TALLER APLICADO DE SEGURIDAD DE LA INFORMACIÓN

Máquinas virtuales

Unidad 2

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Eder Moran Heredia

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar: Alex Flores Fuentealba

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

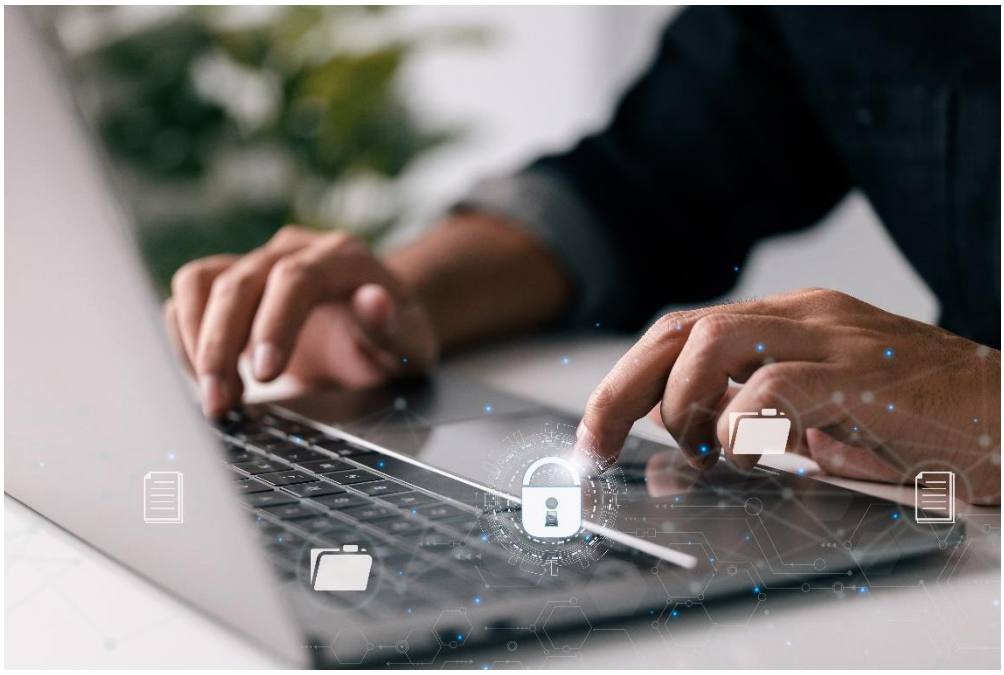
AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Utilizan técnicas y herramientas de Hacking WebServers, de acuerdo a Ethical Hacking y necesidades actuales de la industria.



Introducción

Antes de hablar acerca de cómo protegernos de un ciberataque, debemos tener en consideración de dónde provienen estos ataques —a través de nuestra red LAN (local area network- red de área local) o de la red WAN (wide area network- red de área amplia)—, así como qué tipo de activos podrían ser potencialmente víctimas de este ataque. Así, existen varios factores que considerar al momento de hablar de protección ante un ciberataque. Como una forma de poder separarlos y ordenar la defensa de la red, hablaremos de vectores de ataque, los cuales podemos definir como elementos clave para la prevención y defensa de una red corporativa. Por esto es esencial conocerlos adecuadamente y buscar soluciones adecuadas para la protección de cada uno de los elementos que se encuentran dentro de estos factores de ataque, con el fin de proteger la continuidad del negocio.

En concreto podemos decir que el vector de ataque proviene de un término del ámbito militar: un vector sería un "agujero" o falla que pueda presentar la defensa establecida. Estas fallas pueden tener como consecuencia la filtración de información o una debilidad en la transmisión de un mensaje.

Para poder desarrollar esta temática, abordaremos los diferentes conceptos de web servers hacking, sus ataques y herramientas.

1. Conceptos de “Hacking Webservers”

Como todos sabemos un servidor web está conformado por hardware y software. Por lo general los atacantes hacen uso de exploits del software para poder ingresar a los servidores. En este capitulo revisaremos las variadas técnicas utilizadas para este fín.

1.1 “Web server operations”

El servidor web opera aceptando repetidamente conexiones de los clientes, procesa solicitud HTTP del cliente y transmite los datos de solicitados que lleva un encabezado HTTP de respuesta. Si este contenido solicitado es estático, el documento será leido desde el sistema de archivos. Si en cambio este documento no es ubicado en la memoria caché del sistema de archivos, se realiza una lectura del disco.

Esta copia se produce como parte de la lectura de los datos del sistema de archivos y estos se escriben en el socket que viene adjunto a la conexión TCP del cliente. Los servidores web de que tienen alto rendimiento, por lo general, evitan esta primera copia gracias a la interfaz que proporciona mmap de UNIX, que es el que lee los archivos, a pesar de todo la segunda se mantiene. El almacenamiento en búfer múltiple ocurre porque un documento determinado puede almacenarse simultáneamente en el caché de archivos y en los buffer de retransmisión TCP de clientes múltiples.

1.2 Open source web server architecture

Cuando hablamos de la arquitectura de un servidor web nos referimos al diseño o un "diseño lógico" que tiene servidor web. Esto ocurre en función de para qué fue diseñado, así se desarrolla e implementa este servidor web.

El diseño arquitectónico de los componentes, es esencial para que el servidor brinde los servicios y operaciones que están basados en los requerimientos.

De igual forma hay que tener en cuenta los parámetros del servidor:

- La capacidad física del servidor en términos de almacenamiento y memoria.
- El rendimiento y calidad de servicio proporcionado.
- Los niveles de aplicación se encuentran implementados.
- Las plataformas compatibles (.Net, LAMP).
- El Sistema con que opera (Windows, Linux, Solaris).
- Los modos de conexión y la cantidad de usuarios conectados que puede soportar.

1.3 IIS Web server architecture

IIS es el acrónimo de Servicios de información de Internet. Básicamente consiste en un servidor web de Microsoft que se ejecuta en la plataforma

.NET. Es ampliamente utilizado para alojar aplicaciones web del tipo ASP.NET y para administrar solicitudes. Funciona con motor de proceso propio.

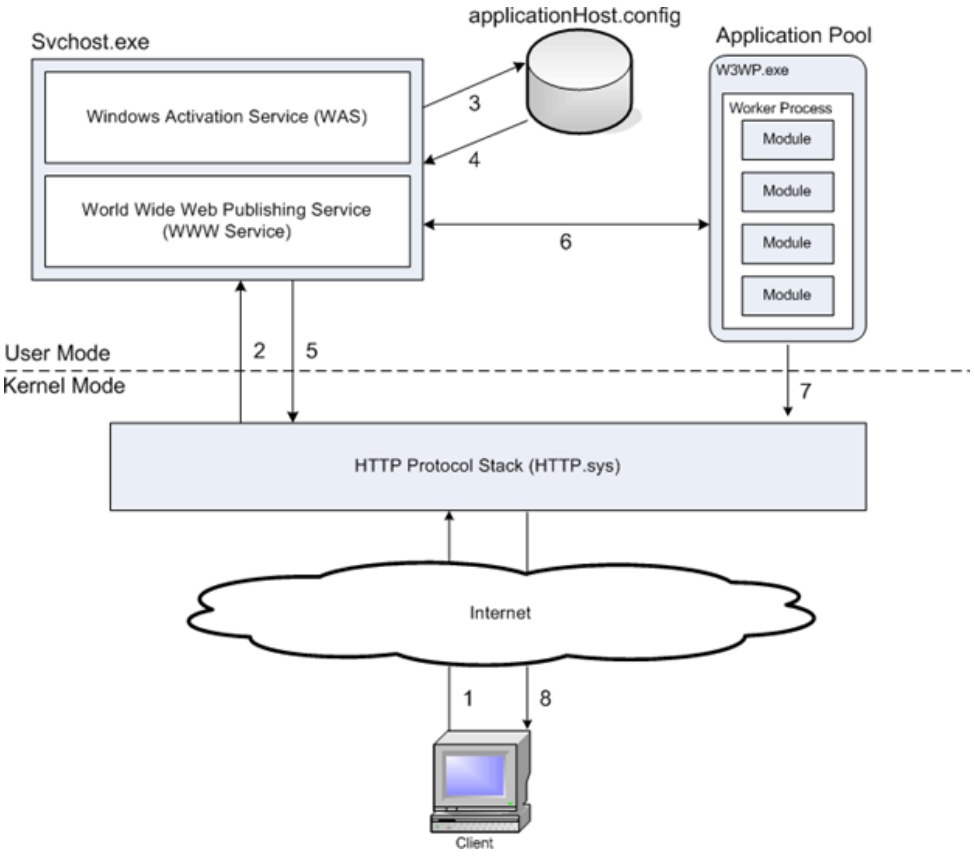


Figura 1. Arquitectura.

Fuente: Microsoft.com (s.f)

Componentes de un IIS

Proceso de trabajo: en las aplicaciones de tipo IIS, el proceso de trabajo es el que ejecuta la aplicación web y es un sistema de manejo de conexiones de clientes que gestiona la solicitud y la respuesta que es comunicada entre los clientes. Así cuando el servidor web recibe una

solicitud de un cliente, el proceso de trabajo genera una solicitud y su respectiva respuesta.

Grupo de aplicaciones: se le llama grupo de aplicaciones a un grupo de procesos de trabajo. Es utilizado para lograr contener el proceso de trabajo con una misma configuración. Así la aplicación web se vuelve más segura, disponible y confiable gracias a estos grupos de aplicaciones. Si algún proceso de trabajo se ve enfrentado a un incidente, los grupos de aplicaciones se aseguran de que los otros grupos no sean afectados. Esto es un gran beneficio ya que el tiempo de inactividad las aplicaciones web no afectará a otras aplicaciones, porque están configuradas en diferentes grupos de aplicaciones.

1.4 Web Server Security Issue

Cuando hablamos de seguridad de los servidores web nos referimos a los procesos y herramientas que se utilizan para resguardar datos y activos que se encuentran alojados en los servidores de una organización, junto con los recursos del servidor. Como contienen información sensible, los servidores terminan siendo el objetivo de los atacantes que buscan explotar las vulnerabilidades para obtener beneficios económicos.

Los servidores son el corazón de la arquitectura informática de una organización. Estos permiten a los usuarios acceder a la información o función de forma remota. Generalmente, se utilizan para alojar correo

electrónico, alimentar Internet y hospedar archivos. El problema, es que una contraseña débil o también, la falta de software antivirus o un simple error del un usuario puede generar una vulnerabilidad para organización y exponerla a pérdidas económicas.

La seguridad de los servidores web debe organizarse en capas para mayor efectividad. Buscando una máxima protección, se tienen que tratar todos los problemas que pueda presentar la red, las aplicaciones y software y los sistemas operativos que están instalados.

1.5 Web server Attacks Impact

La amenaza de ser atacadas para las organizaciones por los ciberdelincuentes es un tema diario, y es bastante lo que se arriesga. Se estima que para 2023, el valor de una vulneración de datos superará los 220 millones de dólares. Además de lo que significa una pérdida financiera, una violación de la seguridad de los servidores web también dan a lugar a publicidad negativa para la organización, que supone un daño a la marca y su reputación.

2. Web Servers Attacks

2.1 Ddos/DDos Attack

En el capítulo anterior revisamos este tipo de ataques, haremos un breve resumen para recordar.

Existen dos técnicas conocidas para realizar ataques de Ethical hacking, DoS o ataque de denegación de servicio (por sus siglas en inglés, Denial of Service) y por otro lado DDos o ataque distribuido de denegación de servicio (por sus siglas en inglés, Distributed Denial of Service).

2.1 Ataque DoS o denegación de servicios

Ésta técnica se utiliza para inhabilitar la utilización de un sistema, un computador o una aplicación, afectando a cualquiera de las instancias de comunicación, desde el origen de la información hasta la red informática de donde proviene. Se caracteriza por efectuarse los ataques desde una máquina o dirección IP.

2.2 Ataque DoS o denegación de servicios distribuido

Esta técnica se utiliza para inhabilitar la utilización de un sistema, un computador o una aplicación, afectando a cualquiera de las instancias de comunicación, desde el origen de la información hasta la red informática de donde proviene. Se caracteriza por efectuarse los ataques desde grandes cantidades de máquinas o direcciones IP.

2.3 DNS servers Hijacking

Al abrir una web con la dirección en el navegador, se emplea un nombre de dominio (DNS). Cuando se visita una web, esta información queda guardada en la memoria caché local, es decir el navegador no tiene

que enviar la solicitud por Internet. Para todos los demás, los dispositivos deben contactar un servidor de nombres, estos son proporcionados por los servidores de internet. En algunos casos se utilizan los servicios de Google se recurre a otros servicios públicos de DNS.

Cuando se establece la comunicación con el servidor es el momento más arriesgado, porque existe un intercambio de datos producido al formular la solicitud y por lo general la respuesta no está encriptada y existe "confianza" en el sistema. Esta situación permite a los hackers interceptar la solicitud y redirigir al usuario a otras páginas de formas diversas.

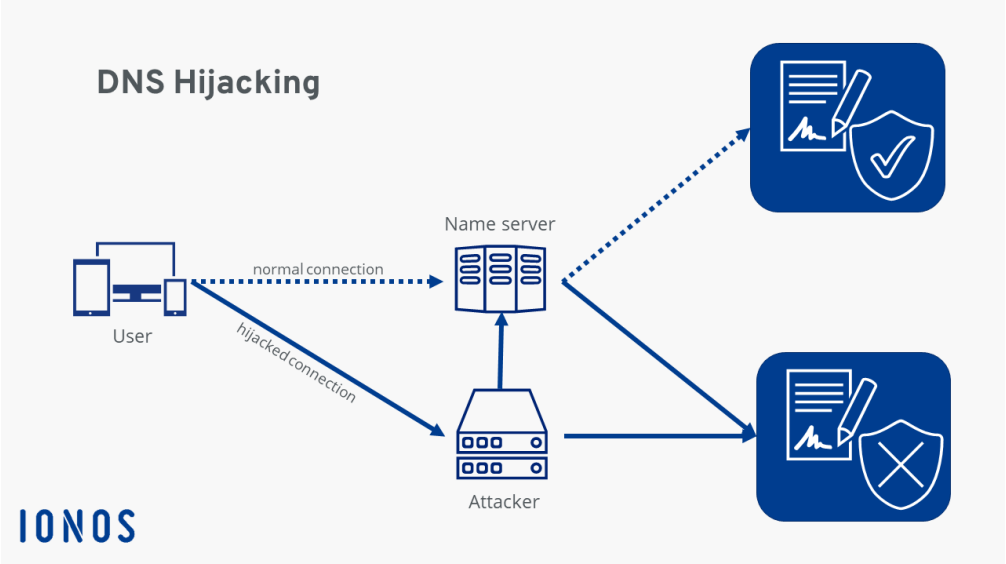


Figura 2. DNS Hijacking

Fuente: ionos.es (s.f)

2.4 DNS amplification Attack

Consiste en un ataque volumétrico de denegación de servicio distribuido (DDoS) en el que un atacante utiliza la funcionalidad de los solucionadores de DNS que se encuentren abiertos para así sobrecargar una red o servidor específico amplificando el tráfico, eso impide el acceso al servidor y a la infraestructura asociada.

Este tipo de ataque aprovecha una diferencia en el consumo de ancho de banda entre el atacante y el recurso web atacado. Cuando la diferencia se multiplica a través de muchas solicitudes, el volumen de tráfico perturba la infraestructura de la red. Así enviando consultas breves que se deriva en extensas respuestas que permiten al atacante alcanzar el objetivo con un esfuerzo mínimo. Si se logra multiplicar este aumento con la ayuda de bots en una botnet (red de bots) que realicen solicitudes similares, el atacante puede evitar ser descubierto y así beneficiarse de un aumento significativo del tráfico de ataques.

EL resultado de que cada bot envíe solicitudes a los solucionadores de DNS que se encuentren abiertos con una dirección IP falsa, en la cual se cambiado a la dirección IP real de la víctima, el servidor recibe entonces una respuesta de los solucionadores de DNS. Entonces, para multiplicar el tráfico, el hacker estructura la solicitud de forma que genera una respuesta más extensa de los solucionadores de DNS. Por todo esto, el atacado recibe una amplificación del tráfico inicial del Hacker y su red se va bloqueando con tráfico ilegítimo, y se provoca una denegación del servicio.

2.5 Directory Traversal Attack

Tener un acceso adecuado es primordial para ejecutar un servidor web seguro. El cruzar directorios conocido como “Path Traversal” es un tipo de ataque HTTP que permite a los hackers acceder a directorios restringidos y ejecutar comandos fuera del directorio raíz del servidor web. Así los servidores web puede proporcionar dos niveles principales de mecanismos de seguridad.

La lista de control de acceso se utiliza para el proceso de autorización de usuario.

2.6 Main in the middle / Sniffing Attack

El tipo de ataque man-in-the-middle es de espionaje, en este los hackers interrumpen una transferencia de datos. Apenas se ponen en el "medio" de la transferencia, los hackers se hacen pasar por los participantes legítimos. Así el atacante intercepte información y datos de cualquiera de las partes y, al mismo tiempo, puede hacer envío de enlaces maliciosos o cualquier otra información a los participantes legítimos de forma que no puede detectarse hasta que sea demasiado tarde.

Un sniffer o analizador de protocolos es una aplicación utilizada para monitorear y analizar el tráfico en la red. Permite capturar el tráfico y examinarlo en función de los protocolos soportados, aplicando distintos tipos de filtros. Originalmente, fue desarrollado para detectar errores y problemas de diseño en la implementación de distintos tipos de redes.

Con este tipo de aplicaciones, es posible capturar datos y visualizarlos cuando son transmitidos en texto plano. Por lo tanto, cualquier protocolo que envíe los datos sin cifrar es susceptible de ser analizado por un sniffer. Dentro de estos protocolos, tenemos ejemplos como HTTP, SMTP, POP3, IMAP, Telnet, FTP, etcétera. (Jara y Pacheco, 2012, pp. 233-234).

2.7 Phishing Attack

Un caso muy común de ingeniería social es el conocido como phishing (suplantación de identidad). Esta actividad ocurre cuando se recibe un correo electrónico que simula ser algo conocido para el usuario y lo invita a realizar clic en un enlace (generalmente, fraudulento) que lo lleva a un sitio web "conocido" o con las mismas características gráficas que el original, para que allí vuelque los datos que se le solicitan, como números de tarjetas de crédito, contraseñas, accesos a home banking, etcétera. Estos datos, al ser cargados en un sitio fraudulento, son enviados de forma directa a los atacantes, que obtienen información valiosa para sus objetivos.

2.8 Website Defacement Web Servers Attack Methodology

El ataque de desfiguración web es aquel en que datos malintencionados penetran en un sitio web y reemplazan el contenido del sitio con sus mensajes propios. Por lo general el contenido de estos mensajes están relacionados con política o religión, insultos u otro contenido que se considere inapropiado para avergonzar a los

propietarios de un sitio web, o también, un aviso de pirateo para difundir desprestigio.

2.9 Information Gathering

Es la instancia previa al intento de ejecutar una intrusión a un sistema por parte de alguien no autorizado. Esto también es utilizado en organizaciones por lo profesionales de seguridad informática para realizar comprobaciones de seguridad. La recolección de información implica llevar adelante una tarea previa y minuciosa de inteligencia, recolectando datos acerca del objetivo o de algún componente que se encuentre relacionado a este o a parte de él. Esta fase está conformada principalmente por la investigación y el análisis.

Un sistema informático está compuesto por incontables piezas, por lo tanto, el agujero de seguridad inicial puede encontrarse en cualquier nivel: desde una falla humana, una falla en la infraestructura (es decir, falla técnica), una falla en la lógica e incluso a raíz de una falla en agentes externos involucrados, como puede ser un proveedor de internet, de hosting, una sucursal que tenga una red desprotegida, etcétera.

Los datos que buscan los intrusos antes de producir un ataque se pueden relacionar con algún empleado (de cualquier rango, ya sea un ejecutivo o un operario), con algún sistema o parte de un sistema o con algún procedimiento u operación que nos permita intervenir un sistema. También puede ser que se busque, en una primera instancia, una

dirección IP, un sitio web, una red, una aplicación, un servicio (por ejemplo, un puerto que se encuentre abierto y sirva para autenticación), un protocolo en particular, un descuido en la programación o la administración de los sistemas, un directorio, un documento, una plataforma o cualquier dato de ubicación física de la organización. Desde ya que, si un intruso tiene la posibilidad de conseguir en primera instancia algún login (acceso), lo hará sin dudarlo, ya que esto permitirá escalar privilegios de forma rápida.

En esta etapa no interesa si el dato es de suma importancia o insignificante, todo es útil a la hora de escalar un sistema, así como para la planificación (simulación de ataque o chequeo).

Antes de proceder con la simulación de un ataque, debemos hacernos algunas preguntas útiles, por ejemplo:

1.- ¿Qué información tenemos acerca del objetivo?

2.- ¿Dónde se encuentran sus redes, sus sitios, por dónde fluye la información de la organización?

3.- ¿Qué partes conforman mi objetivo?

4.- ¿Qué sistemas posee la organización y cómo se conforman?

5.- ¿Cómo se llaman los integrantes de la organización? ¿Qué otros datos de estos tenemos?

6.- ¿Quiénes son los empleados? ¿De qué forma trabajan? ¿Desde dónde trabajan?

7.- ¿Qué información de los empleados existe en internet?

Para poder comenzar a realizar un ataque o una simulación del mismo, es necesario comenzar por el primer paso: saber con qué plataformas trabaja la organización y conocer algunos usuarios del sistema. En este punto, es necesario realizar una diferenciación entre "plataforma", "arquitectura" y "sistema operativo". Estos tres términos no hacen referencia a lo mismo: la plataforma es el sistema que sirve como base para que funcione el hardware, la arquitectura es interna del hardware y es a quién va dirigido el sistema operativo, y el sistema operativo es el que alberga todas las operaciones de sistemas.

2.10 Website servers footprinting

Como ya estudiamos, vamos a llamar footprinting (huella) a la recolección de información. Existen infinidad de métodos para recolectar información; cada atacante y cada profesional de la seguridad informática tiene su propia metodología y recursos durante una búsqueda de información. Mientras más minuciosa e ingeniosa sea esta búsqueda, más posibilidades existen de dar con un descuido, un objetivo o con una pista para comenzar a trabajar. Por ejemplo, alguien (un atacante) que tenga en su poder algunas o varias bases de datos de ISP (proveedores de internet) cuenta con una ventaja sobre el resto, ya que allí, seguramente, haya mucha información útil relacionada con el objetivo, que comprometa al sistema o parte de él.

En esta fase, un atacante tiene mucha ventaja, incluso por encima del profesional de seguridad informática, ya que puede utilizar técnicas o recursos no éticos para la extracción o recolección de información. Si el profesional de seguridad tiene conocimiento de estas ventajas y sabe cómo lidiar con ellas, puede estar seguro de tener un sistema protegido y controlado.

Consultas a bases de datos

La recolección de datos previa a un ataque comienza, generalmente, en algún tipo de base de datos. Cuando son realizadas por intrusos, estas recolecciones, muchas veces, no son legales. Un ejemplo de consulta a una base de datos de forma ilegal sería el caso ya mencionado en el que se tiene acceso a la base de datos completa de un ISP, donde figuran datos personales, passwords (contraseñas), direcciones, IP, etcétera.

Luego de cotejar la información contenida en dicha base de datos (por ejemplo, datos personales) con la realidad, el atacante tratará de utilizar como passwords sus fechas de nacimiento, números de documento, oficios, los propios passwords volcados en la base de datos, etcétera, pero lo hará en las cuentas de correo de la organización que estén expuestas en dicha base de datos o en algún otro servicio que requiera autenticación, como puede ser un FTP, un login de sistema online, SSH, etcétera.

Basándose en los datos contenidos en esa base, un intruso también puede intentar descifrar la entropía y composición de las contraseñas.

Tomemos un ejemplo: supongamos que en su cuenta personal la víctima tiene una pregunta secreta relacionada al libro El principito y el atacante encuentra en un foro que a esa persona le interesa ese libro. Entonces probará diferentes claves, por ejemplo, "elprincipito", "zorro", "invisiblealosojos", "víbora", "exupery", etcétera. Diferentes análisis confirman que, años atrás, el usuario utilizaba en sus cuentas de IPS claves como maradona10, para lo cual el intruso probará otras claves que se relacionen con ella, por ejemplo, "Maradona", "dios", "manodedios", "diegoarmando", etcétera, tratando así de dar con alguna forma actual o evolucionada de la clave. ¿Y esto por qué? Porque es muy probable que hoy en día también las utilice o las haya heredado y las use en otras aplicaciones de ingreso. Incluso los datos personales se utilizan para deducir accesos, por ejemplo, nombre y apellido, y obtener así usuarios, además de passwords. Un típico ejemplo es el USERID de las cuentas de correo corporativo e institucionales, formados muchas veces por la primera letra del nombre y seguido del apellido. Información de este tipo sirve para sacar aún más información desde otros lugares. El intruso, con esta información, buscará a su vez más información en bases de datos ilegales, como tarjetas de crédito, aportes jubilatorios, padrones, entidades privadas, información de servidores previamente atacados, etcétera. Para cualquier intruso, una fuente de passwords o datos personales es atemporal, ya que por más vieja que sea la base de datos, puede cobrar relevancia en un futuro y ser de utilidad.

Es común además que, más allá del análisis íntegro de la organización o del sitio institucional del objetivo, se busque información en otros portales, sitios relacionados a postulaciones laborales (por la cantidad de CV), información de riesgos crediticios, si existen automóviles, reimpresión de patentes, blogs, foros, comunidades online, juicios, eventos, registros de dominios, si posee o está registrado en portales de educación, guías, redes sociales, etcétera. Como podemos ver, la lista de lugares desde donde obtener información y armar bases de datos es muy extensa.

Existen infinidades de bases de datos que se encuentran online, ya que los organismos que las manejan no ven los riesgos que es tener esa información al alcance de cualquier persona. Un ejemplo puede ser la base de datos de mapas donde se puede encontrar la fachada de la casa de una persona u organización, el sitio web de AFIP, donde está la constancia de inscripción, el sitio CUIT online donde se da información personal de alguien, etcétera. Todas estas formas de recolección de datos son pasivas.

Por otro lado, una recolección de información mucho menos pasiva, ligada a base de datos, resulta intrusiva. Por ejemplo, si el intruso programa o utiliza lo que se conoce como "massrooter" (una mezcla de escaneo con exploit remoto que permite meterse dentro de servidores y extraer datos de forma secuencial a mucha velocidad) para barrer rangos de direcciones IP. Estos datos se acumulan para ser utilizados en un futuro o bien, aprovechando la intrusión, se procede a instalar algunas de las siguientes cosas:

Backdoors on the fly: Son "puertas traseras" que se dejan abiertas para poder ingresar cuando se desee, sin despertar sospechas. Estas no dejan abierto ningún puerto o algo remotamente detectable como para saber que existen.

Binarios troyanizados: El intruso, con suficientes conocimientos, suele reemplazar a mano algunos archivos binarios (ps, lsof o ls) para ocultar procesos o archivos propios dentro el sistema operativo. Cuando estos sean utilizados, el administrador del sistema no se dará cuenta de que existen y de que son nuevos dentro del servidor atacado.

Rootkits: Es un kit o serie de aplicaciones que se usa para mantener privilegios de root o administrador dentro de un servidor, no se instala de forma tan artesanal y sirve para mantener procesos ocultos y utilizarlos como puerta de entrada. Existen para todos los sistemas operativos.

Sniffers: Son capturadores de logins o paquetes.

Los archivos más recolectados por esta técnica intrusiva son los shadows (sombras) de los servidores Linux y los SAM de los servidores Windows (estos poseen cuentas de sistema y passwords cifrados). Estos también se pueden comprometer por medio de descuidos del Administrador, no solo por fallas de software. Un ejemplo muy común es la famosa cuenta de SQL, por defecto "sa", sin clave asignada. Si el administrador del sistema deja sin actualizar su servidor por un corto período, el atacante puede aprovechar alguna vulnerabilidad existente y conocida por desactualización, ingresar y comprometer el sistema sin dejar rastro alguno

Buscadores:

Son la mejor fuente de clasificación, análisis, búsqueda y caché de información, tanto confidencial como no confidencial sobre un objetivo. AltaVista fue el buscador preferido en los 90, le siguió Yahoo! cerca del año 2000 y hoy en día es Google por excelencia. Previamente, nos introducimos ya de manera breve en Google Hacking, es decir, la técnica para utilizar el famoso buscador y encontrar datos relevantes del objetivo. Veamos una lista bastante completa de búsquedas determinadas que se pueden hacer para encontrar información. Puede ser de archivos con información sensible, configuraciones, bases de datos internas, detalles de vulnerabilidades, avisos, usuarios, entradas, login, directorios privados, errores típicos de un sistema operativo o aplicación, etcétera.

2.11 Website mirrorning

Cuando hablamos de "mirrorning" nos referimos a crear un sitio espejo que no es más que una réplica completa y exacta de un sitio web existente con una URL diferente. Se ocupan con frecuencia para poder mejorar la accesibilidad al sitio web original y así aligerar la carga del servidor informático cuando genera demasiado tráfico

2.12 Vulnerability Scanning

Organizaciones de todos los tamaños manejan algún tipo de información que un hacker puede extraer. Hasta es posible que un

atacante ingrese a la red disponible de una empresa con el propósito de causar problemas de Seguridad de la web.

Esto puede ser desde historiales médicos de pacientes, como datos de tarjetas de crédito, transacciones de consumidores o incluso secretos comerciales. Si una organización utiliza tecnología para transmitir o almacenar información sensible, tiene que hacerse responsable de generar protección contra vulnerabilidades ante ciberataques. Por lo mismo se ha diseñado herramientas de escaneo y comprobación de vulnerabilidades que son imprescindibles para proteger un sistema de ataques o amenazas.

Lamentablemente, no todas las empresas invierten lo suficiente en las medidas de Seguridad de su red y así evitar vulnerabilidades. Por lo general, los softwares que escanean vulnerabilidades son herramientas de las cuales no se puede prescindir para proteger los activos digitales sin la necesidad de agotar los recursos de IT.

2.13 Session Hijacking

Como el término sugiere el secuestro de sesión es cuando un usuario en una sesión es secuestrado por un atacante y pierde el control de la sesión completamente, entonces sus datos personales son fácilmente robados, como por ejemplo al iniciar sesión en un sitio web bancario, el hacker secuestra la sesión y se queda con el control de la cuenta.

Para lograr esto, el hacker necesita tener conocimientos profundos de la sesión de cookies del usuario. Aunque todas las sesiones pueden ser atacadas, es más común en las sesiones del navegador en las aplicaciones web.

2.14 Web servers password Hacking

Identificación de sistemas vivos

La forma más sencilla de verificar si un host está activo o no es utilizando una herramienta que implemente la técnica de ping sweep. Esta consiste en enviar paquetes ICMP request (uno de los mensajes ICMP utilizados por el comando ping) a todos los hosts de una red. Si un host responde, implica que está online y es potencialmente un objetivo de ataque. (Jara y Pacheco, 2012, p. 103).

Identificación de puertos abiertos

El escaneo es el método utilizado para detectar puertos abiertos en un sistema. Esto implica realizar pruebas sobre cada puerto de cada host en particular; suele brindar más información que ping sweep.

Para realizar el escaneo de puertos, utilizamos diversas técnicas basadas en el protocolo TCP. Estas surgen a partir de la activación de uno o varios de los flags de la cabecera TCP.

La manera más sencilla de identificar el estado de un puerto, es decir, de saber si el puerto está abierto, cerrado o filtrado, es tratando de conectarse a él. (Jara y Pacheco, 2012, p. 104).

Identificación del sistema operativo

El proceso de identificación del sistema operativo (OS fingerprinting), tal como su nombre lo indica, tiene por objetivo detectar cuál es el sistema operativo del equipo que está siendo escaneado. Puede llevarse a cabo en forma pasiva o activa. La detección es pasiva cuando el análisis se realiza solo en función de los paquetes que el host objetivo envía. La herramienta denominada P0f lleva adelante este tipo de detección.

En el caso de la identificación activa, el host que está escaneando envía paquetes armados especialmente (por ejemplo, manipulando los flags TCP), de modo tal de evaluar la respuesta del equipo objetivo. Si bien este tipo de detección es más efectiva, es menos discreta. (Jara y Pacheco, 2012, p. 105).

Identificación de aplicaciones

Una vez que identificamos los puertos abiertos, como regla general podemos asociar a cada uno un servicio en especial.

Quien esté llevando adelante la prueba de intrusión será capaz de determinar qué servicios se están brindando en el equipo objetivo, en función de los puertos por defecto asociados a cada servicio.

Por otro lado, a partir de la detección del sistema operativo podemos inferir qué aplicaciones se están ejecutando en dicho equipo. Por ejemplo, si en el host objetivo está abierto el puerto 80 y el sistema operativo identificado es una distribución Linux, es altamente probable

que la aplicación que esté brindando el servicio web sea Apache. (Jara y Pacheco, 2012, p. 106).

3. Web Servers Attack Tools

3.1 Metaexploit/ Metaexploit NOPS module / Metaexploit payload and Auxiliary Module

Este Framework básicamente es un software open source que en un principio fue codificado en el lenguaje de programación Perl y, luego, fue traducido al lenguaje Ruby para así lograr modernizar y agilizar su funcionamiento. Metasploit viene preinstalado en el sistema operativo Kali Linux actualmente es la herramienta más utilizada para la ejecución de exploits en el mundo del hacking ético. Cuenta también con diferentes herramientas. Aparte del módulo de explotación, existen otros payloads que permiten encriptar malware y así evadir sistemas de detección, entre otros.

Wfetch

wfetch es un recurso informático de Windows que fue escrita en Python (solo funciona en Windows), que es usada para solucionar problemas de conexiones HTTP.

Cierre

Después de revisado el contenido de la semana, podemos extraer los siguientes factores claves:

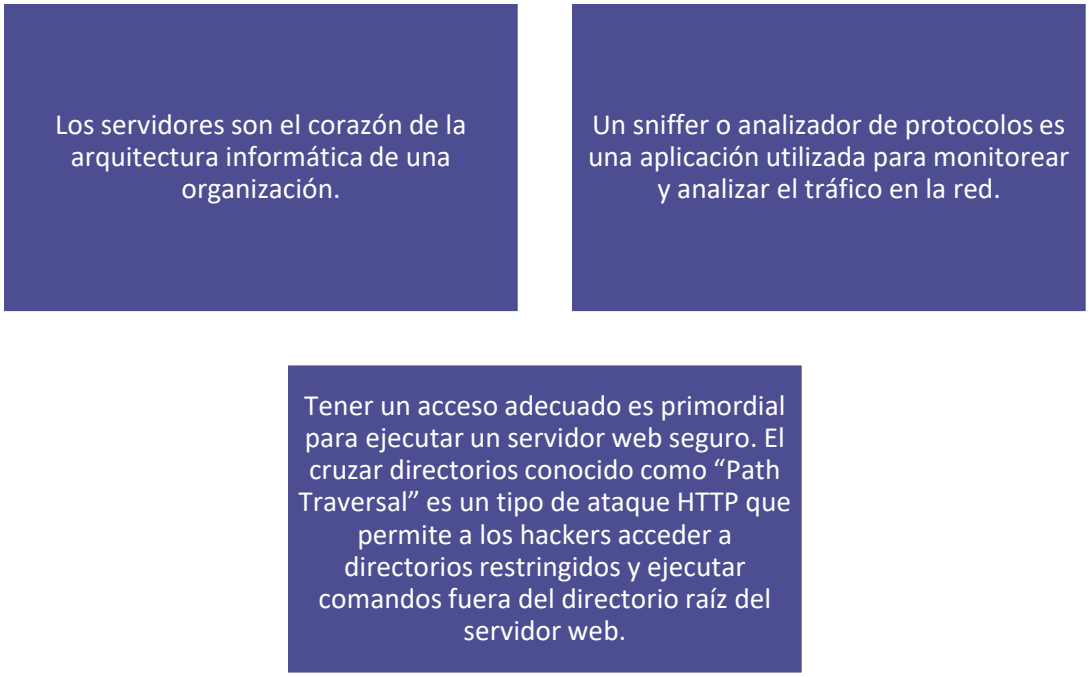


Figura 3. Ideas claves semana 7.

Fuente: Moran, E. (2022)

Referencias

Ataques DoS/ DDoS. Recuperado de https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

International Organization for Standarization/International Electronic Comision (ISO/IEC). (2005). Information Security Management (Norma ISO/IEC 27001). Recuperado de https://www.iso.org/isoiec-27001-information-security.html

Jara, H. y Pacheco, F. G. (2012). Ethical hacking 2.0. Buenos Aires, AR: Fox Andina.

Ataques de directorio. Recuperado de https://www.acunetix.com/websitesecurity/directory-traversal/

Funcionamiento de un servidor web. Recuperado de https://www.usenix.org/legacy/publications/library/proceedings/osdi99/full_papers/pai/pai_html/node14.html#:~:text=A%20Web%20server%20repeatedly%20accepts,read%20from%20the%20file%20system.

Ataque de hombre del medio. Recuperado de https://www.usenix.org/legacy/publications/library/proceedings/osdi99/full_papers/pai/pai_html/node14.html#:~:text=A%20Web%20server%20repeatedly%20accepts,read%20from%20the%20file%20system.

Ataque de amplificación de DNS. Recuperado de https://www.cloudflare.com/es-es/learning/ddos/dns-amplification-ddos-attack/

DNS Hijacking. Recuperado de https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-dns-hijacking/

Ataque de desfiguración del sitio web. Recuperado de https://www.imperva.com/learn/application-security/website-defacement-attack/