Introducción a las pruebas de penetración

Ana Milena Ortiz Castillo.
amoc02@gmail.com;
Especialización en Seguridad Informática
Universidad Piloto de Colombia – Bogotá, Colombia.

Resumen— Actualmente, las pruebas de penetración también conocido como Pentest, es un conjunto de pruebas de seguridad, en donde un profesional de la seguridad ejecuta ataques reales y técnicas especializadas para la detección y explotación de vulnerabilidades que poseen los activos de TI de una organización. En este servicio el consultor toma el rol de un atacante real que busca explotar y aprovecharse de las vulnerabilidades detectadas para penetrar los sistemas y obtener información de carácter confidencial para la organización. Al finalizar la ejecución de las pruebas, se entrega un reporte a nivel técnico y ejecutivo que contiene la información detallada de los hallazgos de seguridad detectados, el nivel de riesgo asociado, el escenario de riesgo, las respectivas recomendaciones para la mitigación del hallazgo de seguridad y una evidencia de la explotación de la vulnerabilidad.

Índice de Términos— Pruebas de penetración (Pentesting), Herramientas, Sistema operativo, para ello se describen las siguientes herramientas, Nmap Attack, Googlee hacking, Foca, Maltego, Osint, Banner grabbing, Hping, Nikto, Nessus, Metasploit, Sniper, Rootkits, botnets, redes c2c, troyanos, Steganography, Tunneling, ELSave, WinZapper para este documento.

Summary— Currently, penetration testing, also known as Pentest, is a set of security tests, where a security professional executes real attacks and specialized techniques for detecting and exploiting vulnerabilities in an organization's IT assets. . In this service the consultant takes the role of a real attacker who seeks to exploit and take advantage of the vulnerabilities detected to penetrate the systems and obtain information of a confidential nature for the organization. At the end of the execution of the tests, a report is delivered at the technical and executive level that contains the detailed information of the security findings detected, the level of associated risk, the risk scenario, the respective recommendations for the mitigation of the security finding. And evidence of the exploitation of vulnerability.

I. INTRODUCCIÓN

Hoy en día, las nuevas tecnologías están al alcance de todo el mundo. Entregamos parte de nuestras vidas a un mundo informatizado, en forma de datos los cuales pueden ser robados y manipulados para el beneficio ajeno. Es por ello que las redes y sistemas informáticos deben estar asegurados y protegidos ante la amenaza del robo de la privacidad de los datos.

De dicho cambio de paradigma tecnológico, aparece la necesidad de realizar y mantener la seguridad informática mediante pentesting e informes. Dicho pentesting son un conjunto de métodos, técnicas y estrategias necesarias para poner a prueba la robustez de un sistema o red con el fin de mejorar y arreglar posibles defectos que pueda tener. Si añadimos la tremenda rapidez con la que la tecnología avanza, se intuye que los conocimientos necesarios para dichas pentesting son elevados. Es por ello que surge la necesidad de estar permanentemente actualizado y la motivación extra de demostrar las técnicas actuales que se utilizan.

Este documento está enfocado a la realización de pruebas de penetración en entornos controlados como máquinas virtuales o webs, sobre los principales puntos existentes de la seguridad informática y el método de los hackers éticos y malintencionados. Se darán algunos conceptos y se mostraran herramientas y concepto relacionados con el Pentesting.

A mediados de la década de 1960, la creciente popularidad de los sistemas informáticos de tiempo compartido accesibles a través de líneas de comunicación telefónica creó nuevas preocupaciones de seguridad. En junio de 1965, por ejemplo, varios de los principales expertos en seguridad informática celebraron una de las primeras grandes conferencias sobre seguridad de sistemas, organizada por la System Development Corporation (SDC), contratista del gobierno de los Estados Unidos. [1] Durante la conferencia, se observa que el empleado de la SDC había sido capaz de evadir fácilmente las protecciones añadidas al sistema informático de tiempo compartido AN/FSQ-32 de la SDC. De este modelo de computadoras solo fueron manufacturadas dos unidades, la otra estaba en manos de la Agencia Central de Inteligencia de los Estados Unidos y evidentemente que era preocupante este suceso acontecido. [2]

Con la esperanza de que el estudio adicional sobre la seguridad de sistemas fuera de utilidad, los asistentes pidieron que "se realicen estudios en áreas tales como romper protecciones de seguridad en el sistema de tiempo compartido." En otras palabras, los participantes de la conferencia iniciaron una de las primeras peticiones formales para usar la penetración de computadoras como una herramienta para el estudio de la seguridad de sistemas. [3]

En la primavera de 1967 muchos de los especialistas en informática más importantes del país se reunieron de nuevo para discutir sus preocupaciones acerca de la seguridad de sistemas. Durante esta conferencia, los expertos en seguridad informática Willis Ware, Harold Petersen y Rein Tern, todos de la Corporación RAND, y Bernard Peters de la Agencia de Seguridad Nacional (NSA), utilizaron la frase "penetración" para describir un ataque contra un sistema informático. En un documento, Ware refiere a los sistemas de tiempo compartido de acceso remoto de los militares, y advirtió que "Es necesario realizar intentos deliberados sobre estos sistemas." Sus colegas Petersen y Gire compartieron las mismas preocupaciones, observando que los sistemas de comunicación en línea "... son vulnerables a las amenazas a la privacidad," incluyendo "penetración deliberada". Bernard Peters de la NSA hizo el mismo punto, insistiendo en que la entrada y salida de datos de las computadoras "podrían proporcionar grandes cantidades de información a un programa de penetración." [4]

II. PLANTEAMIENTO DEL PROBLEMA

Radica en dar a conocer las vulnerabilidades de una red de sistemas de información, equipos conectados a internet, así como conocer que tan vulnerables son los usuarios que hacen uso de los sistemas de información en una organización, para mejorar la implementación de la seguridad y disminuir las vulnerabilidades del sistema. En la actualidad dado el crecimiento y adquisición de componentes con acceso a internet, la tecnología ha presentado un auge rápido y continúo debido a la demanda en la compra de artículos o uso de servicios en la Internet lo que genera a su vez un aumento en la demanda del mercado tecnológico. Lo anteriormente dicho y teniendo en cuenta los múltiples servicios que se ofrecen a través de la red de internet, lo consolidan más que en una exclusividad en una necesidad de primer nivel y requiere contar con una identificación de incidencias a las que se encuentra expuesto y no se dimensionan en la utilización de estos servicios. Por estas vulnerabilidades se propuso un documento que contenga protocolos permitiendo preparar a una persona del común para mitigar la probabilidad de un ciberataque en su organización o en su hogar identificando herramientas y brindando conocimientos para su protección como las pruebas de penetración.

A. ¿Qué es análisis de vulnerabilidades?

Es el conjunto de pruebas de seguridad, en donde un especialista ejecuta técnicas y herramientas especializadas para la detección de fallas o malas configuraciones y vulnerabilidades asociadas a los servicios y activos de TI de una organización. Este servicio se realiza con el enfoque defensivo, de manera que no se realiza la explotación de las vulnerabilidades encontradas en los activos analizados, a diferencia del servicio de Pentest, se entrega un reporte a nivel técnico y ejecutivo con la información detallada de los hallazgos de seguridad detectados, el nivel de riesgo asociado, el escenario de riesgo posibles consecuencias y las respectivas recomendaciones para la mitigación del hallazgo de seguridad.

B. ¿Qué es una prueba de penetración?

El término Pentesting es muy amplio y tiene varias definiciones, tales como:

1. “Es el método para la evaluación de un sistema o red mediante la simulación de un ataque de origen hostil”. [5]
2. “Una prueba de seguridad con un objetivo específico; la prueba se termina cuando el objetivo se logra obtener, o el tiempo disponible termina”. (Manual OSSTMM- Open Source Security Testing Methodology Manual).
3. Prueba de seguridad donde los evaluadores copian los ataques reales para subvertir las características de seguridad de una aplicación, sistema o red (Instituto Nacional de Estándares y Tecnología, NIST).
4. La definición real es que el Pentesting es un conjunto de pruebas objetivas con el fin de detectar las vulnerabilidades desde un sistema, teniendo muy claro que ningún sistema es 100% seguro o inviolable. [5]

Las pruebas de penetración es una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar, las pruebas de penetración pueden ser automatizadas con aplicaciones de software. De cualquier manera, el proceso incluye la recopilación de información sobre el objetivo antes de la prueba reconocimiento, la identificación de posibles puntos de entrada, intentos de entrar ya sea virtualmente o de manera real y el reporte de los resultados.

El principal objetivo de las pruebas de penetración consiste en determinar las debilidades de seguridad. Una prueba de penetración también puede ser utilizando para probar el cumplimiento de la política de seguridad de una organización, la conciencia de seguridad de sus empleados y la capacidad de la organización para identificar y responder a los incidentes de seguridad. Cuando existe incertidumbre acerca de la eficacia de los distintos mecanismos de seguridad como los controles de los firewalls, sistemas de detección de intrusiones, monitorización de integridad de archivos, lo mejor es realizar una prueba de penetración completa. Una de las técnicas más comunes para asegurarse del nivel de efectividad, es una prueba de penetración, que es un análisis de vulnerabilidad para localizar las flaquezas individuales del sistema. [6]

Kali Linux fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux. Trae preinstalados más de 600 programas incluyendo Nmap un escáner de puertos, Wireshark un sniffer, John the Ripper un crackeador de passwords y la suite Aircrack-ng software para pruebas de seguridad en redes inalámbricas. Kali puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal. [7]

C. Kali Linux

Una de las nuevas pruebas de penetración es Kali Linux, la cual es utilizada para Auditorıas de Seguridad y Pruebas de Penetración, es una plataforma basada en GNU/Linux Debían y es una reconstrucción completa, la cual contiene una gran cantidad de herramientas para la verificación de seguridad y vulnerabilidades de una red.

D. Características de Kali Linux

Kali Linux, el sistema se adhiere completamente a los estándares de desarrollo de Debían. Se ha puesto en funcionamiento toda una nueva infraestructura, todas las herramientas han sido revisadas y empaquetadas y se utiliza ahora Git para el VCS, estas son las características de Kali Linux. [8]

- Es de código abierto.
- Árbol Git Open Source.
- Amplio soporte para dispositivos inalámbricos.
- Parches al Kernel para inyección.
- Entorno de desarrollo seguro.
- Paquetes y repositorios firmados con GPG.
- Varios lenguajes.

E. Tipos de pruebas de penetración

Existen diferentes tipos de Pruebas de Penetración, las más comunes y aceptadas son las Pruebas de Penetración de Caja Negra, las Pruebas de Penetración de Caja Blanca más las Pruebas de Penetración de Caja Gris (Figura 1).

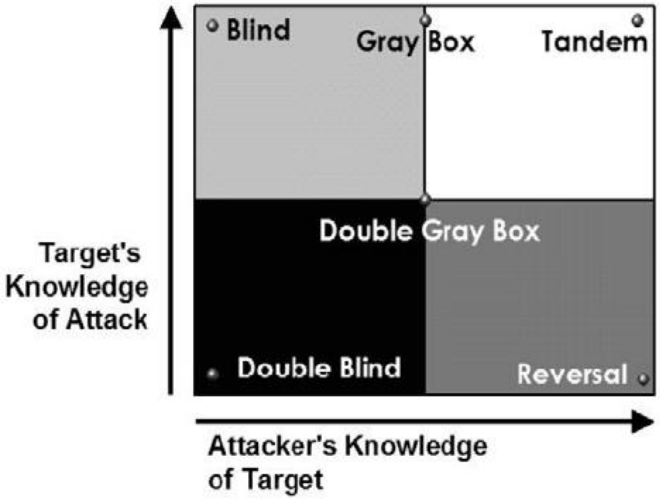

Figura 1. Tipos de Pentesting [6]

Prueba de Caja Negra: En este tipo de auditoría el equipo de consultores no recibe ningún tipo de información sobre los sistemas informáticos y activos pertenecientes a la infraestructura de TI de la organización. En este caso, el equipo de consultores sólo recibe el nombre de la institución, por lo que se trabaja con la información que se puede recolectar a través de medios públicos. Este tipo de pruebas simula el ataque de un cracker, por lo que permite medir el alcance e impacto que tendría un evento real.

Prueba de Caja Blanca: Este enfoque de auditoría se utiliza cuando el cliente necesita realizar un análisis de seguridad a profundidad en los sistemas informáticos. Para que esto suceda, el cliente comparte la mayor cantidad de información posible, de manera que el equipo consultor pueda trabajar directamente sobre los activos a analizar y reduciendo el tiempo de las fases previas a la identificación y explotación de las vulnerabilidades. En este tipo de auditoría, el equipo consultor recibe información con mayor detalle sobre los activos y servicios de la infraestructura tecnológica, tal como: versiones de los servicios que se ejecutan, listas de los sistemas operativos instalados en los servidores, código fuente de aplicaciones, entre otros.

Prueba de Caja Gris: Este tipo de auditoría es una combinación de los tipos anteriores, en dónde el cliente entrega cierta información, pero no toda al equipo de consultores, tal como: segmentos de red, direcciones IP de servidores pertenecientes a la infraestructura de TI, diagramas con la topología de la organización, entre otros. Otra manera de clasificar el tipo de pruebas es respecto al lugar desde el que el equipo de consultores realiza la ejecución de las mismas.

Pruebas de Penetración Externas: Las pruebas son realizadas por el equipo de consultores desde cualquier punto fuera de la infraestructura de TI. El objetivo de este tipo de pruebas es simular el accionar de un atacante remoto hacia los activos tecnológicos de la infraestructura de TI, que se encuentran expuestos en Internet (Figura 2). Este tipo de pruebas permite valorar la visibilidad que tiene el atacante externo y el impacto que asociado a la explotación de las vulnerabilidades detectadas. Este tipo de pruebas son realizadas desde las oficinas de la consultoría.

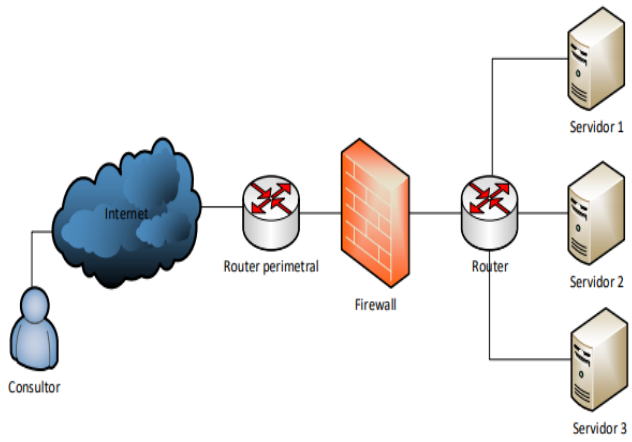

Figura 2. Pruebas Extremas [6]

Pruebas de Penetración Internas: El objetivo de estas pruebas es el de medir el daño que podría causar un atacante que se encuentre dentro de la red interna. Para llevar a cabo las pruebas internas, el equipo de consultores se sitúa en una

estación de trabajo de la organización a evaluar y se le suministra acceso a la red interna (Figura 3). Dependiendo de las necesidades del cliente y del servicio, se podría modelar un atacante interno que posee acceso a la red de usuarios administrativos, a la red de servidores de desarrollo, red de servidores de producción, entre otros.

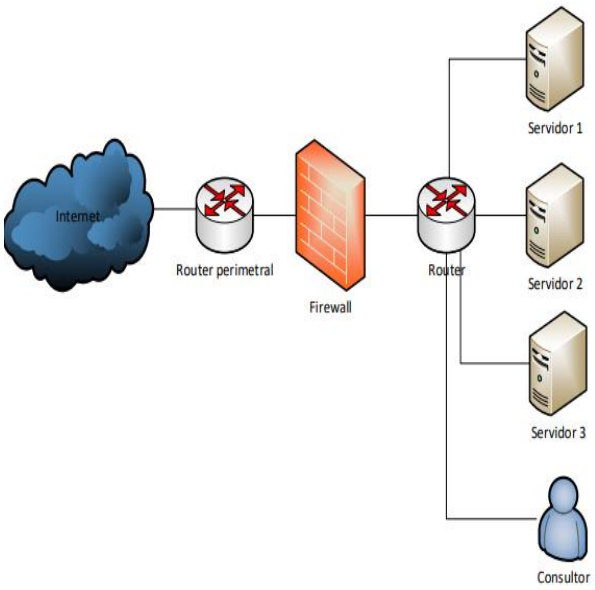

Figura 3. Pruebas Internas [6]

F. Diferencia entre Prueba de penetración y Evaluación de la Vulnerabilidad.

Evaluación de la vulnerabilidad es un proceso para determinar los controles de seguridad internas y externas mediante la identificación de las amenazas que plantean la exposición grave a los activos de las organizaciones. Esta evaluación de la infraestructura técnica no solo apunta a los riesgos en las defensas existentes, sino también recomienda y da prioridad a las estrategias de solución. La evaluación de la vulnerabilidad interna proporciona una garantía para asegurar los sistemas internos, mientras que la evaluación de la vulnerabilidad externa demuestra la seguridad de las defensas perimetrales. Cada activo en la red es rigurosamente atacado con múltiples tipos de ataque para identificar amenazas desatendidas y cuantificar las medidas reactivas.

Las pruebas de penetración van más allá del nivel de la identificación de las vulnerabilidades en el proceso de explotación, un aumento de privilegios, y mantener el acceso al sistema de destino. Otra diferencia importante entre estos dos términos es que la prueba de penetración es considerablemente más intrusiva que la evaluación de la vulnerabilidad, ya que es más agresiva en comparación a todos los métodos técnicos para explotar el entorno de producción en vivo.

G. Beneficios de realizar pruebas de penetración

1. Ofrece una perspectiva detallada de las vulnerabilidades encontradas en los sistemas de información, lo cual es de gran ayuda al momento de aplicar medidas correctivas.

2. Pone en evidencia, problemas de configuración en las aplicaciones disponibles equipos de cómputo, switches, routers, firewalls que pudieran desencadenar problemas de seguridad en las organizaciones.

3. Identifica problemas relacionados con la actualización del sistema.

4. Agiliza y disminuye los recursos requeridos para afrontar situaciones adversas en la organización. Los beneficios no solo se ven reflejados en la parte técnica y operacional de la organización, sino en compañías o empresas donde sus actividades afectan de forma directa en el cliente, los beneficios reflejan una buena imagen y reputación corporativa.

III. METODOLOGÍA DE UNA PRUEBA DE PENETRACIÓN

Para que el equipo de consultores pudiese realizar cada una de las pruebas técnicas, que compone al servicio, se contemplaron una serie de etapas necesarias. Como marco de referencia, se utilizó la metodología establecida en el proyecto PTES, que funge como estándar en el campo de las pruebas de seguridad. El proyecto PTES (Penetration Testing Execution Standard) surgió a principios del año 2009, por un conjunto de profesionales de la seguridad. Este estándar se encuentra en la versión 1.0 y fue diseñado para ofrecer a las empresas y proveedores de servicios un lenguaje y enfoque común para realizar pruebas de penetración.

Figura 4. Metodologías PTES [6]

Pre-engagement Interactions: Esta fase refiere a las interacciones previas a la ejecución de las pruebas técnicas. El equipo de consultores deberá entrevistarse con el cliente para entender las necesidades específicas del servicio y acordar las

condiciones en las que se ejecutarán las pruebas: que tipo y enfoque de pruebas se realizará, los horarios establecidos y la duración de las pruebas. Otro de los aspectos importantes a definir es el del alcance de la prueba, en dónde se establece que activos pueden ser considerados a evaluar y el nivel de profundidad de las pruebas. El nivel de profundidad se refiere hasta que instancias se permite escalar el ataque el equipo de consultores y el tipo de pruebas deben ser excluidas debido a su peligrosidad (DoS). Un documento importante que se debe definir en esta etapa es el Acuerdo de Confidencialidad o NDA (Non-Disclosure Agreenment), el cuál es necesario para proteger la privacidad de la información y hallazgos obtenidos durante la ejecución de las pruebas de penetración.

Intelligence Gathering: Es la primera fase de las pruebas técnicas, se basa en la búsqueda y recolección de la mayor cantidad de información posible sobre el objetivo, por lo que puede que sea la etapa que mayor tiempo demande. Esta etapa podría dividirse en dos: reconocimiento pasivo y reconocimiento activo. El reconocimiento pasivo se realiza para obtener información del objetivo sin tener un contacto directo con el cliente y sus activos. En este enfoque de búsqueda de información, el equipo de consultores recolecta información de sitios públicos de internet, archivos expuestos y sus metadatos, GHDB, redes sociales y servicios que brinden detalles técnicos (DNS, Whois, entre otros.). Por otro lado, el reconocimiento activo se realiza cuando el equipo de consultores interactúa de manera directa con los activos y servicios de la infraestructura objetivo. En esta etapa, el equipo de consultores se apoya de la ejecución de herramientas que interactúen con los distintos protocolos de red y servicios, con el objetivo de descubrir: segmentos de red, direcciones IP de equipos, sistemas operativos, puertos expuestos, versiones de los servicios que se ejecutan y cuentas de usuarios.

Threat Modeling: Para realizar el modelado de amenaza, la metodología se centra en dos elementos principales: los activos y el atacante. En esta etapa se busca identificar que activos son más importantes, cuales son los grupos de riesgo (atacantes o amenazas) que existen y las capacidades o motivaciones que pudiesen tener los grupos de riesgo para causar un daño a la compañía.

Vulnerability Analysis: Es el proceso de describir fallas en los sistemas y aplicaciones, las cuales pueden ser aprovechadas por un atacante para penetra en un sistema o aplicación. Esta etapa comienza con la ejecución de herramientas, pruebas automatizadas y pruebas manuales para la detección de vulnerabilidades. Después se continúa con la validación de los hallazgos detectados, buscando eliminar falsos positivos. Para finalizar, se realiza una investigación de las vulnerabilidades con el objetivo de conocer mayor información relacionada, como: las causas de la vulnerabilidad, si existe un exploit asociado, las consecuencias o efectos secundarios de la explotación y si cuenta con un identificador CVE-ID asociado.

Explotation: Durante esta etapa, el equipo de consultores se poyará de la ejecución de exploits para aprovecharse de las vulnerabilidades previamente identificadas, con el objetivo de acceder a un sistema, evadir controles de autenticación u obtener mayor información. Los exploits contienen un conjunto de instrucciones o carga útil, que se ejecuta después de aprovecharse de la vulnerabilidad y es conocida como payload. Entra las actividades que un payload podría hacer están: añadir usuarios en los sistemas, generar una backdoor, elevación de privilegios, obtener registros de bases de datos, desactivar servicios antivirus, entre otros.

Post Explotation: Esta fase tiene como finalidad la valoración de que tan lejos podría llegar el equipo de consultores, después del acceso al servicio o sistema (Explotación de la vulnerabilidad). Las actividades principales que componen esta fase son: mantenimiento del acceso, búsqueda de información y borrado de huellas. La parte del mantenimiento del acceso se puede realizar a través de la instalación de backdoors, robo de credenciales o la adición de nuevos usuarios. La búsqueda de información permitiría obtener datos o documentos de carácter sensible, archivos de configuración o credenciales almacenadas en el sistema, mismas que podrían ser utilizadas en ataques denominados movimientos laterales. Los ataques de movimiento lateral permiten validar si las credenciales recuperadas son reutilizadas en otros sistemas o equipos, de manera que nos permita ampliar el alcance de la intrusión. Para la parte del borrado de huellas, se elimina la evidencia del acceso de los archivos de registro de actividad logs. También deben eliminarse los rastros de los usuarios y backdoors desplegados en los sistemas.

Reportes (Reporting): Esta es la etapa más importante de la metodología ya que, a través del reporte, el equipo de consultores puede demostrar el trabajo realizado, los hallazgos de seguridad detectados y el impacto que se podría tener en caso de la explotación. Como parte de la evidencia de la explotación y del acceso al sistema, el reporte puede contener: capturas de pantalla de inicios de sesión en servidores, credenciales obtenidas y archivos con información confidencial obtenidos.

IV. FASES DE PRUEBAS DE PENETRACIÓN Y HERRAMIENTAS

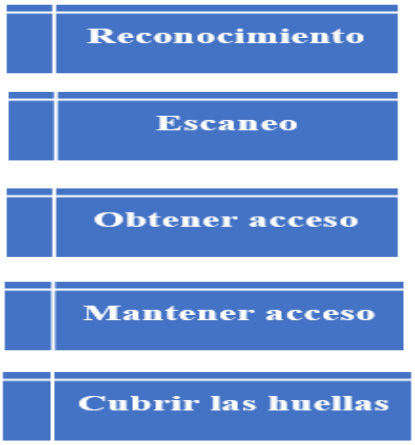

Figura 5. Fases de Penetración [11]

1. *Reconocimiento:* Esta fase consiste en el estudio previo que hace un hacker hacia su víctima u objetivo, lo que se hace básicamente es extraer toda la información posible como ser: el sistema operativo que usa la víctima, las aplicaciones que usa, puertos que tiene habilitados, dirección IP de su máquina, y demás información que le servirá al hacker para posteriormente estudiar a esta víctima más a fondo y poder planear una estrategia de ataque. [11]

Las herramientas que se pueden emplear en un hacker durante la fase de Reconocimiento:

Nmap: Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Este software posee varias funciones para sondear redes de computadores, incluyendo detección de equipos, servicios y sistemas operativos. Estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la red incluyendo latencia y congestión de la misma.

Google hacking: uso de operadores avanzados de Google en su motor de búsqueda para localizar cadenas específicas de texto dentro de los resultados de búsqueda. Algunos de los ejemplos más populares están encontrando versiones específicas de vulnerabilidad de aplicaciones web. Las consultas de búsqueda localizarían todas las páginas web que tiene diferentes tipos de filtros; ya sea por el título (intitle), por texto principal (intext), por url (inurl) o por otros filtros más.

En el buscador de Google escriba intitle: Google Operadores filetype: pdf. Esta línea de comando tiene 3,710 resultados aproximadamente en comparación con escribir solamente Google Operadores en el buscador de Google. Este operador de Google busca información en el buscador de Google acerca de los operadores de Google y que está en formato de datos portables mejor conocido como pdf. El operador tipo de archivo filetype se puede aplicar a cualquier extensión de tipo de archivo.

Foca: permite la extracción y el análisis de metadatos ubicados en un servidor o una página web. Dicha información se obtiene a partir de ficheros tipo Microsoft Office, PDF y SVG entre otros que son localizados utilizando motores de búsqueda como Google, Bing y DuckDuckGo.[12] El análisis por parte de FOCA de dichos metadatos genera un informe con información relevante como configuración de la red, proxy, ficheros de backup.

Manltego: Servicio que tiene el potencial de encontrar información sobre personas y empresas en Internet, permitiendo cruzar datos para obtener perfiles en redes sociales, servidores de correo. A la hora de buscar establecer contacto con una empresa, esta herramienta puede proporcionarnos datos muy útiles como direcciones de correo electrónico como puede ser de recursos humanos, departamento de ventas, soporte técnico, número telefónico, lo que nos facilitaría el contacto con esta empresa o persona; también posee la capacidad de encontrar distintos tipos de artículos como son autos, motos, aviones, entre otros.

2.*Escaneo:* Esta es la fase en la que el hacker organiza toda la información obtenida en la anterior fase, toma aquello que le pueda servir para hacer un análisis, luego identifica las características más importantes de toda la información y la estudia para hallar vulnerabilidades. El hacker deberá sobre todo enfocarse en los puertos ya que es una pieza clave para un ataque. [11]

Las herramientas que se pueden emplear en un hacker durante la fase de Escaneo:

Banner grabbing: es una de las formas de conocer qué infraestructura o sistema se encuentra detrás de una aplicación web o servicio. En otras palabras, está fuertemente relacionado con el fingerprinting para detectar el sistema operativo. Banner grabbing puede aplicarse sobre cualquier tipo de servicio, cómo, por ejemplo, FTP, VNC, HTTP, entre otros, en este caso nos enfocaremos sobre el último debido a que es posible resaltar comportamientos particulares del mismo. Además de la detección del servidor que se aloja detrás del sitio web, en algunos casos es posible conocer la versión del mismo. Cabe destacar que no siempre es posible obtener información completa ya que existen formas de ocultar la información que brinda un servidor frente a diferentes peticiones.

Hping3: es una aplicación de terminal para Linux que nos va a permitir analizar y ensamblar fácilmente paquetes TCP/IP. A diferencia de un Ping convencional que se utiliza para enviar paquetes ICMP, esta aplicación permite el envío de paquetes TCP, UDP y RAW-IP. Junto al análisis de los paquetes, esta aplicación puede ser utilizada también con otros fines de seguridad, por ejemplo, para probar la eficacia de un firewall a través de diferentes protocolos, la detección de paquetes sospechosos o modificados, e incluso la protección frente a ataques DoS de un sistema o de un Firewall.

Nikto: es una herramienta de escaneo de servidores web que se encarga de efectuar diferentes tipos de actividades tales como, detección de malas configuraciones y vulnerabilidades en el servidor objetivo, detección de ficheros en instalaciones por defecto, listado de la estructura del servidor, versiones y fechas de actualizaciones de servidores, tests de vulnerabilidades XSS, ataques de fuerza bruta por diccionario, reportes en formatos txt, csv, html.

Nikto es un proyecto robusto que lleva varios años en desarrollo y se encuentra en constante evolución. Unas de las características más interesantes de esta herramienta son la posibilidad de generar reportes en distintos formatos, la integración con LibWhisker (Anti-IDS), integración con Metasploit.

Nessus: comienza escaneando los puertos con nmap o con su propio escaneador de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Lenguaje, Lenguaje de Scripting de Ataque Nessus.

3. *Obtener acceso*: Esta es una de las fases para el hacker ya que es la fase en la que aplicara la estrategia planteada luego de que en la fase anterior haya encontrado las vulnerabilidades, para esto el hacker deberá hacer uso de todas sus habilidades mejor aún si usa herramientas que existen justamente para lo que desea realizar el hacer. El acceso puede ser localmente o de un medio externo, a través de secuestro de sesión (esto consiste en falsificar la identidad de un ordenador conocido para el ordenador de la víctima, y confundirla haciéndose pasar por esta), incluso tratando de descifrar la contraseña del ordenador de la víctima. Esta fase es decisiva ya que el hacker podrá ver el alcance de éxito que pueda tener su penetración. [11]

Las herramientas que se pueden emplear en un hacker durante la fase de Obtener acceso:

Metasploit: Es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos. Su subproyecto más conocido es el Metasploit Framework, una herramienta para desarrollar y ejecutar exploits contra una máquina remota. Otros subproyectos importantes son las bases de datos de opcodes códigos de operación, un archivo de shellcodes.

4.*Mantener el acceso:* Esta fase consiste en mantener el acceso que gano en el sistema tratando de usar distintas herramientas como los sniffers que son usados para capturar el tráfico de red, este tráfico de red le servirá al hacker para poder obtener información sobre con que ordenadores interactúa su objetivo, lo que le servirá para poder hacer una falsificación de identidad haciéndose pasar por una de la direcciones conocidas y de confianza de sus objetivo, en esta fase debe iniciar sesiones telnet y FTP. En esta fase es importante que el hacker permanezca como indetectable para el objetivo, para esto debe remover el rastro de evidencia que dejo su penetración y haciendo uso de Backdoor y Troyanos para de esta manera intentar conseguir acceso con altos niveles de privilegio es decir como un administrador, como también podrían usar caballos de Troya para transferir información como nombres de usuario, passwords y cuentas de banco que podrían estar almacenadas en el sistema del objetivo. [11]

Las herramientas que se pueden emplear en un hacker durante la fase de Mantener el acceso:

Rootkist: Tratan de encubrir a otros procesos que están llevando a cabo acciones maliciosas en el sistema, si en el sistema hay una puerta trasera para llevar a cabo tareas de espionaje, el rootkit ocultará los puertos abiertos que delaten la comunicación; o si hay un sistema para enviar spam, ocultará la actividad del sistema de correo. Los rootkits, al estar diseñados para pasar desapercibidos, no pueden ser detectados. Si un usuario intenta analizar el sistema para ver qué procesos están ejecutándose, el rootkit mostrará información falsa, mostrando todos los procesos excepto él mismo y los que está ocultando.

Botnets: Las Botnets normalmente usan servicios gratuitos de DNS para IP's dinámicas como DynDns.org, No-IP.com, & Afraid.org para apuntar a un subdominio al cual el creador puede conectarse en caso de que le cierren el servidor de IRC. En muchas ocasiones basta con avisar a estos proveedores para que cancelen su cuenta y de esta manera desarticular la Botnet completa.

Afortunadamente la estructura de servidores de la botnet tiene vulnerabilidades inherentes a su arquitectura, si se encuentra el servidor de IRC y el canal, se tiene acceso a la botnet completa, con lo cual al servidor de IRC le basta con cerrar el canal o poner una g-line o k-line a las ips que intenten entrar a dicho canal.

El control de la botnet se hacía normalmente a través del IRC, pero nuevas versiones de estas botnets han evolucionado hacia control mediante HTTP, con lo que la detección de estas redes es más compleja. Esto hace que las redes de empresas sean más vulnerables también, ya que el tráfico de IRC queda bloqueado.

Uso habitual de los Botnet: Estas redes son usadas en general para generar dinero a través de usos que generan dinero a sus controladores. Entre los usos más comunes están:

Ataques de denegación de servicio distribuidos (DDoS): Si se recibe un ataque de tipo DDoS desde una Botnet, dada la dispersión geográfica de los ordenadores que la componen, es casi imposible encontrar un patrón de las máquinas que están atacando y dado el alto número de ellas que lo estarán haciendo al mismo tiempo, no se puede contemplar el filtrado de paquetes como una solución real que funcione. No obstante, puede ayudar a mitigar el problema hacer un escaneo pasivo de los paquetes para reconfigurar y adaptar el firewall.

Envío de Spam: Lo más frecuente es que una botnet se utilice para enviar spam a direcciones de correo electrónico. Normalmente los creadores de estas Botnets venden sus servicios a los spammers. Por lo menos en un caso una investigación (la red Rustock), consiguió averiguar que un solo hacker había conseguido el control de un millón de ordenadores, utilizándolos como plataforma para sus ataques, con los que era capaz de enviar 30 billones de spam por día. [4]

Minería de Bitcoins: Con la aparición de criptomonedas, ya en 2011 había reportes de un nuevo uso para las botnets: usar el procesamiento de los computadores para generar bitcoins. [5] De esta forma los criminales pueden obtener recursos sin gastar en hardware ni en consumo de energía. [6] El uso siga aumentando en el futuro. [7]

Robo de Bitcoins: Una variante adicional es el robo de bitcoins usando botnets. Es el caso de la red Pony, que robaba información de los equipos infectados. Se estima que con esta red se obtuvieron credenciales usuario/passwords de al menos 2 millones de equipos.

Redes C2c: (Consumer-to-consumer) una estrategia de cliente a cliente. Se utiliza este término para definir un modelo de negocio en la red que pretende relacionar comercialmente el usuario final con otro usuario final. Una estrategia C2C para Internet sería aquélla que define un negocio cuyo objetivo es facilitar la comercialización de productos y/o servicios entre particulares, como por ejemplo eBay, sirviendo la empresa como mera intermediaria y cobrando por sus servicios. C2C también puede hacer referencia a las transacciones privadas entre consumidores que pueden tener lugar mediante el intercambio de correos electrónicos o el uso de tecnologías P2P (Peer-to-Peer).

5. *Cubrir las huellas:* Esta es donde debe cubrir las huellas para poder terminar la obra perfecta, debe usar todas las herramientas posibles para evitar que los administradores puedan encontrar los registros de acceso de un usuario desconocido a través del análisis de tráfico que podrían hacer. Esta para mi es la fase más importante para un hacker ya que de esto depende que no encuentren evidencias, porque simplemente basta con encontrar un registro del acceso de un individuo extraño para que la víctima sospeche y si tiene un buen sistema de seguridad podrían detectarlo y así el hacker terminaría en la cárcel. [11]

Las herramientas que se pueden emplear en un hacker durante la fase de Cubrir las huellas:

Troyanos: a un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos, crean una puerta trasera (en inglés backdoor) que permite la administración remota a un usuario no autorizado.

Steganography: esteganografía y criptografía, en ambas, se intenta ocultar un mensaje para ser enviado, pero ellas son fundamentalmente diferentes, ya que la criptografía solo cifra los mensajes, manteniéndolos visibles pero irreconocibles, aparecen como una secuencia de caracteres ilegibles; para ver su contenido original es necesario conocer una clave. En la esteganografía, el archivo u objeto que contiene el mensaje oculto se observará idéntico al original, y para conocer su mensaje contenido será necesario conocer la clave y el algoritmo software con el que se ocultó.

Tunneling: protocolo de red sobre otro protocolo de red encapsulador, creando un túnel de información dentro de una red de computadoras. El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc. La técnica de tunelizar se suele utilizar para transportar un protocolo determinado a través de una red que, en condiciones normales, no lo aceptaría. Otro uso de la tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales.

WinZapper: Es una herramienta gratuita de utilidad piratería que se utiliza para eliminar eventos del registro de seguridad de Microsoft Windows NT 4.0 y Windows 2000 . Fue desarrollado por Arne Vidstrom como una herramienta de prueba de concepto, que demuestra que una vez que la cuenta del administrador se ha visto comprometida, los registros de eventos ya no son confiables. Según Hacking Exposed: Windows Server 2003, Winzapper funciona con Windows NT / 2000/2003.

Las herramientas son presentadas en diferentes categorías, aquí algunas de las más importantes:

Information gathering: Herramientas de recolección de datos que ofrecen información sobre los objetivos de los análisis, especialmente herramientas de DNS, dominios y direcciones IP. Nmap está en esta categoría.

Aplicaciones web: Herramientas diseñadas para realizar análisis en sitios web a nivel de servidores. Recomendaciones para esta sección: Nikto y w3af para encontrar vulnerabilidades en los sitios.

Ataques a contraseñas: Herramientas para hacer cracking de contraseñas, de forma tal, que se prueban ataques de fuerza bruta o diccionario para encontrar las contraseñas de acceso correctas a un formulario o sistema.

Ataques inalámbricos: Cuando un atacante está conectado a una red wireless puede ejecutar algunos ataques, especialmente cuando intenta interceptar información que está siendo transmitida mediante esa red inalámbrica. Estas herramientas permiten analizar la red y diagnosticar su seguridad.

Herramientas de explotación: Metasploit Framework es la clave de esta sección, entre otras herramientas que permiten explotar vulnerabilidades.

Sniffing/Spoofing: Wireshark y Ettercap son las herramientas más recomendables. Con ellas, es posible ver el tráfico de red que podría permitir el acceso a información confidencial, entre otros ataques.

Ingeniería inversa: Ollydbg es uno de los mejores debuggers que podrían ayudar a comprender qué acciones realiza un archivo en el sistema por medio de un proceso de ingeniería inversa.

Forense: También hay una serie de herramientas para realizar análisis forenses sobre un sistema, es decir, se puede analizar el estado de un sistema justo en el momento que ocurrió

determinado incidente; además se identifican acciones pasadas o archivos ocultos en el mismo, entre otros.

V. CUMPLIMIENTO LEGAL

El presente documento está alineado con la Ley 1712 de 2014 (Congreso de la República de Colombia, 2014) - de Transparencia y del Derecho de Acceso a la Información Pública y Nacional se pueda obtener. Las pruebas de vulnerabilidad se realizan a tres (3) aplicativos Web y tres (3) aplicativos cliente/servidor definidos por la entidad, sobre el protocolo de internet IPv4. Se hacen las recomendaciones pertinentes, para que la selección de los aplicativos pertenezca a los activos críticos de la entidad.

Adicionalmente, se realizan las actividades para la vuelta a la normalidad, generando el menor impacto institucional aceptable, en caso de que las pruebas de vulnerabilidad y análisis generen alguna interrupción de uno o más servicios de TI, o de los sistemas de información que operan. Para las pruebas realizadas a los aplicativos, se estudian los factores y/o recursos que sean utilizados en el almacenamiento, transporte y procesamiento de la información, lo anterior implica hardening, verificación de puertos, configuración de servicios, validación de permisos críticos, existencia y uso de keyloggers, verificación de las actualizaciones de los antivirus y, estado de la actualización de parches críticos y de seguridad. Los tipos de pruebas que se orientan en este documento son credenciales débiles, Cross Site Scripting, SQLi, explotación de vulnerabilidades de componentes Java y finalmente ataques por buscadores web.

¿Cuál es el Objeto de la Ley 1712 de 2014? El objeto de la Ley 1712 de 2014, conocida como la Ley de Transparencia y del Derecho de Acceso a la Información Pública, es regular el derecho de acceso a la información pública que tienen todas las personas, los procedimientos para el ejercicio y la garantía del derecho fundamental así como las excepciones a la publicidad de la información pública.

¿Qué es el Derecho de Acceso a la Información Pública? La Ley Estatutaria 1712 del 6 de marzo de 2014 consagró el Derecho de Acceso a la Información Pública como un derecho fundamental que tienen todas las personas para conocer de la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados, consiste en la posibilidad real que tiene toda persona para conocer acerca de la existencia y poder acceder a la información pública que tengan en posesión o bajo control los sujetos obligados. [16]

VI. CONCLUSIONES

A medida que avanza el desarrollo de nuevas tecnologías de la información, que sirven de apoyo a los distintos procesos de negocio, surgen de manera paralela distintas amenazas. En los últimos años se reportó un incremento de incidentes de seguridad informática que han impactado a grandes compañías a nivel mundial. Por este motivo, muchas empresas adoptaron la práctica de realizar pruebas de penetración a sus infraestructuras de TI, con el objetivo de diagnosticar brechas de seguridad que pudiesen ser aprovechadas por las amenazas/atacantes. En las pruebas de penetración se identifican hallazgos de seguridad que podrían causar una afectación a la confidencialidad, integridad y disponibilidad de la seguridad informática, y que a su vez podrían desembocar en pérdidas monetarias, sanciones por entidades regulatorias, afectación a la reputación, afectaciones a procesos industriales, entre otros. Estos hallazgos de seguridad permitieron a la empresa cliente desarrollar un plan para la pronta atención y mitigación de las vulnerabilidades reportadas.

Algunas de las medidas acordadas son la implementación de un sistema de aplicación de parches de seguridad críticos en los servidores y dispositivos vulnerables, migración de servidores obsoletos a sistemas operativos que cuenten con soporte vigente por parte del proveedor, implementación y mejora de reglas en dispositivos de seguridad (IDS/IPS), adopción de una metodología de revisión de código durante la publicación y desarrollo de aplicaciones, entre otras. Es importante resaltar que estas medidas reducirán los niveles de riesgo y los hallazgos, a un nivel que serán aceptable.

REFERENCES

[1] «System Development Corporation» (html). *CA Highways* (en inglés). Archivado desde el original el 12 de agosto de 2004. Consultado el 12 de julio de 2018. «System Development Corporation evolved out of the System Development Division of the RAND Corporation. The RAND Corporation was a non-profit group incorporated in 1948 by technical engineers and military people who worked together during World War II.

[2] Mize, Roy (5 de abril de 2010). «IBM SAGE» (html). *Ed Thelen Org* (en inglés). Archivado desde el original el 20 de mayo de 2010. Consultado el 12 de julio de 2018. «Number of AN/FSQ-32 computers manufactured: 2 Locations" 1 at SDC; 1 at IBM (One source states that 1 system went to the CIA)».

[3] Hunt (2012), pp. 7-8

[4] Saltar a:*a b* Hunt (2012), p. 8

[5] oficial referencia ISO 31000:2009 - gestión de riesgos - principios y directrices

[6] R.Guirado, “Penetration Testing: conceptos generales y situación actual [en línea]”.

[7] Montevideo, 2009. Disponible en: https://www.isaca.org/chapters8/Montevideo/Events/Documents/penetration%20testing%20-%20conceptos%20generales%20

[8] Penetration Testing: A Hands-On Introduction to Hacking.y%20situacin%20actual.pdf. [Accedido: 22 -mar-2016]

[9] Penetration Testing: A Hands-On Introduction to Hacking.y%20situacin%20actual.pdf. [Accedido: 22 -mar-2016]

[10] https://es.wikipedia.org/wiki/Kali_Linux

[11] http://es.docs.kali.org/introductiones/que-es-kali-linux

[12] www.pentest-stardard.org

[13] https://en.wikipedia.org/wiki/Winzapper

[14] https://ehack.info/las-fases-del-hacking-etico/

[15] https://hectorpedraza10.wordpress.com/2014/11/21/fases-del-haking-etico/

[16] The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws 2nd Edition.

[17] Advanced Penetration Testing: Hacking the world’s most secure networks.

[18] Congreso de la República de Colombia. (2014). Ley 1712 de transparencia y del derecho a la información pública nacional. 6 De Marzo De 2014.