Curso de Introducción: Hacking / Pentesting

Por PlainText

Metodología del Pentesting (PTES)

PTES – The Penetration Testing Execution Standard (Estándar de Ejecución de Pruebas de Penetración)

Este consiste en 7 sesiones principales que cubren todo lo relacionado a una prueba de penetración, desde la comunicación inicial y la definición del objetivo del pentest hasta la generación del reporte.

Una metodología es importante porque define una estructura con el fin de obtener el mejor resultado de la prueba de penetración.

Fuente: http://www.pentest-standard.org

Metodología del Pentesting (PTES)

- Pre-Compromiso
- Reunión de Inteligencia
- Modelado de amenazas
- Análisis de Vulnerabilidades
- Explotación
- Post Explotación
- Reportes

Fuente: http://www.pentest-standard.org/index.php/Main_Page

Pre-Compromiso

Definir el alcance es sin duda uno de los componentes más importantes una prueba de penetración. Descuidar completar correctamente las actividades previas a la contratación tiene el potencial de desencadenar una serie de dolores de cabeza, incluyendo alcances no completados, clientes insatisfechos, e incluso problemas legales.

El ámbito de un proyecto define específicamente lo que se va a probar.

También es importante definir las reglas de penetración donde se discutirá la forma en que se llevará a cabo cada aspecto de la prueba.

Fuente: http://www.pentest-standard.org/

Reunión de Inteligencia

La recopilación de inteligencia permite realizar reconocimientos contra el objetivo con el fin de obtener tanta información como sea posible para ser utilizada durante las fases de evaluación y explotación de vulnerabilidades.

Cuanta más información puedas recopilar durante esta fase, más vectores de ataque podrás usar en el futuro.

La Inteligencia de Fuentes Abiertas (OSINT) es una forma de administración de recopilación de inteligencia que implica encontrar, seleccionar y adquirir información de fuentes disponibles públicamente y analizarla para producir inteligencia procesable.

Fuente: http://www.pentest-standard.org

Modelado de amenazas

Proporciona claridad en cuanto al apetito de riesgo y la priorización de la organización (¿qué activos son más importantes? ¿qué grupo de amenazas son más relevantes?). Además, permite al evaluador centrarse en ofrecer una interacción que emula estrechamente las herramientas, técnicas, capacidades y perfil general del atacante, teniendo en cuenta cuáles son los objetivos reales dentro de la organización, de modo que los controles, procesos e infraestructura más relevantes se pongan a prueba en lugar de una lista de inventario de elementos de TI.

El modelo de amenaza debe construirse en coordinación con la organización que se está probando siempre que sea posible, el evaluador debe crear un modelo de amenaza basado en la vista del atacante en combinación con OSINT relacionada con la organización de destino.

Fuente: http://www.pentest-standard.org/

Análisis de Vulnerabilidades

Las pruebas de vulnerabilidad son el proceso de descubrir defectos en sistemas y aplicaciones que pueden ser aprovechados por un atacante. Estos defectos pueden variar desde la configuración incorrecta del host y el servicio, o el diseño inseguro de aplicaciones. Aunque el proceso utilizado para buscar vulnerabilidades varía y depende en gran medida del objetivo que se está probando, algunos principios claves se aplican al proceso.

En su elemento más simple, las pruebas pueden ser encontrar todas las vulnerabilidades en un sistema; mientras que en otros casos es posible que necesite encontrar todas las vulnerabilidades en los equipos definidos en un inventario.

Fuente: http://www.pentest-standard.org/

Explotación

La fase de explotación de una prueba de penetración se centra únicamente en establecer el acceso a un sistema o recurso mediante eludiendo las restricciones de seguridad. Si la fase anterior, el análisis de vulnerabilidad se realizó correctamente, esta fase debe estar bien planificada y ser precisa. El enfoque principal es **identificar el punto de entrada principal en la organización** e identificar activos de alto valor.

Si la fase de análisis de vulnerabilidades se completó correctamente, debería haberse obtenido una lista de objetivos de alto valor. En última instancia, el vector de ataque debe tener en cuenta la probabilidad de éxito y el mayor impacto en la organización.

Fuente: http://www.pentest-standard.org/

Post-Explotación

El propósito de la fase post-explotación es determinar el valor de la máquina comprometida y mantener el control de la máquina para su uso posterior. El valor de la máquina está determinado por la sensibilidad de los datos almacenados en ella y la utilidad de las máquinas para comprometer aún más la red.

Los métodos descritos en esta fase están diseñados para ayudar al evaluador a identificar y documentar datos confidenciales, identificar los valores de configuración, los canales de comunicación y las relaciones con otros dispositivos de red que se pueden utilizar para obtener más acceso a la red y configurar uno o varios métodos de acceso a la máquina en un momento posterior.

Fuente: http://www.pentest-standard.org/

Reportes

Este documento está destinado a definir los criterios básicos para la notificación de pruebas de penetración. Aunque se recomienda encarecidamente utilizar su propio formato personalizado y de marca, lo siguiente debe proporcionar una comprensión de alto nivel de los elementos requeridos dentro de un informe, así como una estructura para que el informe proporcione valor al lector.

Dividido en:

- Resumen Ejecutivo
- Informe Técnico

Fuente: http://www.pentest-standard.org/

Otras metodologías de Pentesting

- **OSSTMM (Open Source Security Testing Methodology Manual)**
- **OWASP (Open Web Application Security Project)**
- **NIST (National Institute of Standards and Technology)**
- **ISSAF (Information System Security Assessment Framework)**

Fuente: https://www.blog.binaria.uno/2020/04/24/las-5-mejores-metodologias-y-estandares-de-pruebas-de-penetracion/