propia página se encuentran diferentes manuales para su instalación y también para su uso.

Por el otro lado, tenemos a una aplicación concreta como es LINSET (siglas de *Linset Is Not a Social Enginering Tool*), la cual nos permite auditar una red WiFi de forma fácil con el objetivo de conseguir claves mediante la interacción con los usuarios que están conectados de forma legítima. Más que una aplicación, es un gestor que controla diferentes herramientas por debajo, automatizando cada uno de los pasos con esas herramientas para su facilidad y usabilidad.

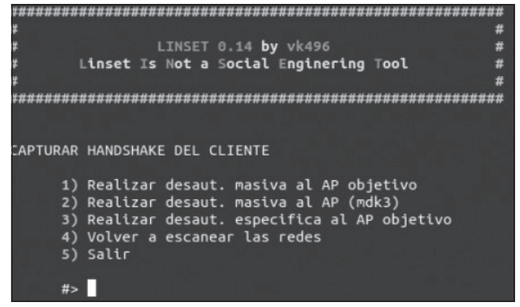

FIGURA 5.30. Captura del *handshake* en WPA2 mediante desautenticación masiva con LINSET.

Tareas posataque

Una vez que se ha conseguido acceso a la red objetivo, el atacante puede intentar permanecer lo más oculto posible o comenzar a buscar otras nuevas redes pivotando desde la red Wi-Fi. En un entorno profesional, sí tiene sentido lo segundo, pero, si el atacante lo único que busca es robar la conexión a su vecino, su objetivo será pasar lo más desapercibido que pueda. Mantenerse oculto completamente es imposible; al estar en una red local, el *router* Wi-Fi tendrá visibilidad a nivel de MAC y las actividades realizadas quedarán registradas en los *logs*. Por ello, lograr que el atacante se mantenga "menos visible" se conseguiría por medio de estas acciones:

- Usar una dirección IP no común. Lo normal es que las direcciones IP en una red Wi-Fi se asignen mediante DHCP comenzando por las más bajas. Si un atacante se conectara así y el usuario legítimo que casi siempre utiliza una IP concreta observa que ya no la utiliza puede levantar sospechas.
- Considerar la red Wi-Fi como una red pública.
- No incluirse en el grupo de trabajo por defecto.
- En un entorno Windows no utilizar:
  - Cliente para redes Microsoft.
  - Compartir impresoras y archivos para redes Microsoft.
  - Protocolo de Internet versión 6, a no ser que sea necesario.

Como recomendación general, la seguridad que se ponga en la nube debe ser, al menos, como la existente en los entornos *on-premise* del cliente. En caso de que no existiera un nivel de seguridad considerablemente aceptable, lo recomendable es construir un modelo de trabajo en nube con la seguridad como principio fundamental y con la tecnología nativa de las nubes como infraestructura de seguridad base. Además, si el modelo de desarrollo del cliente es ágil y con flujos CI/CD, los desarrolladores van a apreciar el uso de soluciones de seguridad nativas o con una fuerte integración vía API con la nube, ya que son fáciles de "codificar" y gestionar dentro del flujo de construcción de productos digitales, sin interrupciones debidas al chequeo de controles (como se puede ver en el capítulo correspondiente).

Por lo tanto, una buena estrategia de seguridad pasa por disponer de una base de análisis de amenazas y gestión del riesgo en *cloud*, así como unos controles de seguridad recogidos en políticas de seguridad que, posteriormente, podamos monitorizar para saber el nivel de salud de seguridad de la infraestructura en nube.

Buenas prácticas de seguridad

Como buenas prácticas generalizadas para el tema de nube, tenemos el **Cloud Controls Matrix** (matriz de controles de nube), definido por la CSA (Cloud Security Alliance). CSA-CCM es una certificación de buenas prácticas que permite conocer la seguridad de un proveedor de servicios en el *cloud* y, de esta manera, pueden ayudar a posibles clientes a tomar decisiones en el caso de que decidan migrar sus servicios. Puede utilizarse por una compañía para autoevaluarse o como base para definir sus propios controles de seguridad. La última versión de los controles puede obtenerse en `https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview`.

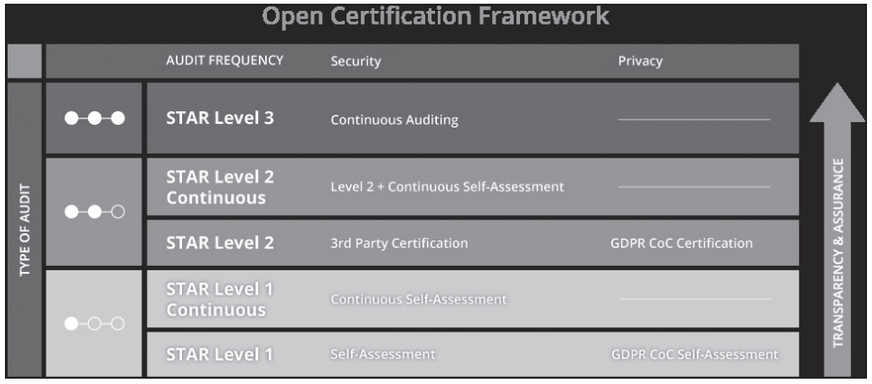

FIGURA 8.22. Certificaciones STAR. Fuente: `http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing/`.

CSA también ha puesto a disposición de los proveedores una serie de certificaciones para poder mostrar públicamente cómo de alineados están con las buenas prácticas de ciberseguridad en *cloud*: la certificación STAR (*Security Trust Assurance and Risk*, aseguramiento y riesgo de la confianza en la seguridad).

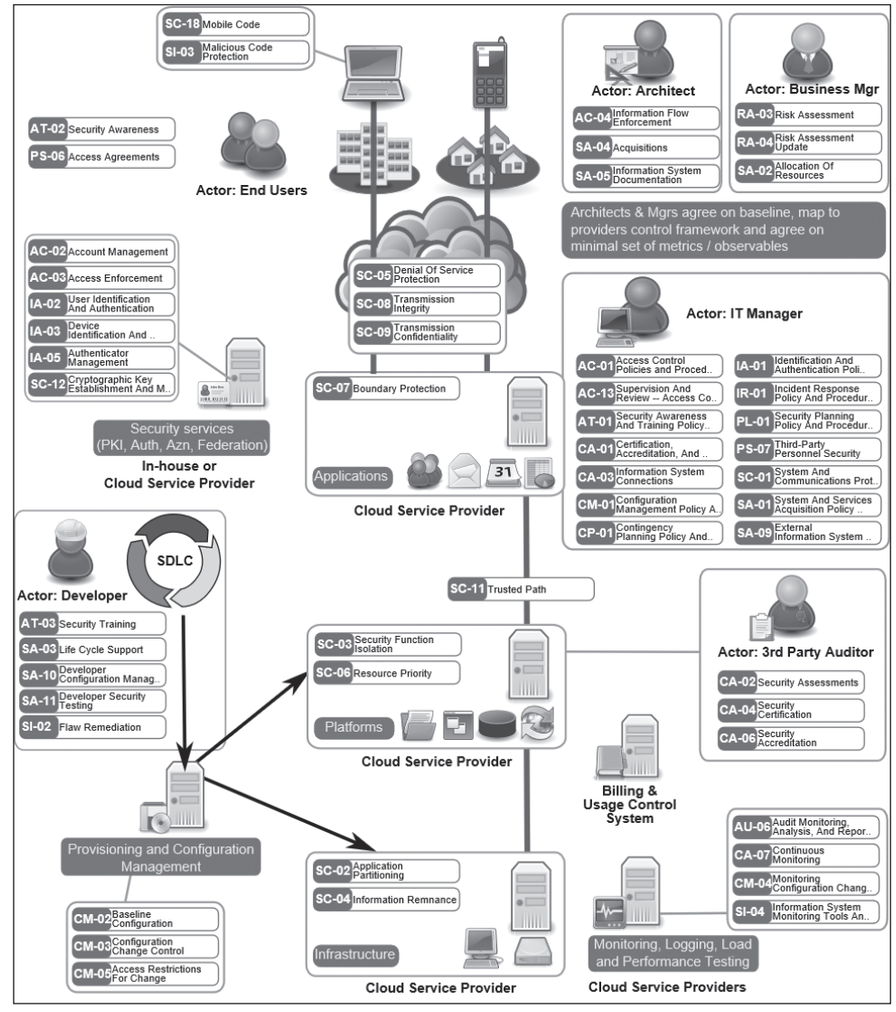

FIGURA 8.23. Arquitectura de seguridad en *cloud* de OSA (Open Security Architecture). Fuente: `http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing/`.

FIGURA 9.6. *Onboarding* digital.

Este servicio almacena información ligada a la identidad digital que puede ser usada y gestionada para realizar transacciones electrónicas, es decir, para autenticar y autorizar servicios. Habitualmente estos servicios están basados en servicios de LDAP (*Lightweight Directory Access Protocol*) y directorio activo. Los componentes y las funciones de IDaaS son los siguientes:

- **Arquitectura basada en nube y multiusuario:** La arquitectura *multitenant* proporciona muchos beneficios, ya que el proveedor lanza actualizaciones o parches automáticos y mejora el rendimiento. También da la capacidad de gestionar el aprovisionamiento de usuarios y realizar el gobierno de los mismos de manera efectiva.
- **Seguridad:** La característica principal de IDaaS es la de gestionar el ciclo de vida de la identidad del usuario. Permite autenticación multifactor o MFA, uso de tarjetas de acceso y biometría, promoviendo el acceso de manera segura.
- **SSO y federación de identidad:** El SSO mejora la experiencia de usuario y mantiene la seguridad y disponibilidad del acceso a la aplicación. El usuario puede utilizar una combinación de contraseña más segura, dado que no tendrá que recordarla siempre si accede de manera regular. Permite también poder gestionar de manera segura la autenticación de servicios *cloud* de terceros.
- **Inteligencia y analítica:** Las capacidades de análisis e inteligencia se utilizan para informar del usuario de privilegios con determinados usuarios, esta relación de usuarios, roles y responsabilidades y cómo utilizan los datos y la función de su trabajo. Esto permite a las compañías detectar anomalías que pudieran estar ocurriendo, determinados patrones de comportamiento extraños y poco habituales que pueden indicar que la persona no es quien dice ser.
- **Gobierno, riesgo y cumplimiento:** El uso de IDaaS permite ciertas capacidades de automatización e inteligencia que ayuda con el gobierno, riesgo y cumplimiento a definir y automatizar procesos específicos de las aplicaciones corporativas de las empresas.

Proveedores de identidad

Existen servicios en el mercado que permiten la identificación de los ciudadanos de manera fehaciente y hay múltiples proyectos y empresas tratando de convertirse en proveedores de identidad. Por ejemplo, el servicio de Verified.Me permite identificar a la persona utilizando información personal con su consentimiento para compartirla en determinadas conexiones como, por ejemplo, nuestro banco. Este servicio proviene de Canadá por la empresa SecureKey Technologies Inc. y está impulsado por las entidades financieras del país: BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank y TD. Se puede consultar en la siguiente URL: `https://verified.me`.

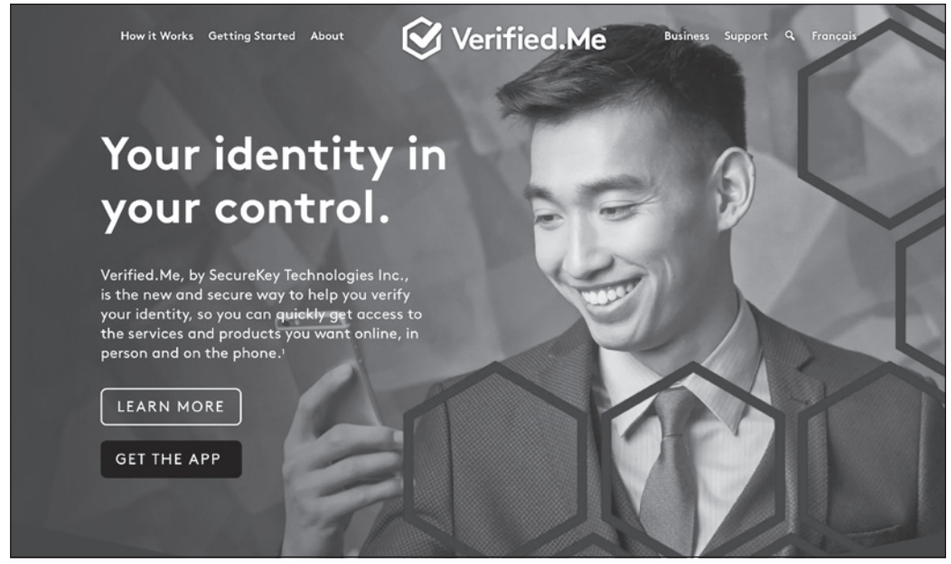

FIGURA 9.7. Servicio de identidad Verified.me.

Otro servicio interesante es el de BankID. Este da la posibilidad de identificar a los ciudadanos y permite que compañías, bancos y agencias gubernamentales se autentiquen y consoliden acuerdos con individuos en Internet. Es un servicio de identificación electrónica de Suecia y Noruega que ha sido desarrollado por los grandes bancos del país, autoridades y algunas compañías. El primer servicio salió a la luz en 2003. Las compañías que participan son Danske Bank, ICA Banken, Ikano Bank, Länsförsäkringar Bank, Nordea, SEB, Skandiabanken, Sparbanken Syd, Svenska Handelsbanken, Swedbank y Ålandsbanken. En Suecia, hay un total de 8 millones de personas utilizando de manera regular el servicio para servicios públicos

11 Metodología de *pentesting*

Introducción

El origen de los test de intrusión, *Penetration Testing* en inglés, se remonta al tiempo de las primeras redes que permitían el acceso a centros de cómputo de tiempo compartido y que comenzaron a desplegarse en entornos militares, académicos y comerciales permitiendo el acceso compartido de usuarios a recursos de procesamiento.

Durante los años 60 y a raíz de algunos incidentes, profesionales del campo de la seguridad comenzaron a plantear preguntas sobre la posibilidad de diversos escenarios en los que la seguridad de los sistemas podría ser burlada. A raíz de estos avisos, el Departamento de Defensa de los Estados Unidos (DoD) encargó la elaboración de un estudio sobre el estado de la seguridad de sus sistemas a un grupo de expertos de diferentes entornos liderados por Willis Ware. El resultado fue un extenso documento en el que se valoraba la situación de la seguridad de los sistemas de cómputo de tiempo compartido y en el que se recogían las diversas vulnerabilidades y amenazas que podrían afectar a estos sistemas.

> El reporte creado por el grupo de Ware fue y sigue siendo considerado uno de los más completos esfuerzos de análisis de seguridad de su tiempo. El documento ha sido desclasificado y es de acceso público. Es posible encontrarlo bajo el código R-609-1 entre las publicaciones de RAND Corporation y está disponible en este enlace: `http://www.rand.org/pubs/reports/R609-1/index2.html`.

La página oficial de la herramienta es `http://www.e-fense.com/helix`. Aquí encontraremos información sobre las últimas versiones de la herramienta Helix 3.

FIGURA 14.2. Helix 3.

Es una herramienta muy completa. Posee la mayoría de las herramientas necesarias para realizar un análisis forense completo, tanto de equipos como de imágenes de discos. Es multiplataformas: Mac Os X, Windows y Linux.

La versión descargada ofrece dos métodos de arranque:

- El primero, que permite iniciarse desde un sistema Windows, nos proporciona un entorno gráfico con un conjunto bastante amplio de herramientas que permiten interactuar principalmente con sistemas vivos, pudiendo recuperar la información volátil del sistema.
- Arranque desde el CD en entorno tipo Linux. En este caso, la herramienta contiene un sistema operativo completo personalizado y optimizado para el reconocimiento de hardware.

Cuando arrancamos la herramienta desde un entorno Windows, estas son algunas de las herramientas que tendremos disponibles:

- **Access PassView:** Permite acceder a la base de datos de contraseñas almacenadas en un archivo `.mdb`, creado con Microsoft Access 95/97/200/XP.
- **Astrick Logger:** Utilidad que revela las contraseñas almacenadas de algunas aplicaciones como CuteFTP, CoffeeCup Free FTP, VNC, IncrediMail, Outlook Express y otros.
- **Drive Manager:** Ayuda a identificar unidades que son del mismo tipo. Además de la etiqueta de volumen, también muestra la información de los proveedores a fin de diferenciar múltiples unidades de CD/DVD y memorias por el nombre del fabricante, versión y fecha de revisión. También permite utilizar el número de serie como un número de identificación exclusivo para cada unidad.
- **FAU:** Herramienta de respuesta a incidentes que sirve para crear la imagen de un sistema y de los dispositivos conectados.
- **FTK Imager:** Permite adquirir imágenes de dispositivos físicos y lógicos.
- **Galleta:** Analiza la información de un archivo de *cookie* y permite que el resultado sea importado a su programa de hoja de cálculo.
- **HoverSnap:** Permite tomar capturas de pantalla.
- **IECookiesView:** Permite ver detalles y manejar las *cookies* que IE almacena en una computadora.
- **IEHistoryView:** Permite ver y modificar el historial de las páginas web visitadas en Internet Explorer.
- **IRCR:** Conjunto de herramientas orientadas en su mayoría a la recopilación de datos en lugar de análisis.
- **Mail PassView:** Herramienta para la recuperación de contraseñas de ciertos clientes de correo electrónico.
- **MEMDump:** Realiza copias de 4 GB de memoria de direcciones bajo MS-DOS y Windows 9x DOS a una consola de texto o archivo binario.
- **MessenPass:** Permite recuperar la contraseña de una amplia variedad de programas de mensajería instantánea.
- **MozillaCookiesView:** Herramienta para el manejo de *cookies* de navegador Mozilla.
- **Recuperación de contraseña de red**.
- **PC Inspector File Recovery:** Programa de recuperación de datos.
- **PC On / Off Time:** Muestra las veces que una computadora ha estado activa durante las últimas 3 semanas.
- **Process Explorer:** Herramienta para el manejo de procesos.
- **Storage PassView:** Utilidad que revela contraseñas almacenadas por Internet Explorer y Outlook Express.
- **PsTools Suite:** Utilidades propias de Windows para el manejo de procesos.
- **Pst Password Viewer:** Obtención de contraseñas para archivos PST.

Todas las novedades del mundo de la seguridad informática y el *hacking* con la nueva edición revisada, actualizada y ampliada.

Cada vez es más la tecnología que nos rodea. Y aunque es indiscutible el valor que nos aporta, también es cierto que esta evolución tecnológica ha ido acompañada de un incremento en los ciberriesgos. Los ciberdelincuentes renuevan constantemente las tácticas, técnicas y procedimientos de los ciberataques, lo que hace que tanto los ciudadanos de a pie como las empresas tengan que evolucionar y conocer las últimas novedades de ciberseguridad y *hacking*.

En esta nueva edición de *El libro del hacker* os mostraremos desde los conceptos básicos de seguridad y técnicas de *hacking* hasta conocimientos avanzados, así como las más novedosas técnicas de ataque. Conoceremos las principales ciberamenazas y actores asociados. Hablaremos de ciberguerra y ciberespionaje. Abordaremos los retos y riesgos de *Cloud*, los datos, identidad digital, criptográfica y *blockchain*. Veremos técnicas de intrusión, *hacking web* y microservicios, *exploiting*, metodologías de *pentesting* y análisis forense. También abordaremos los sistemas tecnológicos industriales e IoT, los riesgos y ataques asociados.

Además, porque es interesante conocerlo, dedicamos un capítulo a indagar, desde un punto de vista psicológico y sociológico, la mente del cibercriminal, la forma de pensar, perfiles y tácticas de influencia, de manera que podamos entender mejor las motivaciones de estos profesionales del bien (*hackers* éticos) como del mal (ciberdelincuentes).

ANAYA MULTIMEDIA

www.anayamultimedia.es

ISBN 978-84-415-4433-8

2315167

9 788441 544338