Capítulo 2

Reconocimiento o footprinting

El reconocimiento, como vimos en el capítulo previo, es la primera fase en la ejecución de un hacking ético o no-ético y consiste en descubrir la mayor cantidad de información relevante de la organización cliente o víctima. Debido a que de la magnitud y certidumbre de la información recopilada dependerá que hagamos un mejor análisis posterior, es muy importante que le dediquemos nuestro mejor esfuerzo y cabeza a esta fase y que invirtamos todo el tiempo necesario en realizar un buen levantamiento de información. “Si tuviera 9 horas para cortar un árbol, le dedicaría 6 horas a afilar mi hacha”, Abraham Lincoln. Ahora bien, dependiendo de si existe o no interacción con el objetivo, las técnicas de reconocimiento pueden ser activas o pasivas.

Reconocimiento pasivo

Decimos que el reconocimiento es pasivo cuando no tenemos una interacción directa con el cliente o víctima. Por ejemplo, entramos a un buscador como Google e indagamos por el nombre de la empresa auditada, entre los resultados conseguimos el nombre de la página web del cliente y descubrimos que el nombre del servidor web es www.empresax.com, luego hacemos una búsqueda DNS y obtenemos que la dirección IP de ese servidor es la 200.20.2.2 (dirección ficticia por supuesto).

Algunos ejemplos de reconocimiento pasivo:

■Buscar en el periódico por anuncios de ofertas de empleo en el departamento de sistemas de la empresa X. Si resulta que buscan un DBA experto en Oracle, eso nos da una pista sobre qué base de datos utilizan, o si quieren un Webmaster que conozca sobre administración de Apache ya sabemos qué webserver utilizan.

■Consultas de directorios en Internet. Cuando una empresa registra un nombre de dominio, el proveedor de hosting publica información de contacto en un base de datos pública denominada Who-Is, por lo que consultándola se puede obtener información valiosa como el nombre de la empresa dueña del dominio, dirección y teléfonos de la oficina matriz, correo electrónico del administrador, rangos de direcciones IP asignados, en fin. Es posible pagar para mantener esta información privada, pero muchas empresas que adquieren un nombre de dominio no contratan elservicio de privacidad de información.

■Búsquedas en redes sociales. Sitios como Facebook, Linkedin, Twitter, entre otros, tienen joyas de información gratuita para los hackers que pueden ser usadas fácilmente en un ataque de ingeniería social.

■Recuperación de información desde la basura. A este método para nada agradable se lo conoce también como dumpster diving, pero aunque suene repulsivo puede resultar muy útil a la hora de adquirir información confidencial de una empresa. Aún en esta época de inseguridad son pocas las empresas que usan trituradores e incineradores para destruir información confidencial y aunque suene de Ripley, son muchos los empleados que "reciclan" hojas impresas de informes que salieron mal o que botan notas post-it con claves a la basura.

Reconocimiento activo

En este tipo de reconocimiento hay una interacción directa con el objetivo o víctima. Ejemplos de reconocimiento activo: Barridos de ping para determinar los equipos públicos activos dentro de un rango de IP's. Conexión a un puerto de un aplicativo para obtener un banner y tratar de determinar la versión. Uso de ingeniería social para obtener información confidencial. Hacer un mapeo de red para determinar la existencia de un firewall o router de borde.

Herramientas de reconocimiento

Existen un sinnúmero de aplicativos sofisticados que nos pueden ayudar a la hora de realizar un reconocimiento. Pero, aunque dichas herramientas nos ahorran tiempo, no significa que no podamos hacer un footprinting si no las tenemos a la mano. En lo personal, a mí me gusta empezar un reconocimiento por lo más simple: una línea de comandos y un navegador. La plataforma de sistema operativo puede ser Windows, Linux o Unix, según su preferencia. Si me preguntan, prefiero usar Kali Linux – antes Backtrack - para mis auditorías; pero en este libro procuraremos usar herramientas tanto de Linux como de Windows indistintamente, para que el lector escoja luego su plataforma de predilección. Para mayores detalles de los requisitos a nivel de sistema operativo, por favor revisar el "Apéndice A: Consejos para realizar con éxito los laboratorios". Allí se incluye información de ayuda sobre instalación de software de virtualización, descarga de máquinas virtuales víctima y referencias sobre instaladores de sistema operativo. Hecha esta aclaración y sin más preámbulos, ¡pasemos a realizar nuestro primer reconocimiento!

Capítulo 2

Footprinting con Google

Aunque existen aún muchos otros buscadores en Internet, sin duda Google es el más utilizado gracias a su tecnología de clasificación de páginas web (Page Rank), la cual nos permite realizar búsquedas de forma rápida y acertada. Para nuestro ejemplo de reconocimiento con Google iniciaremos con lo más simple: buscando por el nombre de la empresa víctima, la cual será por ahora el proyecto Scanme de Nmap 8 . Scanme es un sitio mantenido gratuitamente por Fyodor, el creador del escáner de puertos NMAP. Sobre este estamos autorizados a realizar pruebas de reconocimiento y escaneo solamente 9 , más adelante para los laboratorios de hacking usaremos máquinas virtuales víctimas provistas para tales efectos. Figura 2 - Google footprinting simple Nota: Un hacker ético jamás realiza pruebas de intrusión sobre sistemas, a menos que haya obtenido autorización de la organización propietaria de los mismos. Ni la autora, ni la editorial se hacen responsables por el mal uso derivado de las técnicas de hacking provistas en este libro. Como podemos observar en la Figura 2, la búsqueda ha arrojado más de 11 mil resultados, pero el que nos interesa está ubicado primero en la lista. Esto no siempre es tan fácil, hay empresas que tienen nombres muy comunes o tienen sitios que no están bien indexados, por lo que, no aparecerán entre los primeros resultados. Por ello, para mejorar nuestras búsquedas nos valdremos de los operadores provistos por Google.

. Resolviendo nombres con nslookup

Ahora que conocemos el sitio principal de nuestro cliente, podemos hacer una consulta DNS para conocer cuál es su dirección IP. En un ejemplo real encontraremos posiblemente más de un sitio del cliente referenciado por Google y por ende no será una sola IP la que obtengamos. De hecho la idea al obtener esta primera dirección es estimar el rango de IP's que necesitamos escanear para identificar equipos adicionales que podrían pertenecer al cliente. Asumiendo que se tratase de direcciones IP de versión 4, podríamos probar todo el rango de hosts pertenecientes a la subred. Esto último es poco práctico si se tratan de direcciones de clase A o B, puesto que el barrido de IP's podría llevar mucho tiempo. Para determinar el rango con mayor exactitud es posible valernos de otros medios de información como el directorio Who-Is o realizando ingeniería social, temas que revisaremos más adelante. En este ejemplo haremos una consulta de nombres usando el comando nslookup incluido en el CLI 11 de cualquier versión de Windows, Linux o Unix. Figura 3 - Resolución DNS con nslookup en Windows Al revisar los resultados de nuestra consulta, como se muestra en

la Ilustración 3, observamos que este sitio tiene dos direcciones, una IPv6 y otra IPv4. La dirección IPv4 pertenece a una clase A, dado que el primer octeto es 74 (un número entre 1 y 128), por lo que, el rango de hosts a analizar en un caso real sería muy grande y podría conllevar mucho tiempo. Nota: Al efectuar una auditoría de cualquier tipo es importante ser ordenado y tomar anotaciones de todos nuestros descubrimientos en el momento en que los hacemos. Esto nos permitirá más adelante atar cabos sueltos conforme vayamos desvelando más información. Hay herramientas de software que facilitan esta labor y nos ahorran tiempo a la hora de escribir el informe, tema que desarrollaremos en detalle en el capítulo sobre escritura de informes. Volviendo al comando nslookup, aún podemos obtener más información de nuestro objetivo. Para ello utilizaremos algunas opciones útiles: set type = [NS | MX | ALL] permite establecer el tipo de consulta, NS servicio de nombres, MX servicio de correo (mail exchanger) y ALL para mostrar todo. ls [-a | -d] dominio permite enumerar las direcciones del dominio especificado (para ello el servidor DNS de dicho dominio debe tener habilitada esta opción), -a nombres canónicos y aliases, -d todos los registros de la zona DNS. Veamos un ejemplo para el dominio de nuestro objetivo, en este caso nmap.org. Figura 4 - Nslookup: set type=NS y set type=MX Figura 5 - Nslookup: set type=ALL En la Figura 4 podemos observar que al establecer el tipo de consulta como NS, nos devuelve información respecto a los servidores de nombres para el dominio en que se encuentra nuestro objetivo, mientras que si la consulta es de tipo MX brinda además información acerca de quiénes son los servidores de correo para dicho dominio. Cuando utilizamos la opción ALL obtenemos la combinación de ambas consultas (NS + MX), tal como se presenta en la Figura 5. Estas simples consultas adicionales nos reportan valiosa información de la red pública de nuestro objetivo, como por ejemplo: 1. Que en realidad el dominio nmap.org está alojado en un servidor de hosting externo provisto por la empresa Linode y, 2. Que el servicio de correo es provisto por el servidor mail.titan.net con IP 64.13.134.2, la cual está en un segmento de red diferente a la delservidor scanme.nmap.org.

Obteniendo información de directorios Who-Is

Continuando con nuestro ejercicio de reconocimiento un siguiente paso podría ser obtener información haciendo consultas a una base de datos Who-Is. El Who-Is es un protocolo que permite hacer consultas a un repositorio en Internet para recuperar información acerca de la propiedad de un nombre de dominio o una dirección IP. Cuando una organización solicita un nombre para su dominio a su proveedor de Internet (ISP), éste lo registra en la base Who-Is

correspondiente. En el caso de los dominios de alto nivel (.com, .org, .net, .biz, .mil, etc.) es usualmente el ARIN (American Registry for Internet Numbers) quien guarda esta información en su base WhoIs; pero en el caso de los dominios de países (.ve, .ec, .co, .us, .uk, etc.) quien guarda la información normalmente es el NIC (Network Information Center) del país respectivo. Veamos algunos ejemplos de consultas que podemos hacer, digamos que queremos obtener información de una empresa muy conocida como Cisco Systems, dado que el dominio es cisco.com entonces podemos acudir al ARIN para nuestra consulta. Para ello apuntamos nuestro navegador a http://whois.arin.net y en la caja de texto denominada “SEARCH WHOISRWS” ingresamos el nombre de la organización, para este ejemplo: Cisco Systems. Nota: Es importante recalcar que podemos efectuar consultas Who-Is sin solicitar autorización, debido a que se trata de información que se encuentra en una base de datos pública. Figura 6 - Consulta a la base Who-Is del ARIN Esta acción nos da como resultado información valiosa relativa a nuestra consulta (ver Figura 6). Ustedes pueden analizar todos y cada uno de los resultados, pero para este ejemplo nos limitaremos a revisar la tercera opción bajo el ítem de Organizaciones: Cisco Systems (CISCOS). Como se presenta en la Figura 7, hemos obtenido información relevante sobre nuestro objetivo como la ubicación física de la empresa, cuándo se registró el nombre del dominio por primera vez, cuándo fue actualizado y tenemos además la opción de verificar información adicional visitando los enlaces dispuestos al final del reporte: secciones "See Also" (véase también). Por ejemplo, si deseamos conocer cuáles son los bloques de direcciones IP asignados a Systems, haremos click sobre el enlace "Related Networks" (redes relacionadas) y obtendremos una respuesta como la que se muestra en la Figura 8. Figura 7 - Información detallada de organización en el Who-Is Figura 8 - Who-Is: rangos de IP's asignados al objetivo Esto nos demuestra la importancia de mantener esta información privada, porque si bien es cierto que en el momento en que tenemos equipos dentro de la red perimetral que brindan un servicio público, sus IP's también serán públicas, no hay por qué facilitarle tanto la vida al cracker dándole a conocer fácilmente todos los rangos de direcciones que nos han sido asignados. Una recomendación útil es pagarle al NIC respectivo para que mantenga nuestra información privada, es decir, que no se publique en la base Who-IS. Este es un servicio que normalmente ofrecen los NIC's por una suma anual bastante módica. Algunos de ustedes me dirán que no hay información que no sea ya conocida públicamente sobre nuestro objetivo (Cisco Systems), como para que amerite pagarle al ARIN para que oculte dicha información y en este caso puede ser cierto; pero veamos un ejemplo de un NIC regional para explicar mi punto. A continuación realizaré una consulta Who-IS usando como objetivo a mi alma

máter, la Escuela Superior Politécnica del Litoral (ESPOL) en el NIC de mi país Ecuador. Figura 9 - Consulta al Who-Is del NIC.EC En primera instancia la información que nos muestra (ver Figura 9) es similar a la expuesta por el ARIN, pero observemos la segunda parte del reporte: Figura 10 - Nombres, correos y teléfonos obtenidos del NIC.EC En la Figura 10 podemos ver que la consulta nos muestra nombres de contactos reales que trabajan en la institución, así como números de teléfonos directos y correos electrónicos de dichos funcionarios. Esto podría prestarse para realizar un ataque de ingeniería social, por lo que resulta preocupante que esté divulgado en una base de datos pública.

Usando herramientas todo-en-uno durante el reconocimiento

Bien, hasta ahora logramos algún progreso en nuestros esfuerzos durante la fase de reconocimiento, pero lo hemos hecho de forma dispersa y progresiva usando varios recursos aislados como Google, el comando nslookup y consultas a directorios Who-Is. Hacerlo de esta manera cumple con nuestro objetivo de aprendizaje, pero no es eficiente desde el punto de vista práctico, porque desperdiciamos tiempo valioso que podríamos aprovechar en las siguientes fases de nuestro análisis. Es por esto que ahora revisaremos herramientas de software que no sólo nos ahorran tiempo en el reconocimiento, sino que además nos facilitan la escritura del informe, gracias a que cuentan con interfaces gráficas amigables que muestran la información recolectada de forma ordenada y, en algunos casos, cuentan inclusive con opciones para generar reportes que resultan muy útiles para ser incluidos como anexos de nuestra documentación. En breve revisaremos los aplicativos: Maltego Traceroute visual E-Mail Tracker Pro Maltego

Maltego

es una herramienta que permite recabar datos sobre una organización de forma sencilla, a través del uso de objetos gráficos y menús contextuales que permiten aplicar "transformaciones" a dichos objetos, a través de las cuales se obtiene a su vez mayor información. Una transformación es una operación que aplicada sobre un objeto genera información adicional sobre el mismo, la cual es reflejada en forma gráfica en Maltego mediante una estructura tipo árbol. Esto quizás suena un poco abstracto, conque mejor veamos un ejemplo. Los objetos pueden ser de diferentes tipos: dispositivos, elementos de infraestructura, ubicaciones, pruebas de intrusión, personales y sociales. Los dispositivos pueden ser equipos como teléfonos o cámaras; los elementos de infraestructura incluyen objetos como nombres de dominio, direcciones IP, entradas DNS y

similares. Las ubicaciones se refieren a sitios físicos como ciudades, oficinas, etc. Los objetos de tipo pruebas de intrusión nos permiten agregar información obtenida acerca de tecnologías utilizadas por la organización auditada. Los elementos personales se refieren a información como nombres de personas, documentos, imágenes, números de teléfono y afines, mientras que los objetos sociales involucran datos obtenidos de redes sociales como Facebook, Twitter, entre otras. Para usar Maltego de forma gratuita en su versión de código abierto, Maltego Community, es necesario registrarse y crear una cuenta en los servidores de Paterva (la empresa que desarrolla Maltego). Esto es necesario puesto que son los servidores de Paterva quienes realizan las transformaciones. Dado que dichos servidores son compartidos por todos los usuarios que usan Maltego de forma gratuita, en ocasiones las transformaciones pueden demorar un poco en ejecutarse; debido a esto Paterva ofrece una opción pagada de Maltego que incluye mejoras en tiempos de respuesta. Esta vez usaremos como objetivo a Google, les recuerdo que se trata de información pública y por ende no contravenimos ninguna ley. Figura 11 - Ejecutamos Maltego en Backtrack/Kali Linux Una vez iniciado Maltego (Figura 11) deberemos completar los pasos para la configuración inicial siguiendo las instrucciones en pantalla. Esto incluye la creación de una cuenta para acceso a los servidores y la obtención del paquete de transformaciones actualizado (ver Figura 12). La primera vez crearemos un gráfico en blanco para jugar con él y probar las tan esperadas transformaciones. Empezaremos por expandir el menú "Infrastructure" ubicado a la izquierda y arrastraremos un objeto de tipo "Domain" a un espacio libre en nuestro nuevo gráfico, como se denota en la Figura 13. Para cambiar el nombre de dominio por defecto, seleccionamos el objeto con el puntero del mouse y cambiamos el valor en la caja de propiedades ubicada en la parte inferior derecha de la interfaz. En este ejemplo cambiaremos paterva.com por google.com (Figura 14). Figura 12 - Configuración inicial de Maltego Figura 13 - Agregamos un objeto tipo Dominio en Maltego Figura 14 - Nuestro dominio a analizar es google.com Acto seguido aplicaremos la primera transformación, esto lo haremos haciendo click derecho con el mouse y ejecutando la opción "Run Transform -> DNS from Domain -> All in this set" (Figura 15). Esto le indica a Maltego que debe ejecutar todas las transformaciones relacionadas con el protocolo DNS para el objeto seleccionado, en este caso: el dominio google.com. Como se ilustra en la Figura 16, el resultado es un árbol que contiene distintos hosts que pertenecen al dominio google.com, el cual se muestra como nodo raíz. Las flechas indican que existe una relación entre la raíz y cada nodo hijo. El símbolo de estrella ubicado junto al ícono de un host indica que éste provee servicios de webserver. Figura 15 - Aplicamos todas las transformaciones DNS al dominio google.com Figura

16 - Resultado obtenido al aplicar las transformaciones DNS Ejecutemos ahora una segunda transformación. Dependiendo del tipo podremos aplicarla sobre el nodo raíz, en cuyo caso la misma se replicará de forma recursiva a sus nodos hijos, o sobre un objeto en particular. Para el ejemplo aplicaremos la transformación de resolución de direcciones IP sobre el nodo www.google.com (Run Transform -> Resolve to IP -> To IP Address [DNS]). La ejecución toma algunos segundos y se obtiene información adicional como se muestra en la Figura 17. Figura 17 - Obtenemos las IP's asociadas a google.com Si continuamos aplicando transformaciones nuestro gráfico se irá llenando de información muy útil para nuestro análisis, pero también se volverá difícil de visualizar. Por este motivo Maltego cuenta con tres tipos de vista: la principal que es en la que inicia por defecto y sobre la que hemos estado trabajando, la vista de burbuja y la de lista de entidades. Adicionalmente podemos escoger la disposición de los objetos en la pantalla, seleccionando uno de los íconos ubicados al lado derecho de los botones de vista; esto es posible en la vista principal y de burbuja solamente (ver Ilustraciones 18 y 19). Figura 18 - Maltego vista de burbuja (bubble view) Figura 19 - Maltego lista de entidad (entity list) Usando Maltego no sólo ahorraremos tiempo durante la fase de reconocimiento sino que además podremos visualizar la relación existente entre las diferentes piezas de información recolectadas y disponerla de forma ordenada, lo cual será de gran utilidad al momento de escribir el informe de auditoría. Es importante mencionar que no dependemos sólo de la información obtenida de las transformaciones para armar nuestro gráfico. Si obtuviésemos datos sobre nuestro objetivo por otros medios, podríamos agregarlos como objetos dentro de nuestro gráfico y ejecutar nuevas transformaciones que nos permitan hallar relaciones que de otro modo podrían pasar desapercibidas. Para ilustrar este punto crearé un nuevo gráfico y en esta ocasión añadiré un objeto de tipo personal. El objeto será una persona, en este ejemplo he escogido una figura pública como Bill Gates. Una vez definido el elemento, sobre él ejecutaremos todas las transformaciones posibles (Run Transform -> All Transforms). Para adquirir información más exacta, Maltego nos consulta información sobre el dominio de correo, websites y otros datos útiles. La Figura 20 presenta el resultado obtenido. La cantidad de información recuperada es tan grande que resulta difícil visualizarla y distinguir lo que sirve de lo que no. En los casos de objetos de tipo personal es muy probable que la ejecución de una transformación traiga consigo elementos de información que no vienen al caso. Para eliminar un componente simplemente hacemos click derecho y escogemos la opción "Delete". Cada cierto tiempo conviene verificar que nuestra base de transformaciones se encuentre al día, para actualizar la base basta con

seleccionar la pestaña "Manage" ubicada en la parte superior de la ventana y escoger el botón "Discover Transforms". Figura 20 - Resultados de aplicar todas las transformaciones a un objeto persona Existen muchas más acciones que podemos realizar con Maltego dado que es una herramienta muy versátil, pero un análisis más profundo del mismo escapa del alcance de este libro. Información adicional se encuentra disponible en el sitio web oficial de Paterva. Herramientas de Traceroute visual Durante la ejecución de un hacking externo de caja negra resulta útil conocer la ubicación geográfica de un determinado objetivo. Imaginemos por ejemplo que hemos determinado los nombres del servidor de correo y del servidor web de nuestro cliente y queremos saber si estos servicios están alojados en la red pública administrada por dicha empresa o si por el contrario están ubicados en un hosting externo como Yahoo Small Business, Gator, o similares. ¿Por qué queremos conocer esto? Muy simple, si resulta que están alojados en un hosting externo, en el hipotético evento de que lográramos ingresar a dichos equipos, en realidad estaríamos vulnerando al proveedor de hosting, en cuyo caso nos podríamos enfrentar a una posible demanda legal por parte del mismo. Debido a esto es conveniente realizar un trazado de ruta que nos facilite conocer la ubicación geográfica de un nombre de host o de una dirección IP. De ese modo sabremos si tiene sentido o no tratar de vulnerar dicho equipo. Existen en el mercado diversas aplicaciones de traceroute visual, por mencionar algunas: Visual IP Trace, Visual Route . Algunas de ellas son gratuitas o tienen versiones pagadas que tienen características adicionales como emisión de reportes en formato html. Además de las aplicaciones que se instalan en el PC existen utilidades web para traceroute visual disponibles para uso gratuito en Internet como por ejemplo, la provista por la empresa You Get Signal. Estos aplicativos web tienen como ventaja su simplicidad, pero su debilidad es que no generan informes, por lo que corresponde al investigador realizar capturas de pantalla para incluirlas como evidencia dentro de la documentación. Veamos algunos ejemplos de las utilidades mencionadas. Figura 21 - Trazado visual en Visual IP Trace Figura 22 - Consulta en Visual Route Figura 23 - Traceroute visual desde el aplicativo web de You Get Signal Podemos notar en los gráficos previos (Ilustraciones 21 a 23) la información recuperada al realizar una consulta de traceroute visual para el host www.elixircorp.com. Vale observar que todas las herramientas lo ubican en Estados Unidos, en un servidor de Yahoo, lo cual dado que Elixircorp es una empresa con oficinas en Ecuador nos lleva a concluir que se trata de un hosting externo, por tanto si lográramos ingresar al mismo estaríamos hackeando en realidad a Yahoo; de ahí la importancia de determinar la ubicación geográfica de un host descubierto en un hacking externo antes de pasar a las fases de escaneo y explotación.

Herramientas de rastreo de correos

Es posible que durante la ejecución de un hacking externo nos topemos con un caso como el descrito en el ejemplo previo, es decir que nuestro cliente tenga tercerizados los servicios web, de DNS y correo y resulte que la resolución de IP's y el trazado visual sólo nos lleven hacia el proveedor del hosting. Si adicionalmente ocurre que no hallamos ningún otro servicio público durante el reconocimiento, esto puede resultar en frustración para el consultor. ¿Pero y entonces qué hacemos? Bueno, es seguro que nuestro cliente tiene acceso a Internet, de lo contrario ¿por qué tendría un servicio de correo electrónico corporativo? Además hoy en día resulta sumamente inusual que una organización esté desconectada del Internet. En consecuencia debe haber una red en las oficinas del cliente que quizás tenga servidores internos y por supuesto estaciones conectadas a través de cableado estructurado o por medio de una red inalámbrica, o ambas. Lo anterior implica que como mínimo el ISP ha asignado a nuestro cliente una IP pública para la salida a Internet, por lo cual debe haber un router o un firewall de borde haciendo NAT (traducción de direcciones) para que los usuarios internos puedan navegar. En este caso obtener dicha IP pública es ahora nuestro objetivo, veamos cómo podemos conseguir esto a través del análisis de un correo electrónico. Planteada la nueva meta ahora deberemos lograr que nuestro cliente nos envíe un correo electrónico, para luego poder analizar los datos de la cabecera del mismo y determinar la dirección IP de origen. Esto es bastante sencillo dado que hemos sido contratados por él para ejecutar un hacking ético, podríamos enviarle un correo so pretexto de contarle cómo va nuestro avance en la auditoría y esperar a que nos responda. Para este análisis podemos utilizar cualquier herramienta de rastreo de correos o inclusive revisar manualmente la cabecera del mismo; pero el uso de herramientas automatizadas tiene como ventaja la obtención de un informe que podemos incluir a manera de anexo en nuestro reporte. Es necesario mencionar que las herramientas de análisis de correos no sólo sirven para determinar la IP de origen de un mail, sino que además permiten verificar si el remitente es en efecto quien dice ser, es decir, que podemos usar estos aplicativos para determinar si nos encontramos frente a un mail falso o ante una suplantación de identidad.

Capítulo 2

Laboratorios de reconocimiento

Footprinting con SmartWhoIs

Es una herramienta comercial que permite realizar consultas a directorios Who-Is de forma gráfica. En este sencillo laboratorio descargaremos una versión de prueba para realizar una consulta sobre un domino objetivo. En el laboratorio actual usted usará el aplicativo SmartWhoIS para obtener información sobre dominios objetivos desde un repositorio Who-Is. Nota: Para la ejecución del laboratorio usaremos Windows como estación hacker. El software SmartWhoIs puede descargarse desde http://www.tamos.com/download/main/ en modalidad de prueba por 30 días. 1. Inicie el aplicativo SmartWhois. Tal y como se muestra en la Figura 24, la interfaz es sumamente intuitiva. 2. A continuación realizaremos una consulta por el dominio scanme.nmap.org. Como se observa en la Figura 25 no hay mayor información, debido a que este es un dominio de prueba provisto por Figura 24 - Interfaz de SmartWhoIs Figura 25 - Consulta Who-Is del host scanme.nmap.org 1. Probemos ahora un dominio de una empresa pública cualquiera y observemos la información que nos muestra SmartWhois. Para este ejemplo probaremos con el dominio de Cisco Systems: Figura 26 - Resultados de consultar el dominio cisco.com 1. Como podemos comprobar obtuvimos mayor información en esta ocasión (ver Figura 26). 2. Para protegernos de este tipo de reconocimiento basta con pagar un valor adicional anual al servicio de hosting para mantener privada la información del servicio Who-Is. Sin embargo, no es posible eliminar por completo el reconocimiento, puesto que siempre habrá información pública de la empresa disponible en Internet u otros medios de comunicación.

Reconocimiento con Sam Spade

Sam Spade es una aplicación de descubrimiento que debe su nombre al famoso detective protagonista de la novela El Halcón Maltés y al igual que el personaje, esta herramienta nos permite realizar una labor detectivesca para recabar información sobre nuestro objetivo. La licencia de Sam Spade es gratuita (freeware) y está disponible para plataformas Windows. En la actualidad el autor del software, Steve Atkins, ha dejado de mantener el sitio web original, samspade.org, lo que es una pena; pero gracias a que la utilidad de la herramienta sigue vigente, organizaciones como PCWorld mantienen copias de descarga 14 . En el laboratorio actual usted usará el aplicativo Sam Spade para efectuar reconocimiento sobre un dominio objetivo. Nota: Para la ejecución del laboratorio usaremos Windows como estación hacker. El software Sam Spade

puede descargarse desde http://www.pcworld.com/downloads/file/fid,4709-order,1-page,1-c,alldownloads/description.html gratuitamente. 1. Una vez descargado, la instalación de Sam Spade es sumamente sencilla y basta con ejecutar unos cuantos clicks del mouse. En la Figura 27 podemos ver la pantalla inicial del aplicativo. 2. Luego de cerrar el tip del día procederemos a realizar una consulta sobre un dominio cualquiera. Para este ejemplo usaremos cisco.com. Escribimos nuestra consulta en la caja de texto ubicada en la parte superior izquierda de la ventana y damos Enter. 3. Como se presenta en la Figura 28, dicha consulta nos devuelve información contenida en la base Who-Is del ARIN. Ahora seleccionaremos la opción .net.12.1DNS, con el fin de obtener datos del servicio de nombres, adicionalmente si hacemos click sobre el ícono de IPBlock, Sam Spade intentará determinar rangos asignados al objetivo y la propiedad del mismo (ver Figura 29). Figura 27 - Pantalla inicial de Sam Spade Figura 28 - Consulta sobre dominio en Sam Spade 1. Para la opción de Dig (cavar) es necesario especificar explícitamente la dirección IP de nuestro servidor de nombres; esto lo hacemos escogiendo el menú Edit -> Options -> Basics. Aquí le podemos poner un visto en la opción de usar DHCP o bien escribir manualmente la IP de nuestro DNS server (ver Figura 30). 2. Esta opción nos permite obtener información detallada acerca del espacio de nombres del objetivo (ver Figura 31) de manera similar a como lo muestra el comando nslookup. Figura 29 - Diversas consultas con Sam Spade Figura 30 - Es necesario especificar el servidor DNS para usar la opción "Dig" Figura 31 - Digging con Sam Spade 1. Por supuesto hay opciones adicionales que podemos explorar con Sam Spade que nos ayudarán a recabar más datos sobre nuestro objetivo y dada su simplicidad de uso, es una herramienta que no debe faltar en nuestro portafolio de aplicaciones para hackear.

Análisis de la cabecera de un correo electrónico

En este ejemplo usaremos el aplicativo Email Tracker Pro, para el efecto reproduciremos un artículo de la suscrita publicado en el blog de Elixircorp S.A. (http://blog.elixircorp.biz/2012/08/25/diseccion-de-un-correo-sobre-supuesto-ingresoforzado-a-la-embajada-ecuatoriana-en-uk-para-sacar-a-julian-assange/) sobre un caso real en el cual se analizó un mensaje de correo a pedido de Diario El Universo 15 . En el laboratorio actual realizaremos un análisis de la cabecera de un correo electrónico para establecer la dirección IP de origen y a la vez determinar si se trata de un mensaje legítimo o no. Nota: Para la ejecución del laboratorio usaremos Windows como estación hacker. El software EmailTrackerPro puede descargarse desde http://www.emailtrackerpro.com/download.html en modalidad de evaluación

por 15 días. 1. Correo electrónico masivo recibido por uno de muchos usuarios Date: Wed, 22 Aug 2012 10:21:13 -0400 To: xxxx@xxxx.com From: Sender@El-Universo.net Subject: Policias de Gran Bretana entran a embajada de Ecuador Policías de Gran Bretaña entran a embajada de Ecuador. Policías de Gran Bretaña entran a la embajada de Ecuador a capturar a Julian Assange en un operativo nunca antes visto en el último tiempo...para ver más detalles de la noticia vea el video de lo acontecido. Clic en el enlace para ver el video de la noticia: http://www.eluniverso.com/servidor_videos/index.html?Wikileaks_Video 1. Análisis del correo electrónico Para comenzar podemos observar fácilmente en el cuerpo del mensaje, posicionando nuestro puntero del mouse sobre elsupuesto enlace hacia El Universo, que en realidad es una redirección a otro sitio web con url: http://www.lene-kinesiolog.dk/templates/stripes2/images/eluniverso.php?Wikileaks_Video Figura 32 - Al colocar el puntero del mouse sobre el enlace vemos que no corresponde a El Universo Como se demuestra en la Figura 32, el sitio al que nos redirecciona pertenece a otro dominio en Internet, diferente al del Diario El Universo (www.eluniverso.com). De este primer hallazgo podemos hacer una primera conclusión y es que estamos ante un caso típico de PHISHING. En segundo lugar analizamos las cabeceras del correo electrónico para poder determinar su origen: Cabeceras del correo electrónico recibido: x-store-info:J++/JTCzmObr++wNraA4Pa4f5Xd6uensydyekesGC2M= Authentication-Results: xxxx.com; sender-id=none (sender IP is 67.227.252.136) header.from=Sender@ElUniverso.net; dkim=none header.d=El-Universo.net; x-hmca=none X-SID-PRA: Sender@El-Universo.net X-SID-Result: None X-DKIM-Result: None X-AUTH-Result: NONE X-Message-Status: n:n X-Message-Delivery: Vj0xLjE7dXM9MDtsPTE7YT0xO0Q9MTtHRD0xO1NDTD0y X-Message-Info: aKlYzGSc+LmrJ3Ojfb7kFJVwFnSrX02HeUWFh8nro8gaail7xJJLFWVVd0QXoDfVG0dCyUNULoITTTNb XwqYVhCkC8XqtFk7b1WcAzjmR78wxa9kP60BBOXuT28CVNpmYDvcZa5LchiTikUcecIlkA== Received: from host.xyz.com ([67.227.252.136]) by SNT0-MC3-F8.Snt0.xxxx.com with Microsoft SMTPSVC(6.0.3790.4900); Wed, 22 Aug 2012 07:21:13 -0700 Received: from localhost ([::1]:45501 helo=www.hotelabc.com) by host.xyz.com with esmtp (Exim 4.77) (envelope-from) id 1T4Bo1-0002qB-7w for xxxx@xxxx.com; Wed, 22 Aug 2012 10:21:13 -0400 Date: Wed, 22 Aug 2012 10:21:13 -0400 To: xxxx@xxxx.com From: El Universo Subject: Policias de Gran Bretana entran a embajada de Ecuador Message-ID: X-Priority: 3 X-Mailer: PHPMailer [version 1.73] MIME-Version: 1.0 Content-Transfer-Encoding: 7bit Content-Type: text/html; charset="iso-8859-1" X-AntiAbuse: This header was added to track abuse, please include it with any abuse report X-AntiAbuse:

Capítulo 2

Primary Hostname - host.xyz.com X-AntiAbuse: Original Domain - xxxx.com X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12] X-AntiAbuse: Sender Address Domain - El-Universo.net X-Source: X-Source-Args: X-Source-Dir: Return-Path: Sender@El-Universo.net X-OriginalArrivalTime: 22 Aug 2012 14:21:13.0570 (UTC) FILETIME=[627E0C20:01CD8071] Análisis con el software E-Mail Tracker Pro Tanto en la revisión manual como a través del reporteador incluido con el aplicativo E-Mail Tracker Pro , se puede observar que el correo electrónico no se originó desde el dominio del Diario El Universo, sino que su fuente es el host con dirección IP 67.227.252.136, ubicado físicamente en la ciudad de Lansing en el estado de Michigan en Estados Unidos. Esto nos permite realizar una segunda conclusión y es que se trata de un mail forjado, es decir falso, que fue enviado con el ánimo de hacer creer al receptor que era una noticia legítima proveniente del Diario El Universo. A continuación el reporte del análisis de cabeceras del correo electrónico en mención, generado con la herramienta E-Mail Tracker Pro: From: Sender@El-Universo.net To: xxxx@xxxx.com Date: Wed, 22 Aug 2012 10:21:13 -0400 Subject: Policias de Gran Bretana entran a embajada de Ecuador Location: Lansing, Michigan, USA Misdirected: Yes (Possibly spam) Abuse Address: abuse@liquidweb.com Abuse Reporting: To automatically generate an email abuse report click here From IP: 67.227.252.136 Header Analaysis: This email contains misdirection (The sender has attempted to hide their IP). The sender claimed to be from host.desarollosinlimites.com but lookups on that name shows it doesn't exist. System Information: The system is running a mail server (ESMTP Exim 4.77 #2) on port 25. This means that this system can be used to send email. The system is running a web server (Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.0-fips DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_jk/1.2.32 PHP/5.2.17 mod_perl/2.0.5 Perl/v5.8.8) on port 80 (click here to view it). This means that this system serves web pages. The system is running a secure web server (Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.0-fips DAV/2 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_jk/1.2.32 PHP/5.2.17 mod_perl/2.0.5 Perl/v5.8.8) on port 443 (click here to view it). This means that this system serves encryped web pages. It therefore probably handles sensitive data, such as credit card information. The system is running a file transfer server (will be disconnected after 15 minutes of inactivity) on port 21 (click here to view it). This means users are able to upload and download files to this system. Figura 33 - Origen del correo falso La Figura 33 ubica el origen del correo en la ciudad de Lansing en Estados Unidos. En la Tabla 1 podemos ver la ruta que siguió el correo electrónico desde el origen (#13) hasta el destinatario. Tabla 1 - Trazado reverso de la ruta seguida por el

correo Seguimiento del enlace contenido en el correo Al hacer click sobre el enlace incluido en el correo se nos redirige a un script escrito en lenguaje PHP, el cual hace que el navegador descargue un archivo ejecutable denominado Video_Notica_Wikileaks.exe, el cual contiene malware, es decir software malicioso. Si el usuario escoge la opción de ejecutar y no cuenta con un buen antivirus instalado y actualizado, el malware se instalará en el computador del usuario (ver Figura 34).
Figura 34 - Al hacer click sobre el enlace, se descarga un archivo malicioso en nuestro PC 1. Conclusiones Del análisis realizado podemos concluir lo siguiente: La dirección del remitente (from) es Sender@El-Universo.net, dicha dirección no pertenece a Diario El Universo sino a una empresa norteamericana llamada Brinskster, la cual no tiene relación con el diario. El correo en realidad no fue enviado desde el dominio El-Universo.net, sino que fue forjado por un cracker, es decir que se trata de un mail falso (fake-email). La dirección IP de origen del correo identificada es la 67.227.252.136, ubicada en la ciudad de Lansing en el estado de Michigan en Estados Unidos. Con todo, también hay formas de ocultar la IP para hacer aparecer que proviene de otro lado por medio del uso de software de Proxy. El cuerpo del mensaje contiene un enlace falso que pretende hacer creer al usuario que está alojado en un servidor del Diario El Universo (dominio: eluniverso.com), pero en realidad es un ataque de phishing, puesto que redirige al usuario a la dirección http://www.lene-kinesiolog.dk/templates/stripes2/images/eluniverso.php?Wikileaks_Video Al hacer click sobre el enlace el navegador descarga un software malicioso (malware), archivo Video_Notica_Wikileaks.exe 1. Recomendaciones Para evitar ser víctimas de amenazas de correo electrónico es importante utilizar en primer lugar el sentido común y tomar precauciones antes de hacer click sobre un enlace sospechoso. En segunda instancia es importante verificar siempre que el enlace hacia el que nos lleva una dirección en un correo electrónico, sea efectivamente la dirección real escrita en el cuerpo del mensaje. Esto lo puede hacer cualquier persona muy fácilmente colocando el puntero del mouse sobre el enlace, sin hacer click, y visualizando si la dirección que nos muestra es igual a la que está escrita. En tercer lugar es importante tener instalado software antivirus y antispam en nuestro computador. Dicho software debe ser legal, es decir que debemos adquirir la licencia apropiada, para que estemos seguros de que funciona correctamente y que además está siempre actualizado. Finalmente ante cualquier duda, llame a su consultor de seguridad informática de confianza.

Medidas defensivas

Evitar ataques de reconocimiento en un 100% es virtualmente imposible, porque precisamente el footprinting se basa en la búsqueda de información disponible públicamente sobre la organización víctima. Y si la información es pública es porque es preciso darla a conocer, por ende ocultarla iría en contra de su razón de ser. Por ejemplo, imaginemos que somos la organización ABC S.A. la cual se dedica a vender productos para mascotas a través de su página web y de forma presencial a través de tiendas de distribución minoristas. ¿Tendría sentido mantener secreta la dirección de su página web www.abc.com? Pues de ningún modo, el mismo hecho de publicar el sitio web hace posible que los usuarios lo encuentren a través de máquinas de búsqueda como Google, Altavista, Metacrawler, etc., aún sin invertir en publicidad. ¿Y cómo podríamos vender los productos a través de nuestra página web si los clientes no saben cómo llegar a ella? Por tanto lo que podemos hacer es minimizar nuestra exposición, haciendo público sólo aquello que por necesidad debe serlo. Les comento un caso particular, en una ocasión durante la fase de reconocimiento me topé con que el administrador de redes de mi cliente tenía publicada en Internet la página web de la Intranet. La misma palabra Intranet indica que se trata de un servidor de uso exclusivo interno. Este es un ejemplo de un servicio que no debería estar publicado. Si fuese necesario accederlo desde fuera por un motivo particular, la forma correcta de hacerlo es a través de la implementación de redes privadas virtuales (VPN's), pero no abriendo el puerto en el firewall para que cualquiera desde Internet pueda encontrar a un servidor interno. Aclarado este punto les sugiero algunas medidas preventivas: Mantener oculta la información de la empresa en los servicios de directorios Who-Is a través del pago anual por el servicio de privacidad a la entidad competente. Evitar publicar información detallada sobre sistemas operativos, aplicaciones, hardware y similares en los anuncios de búsqueda de personal. Capacitar a todo el personal de la empresa sobre precauciones de seguridad informática y acerca de cómo evitar ser víctima de un ataque de ingeniería social. Publicar en Internet sólo aquellos servicios de carácter público (web corporativo, servidor de nombres, servidor de correo, etc.) y confinar dichos servidores en una zona desmilitarizada (DMZ). Instalar medidas de seguridad perimetral (firewalls, sistemas IDS/IPS, etc.). Implementar medidas para protección de datos.

Recursos útiles

Capítulo 2

Artículo: Evite ser víctima de estafas electrónicas: reconozca un ataque de ingeniería social16. Documentación: Paterva / Maltego Documentation17. Libro: Google Hacking for Penetration Testers18. Libro: Social Engineering: The Art of Human Hacking19. Presentación: Charla sobre Protección de Datos20. Videos: Paterva / Maltego – You Tube21.