INESEM

BUSINESS SCHOOL

Postgrado en Análisis de Malware y Contramedidas + Titulación Universitaria

+ Información Gratis

titulación de formación continua bonificada expedida por el instituto europeo de estudios empresariales

Postgrado en Análisis de Malware y Contramedidas + Titulación Universitaria

duración total: 425 horas ***horas teleformación:*** 150 horas

precio: 0 € *

modalidad: Online

* hasta 100 % bonificable para trabajadores.

descripción

Este curso en Análisis de Malware y Contramedidas le ofrece una formación especializada en la materia, aprendiendo todo lo necesario sobre las técnicas y la metodología utilizadas por los profesionales del análisis de malwares (o programas maliciosos). La seguridad informática (y ethical hacking), es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. Este curso en en Análisis de Malware y Contramedidas ofrece una formación especializa en seguridad informática - Ethical Hacking.

a quién va dirigido

Todos aquellos trabajadores y profesionales en activo que deseen adquirir o perfeccionar sus conocimientos técnicos en este área.

objetivos

- Conocer la definición precisa de los diferentes tipos de hackers y de sus objetivos.
- Aprender a identificar malware.
- Analizar de manera básica los tipos de malware e implementar contramedidas.
- Comprender las diferentes técnicas de ofuscación.
- Aprender las técnicas y la metodología utilizadas por los profesionales del análisis de malwares.
- Aprender sobre la metodología de un ataque y los medios para identificar las vulnerabilidades o fallos de seguridad a través de los que introducirse en un sistema.
- Conocer los fallos físicos, que permiten un acceso directo a ordenadores, y los fallos de red y Wi-Fi se presentan e ilustran cada uno con propuestas de contramedidas.
- Saber sobre el Cloud Computing (su historia, su funcionamiento) para dominar mejor la seguridad.
- Tener en cuenta la seguridad en la web y los fallos actuales identificados gracias a la ayuda de herramientas que el lector puede implantar fácilmente en sus propios sistemas.
- Identificar siempre los posibles fallos para establecer después la estrategia de protección adecuada.
- Conocer algunos ejemplos los fallos de sistemas en Windows o Linux y los fallos de aplicación, para familiarizarse con el lenguaje ensamblador y comprender mejor las posibilidades de ataque.

para qué te prepara

Este curso en Análisis de Malware y Contramedidas le prepara para aprender a identificar malware, analizar de manera básica los tipos de malware e implementar contramedidas, comprender las diferentes técnicas de ofuscación y aprender las técnicas y la metodología utilizadas por los profesionales del análisis de malwares.

salidas laborales

Seguridad Informática.

titulación

Una vez finalizado el curso, el alumno recibirá por parte de INESEM vía correo postal, la Titulación Oficial que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Esta titulación incluirá el nombre del curso/máster, la duración del mismo, el nombre y DNI del alumno, el nivel de aprovechamiento que acredita que el alumno superó las pruebas propuestas, las firmas del profesor y Director del centro, y los sellos de la instituciones que avalan la formación recibida (Instituto Europeo de Estudios Empresariales).

INSTITUTO EUROPEO DE ESTUDIOS EMPRESARIALES

como centro de Formación acreditado para la impartición a nivel nacional de formación
EXPIDE LA SIGUIENTE TITULACIÓN

NOMBRE DEL ALUMNO/A

con D.N.I. XXXXXXXX ha superado los estudios correspondientes de

Nombre de la Acción Formativa

de XXX horas, perteneciente al Plan de Formación INESEM en la convocatoria de XXXX
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX- XXXX-XXXX-XXXXXX

Con una calificación de SOBRESALIENTE

Y para que conste expido la presente TITULACIÓN en
Granada, a (día) de (mes) de (año)

La direccion General — MARIA MORENO HIDALGO

Sello

Firma del alumno/a — NOMBRE DEL ALUMNO/A

forma de bonificación

- Mediante descuento directo en el TC1, a cargo de los seguros sociales que la empresa paga cada mes a la Seguridad Social.

metodología

El alumno comienza su andadura en INESEM a través del Campus Virtual. Con nuestra metodología de aprendizaje online, el alumno debe avanzar a lo largo de las unidades didácticas del itinerario formativo, así como realizar las actividades y autoevaluaciones correspondientes. Al final del itinerario, el alumno se encontrará con el examen final, debiendo contestar correctamente un mínimo del 75% de las cuestiones planteadas para poder obtener el título.

Nuestro equipo docente y un tutor especializado harán un seguimiento exhaustivo, evaluando todos los progresos del alumno así como estableciendo una línea abierta para la resolución de consultas.

El alumno dispone de un espacio donde gestionar todos sus trámites administrativos, la Secretaría Virtual, y de un lugar de encuentro, Comunidad INESEM, donde fomentar su proceso de aprendizaje que enriquecerá su desarrollo profesional.

materiales didácticos

- Manual teórico 'Seguridad Informática'

- Manual teórico 'Seguridad Informática y Malwares. Análisis de Amenazas e Implementación de Contrame

profesorado y servicio de tutorías

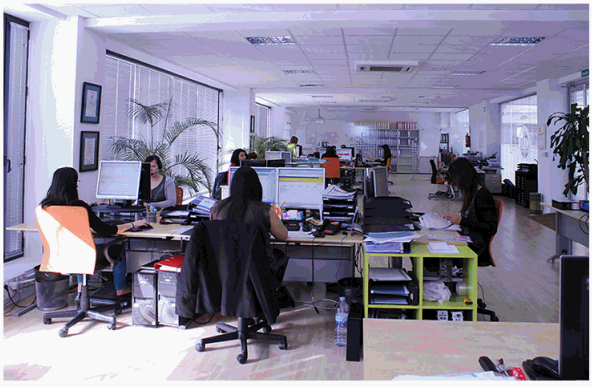
Nuestro equipo docente estará a su disposición para resolver cualquier consulta o ampliación de contenido que pueda necesitar relacionado con el curso. Podrá ponerse en contacto con nosotros a través de la propia plataforma o Chat, Email o Teléfono, en el horario que aparece en un documento denominado “Guía del Alumno” entregado junto al resto de materiales de estudio. Contamos con una extensa plantilla de profesores especializados en las distintas áreas formativas, con una amplia experiencia en el ámbito docente.

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas, así como solicitar información complementaria, fuentes bibliográficas y asesoramiento profesional. Podrá hacerlo de las siguientes formas:

- **Por e-mail**: El alumno podrá enviar sus dudas y consultas a cualquier hora y obtendrá respuesta en un plazo máximo de 48 horas.

- **Por teléfono**: Existe un horario para las tutorías telefónicas, dentro del cual el alumno podrá hablar directamente con su tutor.

- **A través del Campus Virtual**: El alumno/a puede contactar y enviar sus consultas a través del mismo, pudiendo tener acceso a Secretaría, agilizando cualquier proceso administrativo así como disponer de toda su documentación



plazo de finalización

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la misma duración del curso. Existe por tanto un calendario formativo con una fecha de inicio y una fecha de fin.

campus virtual online

especialmente dirigido a los alumnos matriculados en cursos de modalidad online, el campus virtual de inesem ofrece contenidos multimedia de alta calidad y ejercicios interactivos.

comunidad

servicio gratuito que permitirá al alumno formar parte de una extensa comunidad virtual que ya disfruta de múltiples ventajas: becas, descuentos y promociones en formación, viajes al extranjero para aprender idiomas...

revista digital

el alumno podrá descargar artículos sobre e-learning, publicaciones sobre formación a distancia, artículos de opinión, noticias sobre convocatorias de oposiciones, concursos públicos de la administración, ferias sobre formación, etc.

secretaría

Este sistema comunica al alumno directamente con nuestros asistentes, agilizando todo el proceso de matriculación, envío de documentación y solución de cualquier incidencia.

Además, a través de nuestro gestor documental, el alumno puede disponer de todos sus documentos, controlar las fechas de envío, finalización de sus acciones formativas y todo lo relacionado con la parte administrativa de sus cursos, teniendo la posibilidad de realizar un seguimiento personal de todos sus trámites con INESEM

programa formativo

PARTE 1. SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

1.Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
2.Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
3.Salvaguardas y tecnologías de seguridad más habituales
4.La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

UNIDAD DIDÁCTICA 2. ANÁLISIS DE IMPACTO DE NEGOCIO

1.Identificación de procesos de negocio soportados por sistemas de información
2.Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
3.Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

UNIDAD DIDÁCTICA 3. GESTIÓN DE RIESGOS

1.Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
2.Metodologías comúnmente aceptadas de identificación y análisis de riesgos
3.Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

UNIDAD DIDÁCTICA 4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

1.Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio
2.Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
3.Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

UNIDAD DIDÁCTICA 5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1.Principios generales de protección de datos de carácter personal
2.Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal
3.Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización
4.Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

UNIDAD DIDÁCTICA 6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

1.Determinación de los perímetros de seguridad física
2.Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las qu estén ubicados los sistemas informáticos
3.Criterios de seguridad para el emplazamiento físico de los sistemas informáticos
4.Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos
5.Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos
6.Elaboración de la normativa de seguridad física e industrial para la organización
7.Sistemas de ficheros más frecuentemente utilizados
8.Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organizació
9.Configuración de políticas y directivas del directorio de usuarios
10.Establecimiento de las listas de control de acceso (ACLs) a ficheros
11.Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados
12.Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo
13.Sistemas de autenticación de usuarios débiles, fuertes y biométricos
14.Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos
15.Elaboración de la normativa de control de accesos a los sistemas informáticos

UNIDAD DIDÁCTICA 7. IDENTIFICACIÓN DE SERVICIOS

1.Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
2.Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
3.Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

UNIDAD DIDÁCTICA 8. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

1.Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
2.Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas / DMZ
3.Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones
4.Definición de reglas de corte en los cortafuegos
5.Relación de los registros de auditoría del cortafuegos necesario para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
6.Establecimiento de la monitorización y pruebas de los cortafuegos

UNIDAD DIDÁCTICA 9. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

1.Introducción al análisis de riesgos
2.Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, as como criterios de programación segura
3.Particularidades de los distintos tipos de código malicioso
4.Principales elementos del análisis de riesgos y sus modelos de relaciones
5.Metodologías cualitativas y cuantitativas de análisis de riesgos
6.Identificación de los activos involucrados en el análisis de riesgos y su valoración
7.Identificación de las amenazas que pueden afectar a los activos identificados previamente
8.Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
9.Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
10.Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y efecto sobre las vulnerabilidades y amenazas
11.Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializar
12.Determinación de la probabilidad e impacto de materialización de los escenarios
13.Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
14.Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
15.Relación de las distintas alternativas de gestión de riesgos
16.Guía para la elaboración del plan de gestión de riesgos
17.Exposición de la metodología NIST SP 800
18.Exposición de la metodología Magerit

UNIDAD DIDÁCTICA 10. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

1.Herramientas del sistema operativo tipo Ping, Traceroute, etc
2.Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc
3.Herramientas de análisis de vulnerabilidades tipo Nessus
4.Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc
5.Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc
6.Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc

UNIDAD DIDÁCTICA 11. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

1.Principios generales de cortafuegos
2.Componentes de un cortafuegos de red
3.Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
4.Arquitecturas de cortafuegos de red
5.Otras arquitecturas de cortafuegos de red

UNIDAD DIDÁCTICA 12. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

1. Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
2. Guía para la elaboración del plan de auditoría
3. Guía para las pruebas de auditoría
4. Guía para la elaboración del informe de auditoría

PARTE 2. CONSULTOR EN SEGURIDAD INFORMÁTICA IT: ETHICAL HACKING

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN A LOS ATAQUES Y AL HACKING ÉTICO

1. Introducción a la seguridad informática
2. El hacking ético
3. La importancia del conocimiento del enemigo
4. Seleccionar a la víctima
5. El ataque informático
6. Acceso a los sistemas y su seguridad
7. Análisis del ataque y seguridad

UNIDAD DIDÁCTICA 2. SOCIAL ENGINEERING

1. Introducción e historia del Social Engineering
2. La importancia de la Ingeniería social
3. Defensa ante la Ingeniería social

UNIDAD DIDÁCTICA 3. LOS FALLOS FÍSICOS EN EL ETHICAL HACKING Y LAS PRUEBAS DEL ATAQUE

1. Introducción
2. Ataque de Acceso físico directo al ordenador
3. El hacking ético
4. Lectura de logs de acceso y recopilación de información

UNIDAD DIDÁCTICA 4. LA SEGURIDAD EN LA RED INFORMÁTICA

1. Introducción a la seguridad en redes
2. Protocolo TCP/IP
3. IPv6
4. Herramientas prácticas para el análisis del tráfico en la red
5. Ataques Sniffing
6. Ataques DoS y DDoS
7. Ataques Robo de sesión TCP (HIJACKING) y Spoofing de IP
8. Ataques Man In The Middle (MITM).
9. Seguridad Wi-Fi
10. IP over DNS
11. La telefonía IP

UNIDAD DIDÁCTICA 5. LOS FALLOS EN LOS SISTEMAS OPERATIVOS Y WEB

1. Usuarios, grupos y permisos
2. Contraseñas
3. Virtualización de sistemas operativos
4. Procesos del sistema operativo
5. El arranque
6. Hibernación
7. Las RPC
8. Logs, actualizaciones y copias de seguridad
9. Tecnología WEB Cliente - Servidor
10. Seguridad WEB
11. SQL Injection

12.Seguridad CAPTCHA
13.Seguridad Akismet
14.Consejos de seguridad WEB

UNIDAD DIDÁCTICA 6. ASPECTOS INTRODUCTORIOS DEL CLOUD COMPUTING

1.Orígenes del cloud computing
2.Qué es cloud computing
    1.- Definición de cloud computing
3.Características del cloud computing
4.La nube y los negocios
    1.- Beneficios específicos
5.Modelos básicos en la nube

UNIDAD DIDÁCTICA 7. CONCEPTOS AVANZADOS Y ALTA SEGURIDAD DE CLOUD COMPUTING

1.Interoperabilidad en la nube
    1.- Recomendaciones para garantizar la interoperabilidad en la nube
2.Centro de procesamiento de datos y operaciones
3.Cifrado y gestión de claves
4.Gestión de identidades

UNIDAD DIDÁCTICA 8. SEGURIDAD, AUDITORÍA Y CUMPLIMIENTO EN LA NUBE

1.Introducción
2.Gestión de riesgos en el negocio
    1.- Recomendaciones para el gobierno
    2.- Recomendaciones para una correcta gestión de riesgos
3.Cuestiones legales básicas. eDiscovery
4.Las auditorías de seguridad y calidad en cloud computing
5.El ciclo de vida de la información
    1.- Recomendaciones sobre seguridad en el ciclo de vida de la información

UNIDAD DIDÁCTICA 9. CARACTERÍSTICAS DE SEGURIDAD EN LA PUBLICACIÓN DE PÁGINAS WEB

1.Seguridad en distintos sistemas de archivos.
    1.- Sistema operativo Linux.
    2.- Sistema operativo Windows.
    3.- Otros sistemas operativos.
2.Permisos de acceso.
    1.- Tipos de accesos
    2.- Elección del tipo de acceso
    3.- Implementación de accesos
3.Órdenes de creación, modificación y borrado.
    1.- Descripción de órdenes en distintos sistemas
    2.- Implementación y comprobación de las distintas órdenes.

UNIDAD DIDÁCTICA 10. PRUEBAS Y VERIFICACIÓN DE PÁGINAS WEB

1.Técnicas de verificación.
    1.- Verificar en base a criterios de calidad.
    2.- Verificar en base a criterios de usabilidad.
2.Herramientas de depuración para distintos navegadores.
    1.- Herramientas para Mozilla.
    2.- Herramientas para Internet Explorer.
    3.- Herramientas para Opera.
    4.- Creación y utilización de funciones de depuración.
    5.- Otras herramientas.
3.Navegadores: tipos y «plug-ins».
    1.- Descripción de complementos.
    2.- Complementos para imágenes.

3.- Complementos para música.
4.- Complementos para vídeo.
5.- Complementos para contenidos.
6.- Máquinas virtuales.

UNIDAD DIDÁCTICA 11. LOS FALLOS DE APLICACIÓN

1.Introducción en los fallos de aplicación
2.Los conceptos de código ensamblador y su seguridad y estabilidad
3.La mejora y el concepto de shellcodes
4.Buffer overflow
5.Fallos de seguridad en Windows

PARTE 3. ANÁLISIS DE MALWARE

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN

1.¿Qué es un Malware?
2.Tipos de Malware
1.- Backdoor
2.- Ransomware y locker
3.- Stealer
4.- Rootkit

UNIDAD DIDÁCTICA 2. ESCENARIO DE INFECCIÓN Y TÉCNICAS DE COMUNICACIÓN

1.Ejecución de un archivo adjunto
2.Clic desafortunado
3.Apertura de un documento infectado
4.Ataques informáticos
5.Ataques físicos: infección por llave USB
6.Introducción a las técnicas de comunicación con el C&C
1.- Comunicación a través de HTTP/HTTPS/FTP/IRC
2.- Comunicación a través e-mail
3.- Comunicación a través una red punto a punto
4.- Fast flux y DGA (Domain Generation Algorithms)

UNIDAD DIDÁCTICA 3. OBTENCIÓN Y ANÁLISIS DE INFORMACIÓN

1.Analizando datos del registro
2.Analizando datos del registros de eventos
3.Analizando archivos ejecutados durante el arranque
4.Analizando sistema de archivos

UNIDAD DIDÁCTICA 4. FUNCIONALIDADES DE LOS MALWARES. COMO OPERAR ANTE AMENAZAS

1.Técnicas de persistencia
2.Técnicas de ocultación
3.Malware sin archivo
4.Evitar el UAC
5.Fases para operar ante amenzas:
1.- Reconocimiento
2.- Intrusión
3.- Persistencia
4.- Pivotar
5.- Filtración
6.- Pistas dejadas por el atacante

UNIDAD DIDÁCTICA 5. ANÁLISIS BÁSICO DE ARCHIVOS

1.Análisis de un archivo PDF
2.Extraer el código JavaScript
3.Desofuscar código JavaScript

4.Análisis de un archivo de Adobe Flash
1.- Extraer y analizar el código ActionScript
5.Análisis de un archivo JAR
6.Análisis de un archivo de Microsoft Office
1.- Herramientas que permiten analizar archivos de Office

UNIDAD DIDÁCTICA 6. REVERSE ENGINEERING

1.¿Qué es Reverse Engineering?
2.Ensamblador x86
3.Ensamblador x64
4.Análisis estático
1.- IDA Pro
2.- Radare2
3.- Técnicas de análisis
5.Análisis dinámico
1.- WinDbg
2.- Análisis del núcleo de Windows
3.- Límites del análisis dinámico y conclusión

UNIDAD DIDÁCTICA 7. OFUSCACIÓN: INTRODUCCIÓN Y TÉCNICAS

1.¿Qué es la ofuscación?
2.Ofuscación de cadenas de caracteres
3.Ofuscación mediante la API de Windows
4.Packers
5.Otras tipos de técnicas ofuscación

UNIDAD DIDÁCTICA 8. DETECCIÓN Y CONFINAMIENTO

1.Primeros pasos en la detección y confinamiento
2.Compromiso de red: Indicadores
1.- Presentación a los indicadores
2.- Proxys
3.- Sistemas de detectores de intrusión
3.Tips de firmas de archivo
1.- Firmas (o Hash)
2.- Firmas con YARA
3.- Firmas con ssdeep
4.Detección y erradicación a través de ClamAV
1.- Instalación
2.- Usando ClamAV: Funciones básicas

UNIDAD DIDÁCTICA 9. OPENIOC

1.Introducción a OpenIOC
2.Pimeros pasos con
3.Interfaz gráfica de edición
4.Detección