



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

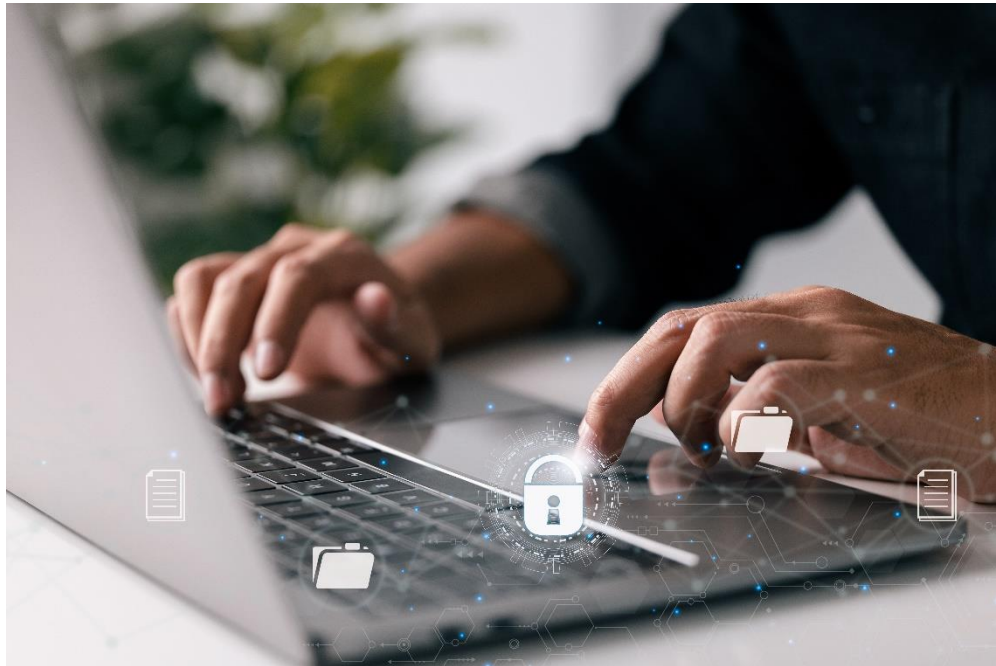
Tabla de contenidos

Aprendizaje esperado	5
Introducción	6
1. Conceptos System Hacking	7
1.1 Footprinting Module	7
1.2 Scanning module.....	18
1.3 Vulnerability Analysis Module	19
1.4 Metodología hacking	26
1.5 Objetivos del System Hacking.....	26
2. Cracking Password.....	28
2.1 Tipos de ataques para romper password	28
3. Penetration Testing	37
3.1 Password cracking.....	39
3.2 Privilege Escalation.....	40
3.3 Executing Applications, Hiding Files, Covering Tracks	40

Cierre	42
Referencias.....	43

Aprendizaje esperado

Utilizan técnicas y herramientas de System Hacking, de acuerdo con Ethical Hacking y los estándares de la industria.



Introducción

En Santiago de Chile, el 24 de mayo de 2018, lugar y fecha exacta de uno de los mayores ataques informáticos declarados en nuestro país, un malware había ingresado a la red del Banco de Chile, el cual dejaba inutilizados los computadores en base a bloqueos de los discos de arranque. Era solo el principio, y un ataque estratégico de distracción, ya que mientras los encargados de seguridad de la información de la institución enfocaban sus esfuerzos en cerrar más de 9000 estaciones de trabajo para proteger la información de sus clientes, una gran cantidad de transferencias eran realizadas en forma automática desde cuentas del banco hacia destinos de bancos internacionales. En ese momento la institución logró captar que el mayor peligro estaba asociado al robo ocasionado por las desviaciones de transferencias irregulares hacia bancos con destinos fuera del país y que el malware en las computadoras era solo una fuente de distracción para mantener ocupados a los encargados de seguridad.

Este ataque fue planificado y realizado con mucha anticipación, se utilizaron muchas estrategias de recolección de información relevante, por ejemplo: Ingeniería Social, Phishing, Pharming, Exploits, entre otros. Los cuales llevaron a encontrar una vulnerabilidad en el sistema Swift, el cual permite la ejecución de transferencias internacionales.

Este tipo ataque es muy sofisticado, y han sido denominados ataques ATP (Advanced Persistent Threat), los cuales corresponden a un conjunto de procesos informáticos llevados a cabo con mucha planificación, preparación y persistencia

para penetrar en un ambiente de seguridad informático específico, que reporte beneficios a los orquestadores del ataque.

El costo total de este ataque reportado por el banco fue de US\$ 10 millones, los cuales no reflejan la pérdida absoluta, ya que se genera una pérdida adicional por credibilidad, confianza y prestigio de la institución, que es muy difícil de recuperar.

Para poder evitar este tipo de situaciones, existen numerosas estrategias de defensa, tales como Firewalls, criptografía, VPN, entre otras, en búsqueda de la mantención de la seguridad de todas las plataformas de la empresa.

De lo mencionado anteriormente por eso es importante que se revisen algunos conceptos de system hacking, cracking password y penetration testing, los cuales se verán en el presente documento.

1. Conceptos System Hacking

1.1 Footprinting Module

En la unidad anterior, se apreciaron los aspectos teóricos y conceptuales relacionados con la etapa de relevamiento, pero también nombramos algunos métodos que se utilizan para reconocer y relevar información que puede ser de utilidad para un atacante.

Para poder desarrollar y llevar adelante esta unidad, vamos a descargar la distribución Kali Linux (tal como se indicó en el tema anterior). Esta es una

distribución Linux de código abierto “orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa” (Nolasco Valenzuela, 2018, p. 438). Anteriormente, esta distribución era llamada Backtrack, por esto existe mucha documentación en la web si se busca con este nombre, la cual es de total utilidad para aplicar en Kali.

Vamos a comenzar realizando la descarga de la distribución desde el siguiente enlace: <https://www.kali.org/get-kali/>. Aquí se pueden ver todas las versiones de descarga que hay de esta distribución. En esta ocasión se va a trabajar, con la máquina virtual (posibilidad de elección de archivo para VMWare o VirtualBox). Se debe contar con el software de VirtualBox (enlace de descarga: <https://www.virtualbox.org/wiki/Downloads>) o VMWare (enlace de descarga: <https://www.vmware.com/>) para poder abrir el archivo descargado. Otras versiones existentes son: en la nube, en un live CD o en un live USB, para arrancar desde ellos sin tocar el sistema operativo



Fuente: captura de pantalla de Offensive Security (s. f., <https://www.kali.org/get-kali/>).

Figura 1. Máquinas virtuales.

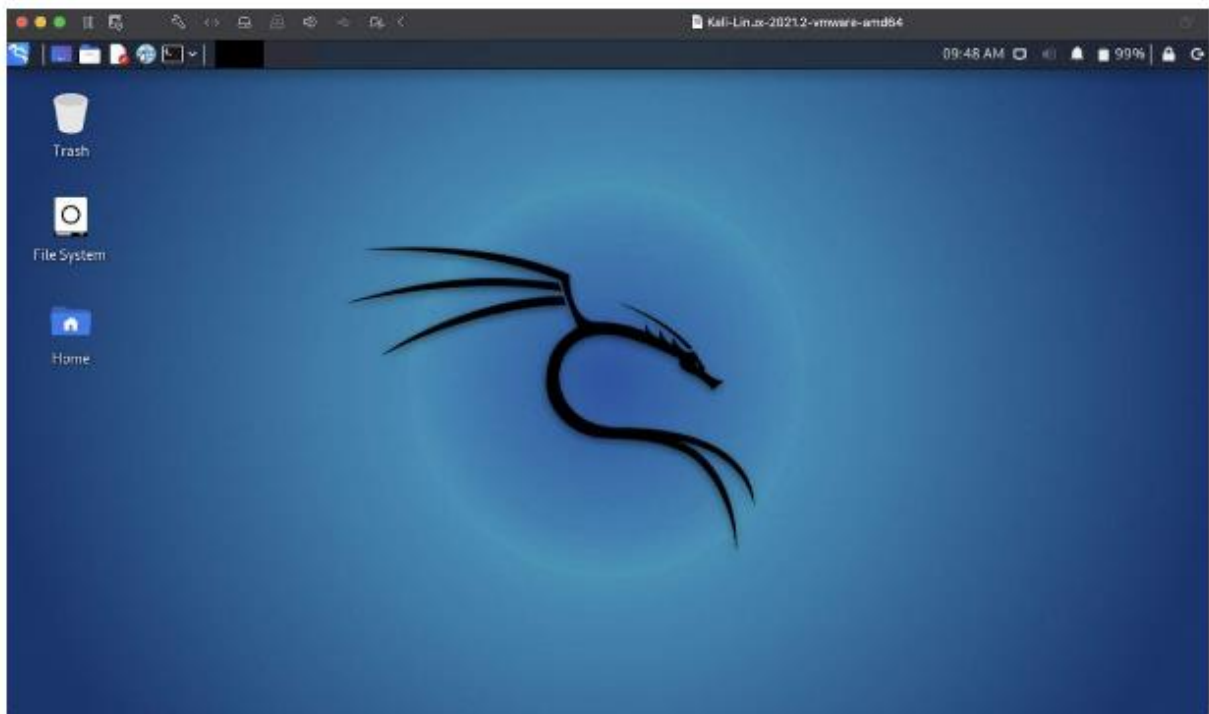
Fuente: Kali.org (s.f)

La máquina virtual está comprimida en formato 7-Zip (fuente de descarga: <https://www.7-zip.org>) y preparada y lista para comenzar a trabajar. Sus credenciales de acceso por defecto son:

Usuario: kali

Pass: Kali

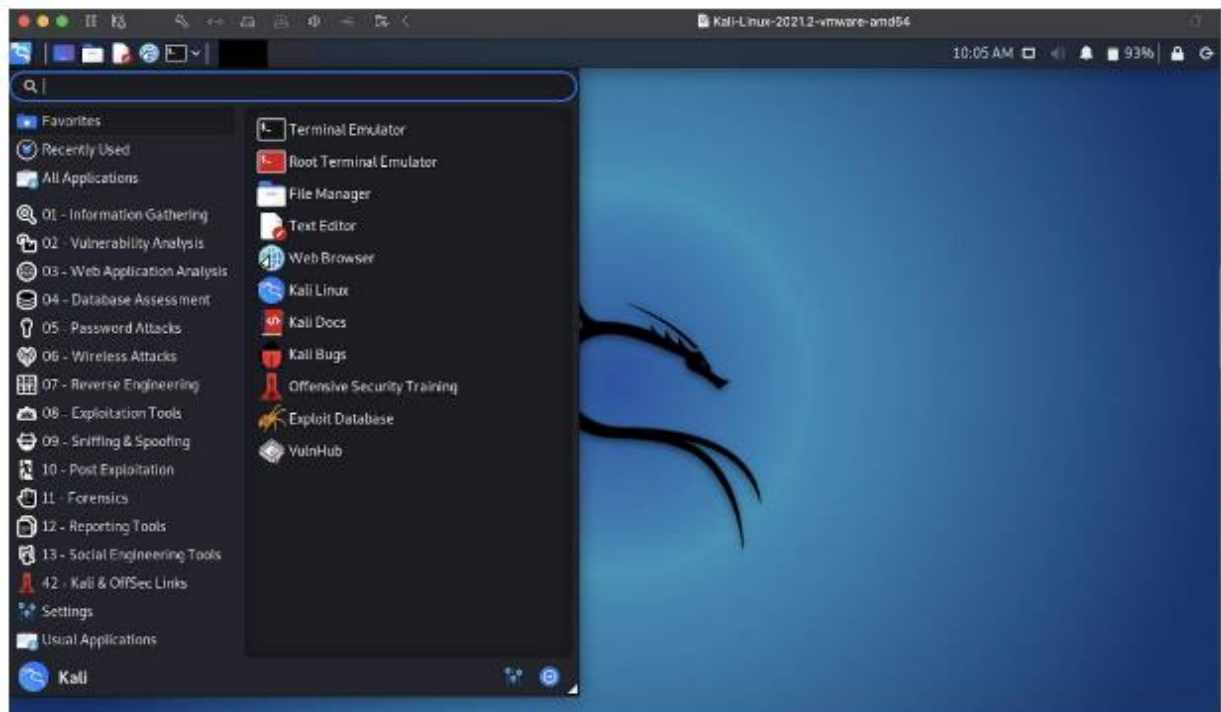
Se verá así al iniciar:



Fuente: captura de pantalla del *software* Kali Linux (Offensive Security, 2013).

Figura 2. Kali linux.

Fuente: Kali.org (s.f)



Fuente: captura de pantalla del software Kali Linux (Offensive Security, 2013).

Figura 3. Kali linux.

Fuente: Kali.org (s.f)

La etapa de relevamiento se separa en tres fases: reconocimiento, escaneo y enumeración de un sistema. Si recordamos lo anterior, tendremos presente el concepto de caja negra, que es el tipo de proceso que más se acerca a un atacante real, ya que este no tiene conocimiento previo de la organización objetivo, más allá de su nombre. Por eso la fase de reconocimiento es la que más tiempo consume dentro de la planificación de un ataque.

La existencia de metodologías de trabajo cada vez tiene más peso en la seguridad informática, por eso conoceremos en la fase de reconocimiento cuáles son los

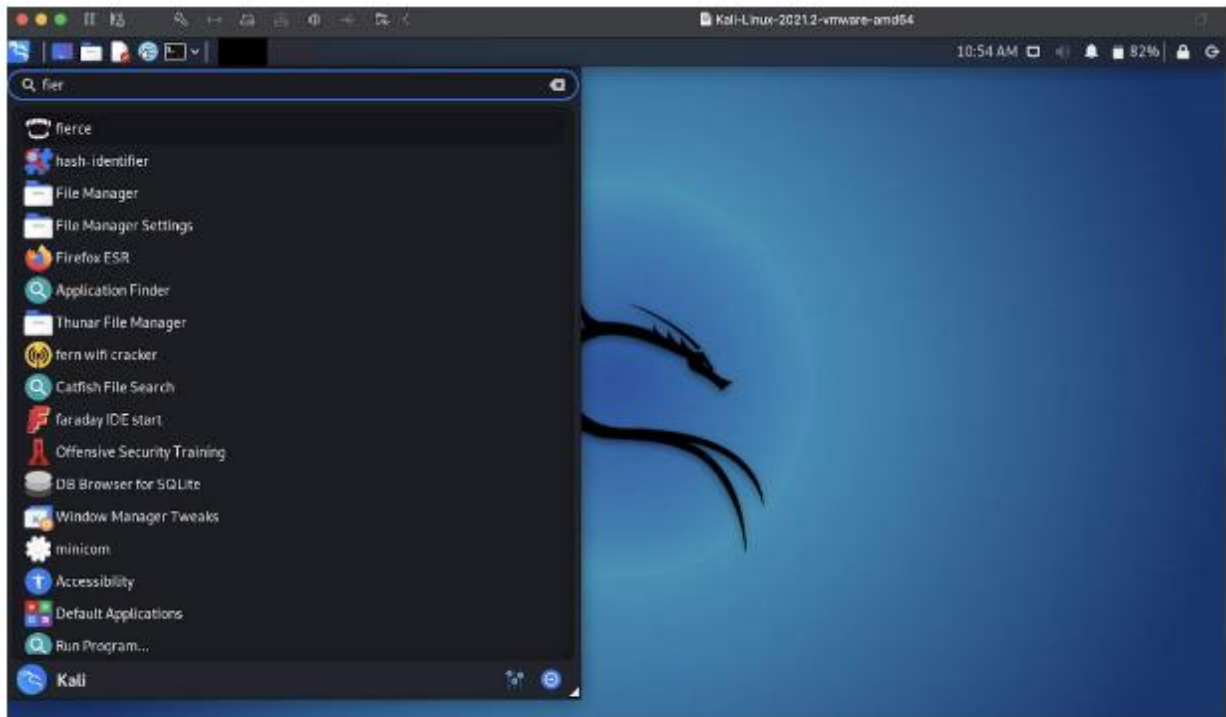
resultados que deben surgir dentro de su ejecución. Por un lado, sabemos que debemos obtener toda la información relacionada con una organización objetivo de ataque, razón por la cual, cuanta más información se obtenga, más se ampliarán las posibilidades de que el ataque sea exitoso.

Algunos de los datos de interés para un atacante son: la formación relacionada con el negocio, el organigrama, los puestos de trabajo dentro de la organización, los perfiles de usuarios, los puestos que ocupa cada persona y sus pasatiempos.

Veamos, a continuación, cómo recopilar información de una organización con la técnica de footprinting en la red (network footprinting) y desde internet.

Network footprinting

Es la fuente más común para obtener información correspondiente a direcciones IP y datos técnicos. Aquellas que ofrece el sistema operativo son, por ejemplo, WHOIS, Traceroute, Dig y Nslookup. A esto se le puede adicionar una de las técnicas más utilizadas, la enumeración de DNS, que tiene por objetivo listar y ubicar todos los servidores DNS y sus registros dentro de la organización (ya que esta puede tener DNS internos y externos), lo que hablaría de objetivos de ataque distintos. Dentro de Kali Linux, existe una herramienta, denominada fierce, que se utiliza para obtener información relevante de una organización. Para acceder a ella utilizando Kali, vamos a buscarla en los programas, como se muestra a continuación.

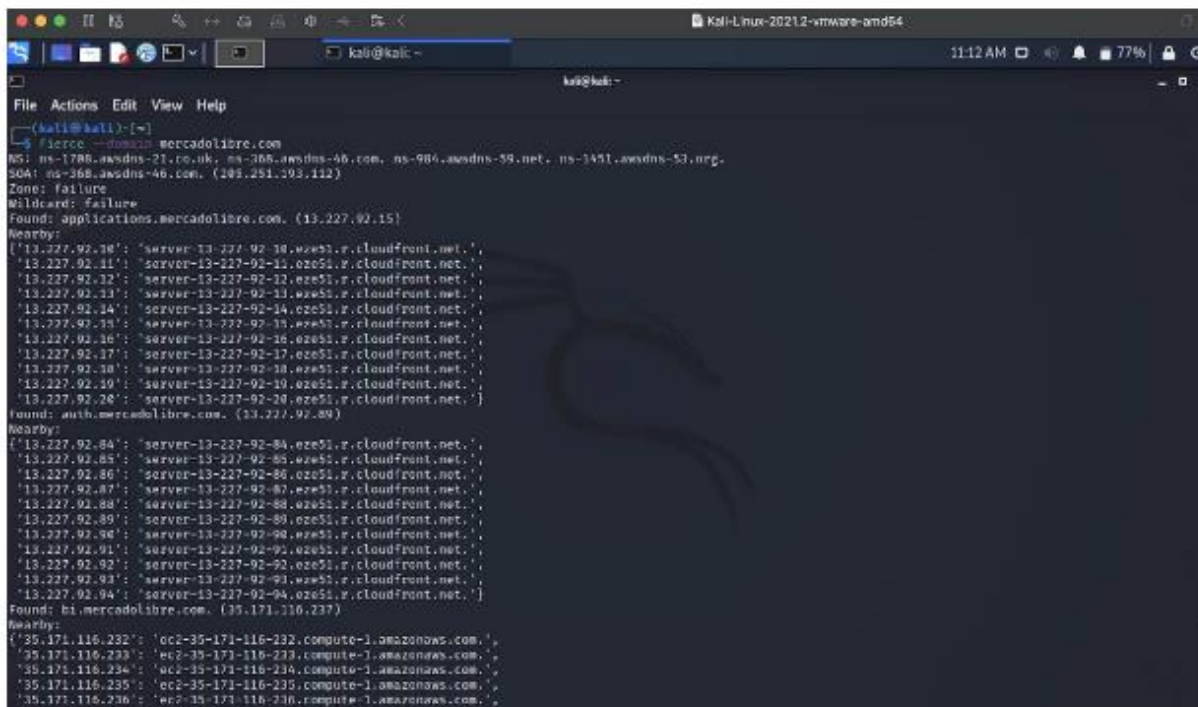


Fuente: captura de pantalla del software Kali Linux (Offensive Security, 2013).

Figura 3. Captura de Kali linux.

Fuente: Kali.org (s.f)

Al abrir la herramienta, se nos mostrará una ayuda en forma de guía para poder conocer los comandos que se deben utilizar. Como ejemplo vamos a proceder a buscar información del sitio www.mercadolibre.com. Para esto, en la consola de fierce, escribimos el comando `fierce --domain sitio` (en este caso, `fierce --domain mercadolibre.com`) y presionamos Enter.



Fuente: captura de pantalla del software Kali Linux (Offensive Security, 2013).

Figura 4. Captura de Kali linux.

Fuente: Kali.org (s.f)

Si observamos la imagen anterior, veremos que fierce realiza diferentes pruebas de dominio. Como primera información, obtienen los servidores DNS del sitio y luego analiza la transferencia de zonas de DNS (DNS zone transfer- zona de transferencia). Este ataque o simulación de ataque permite obtener una lista completa de todos los hosts que se encuentran registrados en la zona DNS de un servidor. Si un servidor se encuentra mal configurado, un atacante, sin utilizar ninguna herramienta más que las propias de un sistema operativo (Nslookup, por ejemplo), podría aprovecharse de esta deficiencia y copiar la lista completa de hosts. Fierce aplica la técnica de fuerza bruta para enumerar los dominios a partir

de una lista de nombres comunes y lleva a cabo esta comprobación realizando diferentes pruebas hasta dar con la correcta. Conocemos que los nombres más utilizados son mail.dominio.com, <ftp.dominio.com>.

WHOIS

Otra forma de revelar información es utilizando las consultas de WHOIS, que es un protocolo TCP que realiza consultas a un conjunto de bases de datos WHOIS con el objetivo de obtener información de carácter administrativo que se encuentre disponible de forma pública por medio de los registros de internet.

A partir de WHOIS, podemos obtener información de registro de un dominio, el nombre de la persona responsable de dicho dominio, el correo electrónico de registro o contacto, el número de teléfono y las direcciones IP de sus principales servidores. Esto permite que atacantes de tipo spammer se hagan con gran cantidad de direcciones de mail. Dependiendo de cuál sea el caso de estudio, muchas veces es posible dar también con el ISP (proveedor del servicio de internet) de la organización.

Esta herramienta se puede utilizar desde la consola de Kali, pero también existen numerosas herramientas (sitios web) en la web que brindan dicha información.


Hasta el momento, pudimos revelar información sobre rangos de direcciones IP, subdominios asociados a una organización (nombre.dominio.com) e información de registro de dominios en línea. Si nos enfocamos en el objetivo principal de esta etapa, lo que pretendemos es acercarnos lo más posible al mapa de red externa

que posee una organización. Por lo tanto, más allá de conocer determinados equipos asociados a direcciones IP, quisiéramos saber si la organización dispone de router o firewall. La herramienta que nos permite obtener esta información es Traceroute. Veámosla.

Traceroute

Esta herramienta permite identificar el camino que sigue un paquete de datos desde un equipo de referencia (puede ser el equipo que se utiliza para un ataque) hasta el objetivo. En función del camino recorrido por el paquete, es posible obtener información adicional que tenga que ver con la configuración de red de una organización, identificando, por ejemplo, rúters, firewalls, etcétera.

Vamos a la consola de Kali (también existe una herramienta gráfica <http://www.visualroute.com>) y ejecutamos el comando `sudo traceroute -T dominio.com`. Al presionar Enter, se ejecutará Traceroute y nos brindará información de interés. Veamos un ejemplo: extraigamos información del sitio web `clarín.com`. Para ello, deberemos ejecutar el comando `traceroute -T clarín.com`, y este nos arrojará información, como se muestra a continuación.



```
kali@kali:~  
File Actions Edit View Help  
kali@kali:~$ sudo tracert -T clarin.com  
[sudo] password for kali:  
tracert to clarin.com (104.18.19.22), 30 hops max, 60 byte packets  
 1 * * *  
 2 192.168.0.1 (192.168.0.1) 10.117 ms 11.889 ms 10.922 ms  
 3 * * *  
 4 * * *  
 5 hnx166.186-153-155.telecom.net.ar (186.153.155.65) 28.019 ms 27.973 ms hnx4234.181-89-50.telecom.net.ar (181.89.50.234) 27.942 ms  
 6 * * *  
 7 * * *  
 8 200.0.17.101 (200.0.17.101) 19.682 ms 23.401 ms 15.715 ms  
 9 104.18.19.22 (104.18.19.22) 16.251 ms 18.308 ms 17.434 ms  
kali@kali:~$
```

Fuente: captura de pantalla del *software* Kali Linux (Offensive Security, 2013).

Figura 5. traceroute.

Fuente: Kali.org (s.f)

Desde el punto de vista de un atacante, siempre se deberán conocer las direcciones IP, la ubicación geográfica y el camino por medio del uso de internet para alcanzar un objetivo. Cada equipo que se encuentra en la ruta hacia el objetivo puede ser una fuente de información útil para procesos futuros.

Como conclusión de lo visto hasta ahora, podemos decir que la gran fuente de información que tiene un atacante es internet. Si bien lo que recopilamos hasta el momento es información de interés, vamos a ver otras fuentes específicas que nos brindarán mayor cantidad y calidad de información.

1.2 Scanning module

FOCA

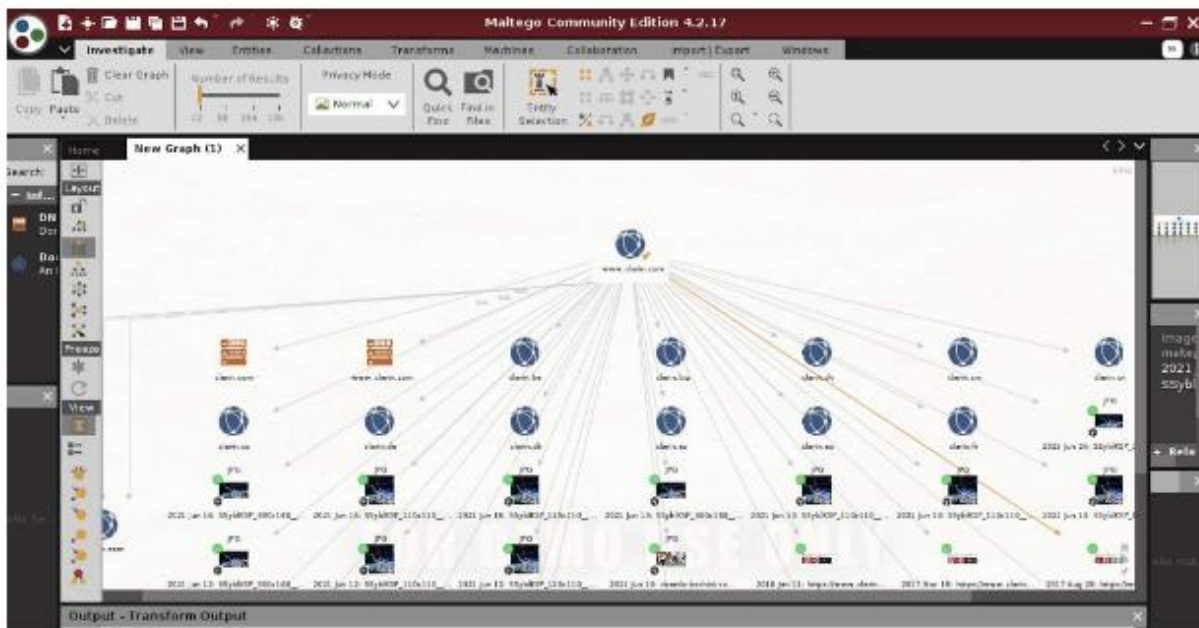
“Es una herramienta que automatiza y optimiza la recopilación de información online” (Jara y Pacheco, 2012, p. 90) relacionada con los metadatos de los archivos. Analizando los metadatos de los archivos, se puede extraer información de interés para un atacante. Por eso esta herramienta es de suma importancia dentro de la suite de herramientas de los analistas de seguridad, ya que permite conocer los metadatos de los archivos que circulan o se intercambian en la web (ya sea por mail o aquellos subidos en un servidor abierto).

La información que se extrae con esta herramienta es muy valiosa, ya que posibilita conocer el autor de un documento, la cantidad de ediciones que tuvo, si fue impreso y, en ese caso, marca y modelo de impresora, las fechas de edición y creación, el sistema operativo de creación, el software de creación, etcétera.

Maltego

Es la herramienta por excelencia utilizada en la etapa de relevamiento no solo por la capacidad que posee para recolectar datos, sino por la manera intuitiva que tiene para presentarlos. A partir de la recopilación, se encarga de forma automática de identificar y mostrar las relaciones existentes entre la información relevada y la presente en forma de gráfico.

Sigamos con el ejemplo del sitio www.clarin.com. Lo vamos a introducir en Maltego y vamos a ver la información que nos muestra.



Fuente: captura de pantalla del software Maltego (Paterva, 2014).

Figura 6. Maltego.

Fuente: Paterva (2014)

Como se puede ver en la imagen, la herramienta nos brinda información acerca del dominio buscado de forma clara y muy útil, aunque hay que aclarar que, si se quiere evitar un ataque, dicha información no debería ser de tan fácil acceso.

1.3 Vulnerability Analysis Module

Hasta lo revisado en este momento lo que se ha realizado es el relevamiento de información que se encuentra a disposición de cualquier atacante. En este punto, el profesional de seguridad informática tiene más claro qué información está más o menos expuesta a nivel de red y a nivel de usuario, así como aquella que se relaciona con el perfil de la organización. A partir de ahora, comienza la fase de

escaneo, que es aquella donde se comienza a analizar todo, pero desde una perspectiva más técnica y con el objetivo de detectar qué servicios y aplicaciones utiliza la empresa, así como qué vulnerabilidades pueden ser explotadas.

El escaneo es la segunda parte de la etapa de relevamiento. Ahora vamos a pasar a identificar servicios, sistemas operativos y aplicaciones con más detalle. En el caso de los sistemas operativos, es conveniente saber no solo qué plataforma, sino qué versión de la plataforma se usa. Por ejemplo, si es plataforma Windows o UNIX y si es Windows server 2003 o 2008, así como si tienen todas las actualizaciones realizadas.

Respecto a las aplicaciones, es importante determinar qué servicio brindan dentro de la organización, si esta cuenta con todas las actualizaciones y qué versión de ella está en funcionamiento. Por ejemplo, si el equipo funciona como un servidor web, deberíamos tener claro si lo hace por medio de Apache o por medio de IIS. Pero también deberemos saber qué versión se utiliza y qué medidas de seguridad se adoptaron al momento de su instalación, haciendo hincapié en el análisis de las vulnerabilidades existentes.

Antes de continuar con la metodología de escaneo, vamos a presentar la herramienta NMAP, la cual que definido como el escáner de puertos que toda persona que tenga una relación con el área de la seguridad debería tener conocimiento. Aunque sabemos que ésta puede descargarse del sitio <http://nmap.org/>, nosotros vamos a utilizar la versión que viene incluida en Kali.

Para NMAP, un (01) puerto pudiese tener la presentación de 3 estados: filtrado, abierto o cerrado. Cuando se observa que un puerto está abierto, quiere decir que el equipo objetivo va aceptando peticiones a él.

Decimos que está filtrado, cuando un dispositivo o firewall de red lo enmascara previniendo que NMAP determina si está o no abierto. Y se encuentra en estado cerrado cuando el puerto ya no permite ningún admisión de alguna conexión, por consiguiente, responde con un paquete TCP que tiene la habilitación del flag RST.

El comando que se utiliza para ejecutar NMAP es nmap IP.



```
File Actions Edit View Help
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oX/-oX/-oS/-oG <file>: Output scan in normal, XML, s|cript kiddi|s,
and Gre|pable format, respectively, to the given filename.
-oO <filename>: Output in the three major formats at once
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iiflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
--sS: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
kali@kali: ~$ nmap 152.170.117.246
Starting Nmap 7.81 ( https://nmap.org ) at 2021-06-25 13:37 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.86 seconds
```

Fuente: captura de pantalla del software Kali Linux (Offensive Security, 2013).

Figura 7. Captura de Kali linux.

Fuente: Kali.org (s.f)

En este sentido, para iniciar es importante destacar el modificador -iL, el cual va permitiendo la incorporación como entrada al escaneo un archivo de texto, en el que cada línea pueda ser una dirección IP.

De esta manera, se podrá ser capaz de incluir cada dirección IP relevada en la etapa de recopilación de información a un archivo de texto que puede ser nombrado como se desee, por ejemplo: [ips.txt].

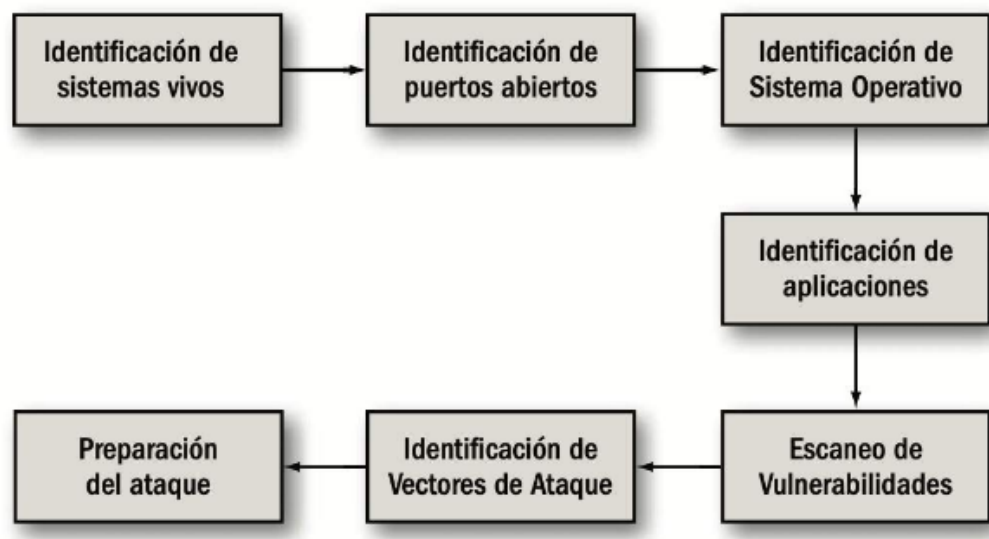
Podemos almacenar la respuesta de los escaneos en un archivo para consultarlo más tarde. Para esto nos interesa el comando -oN, y guardar los resultados en un archivo .txt.

Existen siete pasos que se deben llevar adelante:

En forma secuencial

De tal modo que los resultados puedan servir de entrada para el siguiente. Aunque se saben de la existencia de herramientas que pueden realizar varios de estos pasos juntos, con la intención de aclarar el proceso, se deben trabajar por separado con cada uno de ellos.

Pasos que componen un escaneo



Fuente: Jara y Pacheco, 2012, p. 102.

Figura 8. Pasos que componen un escaneo.

Fuente: Jara y pacheco (2012)

Vamos a entender de forma conceptual los pasos y qué herramientas se utilizan para cada uno de ellos.

Identificación de sistemas vivos

La manera más fácil de realizar la verificación si un host no está activo o si, es mediante la utilización de una herramienta que pueda implementar la técnica denominada ping sweep, la cual consiste en el envío de paquetes ICMP request (es considerado el mejor mensaje ICMP utilizado por el comando ping) a todo el host

de la red. Si uno de los hosts responde, esto quiere decir que está online y es un potencial objetivo de ataque.

Identificación de puertos abiertos

El escaneo se define como el método a utilizar para la detección de puertos abiertos en algún sistema. Esto da razón a la realización de pruebas en el puerto de cada host particular, brindando por lo general mayor información que la ping sweep.

Para la realización del escaneo de puertos, se deben utilizar diferentes técnicas originadas en el protocolo TCP. Estas pueden surgir al momento de la activación de alguno o varios de los flags de la cabecera TCP.

La forma más sencilla de por realizar la identificación el estado de un puerto o de poder saber si el puerto está cerrado, abierto, o filtrado, es intentado conectarse a él.

Identificación del sistema operativo

El proceso de identificación del sistema operativo (OS fingerprinting), tiene por objeto de poder detectar qué sistema operativo del equipo está siendo escaneado.

Puede llevarse de manera activa o pasiva. La detección es pasiva al ver que se analiza solo en función del paquete que el host objetivo puede enviar. La herramienta llamada P0f tiene la función de este tipo de detección.

En relación con la identificación activa, los hosts que escanean envían los paquetes armados primordialmente (se hacen por ejemplo mediante la manipulación de los flags TCP), de tal manera que se pueda evaluar la respuesta del equipo objetivo. Sabemos que este tipo de detección posee mayor efectividad pero menos discreta).

Identificación de aplicaciones

Cuando ya se pudieron identificar los puertos abiertos, se pueden asociar a cada puerto algún servicio en especial. Quien tenga la función de realizar el test de intrusión podrá tener la capacidad de poder determinar cuáles servicios están siendo brindado en el equipo objetivo, en función de los puertos por defecto asociados por cada cada servicio.

En otro orden de ideas, desde el momento de la detección del sistema operativo se puede presumir que las aplicaciones están siendo ejecutadas en dicho equipo. Un ejemplo de ello es que si en el host objetivo está abierto el puerto 80, y observamos que el sistema operativo que ya ha sido identificado como una distribución Linux, es probable que la aplicación que brinde el servicio web sea Apache.

1.4 Metodología hacking

Es evidente que cuando tenemos la posibilidad de recursos y dispositivos de forma externa, la fase de enumeración es realizada desde la red interna, indistintamente si se trata de un test de intrusión interno o porque es realizado por medio de una explotación de algún vector de ataque específico.

El objetivo de la enumeración de un sistema tiene la función de poder obtener una mayor cantidad de información ubicada en la red interna que pueda permitir el lanzamiento de ataques más elaborados o sofisticados.

ID de usuarios, nombres de equipos, grupos de dominio, recursos compartidos y servicios brindados de forma interna son solo uno de los objetivos específicos de esta etapa.

El uso de comandos de [los sistemas operativos (Linux o Windows)], la enumeración de usuarios por el uso del protocolo SNMP y la fuerza bruta son algunos medios que pueden ofrecer información relevante.

1.5 Objetivos del System Hacking

Usuarios y grupos

Para poder enumerar las cuentas de grupos y usuarios. Estas se realizan por medio de CIF/SMB, y el uso de Simple Network Management Protocol (SNMP).

Cuando nos referimos a Linux, en vez de realizarse por medio de CIFS/SMB, es se aplica a través de SMB/NMB o NIS. Además, es trabajado de forma directa sobre Lightweight Directory Access Protocol (LDAP).

En los sistemas Microsoft Windows, en el directorio Support/Tools se pueden encontrar una diversidad de herramientas, de las cuales se usan para poder hacer el proceso de enumeración de sistemas de manera fácil.

Nombres de equipos y dispositivos

Es interesante destacar cuál es el nombre de los diferentes equipos, ya que la nomenclatura a utilizar puede guiarnos en relación con la función que cumple.

Generalmente el administrador más conservador emplea una nomenclatura específicamente definida para poder realizar la identificación clara de los tipos de dispositivo. Entre ellos se puede mencionar que para el caso del servidor, utiliza SERV001, SERVIDOR01, entre otros.

Esta información es de mucha utilidad para un profesional de seguridad informática y la debe tener en cuenta para acotar vulnerabilidades.

Recursos compartidos

La enumeración de recurso compartido es super importante, ya que, por distintos motivos, es frecuente ubicar en la red interna impresoras, carpetas y demás recursos que no poseen la implementación de un control de acceso eficiente en relación la información que aloja.

Es frecuente encontrar alguna carpeta compartida para todos los usuarios que tienen alguna información sensible, entre ellas tenemos los archivos de configuración, datos de tarjetas de crédito, entre otros.

La enumeración de recursos puede realizar por medio de diferentes técnicas. La más utilizada es a través de NETBIOS, transferencia de zonas o enumeración DNS cuando es posible, o por medio del protocolo SNMP.

2. Cracking Password

Los ataques sin tecnología son aquellos en donde no se emplean técnicas, ni software ni accesos indebidos a sistemas, sino que se valen de engañar al usuario lícito. Le generan una necesidad o compromiso a un usuario para que realice cierta tarea que permita luego un ataque. Por eso es de suma importancia capacitar en todo momento al usuario final.

2.1 Tipos de ataques para romper password

Ataques no electrónicos para obtener password

En el área de la seguridad de la información, se puede observar que la ingeniería social el ejercicio práctico para la obtención de algún dato confidencial por medio de la manipulación psicológica del usuario legítimo. La técnica se utiliza para poder acceder a privilegios, conseguir información en los sistemas que permita la realización de algún acto que pueda perjudicar o exponer a un usuario o empresa a abusos o riesgos.

La base en el que se fundamente la ingeniería social es el que da por afirmado que en cualquier sistema el usuario es el elemento más débil. Se observa en la práctica es utilizado el internet o teléfono para poder estafar a la gente simulando. Un ejemplo de ello es cuando un empleado de empresa o bancario, un técnico, un compañero de trabajo, o un cliente obteniendo la información. Por medio del internet, se suele enviar alguna solicitud para la renovación de credenciales de acceso a e-mails, sitios falsos que piden respuestas incluyendo las de mayor fama, que lleva a la revelación de información sensible o a violar políticas de seguridad.

Por medio de este método se aprovecha alguna tendencia natural de la persona en vez de encontrar algún agujero de seguridad en el sistema. El usuario de sistema debería ser advertido de forma temprana frecuente para la no divulgación de contraseñas o informaciones sensibles a personas que dicen ser el administrador (en realidad, el administrador de sistemas ocasionalmente necesita saber la contraseña para realizar su tarea). Otro caso es la utilización de los archivos adjuntos en correos electrónicos, que ejecuta un código malicioso.

La defensa más importante en contra de la ingeniería social es la educación y concientización al usuario en el cumplimiento y uso de las respectivas políticas de seguridad.

Active online Attack Password

Suele ser una de las maneras más sencillas para lograr un acceso no autorizado a un sistema a nivel de administrador. El atacante debe establecer comunicación con las máquinas que son blanco para realizar el acceso con contraseña. Las técnicas

que se emplean por el atacante para realizar vulneraciones de activos incluyen a veces sistemas de adivinación de contraseñas, ataques de diccionario y de fuerza bruta, inyección de hash, phishing, envenenamiento de la red, uso de spyware registradores de claves, troyanos, etc.

Envenenamiento de la red: poisoning

La técnica de poisoning o envenenamiento consiste en redireccionar el tráfico de usuarios lícitos a sitios usualmente controlados por un atacante. Esta técnica suele implementarse a partir de la manipulación de los protocolos ARP y DNS.

El ARP poisoning, también es conocido como ARP spoofing, consiste en generar peticiones y respuestas ARP modificadas con el objetivo de asociar la dirección MAC del atacante con la dirección IP del gateway (puerta de enlace). De este modo, todo el tráfico de ese segmento pasará primero por el atacante, que podrá analizarlo y redirigirlo luego hacia el destino final.

Un modo de protegerse frente al ARP spoofing es utilizando tablas ARP estáticas. Un método alternativo se basa en usar aplicaciones para detección de cambios de las tablas ARP (Arpwatch, por ejemplo) e implementar el uso de la seguridad de puerto que poseen algunos switches (o routers) para evitar cambios en las direcciones MAC. (Jara y Pacheco, 2012, pp. 231-232).

Análisis de protocolos: sniffing

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).

Impersonalización: spoofing

El spoofing es una técnica utilizada para suplantar la identidad de otro sujeto, que puede ser un usuario o un proceso. Dependiendo del protocolo al que se haga referencia, esta técnica se implementará de diversas maneras, aunque las más conocidas son las de IP spoofing, MAC spoofing y mail spoofing.

Claro que, en términos generales, podemos englobar dentro del spoofing a cualquier tecnología de red susceptible de sufrir suplantaciones de identidad. Por esta sencilla razón es que la técnica de ARP poisoning que hemos mencionado hasta este momento también se conoce como ARP spoofing.

El IP spoofing consiste en sustituir la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se le desea suplantar la identidad. Esto se consigue usando programas que implementen esta técnica o, incluso, modificando los paquetes a mano.

Es importante tener en cuenta que las respuestas del host que reciba los paquetes irán dirigidas a la IP falsificada. Por ejemplo, si se envía un ping spoofeado, la respuesta será recibida por el host que posee la IP spoofeada. Una analogía similar podría hacerse al momento de enviar una carta postal.

Cuando una persona envía una carta, si en el sobre el remitente, en vez de colocar su dirección, indica la del vecino, cuando el receptor la reciba y la conteste, la respuesta llegará al vecino, y no a quien realmente la envió.

En el caso del MAC spoofing, existen razones muy diversas para decidir modificar la dirección MAC de un dispositivo de red. Pero ¿Cómo es posible cambiar la MAC de un dispositivo si esta se encuentra grabada en una memoria de solo lectura que no puede ser modificada? (a nivel hardware, de hecho). La respuesta es bastante simple: si bien es cierto que dicha memoria no puede modificarse, también es real que los sistemas operativos no consultan directamente al hardware, sino que lo hacen a través del correspondiente controlador. Es decir, la MAC es leída y almacenada por el controlador, lo que posibilita modificarla desde ese lugar. Al depender del controlador, la forma de modificarla dependerá de cada sistema operativo; por ejemplo, con comandos propios del sistema (en el caso de Linux y

todos los *NIX) o modificando algunas cadenas del Registro (en el caso de Windows).

La técnica del email spoofing es utilizada en algunos ataques de ingeniería social porque, en diversas oportunidades, tiene mayor importancia que el origen del correo electrónico sea confiable para el receptor frente al hecho de que el atacante no reciba respuesta. Por ejemplo, los formularios de recomendación de los sitios web usualmente pueden ser manipulados, permitiendo de esta manera el envío de correos electrónicos a cualquier destinatario por medio de esta plataforma.

Robo de sesiones: hijacking

El concepto de hijacking hace referencia a toda técnica que conlleve el secuestro o robo de información y sesiones por parte de un atacante. Se utiliza en combinación con otras técnicas y ataques, como el spoofing. Su aplicación es muy amplia y puede puntualizarse en varias técnicas específicas. Podemos hablar del secuestro de conexiones de red o sesiones de terminal (session hijacking), servicios, módems, páginas (page hijacking) e, incluso, las variantes como el secuestro del Portapapeles o clipboard hijacking, donde el Portapapeles es capturado y, cada vez que se intenta pegar lo que se debería encontrar en él, aparece una URL con una dirección maliciosa.

Fuerza bruta

Los ataques de fuerza bruta son, esencialmente, ataques que buscan vulnerar mecanismos de autenticación basados en credenciales del tipo usuario y contraseña.

Se basan en probar todas las combinaciones posibles del espacio de claves de un sistema. Por ejemplo, si nuestra aplicación solo permite claves de 8 caracteres y letras minúsculas, el espacio estará determinado por 27^8 claves en total, es decir, 282429536481 claves. De esta forma, cuanto mayor sea la potencia de cálculo de que disponemos, más rápido podremos encontrar la contraseña correcta.

Pero, a medida que el espacio de claves y, en especial, la longitud de estas crece, la capacidad de cálculo actual se vuelve insuficiente para recorrer el espacio de claves total en tiempos humanamente prácticos. Por esta razón, muchas veces, en vez de recorrer por fuerza bruta pura todo el espacio de claves, se utilizan diccionarios con claves organizadas mediante algún criterio en particular. Algunos de ellos pueden ser diccionarios de palabras en español o en inglés, claves por defecto de dispositivos y cualquier otro criterio o combinación que se nos ocurra.

Estos ataques pueden ser remotos, cuando se lanzan a un servicio específico desde una ubicación externa; por ejemplo, un ataque a un servicio FTP, Telnet, SSH, etc.

Herramientas como Hydra, Medusa o Brutus permiten implementar este tipo de ataque dirigido hacia protocolos específicos. (Jara y Pacheco, 2012, pp. 240-245).

Keylogger

Es un software y en algunos casos hardware que permite detectar las pulsaciones del teclado para su posterior guardado del equipo que se encuentra infectado. Su actuar esta entre teclado y el sistema operativo, permitiendo con ellos registrar lo que se escribe en el teclado sin que el usuario se dé cuenta. La información queda almacenada en el PC o en el dispositivo de hardware, aunque en algunos casos existen algunos más complejo que transmiten la información de manera remota por la red.

Spyware

Son programas espías y corresponden a código malicioso cuya finalidad es recopilar información sobre las actividades que realiza un usuario y que a la postre podría servir para infiltrar y escalar privilegios dentro del sistema, atacar sistemas, robar información personal (números de tarjetas de crédito, etc.). Según algunos estudios, cerca del 91% de los computadores personales tiene algún spyware instalado, un informe de la empresa EarthLink, basado en el análisis aplicado a más de 1 millón de computadores conectados a Internet, sostiene que el promedio de programas "spyware" en cada uno era de 2.

Trojan

Troyanos, virus y gusanos: Corresponde aplicaciones maliciosas, que de alguna forma se alojan en los equipos informáticos con la finalidad de proporcionar acceso no autorizado a un potencial atacante, o permitir el control de forma remota de

los sistemas. Un virus, posee la capacidad de destruir o dañar la información del equipo o generar excesivo consumo de recursos que no sea posible de controlar y de esta forma bloquear o negar servicios. La modalidad de propagación es por medio de un archivo ejecutable incrustado en una imagen, dispositivo de almacenamiento, música, video, música, etc. Otra característica de los virus es la capacidad de reproducirse por sí mismos. una vez que se ha alojado en un equipo.

USB cracking password

Son softwares que se instalan en una unidad flash que tienen como objetivo descifrar las contraseñas de acceso de administrador al sistema operativo, pueden funcionar mediante bibilotecas o fuerza bruta.

Hash Injection Attack

Los ataques de inyección SQL explotan cualquier vulnerabilidad existente en una página web para "inyectar" código malicioso. Este se implanta en las bases de datos de SQL, que es un lenguaje utilizado en programación, y este compromete la seguridad y privacidad de los usuarios del sitio web.

Los ataques de inyección SQL consisten en eliminar o editar las bases de datos y así robar información sensible de los usuarios, como contraseñas o datos privados o números de tarjeta de crédito. Estos ataques solo pueden realizarse cuando existen vulnerabilidades en sitio web.

Password Cracking tools

Existe una gran cantidad de Software dedicado al descifrado de contraseñas. En ellos los 5 más populares son:

- Burp Suite.
- CeWL.
- Hashcat.
- THC-Hydra.
- John the Ripper.
- PACK.
- Statsprocessor.

3. Penetration Testing

Para poder llegar a entender lo que representa un test de penetración (pentesting), es necesario revisar el concepto de evaluación de vulnerabilidades (Vulnerability Assessment), término que es utilizado en un sinnúmero de disciplinas y tiene por objetivo principal la búsqueda de debilidades en distintos tipos de sistemas.

Considerando nuestro ámbito asociado a la tecnología informática, el término de evaluación de vulnerabilidades será utilizado cuando es referenciado un análisis técnico sobre las debilidades de una infraestructura informática y/o de redes.

Específicamente al analizar vulnerabilidades asociadas a distintos servidores, redes, sistemas operativos, aplicaciones, entre otros, vinculado a todas aquellas deficiencias técnicas de los dispositivos y nodos en general.

Si llegamos a extender el concepto de evaluación de vulnerabilidades y nos centramos en los procesos vinculados con la información de una empresa, nos orientamos directamente a la definición de Test de Penetración. En este caso, además de analizar las debilidades de base tecnológica, se analizarán otras características que son fundamentales para el negocio. Por ejemplo, el uso de técnicas de ingeniería social a empleados, búsqueda de información de la organización en forma online (a través de recursos de Internet) y offline (a través de medios que no tengan que ver directamente con la información publicada en la red, como las guías de la industria, informes económicos, entre otros). Por lo tanto, nos abocamos a un análisis que se oriente al proceso que llevaría adelante un atacante real, por ello la gran importancia de evaluarlo, analizarlo y aplicarlo.

Por ello, como una definición de Test de Penetración, podríamos mencionar que es un método utilizado para evaluar el nivel de seguridad de una organización, donde quien lleva a cabo dicha evaluación simula ser un atacante real que aplica diversas técnicas y cuyo objetivo es encontrar vulnerabilidades a partir de debilidades en las configuraciones de los equipos o bien en distintos procesos o contramedidas, sean estos de tipo técnico o de otra índole.

3.1 Password cracking

En esta etapa denominada Obtención de Acceso, se desarrolla el acceso al sistema. Esta tarea se logra generando la explotación de las vulnerabilidades que fueron detectadas y que serán aprovechadas por el atacante para comprometer el sistema. En esta situación el atacante intentará acceder al objetivo. Para llevar a cabo dicho paso, se utilizan algunas de estas técnicas:

Explotación de vulnerabilidades: en el caso que existiera algún software instalado que permita la ejecución de código remoto, ésta es una puerta abierta u hoyo de seguridad que permitiría el acceso de intrusos.

Servicios con problemas de configuración: un servicio mal configurado puede permitir que atacantes hagan uso de esa vulnerabilidad, o incluso, que ejecuten código remoto.

Debilidad de password o contraseñas: una contraseña definida en forma débil corresponde a una vulnerabilidad que puede permitir el ingreso de atacantes

Decepción o engaño: ataque contra las personas.

Un ataque puede comenzar con la obtención de un usuario y contraseña de un servicio. El atacante puede lograr acceder a un entorno restringido. Desde este entorno, puede obtener más información, que luego le servirá para acceder a mayores servicios. Recuerde que un atacante no tiene apuro, y puede dedicar todo su tiempo para encontrar la información que necesite

3.2 Privilege Escalation

Este tipo de ataque, puede ser el siguiente paso de un atacante luego de haber obtenido acceso a un sistema, ya que permite obtener permisos como "Administrador" o "SuperUsuario" al equipo, de ese modo no se tienen derechos restringidos.

3.3 Executing Applications, Hiding Files, Covering Tracks

Una vez que un atacante se encuentra dentro del sistema, es decir, lo pudo vulnerar y obtuvo un acceso, tiene como objetivo mantener ese acceso, no ser descubierto y echado por la víctima.

Por lo general, el acceso es solo un paso para la consolidación de la posición, lo que viene a constituir el verdadero objetivo del usuario malintencionado. Los métodos utilizados son distintos, dependiendo de diversos factores, por lo que existen variadas opciones utilizadas para mantener el control en el tiempo. (Jara y Pacheco, 2012, p. 153).

Algunas herramientas que se utilizan para mantener el acceso son:

- Infección mediante malware.
- Ocultamiento de archivos.
- Minimización de huellas.

Por todo lo analizado en la fase de acceso, es importante que un profesional de seguridad informática esté capacitado para realizar pruebas como si fuese un verdadero atacante, ya que es la única forma de poder minimizar al máximo todas las posibles vulnerabilidades o huecos por donde pueda ingresar un ataque.

Cierre

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

La etapa de relevamiento se separa en tres fases: reconocimiento, escaneo y enumeración de un sistema.

El spoofing es una técnica utilizada para suplantar la identidad de otro sujeto, que puede ser un usuario o un proceso.

Los ataques sin tecnología son aquellos en donde no se emplean técnicas, ni software ni accesos indebidos a sistemas, sino que se valen de engañar al usuario lícito.

Figura 9. Ideas claves semana 5.

Fuente: Moran, E. (2022)

Referencias

Albors, J. (2020). Qué es un ataque de fuerza bruta y cómo funciona. Recuperado de <https://www.welivesecurity.com/la-es/2020/06/24/que-es-ataque-fuerza-bruta-como-funciona/>

Astudillo, K. (2013). Hacking ético 101. ¡Cómo hackear profesionalmente en 21 días o menos! Recuperado de <https://eduardmandov.files.wordpress.com/2017/05/security-hacking-etico-101.pdf>

Gobierno de Canarias. (s. f.). Seguridad y Alta Disponibilidad. Recuperado de <https://www3.gobiernodecanarias.org/medusa/ecoblog/flopmarl/seguridad-y-alta-disponibilidad/InternationalOrganizationforStandarization/InternationalElectronic>

Comision (ISO/IEC). (2005). Information Security Management (Norma ISO/IEC 27001). Recuperado de <https://www.iso.org/isoiec-27001-information-security.html>

Interpolados. (2017). Comparación entre el modelo OSI y el modelo TCP/IP. Recuperado de <https://interpolados.wordpress.com/2017/03/01/comparacion-entre-el-modelo-osi-y-el-modelo-tcpip/>

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

José Ignacio. (s. f.). Los 6 ciber ataques más comunes en un eCommerce. Recuperado de <https://www.actualidadecommerce.com/los-6-ciber-ataques-mas-comunes-en-un-ecommerce/>

Junta de Andalucía. (s. f.). Gestionar las líneas base y peticiones de cambio a los requisitos del sistema. Recuperado de <http://www.juntadeandalucia.es/servicios/madeja/contenido/libro-pautas/188>

Paterva. (2014). Maltego (Versión 4.2.19) [Software de computación].

Noguera, B. (s. f.). ¿Qué es una denegación de servicio? Recuperado de <https://culturacion.com/que-es-una-denegacion-de-servicio/>

Nolasco Valenzuela, J. S. (2018). Python. Aplicaciones prácticas. Madrid, ES: Rama.

Offensive Security. (s. f.). [Captura de pantalla de descarga de Kali Linux]. Recuperado de <https://www.kali.org/get-kali/>

Offensive Security. (2013). Kali Linux (Versión 2021.2) [Software de computación]. Recuperado de <https://www.kali.org/>

Panda Security. (s. f.). Exploit. Recuperado de <https://www.pandasecurity.com/es/security-info/exploit/>

Rodríguez, F. (s. f.). Phreakers: Los hackers de los sistemas telefónicos. Recuperado de <https://culturacion.com/phreakers-los-hackers-de-los-sistemas-telefonicos/Portinos>.

¿Quiénes son las personas detrás de los sistemas? Recuperado de <https://blog.portinos.com/la-mateada/quienes-son-las-personas-detras-de-los-sistemas>

Ramírez Ferreira, R. R. (2016). Ante los sueños irrealizados. ¿Más poder y más tiempo? Recuperado de <https://acento.com.do/opinion/ante-los-suenos-irrealizados-mas-poder-mas-tiempo-8398536.html>

Rodríguez Ruiz, S. (s. f.). ¿Qué es una contraseña o password? -Definición de contraseña o password. Recuperado de <https://www.masadelante.com/faqs/password>

Tecnología para los negocios. (s. f.). Qué es el hacking ético. Recuperado de <https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/>

Universidad Complutense de Madrid. (2015). Generalidades sobre Criptografía, Certificación y Firma. Recuperado de <https://www.ucm.es/faq/generalidades-sobre-criptografia-certificacion-y-firma/que-significa-no-repudio-o-irrenunciabilidad>

Universidad Internacional de Valencia. (2018). ¿Qué es la seguridad informática y cómo puede ayudarme? Recuperado de <https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme>