

Práctica de laboratorio: Creación de un acuerdo de prueba de penetración

Objetivos

En esta práctica de laboratorio, creará su propio acuerdo de prueba de penetración.

- Complete un acuerdo de prueba de penetración simple.

Aspectos básicos/Situación

Un acuerdo de pruebas de penetración es un contrato legalmente vinculante entre el cliente o el evaluador de penetración. El acuerdo define todos los términos y condiciones requeridos para el ejercicio de prueba de penetración. El acuerdo incluirá elementos acordados mutuamente por ambas partes. Puede contener elementos, como la fecha de inicio de la prueba de penetración, el alcance del trabajo, el acuerdo de nivel de servicio, la posible fecha de finalización de la prueba de penetración, etc. También se incluirán en el contrato otros términos y condiciones, así como detalles de precios .

Imagine que una empresa lo contrata para realizar las pruebas. Deberá redactar un acuerdo de pruebas de penetración entre su empresa y el cliente. En una situación real, es probable que consulte con un abogado especializado en dichos contratos porque es muy importante comprenderlos y la información que contienen.

Recursos necesarios

- Computadora personal o dispositivo móvil con acceso a internet

Instrucciones

Parte 1: Complete un acuerdo de prueba de penetración simple.

Paso 1: Investigue acuerdos y contratos de prueba de penetración.

NOTA: NO TIENE QUE COLOCAR CAPTURAS DE PANTALLA EN ESTE PASO 1

- a. Con su motor de búsqueda favorito, realice una búsqueda de contratos de pruebas de penetración, extractos de trabajo y acuerdos.
- b. Encuentre varios ejemplos de acuerdos de pruebas de penetración y revise la información contenida en cada sección.

Práctica de laboratorio: Creación de un acuerdo de prueba de penetración

The screenshot shows a web browser with multiple tabs open. The active tab displays a template for a 'Plantilla de acuerdo de pruebas de penetración'. The form includes fields for the Client's information (Name, Address, Email, Telephone), the Service Provider (Name, Address, Email, Telephone), and a note about referring to them collectively as 'Parties'. It also contains sections for Project Scope (specifying IP ranges, servers, databases, etc.), Acceptance of Risks (mentioning social engineering and data destruction), Test Dates (specifying start and end dates), Methodology (mentioning OWASP, NIST, and ISO norms), and Reporting (providing a timeline for initial and final reports). A sidebar on the right offers a 'Prueba gratis' (Free trial) offer for generating a personalized document.

The screenshot shows a web browser displaying a 'Plantilla de contrato de pruebas de penetración' from Vennage. The template is titled 'PENETRATION TESTING CONTRACT' and includes sections for 'SCOPE OF WORK' (Services Provided: External network penetration testing, Internal network penetration testing, Web application testing, Wireless network testing, Social engineering testing, Physical security testing), 'OBJECTIVES' (Identify vulnerabilities, Assess potential impact, Provide remediation recommendations), and 'TIMELINE' (Testing starts on August 1, 2029, and ends by August 31, 2029; initial findings report within 7 days, final report within 14 days). On the right, there is a sidebar with details about the template (Carta (8,5 x 11 pulgadas) size, PNG, PDF, PowerPoint format, Prima plan), a note about personalizability (100% customizable with millions of photos, icons, tables, and graphics), and a cookie consent message. Buttons for 'Empezar a editar' (Start editing) and 'Crea con IA' (Create with AI) are also visible.

Paso 2: Desarrolle el acuerdo de prueba de penetración.

Con la información que recopiló de su investigación en el paso 1, cree su propio acuerdo de prueba de penetración para su empresa. Como mínimo, el acuerdo debe incluir las secciones que se enumeran a continuación.

EN ESTE PASO 2 NO TIENE QUE COLOCAR CAPTURAS DE PANTALLAS. ESTE PASO ES CON SUS PROPIAS PALABRAS.

a. Partes del acuerdo

(Resalte los detalles personales y la información de las partes involucradas).

La sección debe indicar claramente el nombre, la dirección y la información de contacto de la empresa cliente y de la empresa de pruebas de penetración.

Cliente:

Nombre: TechSolutions S.R.L.

Dirección: Av. Juan Pablo Duarte #102, Santiago de los Caballeros, República Dominicana.

Correo: info@techsolutions.com | Teléfono: (809) 555-9821

Proveedor del servicio:

Nombre: SecureRed Consulting, representada por Alan Israel Lozano Tavarez.

Dirección: Carretera La Ciénega, Santiago de los Caballeros, República Dominicana.

Correo: alanlozano@securered.com | Teléfono: (809) 999-2411

Ambas partes acuerdan llevar a cabo una evaluación de seguridad controlada en los sistemas de TechSolutions S.R.L. El propósito de este acuerdo es identificar vulnerabilidades y fortalecer la protección de la información de la empresa.

b. Alcance del trabajo

(Definir las obligaciones y responsabilidades de cada parte).

El evaluador de penetración acepta:

El evaluador de penetración se compromete a:

- Realizar las pruebas de seguridad siguiendo metodologías reconocidas como OWASP y NIST, siempre de forma ética y con autorización del cliente.
- Evitar cualquier acción que pueda dañar los sistemas o afectar la continuidad del negocio.
- Entregar un informe final claro y detallado, explicando las vulnerabilidades encontradas y cómo solucionarlas.
- Mantener la **confidencialidad total** de toda la información a la que tenga acceso durante las pruebas.
- Informar de inmediato al cliente si se detecta una falla crítica que comprometa la seguridad de los datos.

Esta sección debe enumerar las responsabilidades y obligaciones del evaluador de penetración. Esto incluirá cosas como las pruebas que se realizarán, qué acciones se tomarán si se encuentran vulnerabilidades y qué resultados puede esperar el cliente.

El cliente acepta:

El cliente se compromete a:

- Proporcionar la autorización escrita para realizar las pruebas.
- Respaldar la información y sistemas importantes antes del inicio del proyecto.
- Brindar acceso a los sistemas, credenciales o direcciones necesarias para llevar a cabo la evaluación.
- No realizar cambios en los equipos o configuraciones mientras se ejecutan las pruebas.
- Revisar el informe final y confirmar su recepción dentro del plazo acordado.

Esta sección enumera las responsabilidades y obligaciones del cliente. Esto incluirá cosas como obtener los documentos de consentimiento necesarios, realizar copias de respaldo de los datos críticos y proporcionar las adaptaciones adecuadas.

c. Plazo

El trabajo se llevará a cabo de acuerdo con el siguiente cronograma:

Etapa	Descripción	Fechas estimadas
Planificación	Definición de objetivos y permisos	4 al 6 de noviembre de 2025
Ejecución de pruebas	Escaneo, análisis y pruebas controladas	7 al 11 de noviembre de 2025
Análisis y documentación	Revisión de resultados y elaboración del informe	12 al 14 de noviembre de 2025
Presentación final	Entrega y explicación del informe al cliente	15 de noviembre de 2025

Cualquier modificación en las fechas o en el alcance deberá acordarse entre ambas partes por escrito.

(Establezca una línea de tiempo específica para las pruebas de penetración).

Esta sección incluye cosas como una línea de tiempo para los hitos del proyecto, plazos para las fases del proyecto. Las fases pueden incluir planificación, ejecución, análisis, presentación, etc.

a. Tarifas, facturación y detalles de pago

El costo total del servicio es de **RD\$45,000.00**, dividido de la siguiente manera:

- **50 %** al inicio del proyecto (antes de comenzar las pruebas).
- **50 %** al entregar el informe final.

El pago podrá realizarse mediante transferencia o depósito bancario.

Todos los equipos y herramientas necesarias serán provistos por SecureRed Consulting, sin cargos adicionales, salvo que el cliente requiera recursos especiales previamente aprobados.

(Definir cómo y cuándo se realizan los pagos y abordar cómo se obtienen los materiales y equipos).

Esta sección define cómo y cuándo se realizan los pagos, por ejemplo, una suma global o en partes. Esta sección también puede incluir cómo se obtienen los materiales y equipos de prueba necesarios.

b. Rescisión del contrato

Cualquiera de las partes podrá cancelar el acuerdo en los siguientes casos:

- Incumplimiento en los pagos acordados.
- Falta de cooperación o negación de acceso a los sistemas.
- Violación de las normas éticas o de confidencialidad.
- Solicitud formal de cancelación con al menos **cinco (5) días hábiles de aviso previo**.

Si se cancela el proyecto antes de su finalización, el cliente deberá pagar los costos correspondientes al trabajo ya realizado.

Ambas partes se comprometen a mantener la **confidencialidad de toda la información** tratada durante la ejecución del servicio, incluso después de terminado el contrato.

Este acuerdo busca garantizar que las pruebas se realicen de manera segura, profesional y transparente, promoviendo la confianza entre el cliente y el proveedor, y fortaleciendo la ciberseguridad de la organización.

(Definir las circunstancias que conducirían a una rescisión anticipada del contrato).

Esta sección incluye circunstancias y situaciones que pueden conducir a la terminación anticipada del contrato por cualquiera de las partes. Aborda el derecho de la empresa de pruebas de penetración o del cliente a finalizar la asociación por cuestiones como el incumplimiento del pago de las tarifas o las pruebas no realizadas correctamente. Debe explicar el curso de acción a tomar en caso de cancelación anticipada.