Guía para reportes de pentesting

Contenido

1. Introducción

Cuando lo contratan para probar la seguridad de redes y aplicaciones, se le solicita que proporcione:

• Una descripción general completa del estado de seguridad del cliente

• Un resumen exhaustivo y detallado de los problemas de seguridad que encontró

• Las mejores soluciones posibles para lo anterior

1.1. Contratos y cuestiones legales

El cliente puede comenzar su relación comercial dándole un contrato sobre cuáles son sus expectativas y requisitos para que usted haga negocios con él. Es muy importante que revise este contrato en detalle con el Asesor Legal para comprender completamente qué es aceptable para la empresa con la que trabajará y las limitaciones que le puedan imponer.

1.1.1. No divulgación y no competencia

Estos contratos generalmente contienen acuerdos de confidencialidad que protegen al cliente (la organización que lo contrata) de que usted haga pública cualquier información relacionada con la compañía, o use su nombre en cualquier comunicado de prensa sin su consentimiento.

Debe comprender que los acuerdos de no divulgación se refieren no solo a los datos incluidos en el informe, sino también a los datos a los que usted, como pentester, tendrá acceso durante su participación.

El empleo de una política estricta sobre la fuga de datos en su entorno de pruebas de penetración es fundamental en estos casos: cifrado completo del disco, control de acceso físico a sus máquinas, software actualizado y parcheado, etc.

Otra cosa a buscar en cualquier contrato es una cláusula de no competencia.

Las cláusulas de no competencia se utilizan generalmente para garantizar que no trabaje con ningún competidor de otra organización. Si bien los contratos normales pueden no incluir una cláusula de No Competencia, algunos trabajos de consultoría los tienen como lenguaje estándar.

Si existe una cláusula de No Competencia, asegúrese de que su asesor legal lo ayude y verifique que esta cláusula no le impida obtener empleo en otras organizaciones para las que su empresa trabaja.

También comprenda que esta conducta de su cliente es muy común en determinado entorno y no es un acto de desconfianza en su contra.

1.1.2. Retención de datos

Durante su prueba de penetración, encontrará y producirá una cantidad considerable de datos que incluyen:

- Correspondencia (correo electrónico, cartas…)
- Gráficos, trabajos, documentos electrónicos
- Inicios de sesión, contraseñas, direcciones IP, datos personales...
- Prueba de conceptos, código de exploits y vulnerabilidades
- Capturas de pantalla
- Informes y entregables
- Registros de herramientas

La divulgación de estos datos, ya sea que haya firmado una cláusula de no divulgación o no, puede suponer un alto riesgo para el negocio del cliente.

Es importante acordar con su cliente el período de retención de datos por su parte: cuánto tiempo podrá conservar estos datos y cómo. Cuanto menor sea el período de retención, menor será el riesgo para usted de perder los datos de su cliente. Le recomendamos que destruya los datos que no serán útiles para compromisos posteriores con el mismo cliente y que cifre el resto. La autenticación de dos factores (especialmente la biometría) y el cifrado es algo que definitivamente debe emplear en su laboratorio de pruebas de penetración.

1.2. Reglas de compromiso (RoE)

Los documentos de reglas de compromiso son fundamentales en base a las herramientas que el pentester utilizará.

Las RoE le dará al cliente una idea de lo que hace, cómo lo hace y qué puede esperar a cambio. Los documentos de RoE deben ser muy detallados e incluir su metodología, las herramientas que se utilizarán, las pruebas que se realizarán, los requisitos de acceso, equipo o conectividad, y cualquier otra disposición que necesite un pentester para completar su trabajo.

Si es posible, indique al cliente una idea de la duración del compromiso para que sepa cuándo puede esperar que finalice. Por último, asegúrese de detallar en su totalidad la documentación que se le proporcionará al cliente y cuándo puede esperar alguna documentación dentro del encargo.

Este será el documento más importante además del contacto que se intercambiará con usted y el cliente, así que tómese su tiempo y cree una plantilla completa y haga que un asesor legal la revise para asegurarse de que sea completa y, lo más importante, vinculante. En un documento de Reglas de compromiso, usted y su cliente deben definir como mínimo los siguientes aspectos:

- Objetivos en el alcance (IP, dominios, servidores, departamentos...)
- Plazo de realización de las pruebas (fecha de inicio y finalización, horas del día para realizar las pruebas…)
- Cada persona que participa en las pruebas
- Contactos (números de teléfono y correos electrónicos) a los que puede llamar en caso de emergencia durante las pruebas
- Puntos de encuentro a lo largo del tiempo (notificaciones de estado de progreso semanales...)
- Entregables y su nivel de profundidad
- Metodología seguida
- Herramientas utilizadas
- Acuerdo sobre el empleo de ingeniería social u otras técnicas delicadas como el descifrado de contraseñas y la denegación de servicio.

Las fechas, horarios de las pruebas y alcance son tres limitaciones muy importantes que debe tener en cuenta durante todo el compromiso.

Si bien las herramientas utilizadas en la prueba de penetración la mayoría de las veces no son un problema (siempre que no infrinjan otros términos del contrato en su funcionamiento), la violación del alcance y el tiempo realmente puede llevarlo contra un tribunal.

2. Reporte

2.1. Introducción

La fase de reporte es extremadamente importante en una prueba de penetración.

Independientemente de qué tan bien realizó su prueba de penetración, los entregables del proyecto son lo que el cliente juzgará. Esta parte no debe pasarse por alto. La presentación de informes implica habilidades de redacción y presentación.

La fase de reporte no es la última parte del test de penetración. Su contrato puede incluir una cantidad de horas de consultoría sobre sus hallazgos. Durante este período de consultoría, su cliente (generalmente los departamentos habilitados para realizar las correcciones sugeridas) se pondrá en contacto con usted, si es necesario, para solicitar más información o aclaraciones.

El cliente apreciará enormemente la inclusión de un pequeño conjunto de horas de consultoría posterior al informe y esto puede diferenciarlo de otros competidores.

Los reportes comienzan con la prueba de penetración en sí. Cuanto antes comience a recopilar su información, más rápida será la fase de presentación de informes.

Ya debe tener claro que mantener organizados sus datos de pruebas de penetración hace que sus pruebas sean más fáciles y precisas.

Esto se aplica especialmente a la fase de presentación de informes.
Mientras realiza una sesión de prueba de penetración, debe guardar:

- Marca de tiempo exacta (incluida su zona horaria) al comienzo de la prueba

- Alcance de la prueba para esta sesión (en términos de IP o dominios, o áreas de un sitio web, etc.)

- Hallazgos
    - o Tipo de vulnerabilidad
    - o Explotación utilizada o IP / software / dominio / página vulnerable
    - o Breve descripción

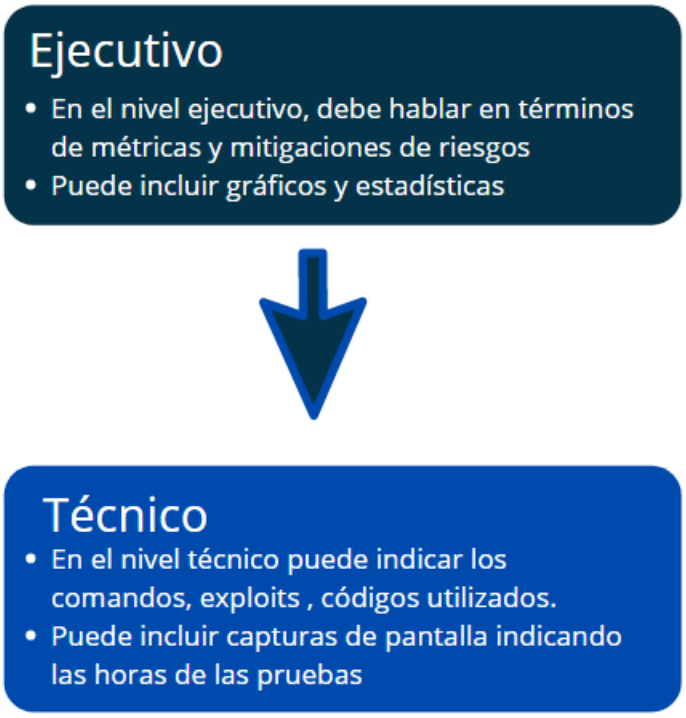
- Notas eventuales, útiles en el reporte

Si recopila lo anterior y lo almacena dentro de una base de datos, una hoja de Excel o incluso en el sistema de archivos y lo organiza por objetivo, encontrará que escribir su informe es mucho más preciso y rápido.

2.2. Estructura de un reporte

Un reporte es el documento que contiene el historial y el resultado de su proyecto.

No puede esperar que su cliente comprenda su idioma. Debe asegurarse de abordar todas las capas de la organización de sus clientes con los argumentos correctos y el lenguaje apropiado.



2.3. Ejemplo de un reporte ejecutivo básico

2.3.1 Objetivo

Identificación y explotación de las vulnerabilidades existentes sobre la infraestructura wireless de la empresa XXZ.

2.3.2 Alcance

La empresa XXZ definió 3 SSID correspondientes a redes inalámbricas visibles desde su establecimiento matriz.

Item	ESSID	BSSID EVALUADO	Modelo	Característica	Modo de seguridad
1	INVITADOS_XXX	00:01:02:03:04:05	Tplink XYZ	Visible	WPA2 Personal
2	VLANXZINT	00:01:02:05:06:07	Tplink XYZ	Oculta	WPA2 Personal
3	VLANYZSIS	00:01:02:07:08:09	Tplink XYZ	Oculta	WPA2 Personal

2.3.3 Resumen

Se efectuaron pruebas en los SSID: INVITADOS_XXX, VLANXZINT y VLANYZSIS de los equipos Tplink XYZ, obteniendo las siguientes conclusiones:

No se identificaron vulnerabilidades explotables de riesgos para el negocio.

Las contraseñas utilizadas en los equipos Tplink XYZ son robustas.

El modo de seguridad empleado (WPA2 Personal) en los equipos Tplink XYZ no es el adecuado para entornos empresariales.

2.3.4 Recomendaciones

Las redes wireless con modo de seguridad WPA2 Personal son lo suficientemente robustas para su uso personal o en el hogar. Sin embargo, para un entorno empresarial se recomienda utilizar WPA2 Enterprise. Las redes wireless WPA2 Enterprise ofrecen un control individualizado y centralizado y se pueden vincular con servidores de Active Directory para una mejor gestión de los usuarios conectados a la red.

2.3.5 Arquitectura recomendada