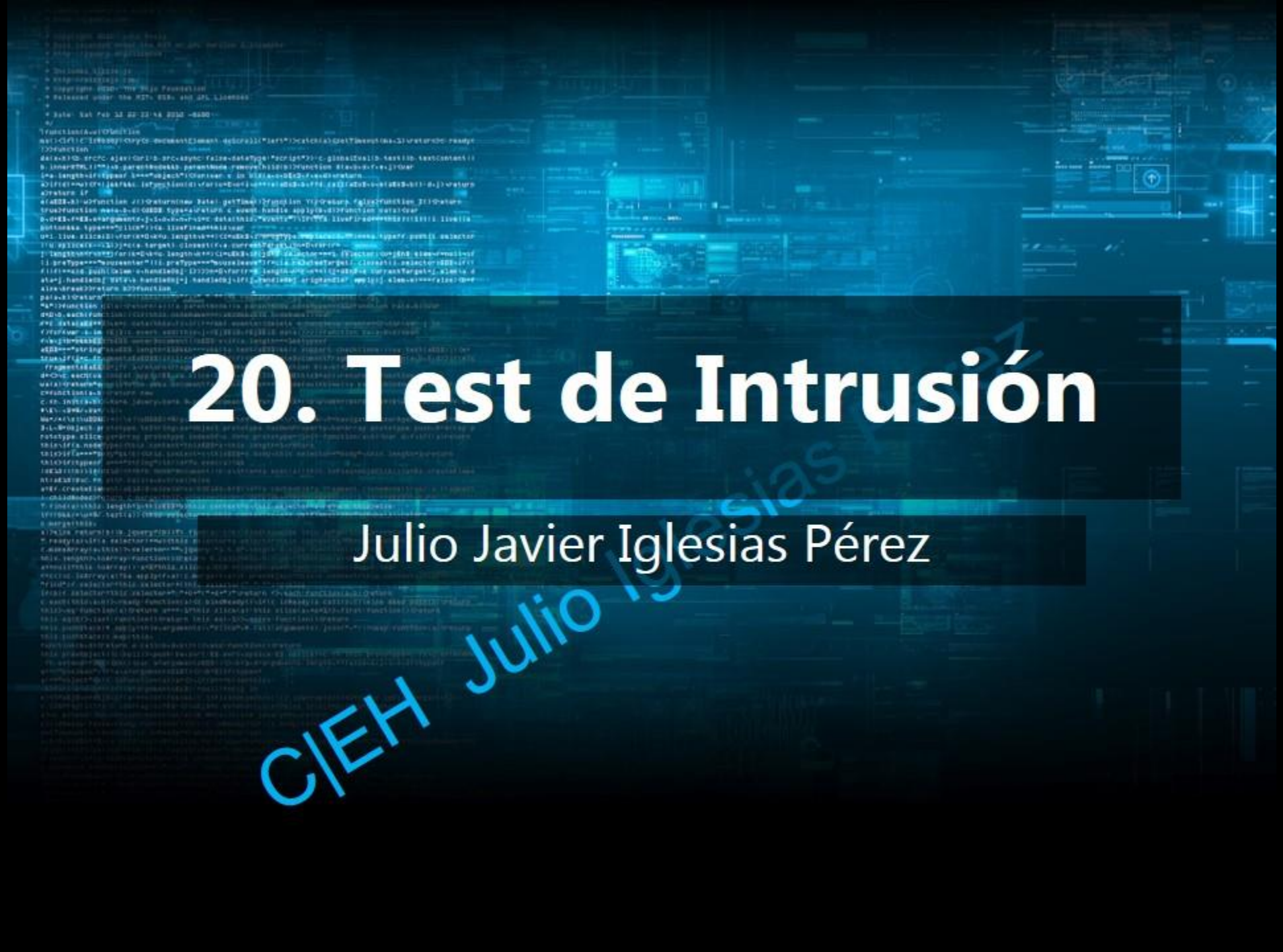
20. Test de Intrusión
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

Conceptos

Introducción a Test de Intrusión.

Un Test de intrusión simula métodos que los intrusos utilizan para obtener acceso no autorizado a los sistemas en red de una organización y luego los compromete.

En el contexto de PenTest, el tester es limitado por recursos, es decir el tiempo, recursos especializados y acceso al equipamiento; como se indica en el acuerdo de penetración.

La mayoría de ataques siguen un acercamiento común a penetrar un sistema.


hacker
Julio Iglesias Pérez
C|EH

Evaluaciones de Seguridad

Cada organización utiliza distintos tipos de evaluaciones de seguridad para validar el nivel de seguridad de los recursos de su red.

Categorías de evaluaciones de Seguridad:

- Auditorías de seguridad.
- Evaluaciones de vulnerabilidades.
- Test de Intrusión.

Cada una de las evaluaciones requiere personas con distintas habilidades.

Evaluaciones de Seguridad

1. Escaneo de Red: Escanea la red en búsqueda de todas las debilidades de seguridad.

2. Herramientas de escaneo: Las herramientas buscan segmentos para dispositivos IP habilitados y enumerar los sistemas, S.O., y aplicaciones.

Evaluaciones de Seguridad

3. Errores de seguridad: Adicionalmente, los escaners de vulnerabilidad pueden identificar errores de configuración de seguridad comunes.

4. Prueba de Sistemas y Red: Los Escáneres de vulnerabilidad pueden probar los sistemas y dispositivos de red y determinar su exposición a ataques comunes.

Limitaciones de las evaluaciones de vulnerabilidad

1. El software es limitado a su habilidad para detectar vulnerabilidades en un punto dado en el tiempo.
2. Debe ser actualizado cuando hay nuevas vulnerabilidades.
3. Esto puede influenciar la evaluación.
4. La metodología utilizada como la diversidad de paquetes de detección de vulnerabilidades, evalúa la seguridad de manera diferente.

Test de Intrusión

Un test de intrusión que no es completamente realizado de manera profesional, puede resultar en pérdida de servicios y ruptura de la continuidad del negocio. Evalúa el modelo de seguridad de la organización como un todo. Revela las consecuencias potenciales de si un atacante real ataca la red. Un Penetration Tester es diferenciado de un atacante solo por su intención y su falta de malicia.

¿Por qué Test de Intrusión?

- Identificar amenazas en los bienes de la organización.
- Reduce costos de seguridad IT y provee una mejor ROSI (Return On IT Security Investment).
- Provee una organización con garantía y una evaluación comprensiva de la seguridad organizativa cubriendo políticas, procedimientos, diseño e implementación.
- Gana y mantiene una regulación de la industria (BS7799, HIPAA, etc.).

¿Por qué Test de Intrusión?

- Adopta las mejores prácticas en conformidad con la ley y regulaciones de la industria.
- Valida la eficiencia de la protección y controles de seguridad.
- Enfatiza en problemas de seguridad a nivel de aplicación.
- Provee un acercamiento comprensivo de pasos de preparación que pueden ser tomados para prevenir explotaciones venideras.

¿Por qué Test de Intrusión?

- Evalúa la eficiencia de los dispositivos de seguridad de la red como firewall, routers, servidores web.
- Para cambiar o actualizar una infraestructura o software, hardware o diseño de red existentes.

¿Qué debe ser testeado?

Una organización debe conducir una operación de evaluación de riesgos antes del test de intrusión que ayudarán a identificar los temas principales como:

- Falla en las comunicaciones, comercio electrónico y pérdida de información confidencial.
- Sistemas de frente público, sitios web, gateways de correo, plataformas de acceso remoto.
- Correo, DNS, firewall, contraseñas, FTP, IIS, servidores Web.

¿Qué es lo que hace bueno a un Test de Intrusión?

- Establecer los parámetros para el test, como objetivos, limitaciones y procedimientos de justificación.
- Contratar profesionales con experiencia y habilidades para realizar el test.
- Elegir un conjunto adecuado de pruebas para que haya un balance de costo-beneficio.

¿Qué es lo que hace bueno a un Test de Intrusión?

- Seguir una metodología con una planeación y documentación apropiada.
- Documentar los resultados cuidadosamente y hacerlo comprensible para el cliente.
- Declarar los riesgos potenciales y resultados de manera clara en el reporte final.

Retorno de Inversión (ROI) de un PenTest

- Las compañías invertirán el PenTest solo si tienen un conocimiento apropiado de sus beneficios.
- Gastos y ganancias.
- Ayudan a identificar, entender y direccionar las vulnerabilidades, lo cual les ahora mucho dinero, resultando en un ROI.
- Proceso crítico para el éxito.

Puntos de prueba

- Las organizaciones tienen que llegar a un consenso en el grado de qué información puede ser divulgada al equipo de test, para determinar el punto de partida del Test de Intrusión.
- Proveer al equipo de penetración con información adicional les puede dar una ventaja no realista.
- Similarmente, se necesita determinar el grado de qué vulnerabilidades necesitan ser explotadas sin cortar servicios críticos.

Ubicaciones del Test

1. El equipo de penetración debe elegir si realizar el test remotamente o en sitio.
2. Una evaluación remota simulará un ataque de un hacker externo. Sin embargo, esto perderá la evaluación interna.
3. Una evaluación en sitio puede ser cara y tal vez no pueda simular un ataque externo exacto.

Tipos de PenTesting

1. Externo: Implica análisis de la información pública disponible, una fase de enumeración de la red, y el comportamiento de los dispositivos de seguridad analizados.

Tipos de PenTesting

2. Interno: Será realizado desde un número de puntos de acceso de la red, representando cada segmento lógico y físico.
   - Black-hat testing/zero-knowledge testing.
   - Gray-hat testing/partial-knowledge testing.
   - White-hat testing/complete-knowledge testing.
   - Announced testing.
   - Unannounced testing.

Test de Intrusión Externo

Implica un análisis comprensivo de la información públicamente disponible acerca del objetivo como ser: Servidores Web, de correo, Firewalls, Routers.

1. Este es un acercamiento tradicional a un Pen Test.
2. El test está enfocado a los servidores, infraestructura y software que comprende el objetivo.
3. Puede ser realizado sin conocimiento del sitio (black box).
4. Revelación total de la topología y ambiente (crystal/white box).

Evaluación de Seguridad Interna

- El test será realizado desde un número de AP de red, representando cada segmento lógico y físico.
- Por ejemplo, esto puede incluir niveles y DMZs dentro del ambiente, la red corporativa o conexiones de compañías socias.
- Una evaluación de red interna sigue una metodología similar al test externo, pero provee una visión más completa de la seguridad del sitio.

Test de Intrusión Black-box

- Sin conocimiento previo de la infraestructura que será sometida a pruebas. Solo se dará el nombre de la compañía.
- El que hará el test deberá recopilar y buscar de manera extensiva la información. Este simula el proceso de un hacker real.
- Toma considerablemente mucha cantidad de tiempo. Consumo de tiempo y tipo de test caro.

Test de Intrusión Gray-box

- El que hace el test usualmente tiene conocimiento limitado de la información.
- Realiza una evaluación y pruebas de seguridad internas.
- Enfoques para las pruebas de vulnerabilidad de la seguridad de las aplicaciones, las que pueden encontrar y explotar los hackers.
- Generalmente realizada cuando un tester inicia un test black box en sistemas bien protegidos y encuentra que necesita tener un poco mas de conocimiento para realizar una revisión exhaustiva.

Test de intrusión White-box

- Completo conocimiento de la infraestructura en donde se realizará el test.
- Esto simula el proceso de los empleados de la compañía.
- La información es provista como: infraestructura de la compañía, tipo de red, implementaciones de seguridad actuales, direcciones IP / Firewall / Detalles IDS, políticas hacer y no hacer de la empresa.

Test Anunciado/No anunciado

Test anunciado: Comprometer el sistema en el cliente con toda la cooperación y conocimiento del staff IT.

- Examinar la seguridad existente en la infraestructura en búsqueda de posibles vulnerabilidades.
- Implica la cooperación del staff IT en los equipos de intrusión para realizar auditorías.

Test Anunciado/No anunciado

Test No Anunciado.

- Es un intento de comprometer los sistemas en las redes de los clientes sin previo conocimiento por parte del personal de seguridad IT.
- Solo la alta administración tiene el conocimiento de estos tests.
- Examina la seguridad de infraestructura y sensibilidad del staff IT.

Test Anunciado/No anunciado

Test automatizado

- - Como con los escáneres de vulnerabilidad, puede haber falsos negativos, o peor, falsos positivos.
- Estos tests ahorran tiempo y gastos sobre los de término prolongado, sin embargo, no puede remplazar a un profesional con experiencia en la seguridad.

Test Anunciado/No anunciado

- Con el test automatizado, no existe un ámbito para ningún elemento de la arquitectura que será testeado.
- Las herramientas tienen una curva de aprendizaje muy grande

Test Anunciado/No anunciado

Test manual

- Es la mejor opción, la organización puede optar por la experiencia del profesional de seguridad.
- El objetivo del profesional es evaluar la postura de seguridad de una organización desde la perspectiva de un atacante.
- Un acercamiento manual requiere planeamiento, diseño del test, programación y documentación diligente (aprovechada) para capturar los resultados del proceso del testing.

Técnicas PenTesting

Técnicas comunes

- Investigación pasiva: Utilizada para obtener toda la información acerca de las configuraciones del sistema de la organización.
- Monitoreo Open Source: Facilita a la organización a tomar los pasos necesarios para asegurarse su confidencialidad e integridad.

Técnicas PenTesting

- Manejo de red y fingerprinting de S.O.: Utilizado para tener una idea de la configuración de la red a ser testeada.
- Spoofing: Es el acto de utilizar un equipo para pretender ser otro. Es utilizado tanto para los tests internos como externos.
- Sniffing de Red: Utilizado para capturar los datos y su viaje a través de la red.

Técnicas PenTesting

- Ataques troyanos: Códigos o programas maliciosos que usualmente son enviados a la red como archivos adjuntos de correo o transferidos mediante mensajería.
- Ataque de fuerza bruta: Es el método de cracking más común. Puede sobrecargar un sistema y posiblemente detener sus solicitudes legales.

Técnicas PenTesting

- Escaneo de vulnerabilidades: Es un examen comprensivo de las áreas del objetivo de una infraestructura de la red de la organización.
- Análisis de escenario: Es la fase final, haciendo evaluación de seguridad de las vulnerabilidades mucho más precisa.

Técnicas PenTesting

Utilizando información de nombre de dominio DNS y dirección IP.

1. La información DNS obtenida sobre la red objetivo puede ser utilizada para mapear la red de la organización.
2. El bloque IP de una organización puede ser discernido para buscar el nombre de dominio e información personal sobre el contacto.
3. El registro DNS también provee información de valor relacionada al S.O. o aplicaciones que están siendo ejecutadas en el servidor.

Técnicas PenTesting

- Enumerando información sobre Hosts en las redes Públicamente disponibles
  - Los rastreadores de sitios web pueden replicar los sitios completos
  - Adicionalmente, el esfuerzo puede proveer subredes filtradas y una lista comprensiva de los tipos de tráfico que están permitidos dentro y fuera de la red.

Técnicas PenTesting

- La enumeración puede ser realizada por herramientas de escaneo de puertos, protocolos IP, y la escucha de puertos TCP/UDP.
- El equipo de testeo puede visualizar un diagrama detallado de la red que puede ser accedido públicamente.

Fases del Test de Intrusión

- Fase previa al ataque.
- Fase de ataque.
- Fase post ataque.

Fase previa al ataque

- Aborda el modo del ataque.
- Localizar, obtener información, identificar y registrar la información.
- Formular un plan de ataque.
- Dos tipos de reconocimiento
  - Pasivo: Recolectar información del objetivo desde los recursos accesibles públicamente.
  - Activo: Obtener información a través de redes sociales, visitas en sitio, entrevistas y cuestionarios.

Fase previa al ataque

Información recibida en esta fase:

- Inteligencia competitiva.
- Información de registro de red.
- Información DNS y servidor de correo.
- Información de los S.O.
- Información de usuario.
- Conexiones análogas.

Fase previa al ataque

- Información de contacto.
- Ubicación física y lógica de la organización.
- Qué rango de productos y ofertas de servicios de la compañía están disponibles online.
- Cualquier otra información que sea potencial de explotación.

Fase de ataque

- Penetrar el perímetro.
- Adquirir el blanco.
- Ejecutar, implantar, extraer.
- Escalar privilegios.

Fase de ataque

Actividad: Testeo del perímetro

- Evaluar reportes de error y administración de error con sondeo ICMP.
- Revisar las listas de control de acceso.
- Medir el umbral para DoS intentando conexiones TCP persistentes, evaluando las conexiones TCP transitorias, e intentando escuchar las conexiones UDP.

Fase de ataque

- Evaluar las reglas de filtrado de protocolo intentando conexiones utilizando varios protocolos como SSH, FTP y Telnet.
- Evaluar la capacidad del IDS saltando contenido malicioso (como URLs malformados) y escaneando el objetivo varias veces.
- Examinar la respuesta del sistema de seguridad del perímetro al servidor Web utilizando múltiples métodos como POST, DELETE y COPY.

Fase de ataque

Enumerando dispositivos.

- Un inventario de dispositivos es una colección de dispositivos de red juntos con información relevante acerca de cada uno, almacenada en un dispositivo.
- Luego de que la red haya sido mapeada y los bienes del negocio identificados, el próximo paso lógico es realizar un inventariado de los dispositivos.
- Una revisión física puede ser conducida adicionalmente para asegurar que los dispositivos enumerados han sido localizados.

Fase de ataque

- Actividad: Acquiring Target
  - Se refiere al conjunto de actividades llevadas a cabo donde el tester somete al equipo sospechoso a retos más intrusivos como escaneos de vulnerabilidad y a evaluaciones.
  - Los métodos incluyen:
    - Ataques activos de sondeo.
    - Escaneo de vulnerabilidades en ejecución.
    - Evaluación de procesos y sistemas confiados.

Fase de ataque

Actividad: Escalada de Privilegios

- Una vez que el objetivo ha sido conseguido, el tester intenta explotar el sistema y obtener acceso a los recursos protegidos.
- Las actividades incluidas son:
  - El tester puede tomar ventaja de las pobres políticas de seguridad y tomar ventaja del correo electrónico y código web sin protección, para obtener información sobre la escalada de privilegios.

Fase de ataque

- Utilizar técnicas como fuerza bruta para lograr estado de privilegio, ejemplos, obtener el administrador y crackes de password.
- Utilizar analizadores de protocolos y troyanos.
- El uso de la información obtenida a través de técnicas como ingeniería social para obtener acceso no autorizado a los a recursos privilegiados.

Fase de ataque

Actividad: Ejecutar, implantar y retraer.

- Comprometer un sistema: En esta fase, el tester compromete efectivamente el sistema adquirido ejecutando código arbitrario.
- Penetrar el sistema: El objetivo es explorar el grado de fallas de seguridad.
- Ejecutar Exploits: Tomar ventana de las vulnerabilidades identificadas en el sistema.

Fase de ataque

Fase posterior al ataque: Fase y actividades

Esta fase es crítica para cualquier test de intrusión y la responsabilidad del tester es restaurar los sistemas a sus estados previos.

Lo mismo a la organización.

Incluye:

Fase de ataque

- Remover todos los archivos subidos al sistema.
- Limpiar todas las entradas del registro y remover todas las vulnerabilidades creadas.
- Remover todas las herramientas y exploits desde los sistemas testeados.
- Restaurar la red al estado previo removiendo los recursos compartidos y conexiones.
- Analizar todos los resultados y presentar.

Fase de ataque

Plantillas entregables del Test de Intrusión

- Un reporte de Pentest llevará detalles de los incidentes que hayan ocurrido durante el proceso de testeo y el rango de actividades llevadas a cabo por el equipo de intrusión.
- Extensas áreas cubiertas incluyendo objetivos, observaciones, actividades llevadas a cabo, e incidentes reportados.
- El equipo también recomendará acciones correctivas pasadas en las reglas del compromiso.

PenTesting Roadmap

Metodología de Test de Intrusión

1. Information Gathering.
2. Análisis de vulnerabilidad.
3. Test de Intrusión externo.
4. Test de Intrusión de red Interna.
5. Test de Intrusión de Router y Switches.
6. Test de Intrusión de Firewall.
7. Test de Intrusión de IDS.

PenTesting Roadmap

8. Test de Intrusión de Test de Intrusión de Redes Wireless.
9. Test de Intrusión de DoS.
10. Test de Intrusión de crackeo de contraseñas.
11. Test de Intrusión de Ingeniería Social.
12. Test de Intrusión de Laptops, PDAs y celulares robados.

13. Test de Intrusión de de Aplicación.
14. Test de Intrusión de la seguridad física.
15. Test de Intrusión de base de datos.
16. Test de Intrusión de VoIP.
17. Test de Intrusión de VPN
18. War dialing.
19. Detección de virus y troyanos.
20. Test de Intrusión de administración de Logs.

PenTesting Roadmap

21. Revisión de la integridad de los archivos.
22. Test de Intrusión de dispositivos Bluetooth y dispositivos de mano.
23. Test de Intrusión de sistemas de comunicación.
24. Test de Intrusión de seguridad de correo electrónico.
25. Test de Intrusión de parches de seguridad.
26. Test de Intrusión de fuga de información.

PenTesting Roadmap

Evaluación de la seguridad de Aplicación

- Incluso en infraestructuras con la seguridad bien implementada, una aplicación débil puede exponer las "joyas de la corona" de la organización a un riesgo inaceptable.
- Esta evaluación está diseñada para identificar y evaluar las amenazas de una organización a través de la medida de la organización, propiedad de aplicaciones o sistemas.

PenTesting Roadmap

- Este test revisa la aplicación para que los usuarios maliciosos no puedan acceder, modificar y destruir datos o servicios en el sistema.

PenTesting Roadmap

Test de Aplicación Web I

- Validación de entrada: El test incluye inyección de comandos de S.O., inyección de script, SQL Inyección, Inyección LDAP y cross-site scripting.
- Saneamiento de salida: El test incluye el análisis de caracteres especiales y verificación de errores en la aplicación.

PenTesting Roadmap

- Control de acceso: Revisión del acceso a las interfaces administrativas, envía datos para manipular los campos de formulario, intenta realizar cadenas de consultas URL, cambia valores en el script del lado del usuario, y cookies de ataque.

PenTesting Roadmap

Test de Aplicación Web II

- El test incluye ataques contra stack overflows, heap overflows y overflows de formato de cadenas.
- Revisa los controles de seguridad en los componentes de los servidores y aplicaciones web que pueden exponer la aplicación web a vulnerabilidades.

PenTesting Roadmap

- Revisa DoS inducidos por entradas de usuario malformadas, bloqueo de usuario, bloqueo de aplicación debido a la sobrecarga del tráfico, solicitudes de transacción o solicitudes excesivas en la aplicación.
- Revisa por lapsos relacionados con la seguridad de datos como almacenamiento de datos sensibles en la caché o rendimiento de datos sensibles utilizando HTML.

PenTesting Roadmap

- Test de Aplicación Web III
- Revisión de confidencialidad: Para aplicaciones utilizando protocolos seguros y encriptación, revisión de los lapsos en el mecanismo de intercambio de claves, longitud de clave adecuada y algoritmos débiles.

PenTesting Roadmap

- Administración de sesión: Revisa la validación de los tokens de sesión, longitud de los tokens, explicación de los tokens de sesión mientras transitan desde recursos SSL a no-SSL, presencia de cualquier token de sesión en el historial o caché de navegación, aleatoriedad de un ID de sesión (revisa el uso de datos de usuario en la generación de ID). (cont.)

PenTesting Roadmap

- Verificación de configuración: Intenta manipular recursos utilizando métodos HTTP como DELETE y PUT, revisa la disponibilidad de la versión de contenido y cualquier código de recurso restringido en dominios públicos, intenta listar archivos y directorios, y revisa por vulnerabilidades conocidas e interfaces de accesibilidad administrativa en servidores y sus componentes.

PenTesting Roadmap

Evaluación de la Seguridad de la Red

- Escanea el ambiente de la red identificando vulnerabilidades y ayuda a mejorar las directivas de seguridad de la organización.
- Descubrir las fallas de seguridad de la red que pueden llevar a los datos o equipamiento ser explotados o destruidos por troyanos, ataques DoS y otras instrucciones.

PenTesting Roadmap

- Se asegura que la implementación de seguridad actual provee la protección que la empresa requiere cuando cualquier ataque tome lugar en la red, generalmente "explotando" una vulnerabilidad del sistema.
- Es realizado por un equipo intentando entrar dentro de la red o sus servidores.

PenTesting Roadmap

Evaluación de Acceso remoto/wireless

- Direcciona los riesgos de seguridad asociados con una fuerza de trabajo cada vez más móviles.
- Incluye:
  - Bluetooth
  - Señales GHz
  - Transmisiones de radio wireless
  - Canales de comunicación de radio
  - 801.11 a,b y g

PenTesting Roadmap

Wireless Testing

Los métodos para las pruebas wireless incluyen, pero no están limitados a:

- Revisión del SSID (Service Set Identifier) por defecto de A.P. Revisión de la difusión SSID y accesibilidad a la red LAN por éste. El test puede incluir ataque de fuerza bruta a la cadena de caracteres del SSID utilizando herramientas como Kismet.

PenTesting Roadmap

- Revisión de vulnerabilidades de acceso por la WLAN a través del router wifi, AP, o gateway. Esto puede incluir la verificación si la clave de encriptación WEP puede ser capturada y descifrada.
- Auditar el faro de difusión de cualquier AP y revisar todos los protocolos disponibles en los AP. Revisar si las redes switcheadas de la capa dos están siendo utilizadas en vez de hubs para conectividad. (cont.)

PenTesting Roadmap

- Autenticación sujetos a la producción de autenticaciones previas para revisar el acceso no autorizado y escalada de privilegios.
- Verificar que el acceso es concedido solo a los equipos cliente con direcciones MAC registradas.

PenTesting Roadmap

Evaluación de seguridad de teléfono

- Direcciona las preocupaciones de seguridad relacionadas con las tecnologías de voz de la organización.
- Incluye el abuso de las PBXs por personas ajenas para enrrutar las llamadas a expensas del objetivo, implementación de buzones y seguridad, integración de VoIP, uso no autorizado del modem y riesgos asociados.

PenTesting Roadmap

Ingeniería Social

- Direcciona al tipo de intrusión no técnica.
- Usualmente implica una estafa; intentando obtener confianza de una fuente confiando en las ganas de ayudar natural que tienen las personas como también sus debilidades, apelando su vanidad, su autoridad y el espionaje son técnicas naturalmente utilizadas.

PenTesting Roadmap

Testeando dispositivos de red y filtrado.

- Se pueden realizar pruebas de instalación por defecto de firewall para asegurar los IDs de usuario y passwords por defecto han sido deshabilitados o cambiados.
- Los servidores proxy pueden estar sujetos a test de estrés para evaluar su habilidad de filtrar paquetes no deseados.

PenTesting Roadmap

- El objetivo del equipo de intrusión es comprobar que todo el tráfico legítimo fluye a través del dispositivo de filtrado.
- Los testers también puede revisar cualquier capacidad de login remoto que haya sido habilitado.

PenTesting Roadmap

Emulación de DoS

- Estos tests revisan la efectividad de los dispositivos anti DoS.
- Algunos sitios online simulan ataques DoS para una carga nominal.
- La emulación de ataques DoS pueden utiliza intensamente los recursos.
- Los ataques DoS pueden ser eliminados utilizando hardware.

Outsourcing PenTesting Services

Test de Intrusión de los servicios externalizados

- Controladores para pentest de los servicios externalizados: Para se auditados por una agencia, para adquirir un punto de vista del intruso. La organización puede requerir una evaluación de seguridad específica y sugerencias de contramedidas correctivas.
- Test de intrusión de suscripción: Se debe pagar un seguro de responsabilidad profesional si hay resultado en las acciones o si los hay. También conocido como seguro de E&O o seguro de indemnización profesional.

Outsourcing PenTesting Services

- Términos de compromiso
- La organización sanciona al test de intrusión contra cualquiera de sus sistemas de producción acortadas explícitamente en las reglas de compromiso establecidas.
- Debe establecer los términos de preferencia bajo los cuales la agencia interactúa con la organización.
- Puede especificar el código de conducta deseado, los procedimientos a ser seguidos y la naturaleza de la interacción entre los testers y la organización.

Outsourcing PenTesting Services

Ámbito del proyecto

- Determinar el ámbito del test de intrusión es esencial para decidir si el test es una prueba específica o una prueba comprensiva.
- Las evaluaciones comprensivas son esfuerzos coordinados por la agencia de test de intrusión para descubrir cuantas más vulnerabilidades como sean posibles en la organización.
- Una prueba específica buscará identificar las vulnerabilidades en sistemas y prácticas específicas

Outsourcing PenTesting Services

Acuerdos de nivel de servicio del Test de Intrusión

- Es un contrato que detalla los términos de servicio que un externo proveerá.
- Los SLAs están hechos por expertos o los profesionales pueden incluir ámbitos, remedios y penalidades.
- La línea de fondo es el SLAs que define los niveles mínimos de disponibilidad desde los testers y determinar qué acciones deben ser tomadas en el evento de una ruptura seria.

Outsourcing PenTesting Services

Consultores de Test de Intrusión

- Contratar pen testers altamente calificados resultará en un test de intrusión con alta calidad.
- Un Test de intrusión de una red corporativa examinara numerosos host distintos (con un número de sistemas operativos distintos), arquitectura de red, políticas y procedimientos.
- Las habilidades para Test de Intrusión no puede ser obtenida sin años de experiencia en los campos de TI, como desarrollo, administración de sistemas o consultoría.

Herramientas PenTesting

Evaluación de los distintos tipos de herramientas de Pentest

- Capacidad de reporte.
- Compatibilidad.
- Fácil uso.
- Costo.
- Plataforma.

Herramientas PenTesting

Herramienta de evaluación de seguridad de aplicación: Webscarab.

- Es un marco de trabajo para el análisis de aplicaciones que se comunican utilizando protocolos HTTP y HTTPS.

Otras: Acunetix, etc.

Herramientas PenTesting

Herramienta de evaluación de seguridad de red: Angry IP Scanner: Escanea rango de IPs como también puertos en cualquier rango.

características:

- Información NetBIOS.
- Rangos de direcciones IP favoritas.
- Detección de servidores web.
- Abridores personalizables.

Herramientas PenTesting

Herramienta de evaluación de seguridad de red: GFI LANguard

Es un escáner de seguridad de redes y solución de administración de parches. Asiste en las siguientes áreas:

- Administración de parches.
- Administración de vulnerabilidades.
- Auditoría de software y red.
- Administración de cambios.
- Inventario de bienes.
- Análisis de riesgo y cumplimiento.

Herramientas PenTesting

Herramienta de evaluación de acceso remoto wireless: Kismet

- Es un detector de redes wireless de capa 2, sniffer e IDS.
- Identifica redes recolectando paquetes pasivamente.
- Detecta redes ocultas y la presencia de redes de no balizamiento vía tráfico de datos.

Herramientas PenTesting

Herramienta de evaluación de seguridad telefónica: Omnipeek

Es un analizador de red que ofrece análisis y monitoreo VoIP combinado con ethernet, wireless, 10GbE, Gigabit, y WAN.

Herramientas PenTesting

Herramienta de testeo de dispositivos de red y filtrado: Traffic IQ Professional

Habilita a los profesionales de seguridad a auditar y validar el comportamiento de los dispositivos de seguridad generando un tráfico o ataque de aplicación estándar o tráfico entre dos equipos virtuales.

Puede ser utilizado para evaluar, auditar y testear las características del comportamiento de cualquier filtro de paquete no proxy, incluyendo:

- Firewalls en la capa aplicación.
- IDSs.
- Sistemas de prevención de intrusos.
- Routers y switches.


¡Muchas Gracias!
C|EH Julio Iglesias Perez