Guía de buenas prácticas para la realización de un Etical hacking basado en la metodología OSSTMM.

Fabian Isidro Rivera Mejia.
Especialización seguridad Informática.
Universidad Piloto de Colombia.
Bogotá – Colombia.

***Abstract* — An ethical hacking contains some skills and knowledge that is used to audit and test the current state of security from an asset within an organization, the goal here is found the most possible vulnerabilities and try to exploit them in an controlled environment, all this using the methodology Open Source Security Testing Methodology Manual.**

***Resumen* — Un Etical Hacking consta de una serie de conocimientos y habilidades utilizadas para auditar y validar el estado de seguridad de la información de un activo en una infraestructura tecnológica, el objetivo final de un Etical Hacking es encontrar la mayor cantidad de vulnerabilidades posibles sobre un activo, tratar de explotar esas vulnerabilidades bajo un ambiente controlado emulando un ataque como si fuera real (hay que tener y prestar atención en no generar un ataque de denegación de servicio u otro tipo de indisponibilidad al realizar estas pruebas), actualmente existen varias metodologías para la realización del Etical Hacking, razón por la cual el objeto de este paper es brindar una guía de mejores prácticas para la realización del análisis de vulnerabilidades, pruebas de penetración, generación de reportes, análisis y conclusiones.**

***Index Terms*— Análisis de vulnerabilidades, pruebas de penetración, amenaza, vulnerabilidad, riesgo, exploit, ataque, hacker, cracker, caja negra, caja gris, caja blanca, auditoria, intrusión, visibilidad.**

I. INTRODUCCIÓN

Dado que la información es uno de los activos más importantes de las organizaciones, nace una necesidad fundamental de buscar los diferentes métodos y estrategias para proteger dicha información, con el objetivo de garantizar y preservar la confidencialidad, integridad y disponibilidad de la información como pilares fundamentales.

Durante el transcurso de los años se ha evidenciado el auge que han tenido las diferentes herramientas tecnológicas que se han desarrollado, con el objetivo de brindar mayores facilidades y comodidades en las labores que desarrolla el hombre en su día a día, con el desarrollo de estas herramientas se generó un gran conocimiento tanto es su uso como aplicabilidad (una orientada a aprovechar y sacar utilidad de las herramientas creadas y otras personas poco éticas orientadas a aprovecharse de las vulnerabilidades de esas herramientas con fines poco éticos y fraudulentos) he aquí donde nacen dos conceptos fundamentales Hacker, Cracker, a continuación se describen algunas de las características y habilidades de estos conceptos, ver Figura1.

Cracker	*Hacker*
Robo de identidad	Accesos por conocimiento
Acciones fraudulentas	Fines pedagógicos
Cyber-Crimen	Hacking Ético
Cyber-Guerra	

Figura 1: Hacker – Cracker características, 07 de Diciembre de 2015, Imagen del autor.

Con la aparición de estos términos se han generado pre conceptos acerca de la motivación y fines por las cuales estos personajes realizan las diferentes intrusiones a las organizaciones, a continuación se muestras algunas de las que podrían ser esas motivaciones, Figura 2.

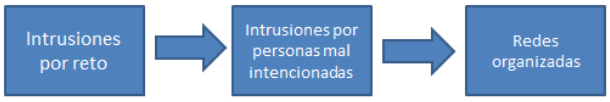

Figura 2: Hacker – Cracker motivaciones, 07 de Diciembre de 2015, Imagen del autor.

Intrusiones por reto: simplemente la persona trata de demostrar que es mejor que otra, su objetivo es quebrar las barreras de seguridad de alguna organización, su objetivo es más educativo, retos personales mas no es robar o modificar información.

Intrusiones por personas mal intencionadas: Son personas con conocimientos básicos o avanzados en redes y seguridad, cuyo objetivo es realizar intrusiones para robar información confidencial.

Redes organizadas: Son un grupo de personas organizadas con el objetivo de realizar diferentes ataques a gran escala, para la obtención de información confidencial la cual después pueden vender en el mercado negro o en algún otro tipo de intercambio, un ejemplo de estos grupos es Anonymous.

Bajo la metodología OSSTMM existen varios términos dependiendo de las pruebas de seguridad realizada a redes y sistemas informáticos, los cuales están basados en el tiempo que se puede tardar y el costo que puede generar cada tipo de prueba.

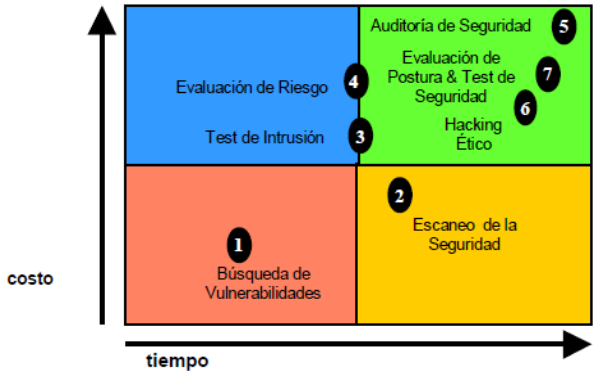

Figura 3: Tipos de pruebas de seguridad, 07 de Diciembre de 2015, imagen tomada del sitio: http://images.slideplayer.es/1/35183/slides/slide_24.jpg

Búsqueda y vulnerabilidades: Revisiones y comprobaciones automáticas realizadas a algún sistema informático (elementos de red, servidores, aplicaciones, entre otros).

Escaneo de la seguridad: Realizar la búsqueda de vulnerabilidades la cual incluye verificaciones manuales de falsos positivos, identificación de puntos débiles de la red y análisis detalla de los diferentes elementos que interactúan en la infraestructura informática.

Test de intrusión: El objetivo es identificar un objetivo dentro de la red e intentar explotar alguna de las vulnerabilidades del sistema, con el fin de tener acceso privilegiado al sistema, estas pruebas pueden ser catalogadas de tres maneras, caja blanca (La persona encargada de hacer las pruebas tiene conocimiento total del sistema y del entorno que va a ser testeado), caja gris (La persona encargada de las pruebas posee un conocimiento básico del objetivo a ser testeado, conoce los servicios que presta pero no en detalle cómo funciona), caja negra (La persona encargada de las pruebas no posee ningún tipo de conocimiento sobre el objetivo a ser testeado)

Evaluación de riesgo: Hacer el respectivo análisis de riesgos sobre los objetivos a testear, identificando el impacto y riesgo de cada uno de ellos, se puede utilizar cualquier metodología para realizar este análisis.

Auditoria de seguridad: Hace referencia a la inspección manual con privilegios administrativos del sistema operativo y de los programas o aplicaciones dentro de la infraestructura tecnológica.

Hacking Ético: Es la realización de los diferentes test e intrusión con el objetivo de obtener acceso a un sistema dentro del tiempo de la duración del proyecto de análisis de seguridad.

II. APLICACIÓN

Con el fin de realizar una Etical Hacking en una organización de una manera estructurada se debe tener en cuenta alguna metodología de la industria, es este papper nos vamos a centrar en la metodología OSSTMM sección ***Seguridad en las Tecnologías de Internet***, la cual es un conjunto de reglas y lineamientos para saber cuándo, que y cuales eventos de seguridad deben ser probados.

Aparte de la sección Seguridad en Tecnologías de Internet el OSSTMM tiene un completo mapa de seguridad, el cual consta de varias secciones que también pueden ser auditadas, a continuación se muestra el mapa seguridad.

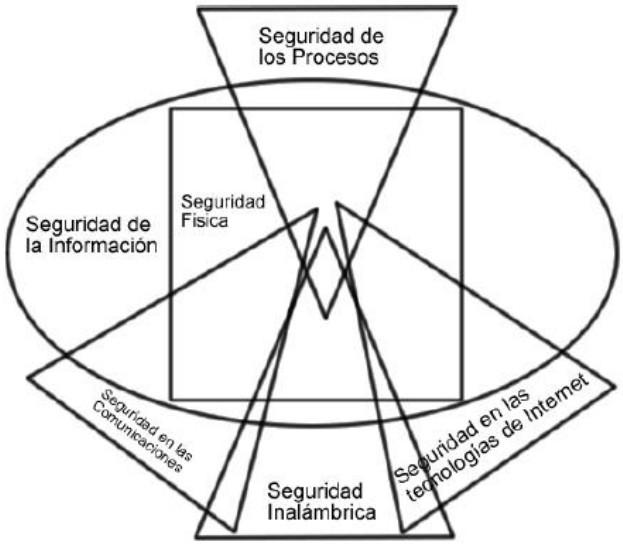

Figura 4: Mapa de seguridad OSSTMM, 07 de Diciembre de 2015, imagen tomada del sitio: http://www.conganat.org/SEIS/inforsalud04/images/Image418.gif

Esta metodología cubre las pruebas de seguridad realizadas desde un entorno externo, cuyo objetivo es lograr evadir los componentes de seguridad y los diferentes controles implementados en alguna organización.

A continuación se describen las fases utilizadas para la realización de estas pruebas:

Logística y Controles: En esta fase el objetivo principal es tratar de minimizar los falsos positivos y falsos negativos que se pueden presentar en el análisis, realizando los ajustes necesarios en las diferentes herramientas utilizadas para este fin.

Sondeo de red: Es la forma básica de empezar con las pruebas, el objetivo es la recolección y obtención de información sobre los objetivos a testear, se debe definir y limitar a nivel legal y contractual cuáles serán los activos a analizar, en esta fase no se realiza ninguna intrusión.

Acá se realizan las siguientes actividades:

- ✓ Buscar información del registro de dominio en busca de servidores.

- ✓ Encontrar el nombre del propietario del direccionamiento público registrado ante el ISP.
- ✓ Búsqueda de host y subdominios.
- ✓ Realizar diferentes trazas para definir los saltos y poder tener un diagrama de la red.
- ✓ Buscar en bases de datos de empleos ofertas de trabajo en tecnología dentro de la organización para buscar las referencias de hardware y software.

Los resultados esperados en esta fase son, Figura 3.

Resultado
Nombres de dominio
Nombres de servidores
Direcciones IP
Mapa de red
Informacion del ISP

Figura 5: Resultados Fase sondeo de red, 07 de Diciembre de 2015, Imagen del autor.

Identificación de los servicios: Realizar escaneo de puertos a los objetivos con el fin de enumerar los puertos abiertos que tiene el sistema (es una prueba invasiva en los niveles de transporte y red), también se realiza este escaneo para validar que otros dispositivos de red se encuentran activos, una vez identificados los puertos abiertos en el sistema de debe iniciar un análisis de la aplicación que escucha en cada puerto, con el fin de conocer cómo funcionan las aplicaciones.

Las actividades a realizar en esta fase son:

- ✓ Analizar BroadCast de la red.
- ✓ Utilizar ICMP para listado y enumeración de direcciones IP.
- ✓ Emplear diferentes paquetes TCP con flags modificados para ver la respuesta del servidor.
- ✓ Usar escaneos TCP SYN sobre los puertos 21, 22, 25, 80 y 443 para todos los servidores de la red.
- ✓ Revisar patrones de tráfico y protocolos de enrutamiento.
- ✓ Verificar y examinar los protocolos no estándar encontrados en la red.
- ✓ Revisar los protocolos cifrados utilizados en la red
- ✓ Relacionar cada puerto abierto con un servicio y protocolo.
- ✓ Identificar el nivel de parcheo de los dispositivos analizados.
- ✓ Identificar la aplicación utilizada y su versión.
- ✓ Buscar ofertas de empleo asociadas a la organización donde se pueda obtener información sobre los servidores y aplicaciones del objetivo.

En esta etapa se debería obtener la siguiente información:

Resultados
Puertos abiertos, cerrados, filtrados
Direcciones IP de los dispositivos activos en la red
Direccionamiento de la red
Servicios activos
Tipos de servicios
Sistema Operativo
Listado dispositivos activos
Mapa de la red

Figura 6: Resultados Identificacion de los servicios, 07 de Diciembre de 2015, Imagen del autor.

Búsqueda de información competitiva: Es una búsqueda de información útil a partir de la presencia del contenido alojado en la nube acerca de la compañía que puede llegar a ser catalogada como información sobre el negocio, dando un valor añadido a diferentes componentes que ayudan a justificar a nivel de negocio la necesidad de la implementación de nuevos servicios o controles.

Algunas de las actividades a realizar en esta fase son:

- ✓ Realizar búsquedas en redes sociales, bolsas de empleo.
- ✓ Buscar en bases de datos tales como WHOIS en búsqueda de servicios relacionados con los nombres de los servidores.
- ✓ Tratar de encontrar correos electrónicos de los empleados asociados al dominio de la compañía.
- ✓ Encontrar la estructura de directorio de los servidores Web y FTP.

Resultados esperados:

Resultados
Tamaño y alcance de la presencia de la organiazcion en Internet
Justificaciones de negocio sobre la red de la organización

Figura 7: Busqueda de información competitiva, 07 de Diciembre de 2015, Imagen del autor.

Revisión de la privacidad: Es la verificación de la privacidad que se enfoca en cómo se gestiona desde un punto de vista ético y legal, el almacenamiento, trasmisión y control de datos de información privada perteneciente a empleados y clientes.

En este punto se debe tener muy claro la diferencia entre información privada e información personal.

Información Privada: aquella información que generalmente sólo es conocida por la persona a la que pertenece y la autoridad que ha recopilado dichos datos.

Información personal: es aquella información que describe una persona o su estilo de vida, como por ejemplo la fecha de nacimiento, color de pelo, ojos, nombre de los miembros de su familia, entre otros.

Búsqueda y verificación de vulnerabilidades: En esta fase el objetivo es la identificación, verificación y comprensión de las debilidades del sistema, errores de configuración y vulnerabilidades en un servidor determinado, esta búsqueda se realiza utilizando herramientas automáticas tales como nessus, OpenVas, Core Impac, NexPose entre otras, las cuales ayudan de gran manera en la determinación de agujeros de seguridad, niveles de parcheado de los sistemas.

Algunas de las actividades realizadas en esta etapa son:

- ✓ Utilización de herramientas de análisis de vulnerabilidades.
- ✓ Priorizar las vulnerabilidades por tipo de aplicación y sistema.
- ✓ Categorizar que vulnerabilidades afectan a cuales servicios y/o aplicaciones.
- ✓ Realizar análisis redundantes, por lo menos hacer esta tarea dos veces para tener un punto de partida y poder comparar estos análisis.
- ✓ Identificar todas las vulnerabilidades a aplicaciones y a sistemas operativos para dar un tratamiento a cada una de ellas.
- ✓ Hacer re análisis con el objetivo de evitar falsos positivos y falsos negativos.

Los resultados esperados en esta fase son:

Resultados
Vulnerabilidades por aplicación o servicio
Nivel de parches de los sistemas y aplicaciones
Categorización de vulnerabilidades
Servicios y aplicaciones publicadas en Internet

Figura 8: Busqueda de vulnerabilidades, 07 de Diciembre de 2015, Imagen del autor.

Testeo de aplicaciones de Internet: Son las pruebas realizadas a las diferentes aplicaciones cliente servidor desde Internet, sin portar la tecnología o lenguaje de programación, estas pruebas se pueden clasificar de dos maneras, de caja negra o de caja blanca.

Se deben realizar múltiples actividades en esta fase:

- ✓ Determinar las especificaciones de protocolos utilizados por las aplicaciones Cliente/Servidor.
- ✓ Identificar los diferentes mensajes de error/debug en las salidas del programa y del sistema.
- ✓ Buscar las posibles combinaciones para realizar ataques de fuerza bruta a los sistemas y aplicaciones.
- ✓ Tratar de identificar cuentas de usuario válidas.
- ✓ Identificar la lógica de las aplicaciones para mantener las sesiones de autenticación (número de sesiones concurrentes, numero intentos fallidos de autenticación antes de que se bloquee el usuario, autenticarse en horarios no laborales, entre otras).
- ✓ Determinar los privilegios de acceso en las aplicaciones, duración de las sesiones.
- ✓ Identificar si la aplicación se ejecuta sobre protocolos de red seguro, con el fin de utilizar ataques de hombre en el medio.
- ✓ Encontrar limitaciones de las variables de las aplicaciones, longitud de datos, tipos de datos permitidos, formato de la estructura.
- ✓ Utilizar cadenas de caracteres lo suficientemente largas para encontrar vulnerabilidades de Buffer OverFlow.
- ✓ En los campos de entrada de las diferentes aplicaciones inyectar comando de SQL, con el fin de tratar de vulnerar las bases de datos.
- ✓ Revisar la información en los banners de la aplicación, instrucciones de uso, mensajes de bienvenida, mensajes de ayuda, mensajes de error.

Algunos de los resultados que se pueden obtener en esta fase son:

Resultados
Listado de aplciaciones
Listado de los compenentes de las aplicaciones
Listado de las vulnerabilidades de las aplicaciones

Figura 9: Pruebas de vulnerabilidades, 07 de Diciembre de 2015, Imagen del autor.

Enrutamiento: Diferentes tipos de protección son implementados a través de los Routers, donde se restringe el tráfico a la red baso en listas de control de acceso, las cuales permiten o deniegan trafico basado en un conjunto de reglas las cuales deben estar expresamente definidas.

Se deben identificar las diferentes características técnicas utilizas por los Routers como:

- ✓ Determinar si el Routers está haciendo funciones de NAT.
- ✓ Probar las listas de control de acceso del Routers contra las políticas de seguridad y contra la regla DENY.
- ✓ Verificar que el Routers está filtrando el tráfico de entrada y de salida a la red.
- ✓ Identificar si el Router tiene algún modo para detectar IP Spoofing.

- ✓ Identificar la capacidad que tiene el Router para manejar paquetes mucho más grandes al estándar.

Algunos de los resultados que se espera encontrar en esta fase son:

Resultados
Tipo de Router y caracteristicas implementadas
Información del Router como servicio y SO
Politicas de seguridad (ACL)
Respuestas del servidor a diferentes tipos de trafico

Figura 10: Enrutamiento, 07 de Diciembre de 2015, Imagen del autor.

Pruebas de control de acceso: En la mayoría de las organizaciones el Firewall es el punto central, en donde se controla el tráfico hacia la red Interna, la DMZ e Internet, su funcionamiento es basado en políticas de seguridad las cuales están compuestas por diferentes listas de control de acceso, en esta prueba se debe asegurar que únicamente lo explícitamente permitido es aceptado por el Firewall y el trafico restante debe ser denegado.

- ✓ Verificar la posibilidad de escanear a través de técnica SYN.
- ✓ Identificar las respuestas dadas por el Firewall cuando se modifican las banderas TCP (SYN, FIN, RESET, NULL).
- ✓ Verificar las políticas de seguridad que están implementadas en el Firewall.
- ✓ Revisión de logs sobre el Firewall para auditar el tráfico a nivel general de red.

Resultados
Información del Firewall caracteristicas implementadas
Perfil de la politica de seguridad
Tipos de paquetes permtidos en la red
Protocolos permitidos por el Firewall
Logs de trafico y de eventos

Figura 11: Pruebas de control de acceso, 07 de Diciembre de 2015, Imagen del autor.

Pruebas de Denegación de servicio: Se trata de una situación o circunstancia intencional o accidental en la cual el sistema recibe una mayor cantidad de tráfico y peticiones para el cual no fue diseñado, en este punto se afecta drásticamente el rendimiento del sistema hasta hacer el servicio inoperable.

Se deben realizar las siguientes actividades:

- ✓ Garantizar que las cuentas administrativas y permisos de acceso a los recursos están concedidos bajo la premisa del menor privilegio.
- ✓ Verificar las restricciones de los sistemas expuestos en Internet.
- ✓ Validar que se cuente con una línea base en la operación de las aplicaciones así es mucho más fácil identificar un comportamiento anómalo en los sistemas.
- ✓ Realizar diferentes pruebas de carga de red y servidores.

Bajo esta metodología se usa el termino Seguridad Perfecta, el cual hace referencia a un conjunto de mejores prácticas, regulaciones de la industria que aplican al negocio de la organización, justificaciones de negocio, políticas de seguridad entre otros, algunas características para cumplir con la seguridad perfecta son:

- ✓ No usar acceso remoto no cifrado.
- ✓ No usar acceso remoto no autenticado.
- ✓ Por defecto restringir todos los accesos e ir permitiendo explícitamente lo necesario.
- ✓ Monitorear todos los componentes de la infraestructura tecnológica y tener registro de logs de eventos de ello.
- ✓ Limitar las diferentes relaciones de confianza entre los sistemas.
- ✓ Instalar únicamente las aplicaciones y servicios requeridos en los diferentes sistemas.
- ✓ No utilizar configuraciones por defecto en los servidores y aplicaciones.
- ✓ Utilizar diferentes capas de seguridad para proteger los sistemas.

III. INFORMES

Los informes generados después de las pruebas realizadas deben incluir soluciones prácticas orientadas a resolver los problemas de seguridad que se han identificado, se deben incluir todos los hallazgos y especificar claramente el estado de seguridad encontrado en la organización.

También deben contener indicadores cualitativos para la medición de riesgos, utilizando alguna metodología para la evaluación y tratamiento de riesgos aceptado por la industria.

IV. CONTROLES

La seguridad debe ser una función de separación, el objetivo es separar un activo de cualquier amenaza exista o no, hay tres maneras lógicas y proactivas para realizar esta actividad.

- ✓ Crear una barrera lógica o física entre el activo y la amenaza.
- ✓ Tratar la amenaza para dejarla en un estado inofensivo.
- ✓ Eliminar la amenaza.

Cuando se analiza el estado de seguridad de un activo, se debe tener en cuenta las interacciones que este activo puede llegar a

tener con una amenaza (visibilidad, acceso y confianza), los controles son el medio por el cual se influye en el impacto de la amenaza y los efectos que puede generar cuando una interacción es requerida.

Los controles activos influyen directamente en las interacciones de visibilidad, acceso, y confianza, existen 5 tipos base de controles interactivos:

Autenticación: Es un control basado en credenciales con las cuales se otorga identificación y autorización.

Indemnización: Es un control mediante un contrato entre el propietario del activo y un ente tercero, en el cual pueden llegar a establecerse temas legales si determinadas reglas no se siguen de acuerdo a las especificaciones (un seguro).

Resistencia: es un control sobre todas las interacciones para mantener la protección de los activos en caso de que ocurra una falla.

Subyugación: Es un control mediante el cual se asegura que las interacciones solo pueden ocurrir de acuerdo a los procesos definidos.

Continuidad: es un control sobre todas las interacciones para mantener la interactividad de los activos en caso de que ocurra una falla.

Los otros controles que se deben aplicar son aquellos con que son usados para crear procesos defensivos, estos controles no influyen directamente en las interacciones ya que estos protegen el activo una vez la amenaza se ha presentado, estos controles son los siguientes:

No repudio: Es un control que provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma.

Confidencialidad: Es un control el cual da la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo.

Privacidad: Es un control el cual garantiza que el proceso es conocido únicamente por los sistemas o partes involucradas.

Integridad: Es un control para asegurar que el intercambio de información entre dos partes no ha sido modificada por alguien no autorizado.

Alarma: Es un control para notificar que una interacción está ocurriendo o ha ocurrido.

V. CONCLUSIONES

Durante el desarrollo de este papper se observaron las diferentes técnicas y herramientas utilizadas para llevar a cabo las labores de Etical Hacking, en las cuales se ve cierta dificultad al momento de llevar acabo las diferentes actividades debido a la gran cantidad de información que se puede manejar, se puede probar diferentes ámbitos de seguridad tales como seguridad física, seguridad inalámbrica, seguridad de comunicaciones, seguridad de la información, seguridad de procesos por nombrar algunos, en este papper nos centramos en la sección denomina seguridad de las tecnologías de Internet.

Para que el Etical Hacking sea realmente efectivo y genere valor agregado a la organización se deben tener muy en cuenta otros factores tales como la valoración de riesgo de los diferentes activos, las políticas de seguridad con las que cuenta la organización, aspectos ambientales, formación de la organización en temas de conciencia de seguridad de la información.

No existe un método único y verdadero para la realización de las diferentes pruebas pero uno se puede basar en guías como OSSTMM la cual ha sido desarrollada y probada por un grupo de expertos en la industria, lo cual significa que es un proceso maduro y ha brindado los mejores resultados.

VI. REFERENCIAS

[1] Institute For Security And Open Methodologies, ISECOM, Online http://www.isecom.org/mirror/OSSTMM.3.pdf, Diciembre 2015.

[2] The Best Guides For Information Security Management, Crypt gen,Online, http://www.crypt.gen.nz/papers/infosec_guides.html#REF1, Diciembre de 2015.

[3] Network Security Tools, SecTools, Online, http://sectools.org/tag/vuln-scanners/, Diciembre 2015.