



GRUPO 1

***Eneko
González,
Xabier Parra y
David Lobo.***

Contenidos

1.	Formulario de autorización de Pentesting	3
2.	Tipos de pruebas (Pentesting.)	4
2.1.	Restricciones y conformidades	5
3.	ACUERDO DE CONFIDENCIALIDAD	5
3.1.	Obligaciones DEX	5
3.2.	Exclusiones	6
3.3.	Derechos de propiedad	6
3.4.	Vigencia	6
3.5.	Legislación aplicable.	7

Fecha: 15/01/2022

- Condiciones:
 - Las pruebas serán externas e internas y se realizarán desde fuera y dentro de la red del cliente utilizando Internet y para acceder a los activos incluidos en el alcance.
 - Se realizarán dos TEST de penetración:
 - Caja negra.
 - Caja gris
- Planificación temporal:
 - Fechas: Del 15 de enero al 1 de febrero 2022. Días laborables comprendidos entre el L-V.
 - Horario: **Preferiblemente de 8.00h a 14.00h**

- Teléfonos de soporte en caso de caída de servicio:
 - **Por parte del equipo de producto o cliente:**
 - Nombre: DANI IRAZOLA
 - Teléfono: 946 81 00 58
 - Email: Dani.irazola@maristak.net
 - **Auditor(DEX):**
 - Nombre: Eneko Gonzalez, David Lobo, Xabier Parrra
 - Teléfono: 946319070
 - Email: Eneko.gonzalez@maristak.net, David.lobo@maristak.net, Xabier.parra@maristak.net

2. Tipos de pruebas (Pentesting.)

El servicio de tests de intrusión nos permite testear la fortaleza de la infraestructura IT para medir su nivel de seguridad técnico y si cumple los niveles requeridos por la política organizativa. Estos tests son realizados por expertos en seguridad sobre todos los servicios expuestos a internet y aquellos que puedan accederse remotamente.

Se pueden realizar dos tipos distintos de Tests de Intrusión, Externo o Interno dependiendo desde dónde se lancen los ataques.

- El **Test de Intrusión Externo:** se realiza desde internet sobre la infraestructura del cliente, más concretamente, sobre aquellos dispositivos de la organización que están expuestos a internet, por ejemplo, router, firewall, servidor web, servidor de correo, DNS, etc.
- El **Test de Intrusión Interno:** se realiza desde dentro de la red del cliente desde donde pueden localizarse más problemas de seguridad que desde fuera.
- Propósito del *pentest*: Comprobar el estado de las vulnerabilidades que presenta la aplicación web objeto del mismo.

Se pueden realizar dos tipos distintos de Tests de Intrusión, Externo o Interno dependiendo desde dónde se lancen los ataques.

- **Tests de Intrusión de Caja Negra:** este es un tipo de test de intrusión externo, sin información o solo con muy poca información del objetivo (solo lo que debe ser auditado). Por ejemplo, dada una web o portal publicado, intentar atacarlo desde una red externa sólo a partir de información básica disponible, desconociendo información relativa a arquitectura, usuarios, etc.
- **Test de Intrusión de Caja Gris:** este tipo de test puede ser interno o externo, poseyendo solo información limitada sobre el objetivo como, por ejemplo, credenciales de autenticación básicas.
- **Test de Intrusión de Caja Blanca:** este tipo de test es interno, accediendo a la red desde un punto de acceso y teniendo el diagrama de red, las plataformas, los servicios principales, y varios perfiles con distintas credenciales y privilegios, etc.

Dada la naturaleza de los trabajos a realizar cabe la posibilidad de que, de forma no intencionada, se produjese algún efecto colateral indeseado. Si así fuese, el Auditor de DEX lo notificaría inmediatamente al Teléfono de soporte correspondiente o se pondría a disposición del cliente para aportar la información requerida sobre las acciones realizadas.

2.1. Restricciones y conformidades

Las siguientes restricciones se aplicarán a esta autorización:

- Esta autorización estará vigente desde el Del 15 de enero al 1 de febrero 2022, ambos inclusive.

De conformidad con la concesión de esta autorización, el Cliente declara que:

- El cliente es dueño de los sistemas donde se realiza la auditoria de vulnerabilidades y el suscrito tiene la autoridad adecuada para poder llevar a cabo las actividades de verificación de seguridad de aplicaciones.
- El cliente ha creado una copia de seguridad completa de todos los sistemas dentro del ámbito de las pruebas de vulnerabilidades, y se ha comprobado que el procedimiento de copia de seguridad permitirá al cliente restaurar los sistemas a su estado pre-test.
- El servicio implica necesariamente el uso de herramientas y técnicas diseñadas para detectar las vulnerabilidades de seguridad, y que es imposible identificar y eliminar todos los riesgos que implica el uso de estas herramientas y técnicas.
- El cliente se compromete a no modificar el sistema o aplicativo durante la ejecución del pentesting. Si esto sucediera se entenderá como un cambio de alcance, de tal modo que el pentesting se dará por finalizado y se entregará el informe al cliente con los resultados obtenidos hasta ese momento, con lo que el Auditor cumplirá totalmente con el alcance inicialmente acordado. Si el cliente desea realizar un pentesting al sistema o aplicativo que ha modificado deberá volver a negociarlo con DEX considerándose en todo caso como el encargo de un nuevo trabajo.

Cualquier cambio a las limitaciones y condiciones descritas deberá realizarse por escrito y ser aceptado por ambas partes.

3. ACUERDO DE CONFIDENCIALIDAD

Será considerada como “Información Confidencial” toda aquella información, ya sea técnica, financiera, comercial o de cualquier otro carácter, suministrada y divulgada por la empresa cliente a DEX en relación con el alcance del contrato, mediante cualquier tipo de soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro (papel, informático, etc.) o de forma verbal.

3.1. Obligaciones DEX

Nada más recibir la Información Confidencial, DEX la mantendrá en estricta confidencialidad, la utilizará solamente en relación con las pruebas del alcance, no la revelará a una tercera parte sin el previo consentimiento escrito de la empresa cliente y sólo podrá revelar dicha Información Confidencial a los empleados de su compañía o que tengan necesidad expresa de conocerla en relación con las pruebas contratadas.

DEX no podrá copiar ni reproducir la Información Confidencial suministrada por la otra Parte en formato o soporte alguno, excepto si ello fuera preciso con arreglo a lo previsto en el párrafo anterior. Toda copia o reproducción que se haga deberá contener el mismo sello, marca o leyenda que su original.

3.2. Exclusiones

Las Partes acuerdan que las obligaciones contenidas en este Acuerdo no se aplicarán respecto de aquella información que:

- Esté, sea o llegue a ser de público conocimiento sin mediar acto proveniente de DEX en contravención de los términos de este Compromiso;
- Deba ser difundida por imperativo de una disposición legal, contractual o judicial;
- Sea explícitamente identificada, de conformidad con este Compromiso, como Información No Confidencial;
- Cuya comunicación o uso sin restricciones haya sido aprobada por la empresa cliente;
- Sea independientemente generada por DEX sin hacer uso de la Información Confidencial;
- Haya sido requerida a la Parte receptora mediante una resolución firme por Autoridades Administrativas o Judiciales competentes. En este caso deberá notificarse
- Inmediatamente esta circunstancia a la empresa cliente sobre el requerimiento recibido, siempre que no exista obligación de guardar secreto sobre el mismo por mandato legal, administrativo o judicial. Asimismo, DEX sólo revelará aquella parte de la Información que sea requerida.

3.3. Derechos de propiedad

Este Acuerdo no supone la concesión, expresa o implícita, de derecho alguno sobre la Información Confidencial que la empresa cliente suministre, salvo el que en cada caso sea otorgado expresamente en relación con el Alcance del presente contrato.

En consecuencia, el suministro de dicha Información no podrá entenderse, en ningún caso, como concesión de patente, licencia o cualquier otro derecho de propiedad intelectual y/o industrial alguno, considerándose que aquella permanecerá en todo momento en el ámbito de propiedad de la empresa cliente o del tercero a quien pertenezca.

3.4. Vigencia

Las obligaciones previstas en la cláusula 2 permanecerán en vigor hasta que hayan transcurrido 3 años contados a partir de la fecha de entrega del informe de resultados del presente contrato.

3.5. Legislación aplicable.

Este Compromiso se interpretará de conformidad con las leyes españolas.

Si alguna de las Partes es objeto de una fusión u otro tipo de reorganización societaria, se acuerda que este Compromiso será vinculante para el que le suceda de acuerdo con la ley aplicable.

POR EL CLIENTE:	Auditor (DEX):
Fdo: Maristak Durango Fecha: 15/01/2022	Fdo: Eneko, David y Xabier Fecha: 15/01/2022



