Tipologías de Tests de Intrusión

CONSORCI AOC

Administració Oberta de Catalunya

Ref.: 69.254
Fecha: 20/02/2025

www.ayesa.com

ÍNDICE

1 AVISO LEGAL

Este documento contiene información confidencial y propietaria. Su objetivo es ser de uso exclusivo para **CONSORCI AOC.** El uso no autorizado y/o reproducción de este documento está prohibido.

CONTROL DOCUMENTAL

Tipo de documento	Informe **Tipologías de Tests de Intrusión**		
Cliente	**CONSORCI AOC**		
Clasificación	CONFIDENCIAL		
Versión	1.0		
Autor[es]	Área Seguridad Ofensiva - Ayesa	**Fecha:**	20/02/2025

HISTORIAL DE REVISIONES

Versión	Fecha	Autor	Descripción de Cambio
1.0	20/02/2025	EPI	Generación del documento

APROBACIÓN

Elaborado	Revisado	Aprobado
Eder Pérez Ignacio	Eder Pérez Ignacio	Lluis Cusco Sureda

2 INTRODUCCIÓN

AYESA ha sido contratado por **CONSORCI AOC** (en adelante **AOC**) para llevar a cabo el servicio de **Seguridad Ofensiva** asociado a la oferta con Identificador de Servicio **69.254**.

Dentro del servicio, en concreto dentro de la línea de test de intrusión, puede existir la necesidad de realizar pruebas de seguridad con diferente tipo de exhaustividad, alcance y esfuerzos.

Este documento tiene como objetivo recoger las dos agrupaciones de test de intrusión a realizar en base al alcance, y las diferentes tipologías de test de intrusión en base al activo auditado.

3 AUDITORÍAS TÉCNICAS DE SEGURIDAD

A continuación, se definen las dos agrupaciones en las que se pueden enmarcar los test de intrusión solicitados. Para cada caso se definirá en conjunto con AOC la tipología a realizar, siempre en base a sus necesidades y objetivos específicos.

3.1 Test de intrusión

Se trata de un test de intrusión convencional, que pretende identificar y explotar el mayor número de vulnerabilidades en el activo dentro del alcance, evaluar su nivel de seguridad global y definir un plan de recomendaciones táctico y estratégico. Es exhaustivo y ambicioso en el alcance.

A continuación, se exponen algunos ejemplos en los que sería oportuno realizar este test de intrusión:

- Requerimientos normativos, por un tercero o políticas internas de pase de test de intrusión sobre un activo / infraestructura.
- Necesidad de obtener el nivel de seguridad global de un activo / infraestructura.
- Realización de grandes cambios dentro de un activo / infraestructura.
- Realización de cambios que puedan inferir en el resto de activo / infraestructura.
- Aplicaciones que nunca antes han sido auditadas a través de este tipo de análisis.

3.2 Test de intrusión dirigido

Se trata de un test de intrusión con un alcance mucho más acotado. No pretende medir el nivel general de seguridad de un activo o infraestructura al completo, sino que se centra en funcionalidades, secciones particulares y acotadas. De esta manera, otorga una visión parcial del nivel de seguridad, al no contemplar el activo en su totalidad. Si bien no es exhaustivo en cuanto al alcance, puede tener profundidad sobre una funcionalidad específica.

A continuación, se exponen algunos ejemplos en los que sería oportuno realizar este test de intrusión más acotado:

- Como complemento a otros test de intrusión realizados sobre ese mismo activo recientemente.
- Previo a un pase a producción sobre cambios medios o cambios específicos.
- Con el objetivo de testear una funcionalidad específica.

4 TIPOLOGÍAS EN BASE AL ACTIVO AUDITADO

Independientemente de la clasificación anterior de test de intrusión, dependiendo del activo sobre el que se realizará la auditoría de seguridad se pueden definir diferentes tests de intrusión.

4.1 Test de intrusión de aplicaciones web / APIs

Los servicios Web son uno de los principales puntos de exposición de los sistemas informáticos existiendo muchas (y cada vez más sofisticadas) vías de explotación en diferentes plataformas, pudiendo comprometer la seguridad de las infraestructuras que albergan estos aplicativos. Esta situación los expone a múltiples amenazas como, por ejemplo:

- Externos que pueden acceder al sistema desde Internet o desde las redes autorizadas del cliente (crackers, la competencia, usuarios malintencionados …) con fines maliciosos.
- Exposición de información de los sistemas, aplicaciones y datos de usuarios.
- Interrupción de los sistemas en producción.
- Filtración de información.

El objetivo es analizar y evaluar el aplicativo web en busca de vulnerabilidades que puedan dar acceso no autorizado a la organización o que conlleven una exposición de datos, además de permitir evaluar el nivel de conformidad contra distintas normativas de seguridad y de protección de datos.

En función del nivel de profundidad que se requiera, se pueden seguir dos aproximaciones distintas (o secuenciales la una a la otra):

- **Pre-Autenticación (Caja Negra):** Evaluación de la seguridad de los aplicativos e infraestructura desde el exterior y sin información previa de estos.
- **Post-Autenticación (Caja Gris):** Evaluación de los mecanismos de seguridad implementados en el aplicativo haciendo uso de credenciales suministradas por el cliente, en la cual no solo se buscan principalmente vulnerabilidades asociadas a la tecnología, sino también a la lógica del aplicativo, en cuanto a sus mecanismos de autenticación, autorización, etc.

La ejecución de este tipo de test de intrusión permitirá entender el riesgo que suponen los aplicativos webs expuestos a Internet, la probabilidad de que sean comprometidos, y cumplir con ciertos requerimientos de protección de datos o normativos, como puede ser PCI-DSS.

Algunos ejemplos de resultados son:

- Explotación de vulnerabilidades web con posterior acceso a Base de Datos, obteniendo así acceso a datos bancarios, financieros y demás PII (Información Personal Identificable).

- Explotación de malas implementaciones de Endpoint API comprometiendo datos y claves de acceso
- Etc.

En este servicio se utilizará la siguiente metodología:

- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Testing Methodology Manual)
- OWASP Top 10
- OWASP Web Secuity Testing Guide
- OWASP ASVS

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- Burp Suite
- Scripts particulares

4.2 Test de intrusión de aplicaciones móviles

Se tratan de análisis de aplicaciones destinadas a terminales móviles para identificar posibles vulnerabilidades de seguridad de las mismas mediante análisis estáticos y dinámicos, pruebas de intrusión, suplantación de identidades, etc.

Las pruebas y análisis de seguridad analizaran los siguientes puntos:

- Descubrimiento de aplicaciones
- Identificación de puntos de entrada a la aplicación
- Posibilidades de inyección de código
- Gestión de sesiones y análisis del esquema de autenticación
- Escalada de privilegios
- Pruebas de autorización y autorización entre aplicaciones
- Análisis de códigos de error
- Propagación de vulnerabilidades
- Ingeniería inversa de protocolos y/o posibles exploits que se pudieran usar
- Pruebas de denegación de servicio
- Sistemas de autenticación
- Posibles suplantaciones de entrada de datos y de tráfico y comunicaciones.

Objetivos de Identificación:

- Vulnerabilidades de la propia aplicación
- Información técnica relevante
- Enlaces a otros elementos (APIs, etc…)

En este servicio se utilizará la siguiente metodología:

- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Testing Methodology Manual)
- OWASP Mobile Application Security

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- Zed Attack Proxy
- Burp Suite
- Android Debug Bridge
- Acunetix
- Netsparker

Este tipo de ataque podría proveernos de:

- Nuevas referencias (otros hilos de los que tirar, etc.)
- Acceso no autorizado a información gestionada por dicha aplicación
- Acceso remoto a sistemas (mediante Webshell)

4.3 Test de Intrusión en la red desde Internet

También conocido como Test de Intrusión Externo o perimetral. Mediante este servicio se busca identificar posibles vulnerabilidades es en los múltiples servicios que **AOC** pudiera tener expuestos a Internet.

En este servicio se utilizará la siguiente metodología:

- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Testing Methodology Manual)

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- Escáner de Vulnerabilidades
- Herramientas específicas de cada servicio
- Herramientas específicas de cada vulnerabilidad

Este tipo de ataque podría proveernos de:

- Acceso remoto a la red
- Acceso a información o aplicaciones

4.4 Test de intrusión de información accesible desde Internet

También conocido como estudio OSINT (Open Source Inteligence). Identificación de toda la información que pudiera estar accesible desde internet y que, de algún modo, pudiera servir a un atacante para sus objetivos. (información técnica, personal, etc…) y recomendaciones para su eliminación.

En esta tipología de servicio se utilizará la siguiente metodología:

1. Recogida de inteligencia: Estudio de la organización, de su sector, de sus empleados, de la estructura de correos o números telefónicos, de proveedores, etc.

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- Fuentes OSSINT
- Herramientas propietarias

Este tipo de ataque podría proveernos:

- Acceso a Información
- Credenciales

4.5 Test de intrusión de la red interna

También conocido como Test de Intrusión Interno. Mediante este servicio se busca identificar posibles vulnerabilidades existentes desde múltiples puntos de la red interna.

Los puntos de entrada, las condiciones y redes de destino/alcance definirán en gran medida la metodología.

En este servicio se utilizará la siguiente metodología:

- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Testing Methodology Manual)

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- Escáner de Vulnerabilidades
- Herramientas específicas de cada servicio
- Herramientas específicas de cada vulnerabilidad

Este tipo de ataque podría proveernos de:

- Acceso remoto a la red
- Credenciales
- Acceso a información

4.6 Test de intrusión de ingeniería social

Se trata de ejercicios con el objeto de obtener información confidencial a través de la manipulación de usuarios legítimos.

Los ataques de ingeniería social buscan poner a prueba a los empleados de la organización.

Podemos identificar 2 tipologías: Remotas y Físicas

4.6.1 Remotas

Para ello, se utilizarán técnicas de envío de correo (Spear Phishing) o telefónicas (Vishing), basadas en pretextos alineados con la organización, para que los empleados den información sensible o realizan acciones no deseadas.

- Correo electrónico
- Mensajería electrónica (whatsapp, SMS,..)
- Llamadas telefónicas

En esta tipología de servicio se utilizará la siguiente metodología:

1. Recogida de inteligencia: Estudio de la organización, de su sector, de sus empleados, de la estructura de correos o números telefónicos, de proveedores, etc.

2. Creación de pretextos y payloads: se crean pretextos dirigidos a los empleados que se han seleccionado como objetivos potenciales, además de generar payloads personalizados con diferentes objetivos, como puede ser obtener información, acceso a máquinas, etc.
3. Ataque de objetivos: Se hacen envíos de correos de phishing o llamadas telefónicas desde infraestructuras personalizadas para el cliente, haciendo uso de dominios dedicados y debidamente configurados para maximizar la probabilidad y evitar levantar sospechas.

Algunas de las técnicas que se pueden llevar a cabo son:

- Obtención de credenciales mediante portales maliciosos (credential harvesting).
- Evasión de sistema 2FA para acceso a sistemas externos.
- Ejecución de código malicioso en equipos corporativos (MACROs, HTAs, etc.).
- Hacer al usuario instalar software malicioso o dar acceso remoto al equipo vía suplantación telefónica.
- Etc.

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- Proofpoint Security Awareness Training Platform (PSAT)

4.6.2 Hibridas/Locales

Media Dropping

Dependiendo del acceso físico y cuanto más próximo al personal objetivo (suelo de la oficina, mesas de los empleados, lanzando el USB, etc…) se podrían distribuir USBs maliciosos, conteniendo software de control remoto.

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- Malware personalizado

Este tipo de ataque podría proveernos de (depende de malware usado):

- Acceso remoto a sistema de usuario (mediante malware de C&C)

- Acceso a Información
- Acceso a la red (proxy)
- Credenciales (keylogger, etc…)

4.7 Test de intrusión de redes WiFi

Los ataques inalámbricos buscan comprometer el perímetro inalámbrico de la organización y/o interceptar comunicaciones de los empleados que las utilizan. Para ello, se pueden tomar aproximaciones de ingeniería social contra los usuarios corporativos o aproximaciones de ataques contra la propia infraestructura y configuraciones del despliegue inalámbrico.

En general, estos ataques podrán realizarse en el exterior (zonas públicas) o en las áreas de acceso público, siendo difícil su detección.

4.7.1 Ataques contra claves compartidas

Los ataques contra claves compartidas persiguen, mediante un gran número de técnicas, obtener la clave o el acceso a la red Wi-Fi.

En este servicio se utilizará la siguiente metodología:

- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Testing Methodology Manual)
- OWISAM (Open Wireless Security Assessment Methodology)

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- WiFi Pineapple

Este tipo de ataque podría proveernos de:

- Credenciales
- Acceso remoto a la red
- Acceso remoto al equipo de usuario final

4.7.2 Ataques contra portales cautivos

Si la red Wi-Fi se encuentra gestionada por un portal cautivo, se puede intentar evadir dicho control y obtener un acceso ilimitado a la red, etc…

En este servicio se utilizará la siguiente metodología:

- PTES (Penetration Testing Execution Standard)
- OSSTMM (Open Source Security Testing Methodology Manual)
- OWASP

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- Burp Suite

Este tipo de ataque podría proveernos de:

- Acceso remoto a la red

4.7.3 Ataques de falso punto de acceso

Suplantación de las redes inalámbricas legítimas con el objetivo de obtener información de autenticación de dichas redes.

Se crearían redes inalámbricas simulando las redes legítimas del organismo, se intentaría bloquear la señal de los puntos legítimos y capturar el tráfico enviado y/o intentar acceder al sistema final a través de dicha red.

En este servicio se utilizará la siguiente metodología:

- OWISAM (Open Wireless Security Assessment Methodology)

En este servicio se podrán llegar a utilizar las siguientes herramientas:

- WiFi Pineapple

Este tipo de ataque podría proveernos de:

- Credenciales
- Acceso remoto al equipo de usuario final

AYESA
T. +34 902 10 26 55
E. marketing@ayesa.com

www.ayesa.com