Metodología PTES (Penetration Testing Execution Standard)

Metodología PTES (Penetration Testing Execution Standard)

- La metodología se divide en 7 aspectos los cuales se basan en técnicas a como se estructura una prueba de penetración.
- Fase de Pre-acuerdo
- Fase recolección de información
- Análisis de vulnerabilidades
- Modelado de amenaza
- Fase de explotación
- Fase de Post-explotación
- Fase de reportes

Fase de contacto Preacuerdo

- En esta fase es donde se tiene el contacto entre el analista de seguridad o el auditor y el cliente, se hace el acuerdo entre el alcance del test, los formularios que se auditarán, los sistemas, los dominios si es una empresa grande, los costos por la auditoría.

- Se definen las fechas estimadas en entrega del reporte final, regularmente los primeros formularios son los que se cobran mucho más caros, ya que no conocemos la estructura de su código

Tipos de test de penetración

- **Test de caja negra (Black Box)**
- Las pruebas de caja negra implican la realización de una evaluación de la seguridad y pruebas sin
- conocimiento previo de la infraestructura o de la infraestructura de red a probar. La prueba simula
- un ataque de un hacker malicioso fuera del perímetro de seguridad de la organización.

Tipos de test de penetración

- **Test de caja gris (Gray Box)**

- Las pruebas de caja gris implican la evaluación de la seguridad y pruebas internas.
- Las pruebas examinan el grado de acceso a información privilegiada dentro de la red.
- El propósito de esta prueba es para simular las formas más comunes de ataque, los que se inician desde dentro de la red.

Tipos de test de penetración

- **Test de caja blanca (White Box)**

- Las pruebas de caja blanca implican la evaluación de la seguridad y las pruebas son con conocimiento completo de la infraestructura de red, en este caso se conoce como auditorías internas.

Fase de recolección de información.

En la Fase de recolección de información tenemos muchos métodos sobre cómo hacerlo.

La recolección de información es importante porque a través de esto nos dará ideas sobre el objetivo sobre el cual estamos trabajando. Los métodos más comunes son:

- Google Hacking
- Osint
- Doxing

Lo que se pretende es sacar la mayor cantidad de información para proceder a hacer un perfil, como, por ejemplo, la identificación del sistema, registro de dominio, tipo puertos abiertos, el sistema web si corresponde a un cms.

- La información se obtiene con herramientas automatizadas, basándose incluso en listados de incidentes previos, forados de seguridad que se consiguen del lenguaje de programación de la página como Drupal, Joomla o WordPress.
- O en el caso de base de datos, problemas de configuración SQL Injection, Cross-site scripting incluso Dorks como colocar las palabras (index of .gob.es) en un browser que permite conocer arquitectura y problemas de configuración de información pública, verificación de errores de código con W3C y otros servicios que permiten a cualquier administrador mejorar la seguridad de sus entidades.

- https://www.exploit-db.com/google-hacking-database

La información a recopilar será:

- Nombre de personas que trabajan en la empresa, sus puestos, responsabilidades, teléfonos emails corporativos, redes sociales que usan, por ejemplo, es común encontrar en redes profesionales como LinkedIn este tipo de información, además muchas veces los trabajadores aclaran en sus perfiles tecnologías concretas con las que trabajan que nos pueden dar una idea de la infraestructura de la empresa objetivo.
- Ubicaciones físicas de las instalaciones.
- Análisis de direcciones IP y rangos.
- Análisis de sistemas autónomos (ASNs).
- Dominios, subdominios y relaciones.
-

- Se usan técnicas como Browser Hacking, es decir usar los operadores adecuados para realizar búsquedas muy finas en buscadores como Google, lo que se conoce como Google hacking, y en concreto, las búsquedas son los Dorks de Google que podemos encontrar en bases de datos como Exploit-db.

Enlace a la web: https://www.exploit-db.com/google-hacking-database

- Podemos usar herramientas como Shodan, un buscador muy especial que tiene cacheados todos los sistemas públicos en internet y servicios que corren en los mismos

https://www.shodan.io

Maltego, capaz de extraer mucha información de internet a través de sus transformadas

Fase de Análisis de vulnerabilidades.

Como el nombre lo indica es donde ya comenzamos a interactuar de forma activa con el objetivo y la finalidad es:

Analizar el sistema de forma manual o automática para identificar posibles vulnerabilidades

En este apartado básicamente se define el ámbito y alcance del test de intrusión. Se llega a un acuerdo con el cliente acotando la profundidad de las pruebas a realizar, permisividad de ataques (ataques DOS, fuerza bruta…), enfoque del test (caja negra, gris o blanca) presentación de evidencias (goals), etc.

Análisis pasivo de sistemas vivos, o lo que es lo mismo, que están activos, en el que no tenemos interacción directa con los equipos objetivo, ya que estaremos usando herramientas online para la obtención de información, eso sí, como ya te expliqué anteriormente es conveniente que hagas uso del anonimato, ya que estas webs pueden guardar registros (logs) de tus visitas y búsquedas, así mismo Google acaba mosqueándose y vas a tener que estar todo el rato buscando aviones, autobuses y motos en los captchas.

Análisis pasivo de servicios habilitados, también con herramientas online.

Escaneo de red mediante ARP, para identificar equipos vivos dentro de la red, aquí ya estamos haciendo un análisis activo.

Escaneos de red, con el objetivo de conocer los puertos que están abiertos en un equipo, los servicios que corren detrás de esos puertos, sus versiones, con lo que podemos saber si son o no vulnerables o si hay puertos inseguros que pudieran ser un vector de ataque. Aquí principalmente haremos uso de NMAP, aunque existen otras muchas herramientas, que no sólo de NMAP vive el hombre. En este caso también estamos haciendo análisis o reconocimiento activo.

Enumeración mediante DNS, identificando dominios y subdominios, realizando transferencias de zona AXFR si es posible, etc.

Fase de modelado de amenaza.

Para esta fase es muy importante ver que ya hemos extraído la información necesaria, porque con base a toda la información recaudada vamos a gestionar nuestro perfil de ataque, y veremos sobre la creación de nuestros diccionarios para ataques de fuerza bruta.

Un **modelo de amenazas** es en esencia una representación estructurada de toda la información que afecta a la seguridad de una aplicación. En sí, es una vista de la aplicación y su entorno a través de los "anteojos" de la seguridad.

El modelado de amenazas es un proceso para capturar, organizar y analizar toda esta información. Permite tomar decisiones informadas sobre los riesgos de seguridad en las aplicaciones. Además de producir un modelo, los esfuerzos para un modelado de amenazas típico también producen una lista priorizada de mejoras de seguridad en los requisitos, diseño e implementación de las aplicaciones.

Fase de Explotación

Una vez ya realizado nuestro modelado de amenaza que es el que nos ayuda a ver de qué manera atacaremos al sistema, porque puerto acceder, o que vulnerabilidad activa vamos a explotar todo esto con la finalidad de acceder al sistema objetivo. Por ejemplo, si un sistema tiene el servidor con el puerto 21 activo y tienen las credenciales por defecto es por donde nosotros vamos a acceder y si no tienen credenciales por defecto haremos uso de la fuerza bruta por diccionario que ya previamente se deben haber hecho con la información obtenida.

Fase de post-explotación.

Esta fase solo tiene que ver si la intrusión al sistema es decir la explotación se ha llevado con éxito, esta fase se lleva a cabo siempre después de ganar el acceso y consta de la recolección de información privilegiada como por ejemplo archivos alojados en un servidor o sistema, consta de implantar un backdoor, troyano o keylogger (Claro eso si no fuera un test ético) la finalidad es demostrar al cliente que si alguien con malas intenciones hiciera un test podría acceder al sistema y robar la información de igual forma y sobre todo plantar un backdoor o dejar ese servidor como botnet.

Fase de limpieza

realizaremos acciones que nos permitan no dejar rastro como:

Borrar caché y cookies.

Ocultar ficheros: ADS Streams.

Modificar algunos valores del registro.

Volver a habilitar auditorías que hayamos deshabilitado previamente.

- Auditpol.exe /disable
- Auditpol.exe /enable

Borrar alertas que se hayan generado en el visor de sucesos (Event Viewer).

- Hay que tener en cuenta que se borran todos los sucesos, pero queda un registro de log referente a la acción del borrado.
- Herramientas como Elsave o Winpazer permiten el borrado del registro de sucesos de forma remota, obviamente teniendo los privilegios adecuados.

Fase de limpieza

Borrar correos enviados, si por ejemplo hemos usado técnicas de Phishing.

Borrar la papelera de reciclaje, caché del navegador, historiales, temporales, etc.

- Se pueden usar herramientas como Evidence Eliminator.

Ocultar ficheros con el uso de los atributos de ficheros o mediante esteganografía.

Borrar logs que nos comprometan.

Cerrar los puertos abiertos.

Desinstalación de aplicaciones usadas para lograr nuestros objetivos.

Borrar usuarios creados en el sistema.

Generación de reportes.

Existen dos tipos de reportes que se deben de generar

Reporte técnico (Para los administradores del sistema)

Esta clase de reportes las generamos y escribimos las terminologías apropiadas y de ser posible se anexan las posibles soluciones que deberían llevar a implementación, de tal manera que sea lo mejor detallado posible.

Reporte ejecutivo (Para la mesa directiva)

Este reporte se diferencia del otro tipo en que este reporte se debe escribir las palabras apropiadas para que personas ajenas al mundo de la informática pueda entender.

Tendremos que hacer unas recomendaciones de las medidas correctoras que se pueden aplicar para cada no conformidad. Por ejemplo, si hemos detectado una vulnerabilidad CVE-XXXX-XXXX podemos consultar la web de cve-mitre, donde encontraremos una descripción de la misma y enlaces a documentos que permiten solventar esa vulnerabilidad, o en la propia web de los fabricantes, por ejemplo, en la web de Microsoft, Cisco, etc.

https://cve.mitre.org/cve/search_cve_list.html