



Máster en Reversing, Análisis de Malware y Bug Hunting

Conociendo el comportamiento de las aplicaciones maliciosas.



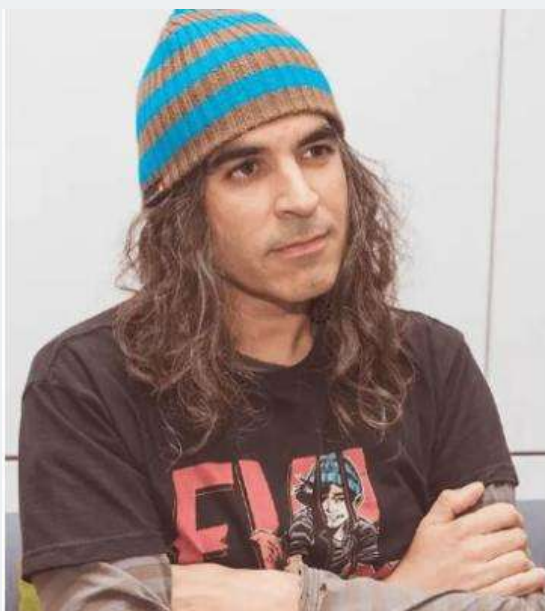


UCAM
UNIVERSIDAD
CATÓLICA DE MURCIA



ENIIT INNOVA IT
BUSINESS SCHOOL

Chema Alonso colabora como Mentor de los Programas Máster del Campus Internacional de Ciberseguridad



Durante el curso 2021-2022 Chema Alonso realizará labores de mentorización de los programas de máster para ayudar a definir los contenidos formativos con sus conocimientos, experiencia, valores y habilidades en el área

de seguridad informática en particular, y en el de tecnología de la empresa en general. Además, propondrá tres Trabajos de Fin de Máster para que algunos alumnos puedan trabajar en alguna de sus innovadoras ideas en materia de seguridad informática, que le han llevado a firmar más de una decena de patentes a lo largo de su vida profesional, así como a crear decenas de productos, servicios y papers de investigación.

Descubre más aquí: <https://eniit.es/chema-alonso-mentor-del-campus-internacional-de-ciberseguridad/>

Sube al tren de la Innovación

El mundo de la Ciberseguridad se está profesionalizando de la mano de procesos de transformación digital altamente innovadores.

La Ciberseguridad cada vez, toma una mayor importancia y debido a ello nace de la necesidad de impartir formación para analizar el comportamiento de las aplicaciones maliciosas y poder subsanar su ataque e incluso prevenirlo

Una disciplina de máxima actualidad y en continua evolución

Las aplicaciones maliciosas e incluso el Reversing forman ya parte de nuestro lenguaje cotidiano.

La privacidad, los ataques, las vulnerabilidades, el malware, ciberspionaje... son conceptos que se han incorporado a nuestro día a día no sólo desde el punto de vista del ciudadano, sino desde la perspectiva de los gobiernos, organizaciones, dirigentes, **ingenieros, estrategias... internet y las redes** están tan integradas en tantas disciplinas, que la seguridad resulta transversal a todas las áreas e imprescindible en la inmensa mayoría.

Desde principios de este siglo con ataques esporádicos y artesanales a usuarios y sistemas, hasta las ciberguerras y espionaje consolidado que actualmente se libra en la Red: la tendencia a considerar la seguridad como espina dorsal que debe vertebrar todas las comunicaciones entre personas y dispositivos, es cada vez mayor.

1 Programa Innovador

Con el objetivo de adaptarse a una realidad donde el malware y el software han ganado en complejidad

Dentro de la gran variedad de perfiles que puede aglutinar el título de “Experto en ciberseguridad”, el “Reversing” o la capacidad de analizar los programas (especialmente si hablamos de malware) es a su vez una de las aptitudes más demandadas. Las ciberarmas y amenazas en general de hoy nos atacan en forma de programas y código, y pocas veces vienen con manual de instrucciones.

2 Disciplina en auge

La Seguridad Informática se ha convertido en una de las profesiones más cotizadas.

Mediante una combinación equilibrada de teoría y práctica los estudiantes serán capaces de hacerse las preguntas correctas ante un incidente, aplicar las medidas de análisis más eficaces, analizar los datos asociados, mitigar los daños en el sistema operativo y analizar la red en busca de amenazas.

Dirección Académica

Grandes profesionales al servicio de la Ciberseguridad:



Sergio de los Santos

Coordinador del área de Innovación y Laboratorio de Telefónica Tech. Desde 2000 ha trabajado como auditor y coordinador técnico, ha escrito un libro sobre la historia de la seguridad, y tres libros más técnicos sobre hacking y seguridad en Windows.



¿Y después de finalizar el Máster?

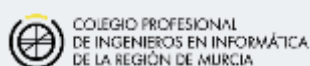
Formamos profesionales que lideren la transformación a través de la aplicación de la Ciberseguridad.

Al finalizar el master, los alumnos contarán con el potencial suficiente para cubrir algunos de los perfiles más demandados en el campo de la ciberseguridad, de la mano de profesionales que se dedican en su día a día a desarrollar las habilidades que van a impartir para desempeñar su trabajo.

Animate a formar parte de un Máster único, desarrollado por profesionales de máximo nivel en el sector, certificado por la UCAM y apoyado por las principales entidades del mundo de la Ciberseguridad. Ven a vivir esta aventura.



El Máster, cuenta con el apoyo de las principales empresas y entidades de la Industria.



Máster en Reversing, Análisis de Malware y Bug Hunting

Objetivos pedagógicos

Entre los principales objetivos del Máster, podemos destacar:

- Ofrecer una visión realista sobre los diferentes campos del Reversing actual.
- Comprender el análisis de código desde sus cimientos, para construir un discurso completo que abarque desde el código fuente hasta las muestras más complejas y la inteligencia asociada a los incidentes.
- Actualizar la información sobre ciberseguridad y reversing al verdadero estado del arte del momento actual.
- Incorporar conocimiento demandado actualmente en la industria, como análisis de código, protocolos, redes, sandboxes y OSINT.
- Comprender no solo el punto de vista del atacado, sino del atacante



Máster en Reversing, Análisis de Malware y Bug Hunting

Competencias

Una vez finalizado el Máster, nuestros estudiantes serán capaces de:

- Analizar incidentes de seguridad que comprendan código dañino desde un punto de vista profesional y realista.
- Comprender el malware actual y aplicar las contramedidas más eficaces.
- Conocer los entornos de análisis más comunes y usarlos eficientemente para el reversing de muestras.
- Realizar investigaciones online y la recopilación de datos asociadas a una muestra.
- Conocer las técnicas habituales de análisis estático y dinámico y cómo proceder ante cada tipo de malware.
- Comprender cómo funciona el sistema operativo a varios niveles de privilegios en memoria.
- Conocer los principales algoritmos criptográficos.



¿A quién va dirigido el Máster?

Profesionales como programadores o desarrolladores

El Máster, va dirigido a Titulados Superiores, programadores, desarrolladores y arquitectos, enfocados en la seguridad como requisito.

Igualmente a Analistas de seguridad e inteligencia, Consultores y gestores de seguridad integral, Pentesters y auditores de seguridad, Administradores en general con foco en la seguridad como elemento clave y a cualquier persona que, con perfil técnico, esté interesado en orientar o reorientar su Carrera profesional en el mundo de la Ciberseguridad.

Titulados Superiores



Programadores, Desarrolladores enfocados en la Ciberseguridad

Para exprimir al máximo este programa formativo, es necesario contar con un perfil orientado a la Seguridad Informática: Titulados Superiores, programadores, desarrolladores y arquitectos, enfocados en la seguridad como requisito.

Pentesters, Auditores



Consultores. Gestores de Seguridad

Analistas de Seguridad e inteligencia, Consultores y gestores de seguridad integral, Pentesters y auditores de seguridad, Administradores en general con foco en la seguridad como elemento clave o cualquier persona interesada en orientar su carrera hacia la Ciberseguridad.



En modalidad 100% on-line

Preparado para poder ser cursado por profesionales y estudiantes para que puedan compaginar el Máster con sus actividades

A través del Aula Virtual, los participantes podrán: acceder a los contenidos del Máster, tanto a los manuales de las asignaturas como a los audiovisuales; realizar y entregar las actividades de evaluación; consultar los materiales complementarios y de refuerzo; interactuar con el claustro docente y consultar los feedbacks a las distintas tareas; participar en las actividades colaborativas propuestas; acceder a las herramientas de tutorización, tanto síncronas como asíncronas; consultar su histórico y el libro de calificaciones. Además, tendrán acceso a tutorías en directo y MasterClass impartidas por profesionales de máximo y reconocido prestigio en el sector.

Metodología Learning By Doing

Avalados por más de 20 años de experiencia, Nuestra metodología de **se sustenta sobre la base al “Learning by doing”, combinando la** exposición y estudio de contenidos teóricos enfocado a la realización de tareas prácticas del mundo real, en este caso, trabajando, de primera mano, todos aquellos aspectos esenciales del mundo de la Ciberseguridad, estudiados a lo largo de los distintos módulos del Máster.

A lo largo de la impartición, tanto por medio de los tutores como de la Dirección Académica, se fomentan la interacción, la participación y la colaboración de los estudiantes, tanto con el equipo docente como con sus propios compañeros.

Certificado por la UCAM



Certificado por la UCAM como Máster en Reversing, Análisis de Malware y Bug Hunting

El Máster está Certificado por la Universidad Católica de Murcia (UCAM) como “Máster en Reversing, Análisis de Malware y Bug Hunting”.

Además, está impartido por expertos de las principales compañías de Ciberseguridad, el Claustro docente del Máster en Reversing, Análisis de Malware y Bug Hunting está formado por profesionales de reconocido prestigio y contrastada experiencia en Proyectos de Ciberseguridad que más adelante presentaremos.



Libros de la editorial Oxword

Durante la realización del Máster en Reversing, Análisis de Malware y Bug Hunting recibirás de manera TOTALMENTE GRATUITA los libros de la editorial Oxword:

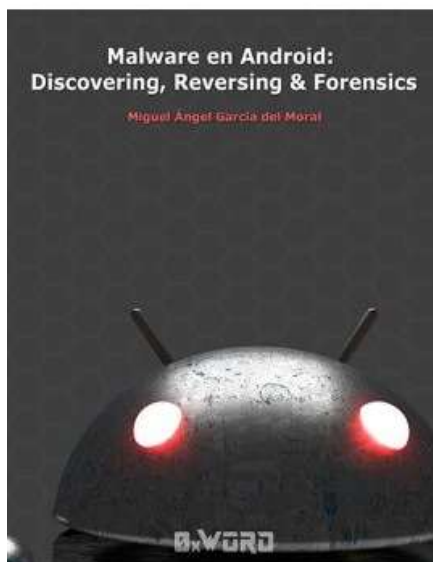
- Bug Bounty: De profesión cazarecompensas (Pablo García)

<https://Oxword.com/es/libros/191-bug-bounty-de-profesion-cazarecompensas.html>



- Malware en Android: Discovering, Reversing and Forensics (Miguel Ángel García)

<https://Oxword.com/es/libros/76-malware-en-android-discovering-reversing-and-forensics.html>



Plan de Estudios: Máster en Reversing, Análisis de Malware y Bug Hunting

A continuación, te presentamos la información completa acerca del programa y los módulos que componen el Máster en Reversing, Análisis de Malware y Bug Hunting de ENIIT, el Campus Internacional de Ciberseguridad y la UCAM.

Es información muy detallada, pero preferimos que tengas la máxima información para tomar la decisión de embarcarte en esta aventura.

Módulo 1. Criptografía y criptoanálisis

[5 Créditos ECTSs – 125 horas]

La criptografía ha jugado un papel fundamental en la historia en relación con la protección de secretos y ha evolucionado a lo largo del tiempo, pasando de los sencillos algoritmos iniciales a sistemas mucho más complejos con un fuerte fundamento matemático.

Este módulo va encaminado a que el alumno conozca los diferentes aspectos de la criptografía, haciendo un repaso de los principales algoritmos criptográficos, de los que se analizará su funcionamiento y características, así como su seguridad y

puntos débiles que pueden permitir que se realice un criptoanálisis. El repaso de estos algoritmos se inicia brevemente con los clásicos y a continuación se estudia la criptografía simétrica, distinguiendo entre la criptografía en flujo y la criptografía en bloque. Se analizarán los algoritmos más importantes, así como el estándar de cifrado actual.

Además, se analizan las funciones hash y criptografía de clave asimétrica. En este apartado se incluye el estudio de la firma digital, certificados digitales e infraestructuras de clave pública (PKI).



Programa de la asignatura

- Criptografía clásica: versiones de los cifradores clásicos todavía en uso y cómo romperlos.
- Criptografía de clave secreta: cifradores en flujo y cifradores de bloque.
- Criptoanálisis de clave pública.
- Funciones hash y firmas digitales.

Objetivos

- Conocer los principales algoritmos criptográficos, así como su seguridad, desde los algoritmos clásicos, pasando por los simétricos y algoritmos asimétricos.
- Conocer aplicaciones actuales de la criptografía y fundamentos del criptoanálisis
- Conocer los principales algoritmos criptográficos y sus posibilidades desde el punto de vista del criptoanálisis.
- Conocer las herramientas necesarias para realizar un criptoanálisis a textos, datos o flujos cifrados.
- Disponer de la capacidad de análisis de datos y potencial recuperación de la información ante un ataque criptográfico o caso de ocultación de datos.

Competencias, aptitudes y destrezas

- Conocer qué es la criptografía, el criptoanálisis y las diferentes ramas que abarcan.
- Conocer los principales algoritmos criptográficos.
- Conocer la seguridad de los algoritmos criptográficos, así como los puntos débiles que los pueden hacer vulnerables.
- Saber distinguir las fortalezas y debilidades de cada tipo de algoritmo.
- Conocer algunas de las principales aplicaciones de la criptografía.

Bibliografía

- Al Sweigart, Cracking Codes with Python: An Introduction to Building and Breaking Ciphers, No Starch Press (2018).
- Christof Paar, Jan Pelzl, Understanding cryptography: a textbook for students and practitioners, Springer-Verlag Berlin Heidelberg (2009).
- Jean-Philippe Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press (2017).
- Joachim von zur Gathen, CryptoSchool, Springer (2015).
- Joshua Holden, The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption, Princeton University Press (2017).
- Serge Vaudenay, A Classical Introduction to Cryptography: Applications for Communications Security, Springer (2005).
- William Stallings, Cryptography and Network Security: Principles and Practice, Pearson (2017)

Módulo 2. Entornos de análisis de malware

[5 Créditos ECTSs – 125 horas]

Analizar un programa en general y el malware en particular requiere, indefectiblemente, un entorno adecuado de análisis. No sólo el sistema operativo adecuado, sino también las redes, los programas y, sobre todo, el aislamiento.

Para todo ello existen multitud de entornos (principalmente virtuales) para poder analizar programas de la forma óptima y sobre todo, segura. En análisis de malware, se ha convertido durante los últimos años, en un servicio cada vez más necesario para comprender el alcance que ha tenido o puede

llegar a tener este tipo de amenazas. Inicialmente este análisis de malware se realizaba de manera manual utilizando herramientas como puedan ser depuradores, analizadores de memoria, comportamiento del sistema operativo o tráfico de red.

En este módulo se estudiará como realizar análisis de malware automatizado utilizando diferentes tipos de sandboxes, como interpretar los resultados, problemas asociados a la utilización de sandboxes y se profundizará en detalles internos de cómo funcionan estas sandboxes y cómo podemos modificarlas para incorporar nuestra funcionalidad.



Programa de la asignatura

- Introducción a los entornos de Sandbox.
- Instalación y configuración de Cuckoo Sandbox.
- Instalación y configuración de CAPE Sandbox.
- Evaluación de sandboxes ante malware evasivo
- Sandbox internals.

Objetivos

- Comprender las herramientas disponibles para disponer de un entorno óptimo de análisis automatizado
- Configurar los entornos y diferentes herramientas para poder recolectar y analizar los resultados obtenidos.
- Adquirir conocimientos avanzados sobre sandboxes.
- Configurar los entornos para evitar la detección y maximizar los resultados.
- Comprender como funciona una sandbox internamente.

Competencias, aptitudes y destrezas

- Ser capaz de montar el entorno óptimo para cada análisis.
- Conocer cómo recopilar y analizar la información recolectada en cada entorno.
- Conocer las características de cada entorno y las posibilidades de cada sandbox.

Bibliografía

- Cuckoo Malware Analysis Por: Digit Oktavianto, Iqbal Muhardianto

Módulo 3. Análisis de código fuente

[6 Créditos ECTSs – 150 horas]

La tarea central de la ingeniería inversa es entender cómo funciona el programa objeto de análisis y su entorno de ejecución (librerías, recursos, etc.) Una de las aproximaciones empleadas es el análisis estático.

. Esto es: el estudio de una unidad de ejecución antes de que esta sea convertida en un proceso. Para ello, es necesario obtener el

código a ejecutar, ya sea un binario nativo, una librería o código objeto para una máquina virtual.

En ocasiones, ya sea porque se ha publicado bajo una licencia abierta o por que ha sido liberado mediante una filtración, es posible disponer del código fuente de un determinado programa. En contraposición, aunque no se disponga de las fuentes, existen diversas técnicas para transformar el código objeto en una forma más entendible (o de más alto nivel) para facilitar el análisis y estudio.



Programa de la asignatura

- Análisis y estudio del código fuente, entornos y herramientas.
- Decompilación y desensamblado.
- Análisis de código fuente en Javascript.
- Análisis del código fuente en C y C++.
- Análisis del código ensamblador.

Objetivos

- Conocer las diferentes técnicas a emplear para desensamblar o decompilar un programa.
- Detectar y reaccionar correctamente frente a contramedidas de ofuscación.
- Saber orientarse en la navegación del código y entender su función.
- Detectar potenciales fallos de seguridad mediante la lectura del código fuente.
- Conocer las principales características de los lenguajes de alto nivel .NET, Java y Python.
- Conocer las principales características de los lenguajes de bajo nivel, ensamblador, C y C++.
- Conocer herramientas y entornos que faciliten el analizar el código fuente de en búsqueda de vulnerabilidades en diferentes lenguajes de programación.

Competencias, aptitudes y destrezas

- Entender la sintaxis y características principales de los lenguajes de programación de alto nivel.
- Entender la sintaxis y características principales de los lenguajes de programación de bajo nivel.
- Saber desensamblar y decompilar código objeto, además de poder interpretar la lógica subyacente del producto obtenido.
- Conocer la seguridad de los diferentes lenguajes de programación en sus estructuras básicas, funciones, modelos, etc.
- Interpretar correctamente el código fuente de los programas.

Bibliografía

- Practical Binary Analysis - NoStarch Press, Dennis Andriesse - 2018
- Practical Reverse Engineer - Wiley, Bruce Dang et al - 2014

Módulo 4. Vulnerabilidades y herramientas de análisis de malware.

[6 Créditos ECTSs – 150 horas]

Una vulnerabilidad es un fallo en el código del software o en su configuración que provoca un comportamiento no esperado o erróneo, que puede llevar a comprometer la seguridad de un equipo informático

Las consecuencias pueden ser desde una denegación de servicio hasta una ejecución arbitraria de código pasando por una elevación de privilegios. Las vulnerabilidades y los fallos de seguridad son la piedra angular que

habitualmente sostienen los fundamentos de ataques a todas las escalas.

El malware en general suele aprovechar vulnerabilidades para poder ejecutarse en el sistema, replicarse o tomar el control. Por tanto, conocer qué es una vulnerabilidad, cómo funciona o de qué herramientas dispone el sistema operativo para mitigarlas, resulta una parte fundamental del reversing.

También se profundizará sobre las diferentes herramientas necesarias para realizar un reversing, sus posibilidades y funcionalidades a través de ejercicios prácticos de detección de vulnerabilidades para su futura explotación.



Programa de la asignatura

- Introducción al Olly e Immunity.
- Introducción al IDA.
- Introducción a Radare.
- Vulnerabilidades, exploits y payloads. Detección y análisis.
- Funciones prohibidas por Microsoft.
- Otras herramientas.

Objetivos

- Entender los principales tipos de vulnerabilidades y cuáles son los criterios de la seguridad de la información a los que afecta.
- Conocer las herramientas de análisis de malware más habituales.
- Comprender qué es una vulnerabilidad, un exploit y un payload.
- Detección de funciones potencialmente vulnerables y detectar si son explotables.
- Programar un exploit y configurar diferentes payloads.
- Familiarizarse con el uso de las herramientas más habituales del mercado y aprovechar sus funcionalidades de análisis.

Competencias, aptitudes y destrezas

- Ser capaz de entender cómo funciona la explotación de las vulnerabilidades de software más comunes.
- Aprovechar las características de las herramientas de ingeniería inversa para detectar y explotar vulnerabilidades.

Bibliografía

- The Shellcoder's Handbook: Discovering and Exploiting Security Holes:
https://www.amazon.com/ShellcodersHandbookDiscoveringExploitingSecurity/dp/047008023X/ref=pd_sbs_14_t_0?_encoding=UTF8&psc=1&refRID=PTGX1SNTXE1J8D077E42
- Hacking: The Art of Exploitation, 2nd Edition:
https://www.amazon.com/HackingArtExploitationJonErickson/dp/1593271441/ref=pd_sim_14_7?_encoding=UTF8&psc=1&refRID=PTGX1SNTXE1J8D077E42
- A Guide to Kernel Exploitation: Attacking the Core:
<https://www.amazon.com/Guide-Kernel-Exploitation-Attacking-Core/dp/1597494860>
- The Hacker Playbook 2: Practical Guide To Penetration Testing: https://www.amazon.com/Hacker-Playbook-Practical-PenetrationTesting/dp/1512214566/ref=pd_sim_14_1?_encoding=UTF8&psc=1&refRID=KBESC9Y5HVR35D28YKJ3
- Radare2 book: <https://radare.gitbooks.io/radare2book/>
- IDA Pro Book:
<https://repo.zenksecurity.com/Reversing%20.%20cracking/The%20IDA%20Pro%20Book2nd%20Edition-2011.pdf>

Módulo 5. Análisis de comportamientos y metodología OSINT.

[6 Créditos ECTSs – 150 horas]

La información presente en fuentes abiertas es un componente fundamental para el analista de seguridad. La inteligencia de fuentes abiertas (OSINT) se corresponde con un tipo de inteligencia elaborada a partir de información que se obtiene de fuentes de información de carácter público.

La definición de fuentes abiertas acapara una gran variedad de contenidos disponibles en multitud de soportes (papel, fotográfico, **magnético, óptico...**) y que se transmite por diversos medios (impreso, sonoro, audiovisual...) y a los que se puede acceder en modo digital o no, pero que ha sido puesto a disposición pública, con independencia de que

esté comercializado, se difunda por canales restringidos o sea gratuito. Por este motivo, el hecho de que esta información sea pública no implica necesariamente que se encuentre en un estado aceptable como para ser de utilidad para un analista en ciberseguridad.

En el ámbito del ciberespacio es necesario que el analista conozca cuáles son las herramientas a su disposición para trabajar con la información disponible a través de este tipo de fuentes con el objetivo de conseguir maximizar los recursos a su alcance a la hora de clarificar el origen de cualquier acción que tiene lugar en la red y entender mejor el quién y el porqué de cualquier incidente de seguridad. En el mundo del reversing, analizar la información disponible más allá del objeto analizado es tan importante, como conocer las debilidades intrínsecas al comportamiento humano.



Programa de la asignatura

- Introducción al OSINT en internet.
- Usos avanzados de buscadores.
- Metodologías para la realización de ejercicios de atribución.
- Extracción de metadatos y análisis de distintos tipos de ficheros.
- OPSEC y anonimato orientado a las investigaciones en la red.

Objetivos

- Entender la estructura de internet y las limitaciones a la hora de obtener información de las distintas fuentes que se presentan.
- Desarrollar métodos de trabajo que les permitan entender el proceso de atribución de una acción que tiene lugar en la red.
- Adquirir conocimientos avanzados sobre el uso de los buscadores principales y de los mecanismos existentes para indexar información.
- Conocer la información que es posible obtener a partir de los diferentes inputs de información que se le pueden presentar en el transcurso de una investigación.
- Desarrollar una concienciación a la hora de controlar la información que un analista expone sobre sí mismo a la hora de investigar.

Competencias, aptitudes y destrezas

- Ser capaz de realizar búsquedas avanzadas en los principales buscadores genéricos y específicos de la red.
- Conocer la información que se puede extraer de un fichero en función de su naturaleza y de los metadatos que contiene.
- Manejar con soltura las soluciones existentes para prevenir la filtración de información sobre su persona.

Bibliografía

- "Open Source Intelligence Techniques". Michael Bazzel, 5th Edition (2016).
<https://inteltechniques.com/book1.html>
- "Google Hacking for Penetration Testers". Johnny Long, Bill Gardner, Justin Brown, Syngress.
<https://www.amazon.com/gp/product/1597491764?ie=UTF8&tag=ihackstuff20&linkCode=as2&camp=1789&creative=9325&creativeASIN=%201597491764>
- "Hacking con buscadores: Google, Bing & Shodan + Robtex". Enrique Rando, OxWord, 3ª Edición. <http://Oxword.com/es/libros/20-libro-hacking-buscadores-google-bing-sodan-robtex.html>
- "The Tao of Open Source Intelligence". Stewart K. Bertram.
<https://www.jstor.org/stable/j.ctt155j4bh>
- "Técnicas analíticas estructuradas para el análisis de inteligencia". Randolph H. Pherson y Richards J. Heuer. <https://www.amazon.es/T%C3%89CNICAS-ANAL%C3%8DTICAS-ESTRUCTURADASAN%C3%81LISIS-INTELIGENCIA/dp/8415271670>
- "Automating Open Source Intelligence: Algorithms for Osint". Robert Layton, Paul A. Watters, <https://www.goodreads.com/book/show/26260622-automating-open-source-intelligence>
- "Elasticsearch Essentials". Bharvi Dixit Packet: https://www.amazon.com/gp/product/1784391018/ref=as_li_qf_sp_asin_il_tl?ie=UTF8&tag=w_hatpixel20&camp=1789&creative=9325&linkCode=as2&creativeASIN=1784391018&linkId=7c3689613866114e08fcb8b1360d088c
- "Glosario de inteligencia". Esteban Navarro, Miguel Ángel. Ministerio de Defensa, 2007

Módulo 6. Reversing en sistemas operativos (Windows).

[6 Créditos ECTSs – 150 horas]

Cuando se analizan o desarrollan programas, encontraremos en la mayoría de las ocasiones que nos circunscribimos en el modo usuario puesto que es en el que se ejecuta la mayoría de software que conocemos del sistema.

Sin embargo, existen un campo muy importante para definir y entender un sistema operativo, obviado en ocasiones en el mundo del reversing, relacionado con conceptos como “KERNEL”, “BIOS”, “MODO PROTEGIDO”, en el que resulta esencial conocer sus características y posibilidades, entender su motivación y por qué son necesarios.

En el mundo del reversing y malware, el conocimiento de lo que podríamos llamar “el

más allá del modo usuario” sí es una competencia que completará las habilidades requeridas para un profesional del sector, por varias razones. Por ejemplo, para poder hacer frente a uno de los tipos de malware más peligrosos que existen son los rootkits y los bootkits que éstos viven fuera del mundo usuario.

Y es que en general, para conocer el malware o cualquier programa y entender qué hace y cómo se hace, es imprescindible conocer primero cómo funciona el sistema operativo a nivel de gestión de recursos, privilegios, etc. A su vez, entender este funcionamiento permite conocer cómo trabaja el malware que, en la mayoría de las ocasiones, se basa a su vez en este conocimiento para aprovechar y exprimir las capacidades del sistema que infecta.



Programa de la asignatura

- BIOS / UEFI.
- Transición hacia el modo. kernel
- Modo usuario / Modo kernel.
- Desarrollo de drivers.
- Debug y análisis del sistema operative.

Objetivos

- Entender el funcionamiento avanzado de los sistemas operativos, en especial de Windows a la hora de manejar memoria y privilegios.
- Conocer las herramientas y fórmulas más habituales para analizar el comportamiento del sistema en modo kernel.
- Comprender qué procesos ocurren desde que encendemos un ordenador hasta que se ejecuta el kernel del Sistema Operativo.
- Comprender cómo funciona el sistema operativo en varios niveles.
- Programar drivers, interrupciones, etc.
- Familiarizarse con el uso de las herramientas más habituales para analizar el sistema operativo a bajo nivel.

Competencias, aptitudes y destrezas

- Ser capaz de entender cómo funciona un sistema operativo a nivel de sistema y gestión de memoria y privilegios.
- Aprovechar las características de las herramientas de análisis de sistema para analizar el comportamiento de los programas.
- Ampliar el set de herramientas disponibles para tareas de reversing.
- Enseñar técnicas que permitan desarrollar nuevas herramientas personalizadas.

Bibliografía

- Windows Internals: Mark E. Russinovich, Alex Ionescu
- Windows Kernel Programming: Pavel Yosifovich
- The rootkit Arsenal: Bill Blunden
- Rootkits and Bootkits: Reversing Modern Malware and Next Generation Threats: Alex Matrosov

Módulo 7. Debug y análisis del sistema operativo (Linux).

[5 Créditos ECTSs – 125 horas]

No todo el malware se produce para atacar a sistemas Windows. Aunque en menor proporción, los sistemas UNIX en general pueden contener código malicioso y en ciertos entornos resulta esencial proteger ciertos sistemas de esta amenaza.

Para conseguirlo es necesario entender cómo funciona el sistema operativo a todos los niveles, cómo gestiona la memoria, las tareas, los procesos y sobre todo, qué registros o indicios pueden denotar una anomalía. De esta manera es posible conocer qué, cómo y cuándo un programa ha podido alterar el sistema.

En este módulo se impartirán los fundamentos del sistema operativo UNIX, permisos,

procesos, tareas, registros, memoria, etc. Desde un punto técnico y práctico para poder entender cómo podría atacar un programa malicioso y descubrir sus acciones.

Desde rootkits hasta scripts, se describirán las acciones más habituales que utiliza el malware para ocultarse, pasar desapercibido o reproducirse. En estos casos, el análisis del sistema es tan fundamental o más que el análisis del binario o programa infeccioso a la hora de comprender la amenaza.

Se impartirán los conocimientos necesarios para auditar un sistema UNIX en general y para conocer las posibilidades de que haya sido comprometido, así como un repaso del bastionado en general para evitar potenciales infecciones.



Programa de la asignatura

- Introducción al sistema operativo.
- Modo usuario / Modo kernel.
- Debug y análisis del sistema operativo.
- Rootkits y otros tipos de infecciones.

Objetivos

- Entender el funcionamiento avanzado de los sistemas operativos UNIX.
- Conocer las herramientas y fórmulas más habituales para analizar el comportamiento del sistema tanto en modo kernel como en modo usuario.
- Conocer las herramientas y fórmulas más habituales para analizar el impacto de los programas en el sistema operativo.
- Comprender cómo funciona el sistema operativo a varios niveles de privilegios en memoria.
- Entender la organización del sistema operativo en general.
- Familiarizarse con el uso de las herramientas más habituales para analizar un sistema operativo UNIX a bajo nivel.

Competencias, aptitudes y destrezas

- Ser capaz de entender cómo funciona un sistema operativo UNIX a nivel privilegios, memoria y registros.
- Aprovechar las características de las herramientas de análisis de sistema para analizar el impacto de los programas en él, así como reconocer los principales tipos de amenazas y ataques a tener en cuenta.

Bibliografía

- http://www.makelinux.net/kernel_map/
- <https://www.os-book.com/OS10/index.html>
- <https://0xword.com/libros/55-linux-exploiting.html>
- <https://www.agapea.com/libros/Hacking-Tecnicas-fundamentales-9788441524699-i.htm>
- <https://github.com/mzet-/linux-exploit-suggester>
- <https://shenaniganslabs.io/2019/02/13/Dirty-Sock.html>
- <https://github.com/xairy/linux-kernel-exploitation>

Módulo 8. Reversing sistemas operativos (móviles).

[4 Créditos ECTSs – 100 horas]

El malware para dispositivos móviles es mucho más habitual en estos días en sistemas Android que otros sistemas operativos como iPhone (y casi inexistente en el resto debido a su escasa penetración). Suponen una amenaza real porque permiten no sólo la explotación de los recursos de la víctima como puede ocurrir en el escritorio, sino el espionaje de las comunicaciones.

En este módulo se impartirán los fundamentos del sistema operativo Android, permisos, procesos, aplicaciones, firmas, seguridad, etc. Desde un punto de vista técnico y práctico para

poder entender cómo suelen funcionar los ataques bajo este sistema operativo, muy diferentes a los sistemas de escritorio en general tanto en fórmula como en filosofía.

Se mostrarán las amenazas más habituales, además de cómo reconstruir un entorno válido en el que poder analizar este malware tan específico. En él, se realizarán prácticas de análisis de malware específico de Android, lo que incluye descarga, decompilación, análisis, desofuscación, etc.

Se impartirán los conocimientos necesarios para analizar malware para Android en general y para conocer el ecosistema de infecciones más típicos, así como un repaso del bastionado en general para evitar potenciales infecciones.



Programa de la asignatura

- Introducción al sistema operativo y a las apps.
- Preparación del entorno de análisis.
- Análisis de malware para Android.
- Introducción al malware para IOS.

Objetivos

- Entender el funcionamiento avanzado del malware para Android.
- Conocer las herramientas y fórmulas más habituales para analizar el malware en Android.
- Disponer de un entorno de trabajo seguro donde realizar los análisis.
- Comprender cómo funciona el sistema operativo Android y el malware que le amenaza.
- Familiarizarse con el uso de las herramientas necesarias para el análisis de malware en Android, así como con la preparación de un entorno adecuado.

Competencias, aptitudes y destrezas

- Ser capaz de analizar y entender cómo funciona Android y el malware disponible en markets tanto oficiales como no oficiales.
- Implementar la infraestructura necesaria para ese análisis de forma segura.

Bibliografía

- Altomare, D. (2015). Android Reverse Engineering. <http://www.fastqueue.com/android-reverse-engineering-101-part-1/>
- Estructura de una aplicación Android <http://www.tuprogramacion.com/programacion/estructura-deuna-aplicacion-android/>
- El formato APK. <http://www.androidcurso.com/index.php/curso-androidavanzado/48-unidad-9-ingenieria-inversa-en-android/340-elformato-apk>
- ¿Qué es una APK?. <http://www.proyectobyte.com/android/que-es-una-apk>
- https://www.owasp.org/index.php/Android_Testing_Cheat_Sheet
- https://www.owasp.org/index.php/OWASP_Mobile_Security_Project_-_Android

Módulo 9. Reversing de redes y protocolos

[5 Créditos ECTSs – 125 horas]

El malware, hoy por hoy, no tiene demasiado recorrido si no se comunica con el exterior. La comunicación con los llamados **“Command and Control” (C2)**, la búsqueda de nuevas víctimas en red local o externa, los intentos de pasar desapercibidos.

Las redes y los protocolos también deben ser estudiados para poder comprender qué hacen los programas, más allá de las posibilidades que ofrece el análisis del código y en ocasiones, como única posibilidad de análisis

por no disponer del código o la imposibilidad de analizarlo.

En este módulo se impartirán las técnicas necesarias para el análisis de red en profundidad, se explicarán los protocolos TCP/IP más habituales para poder comprenderlos, se mostrará cómo analizar redes Wi-Fi, comunicaciones Bluetooth o USB, para poder analizar dispositivos IoT, depurar fallos de red, encontrar intrusos o analizar comportamientos fuera de lo común que puedan derivar en un potencial ataque.



Programa de la asignatura

- Introducción al análisis de red.
- Repaso de los protocolos TCP/IP más habituales.
- Otros protocolos: WiFi, Bluetooth, USB.
- Herramientas de captura y análisis de red.
- Reversing de protocolos de red.

Objetivos

- Entender el funcionamiento de los protocolos de red TCP/IP más habituales y los empleados por dispositivos.
- Conocer las herramientas y mecanismos más habituales para capturar **analizar tráfico de red.** • **Procesar, entender y analizar capturas de red para** su posterior análisis.
- Comprender el comportamiento de los protocolos y aplicaciones de red a partir de su tráfico.
- Comprender cómo funcionan los protocolos de red TCP/IP más habituales.
- Entender el funcionamiento de los protocolos de comunicaciones empleados por dispositivos como WiFi, Bluetooth o USB.
- Conocer las herramientas más habituales de captura y análisis de tráfico.
- Conocer los mecanismos de captura de tráfico más habituales, así como las técnicas para capturar el tráfico de un objetivo dado.
- Conocer los mecanismos de interceptación de tráfico enviado por protocolos seguros, como SSL/TLS o SSH.
- Entender el comportamiento de un protocolo o aplicación de red a partir del tráfico de red que genera y ser capaz de descubrir la información que intercambia.

Competencias, aptitudes y destrezas

- Ser capaz de analizar y entender las redes y protocolos TCP/IP más habituales.
- Ser capaz de desplegar la infraestructura necesaria para realizar capturas de tráfico y de emplear mecanismos de ataque para capturar el tráfico deseado.
- Ser capaz de emplear las herramientas de captura y análisis de tráfico más populares.
- Ser capaz de interceptar el tráfico de protocolos seguros como SSL/TLS o SSH.
- Ser capaz de realizar la ingeniería inversa de un protocolo de red, para entender su funcionamiento y el comportamiento de la aplicación que lo genera.

Bibliografía

- James Forshaw. “Attacking Network Protocols”. No Starch Press. 2018.
- Chris Sanders. “Practical Packet Analysis”. No Starch Press. 2017.
- W. Richard Stevens. “TCP/IP Illustrated, Volume 1: The Protocols”. Primera edición. Addison Wesley Professional Computing, 1993

Mg

Módulo 10. Técnicas de análisis de malware

[6 Créditos ECTSs – 150 horas]

Analizar el malware es una de las habilidades más demandadas hoy en la industria. En tiempos en los que una pieza de software puede considerarse una ciber-arma, es fundamental conocer cómo se comporta, qué hace y cómo para poder analizar su repercusión.

En el caso del malware, además de la carga efectiva, los atacantes suelen utilizar técnicas en el código únicamente destinadas a imposibilitar ese análisis.

Ya sea a través de la ofuscación, técnicas anti-debugging o el empaquetado. En los últimos tiempos estas fórmulas son cada vez más sofisticadas de modo que el análisis del malware se convierte en un reto si no se disponen de las herramientas y habilidades adecuadas.

En este módulo se pretende dar a conocer al alumno las técnicas de análisis más útiles, prácticas y relevantes para poder comprender cómo se comporta el malware en general o cualquier programa en particular.



Programa de la asignatura

- Introducción al malware y su análisis.
- Análisis estático.
- Análisis dinámico.
- Técnicas anti-debuggin y ofuscación.
- Empaquetado y otras técnicas de ofuscación.

Objetivos

- Conocer las técnicas de análisis de malware más habituales.
- Conocer las técnicas de defensa anti-análisis que más utilizan los atacantes y poder sortearlas.
- Obtener los conocimientos mínimos necesarios, tanto de la arquitectura y componentes de procesamiento del Sistema Operativo, como de las estructuras básicas del lenguaje ASM.
- Adquirir conocimientos avanzados sobre análisis estático del malware.
- Adquirir conocimientos avanzados sobre análisis dinámico del malware.
- Desarrollar habilidades para sortear los obstáculos habituales a la hora de analizar malware para poder conocer su comportamiento.
- Conocer las diferentes tipologías de malware y sus características específicas
- Adquirir conocimientos sobre las herramientas y necesarias para la realización de un análisis de malware

Competencias, aptitudes y destrezas

- Ser capaz de entender cómo funciona el malware, independientemente de las técnicas anti-análisis que implemente.
- Conocer las técnicas habituales de análisis estático y dinámico y cómo proceder ante cada tipo de malware.

Bibliografía

- Honing, A. & Sikorski, M. (2012). Practical Malware.
- Analysis: The Hands-On Guide to Dissecting Malicious.
- Software. San Francisco, USA: no starch press.

Módulo 11. Proyecto Fin de Máster.

[6 Créditos ECTSs – 150 horas]

A lo largo de este módulo, el estudiante llevará a cabo la realización, presentación y defensa de un Proyecto fin de Máster en el que, de una forma guiada, deberá aplicar los conocimientos adquiridos a lo largo de los módulos del máster y demostrar que ha adquirido las competencias y destrezas necesarias para trabajar en el ámbito de la Ciberseguridad.

El trabajo se revisará “a pares”, tanto por un tutor como por un compañero. De esta forma, los estudiantes conocerán, de primera mano, dos ámbitos de estudio, el suyo propio y el de un compañero, duplicando el impacto pedagógico de la realización de este proyecto.



Programa de la asignatura

- Introducción a la realización de Proyectos de Ciberseguridad.
- Pautas esenciales para la organización del Proyecto.
- Realización del Proyecto Fin de Máster.
- Presentación.
- A lo largo del proceso de estudio y realización del proyecto fin de Máster, el estudiante, estará acompañado por un tutor/mentor que le irá guiando en el proceso.

Objetivos

- Aplicar los conocimientos adquiridos a través de los módulos estudiados al o largo del Máster.
- Seleccionar la temática o campo de aplicación sobre el que se va realizar el proyecto.
- Realizar un estudio previo a la implementación del proyecto.
- Desarrollar un proyecto de Ciberseguridad siguiendo las indicaciones del mentor.
- Realizar una presentación ejecutiva del proyecto.

Competencias, aptitudes y destrezas

- Ser capaz de articular, de forma completa, un proyecto de Ciberseguridad.
- Ejecutar, de forma eficiente, dicho proyecto.
- Comunicar de forma clara y expositiva, el trabajo realizado.

Claustro Docente

Un Equipo Académico al Servicio de la Seguridad Informática



Luis Alberto Segura

Analista de malware en Hispasec. Ha dedicado su Carrera al ámbito de la Ciberseguridad, Ingeniero informático, Doctor of Philosophy (PhD) y Experto Universitario en Ingeniería Inversa e Inteligencia de Malware.



David R. Sáez

Director de ENIIT Innova IT Business School y Director del Campus Internacional de Ciberseguridad. Lleva más de 16 años dirigiendo proyectos de e-learning Es experto en tecnología educativa, producción y gestión



Juan José Salvador

Coordinador Académico Técnico Superior en Administración de Sistemas Informáticos y Experto en Ciberseguridad y Seguridad de la Información. Profesional con más de 20 años de experiencia vinculada a los sistemas y las telecomunicaciones



Gonzalo Álvarez Maraño

Security Innovation Ambassador de Telefónica Tech. Ha trabajado en el Consejo Superior de Investigaciones Científicas (CSIC) y ha publicado más de 500 artículos sobre criptografía y seguridad en Internet, dos libros e imparte cursos a empresas y



Jose Ramon Palanco

VP Threat Intelligence at Telefonica Tech. Ha sido conferenciante en la OWASP, ROOTEDCON, ROOTCON, MALCON, y FAQin. Ha encontrado 4 CVEs y ha desarrollado diferentes herramientas open source para la ciberseguridad como nmap-scada, ProtocolDetector.



David Garcia

Security Researcher en Telefonica Tech. Anteriormente ha desempeñado la coordinación de auditorias en Hispasec, donde ha trabajado durante más de diez años. También ha sido ponente en varias conferencias como la Microsoft Digital Crimes



Yaiza Rubio

Analista de Inteligencia en Telefónica Tech, estudió Ciencias de la Información y tiene tres másteres en Análisis de Inteligencia, Logística y Economía de la Defensa, y Derecho Tecnológico y de las TICS.



Roberto Santos

Analista de malware en Telefónica. En el ámbito laboral ha desarrollado diversas funciones, trabajando como desarrollador y consultor de gobierno de ciberseguridad. En los últimos tiempos su trabajo se enfoca más en el campo del Malware



Félix Brezo

Incident Response Engineer en Telefónica. Doctor en Ingeniería Informática y Telecomunicación. Ingeniero Técnico en Informática de Gestión, Ingeniero en Informática e Ingeniero en Organización Industrial.



Jose Torres Velasco

Tech Lead en Telefónica. Participa de forma habitual como ponente en conferencias especializadas tanto nacionales como internacionales de referencia (RootedCON, NIC, ICISSP, etc), y ha publicado en diferentes revistas y publicaciones de amplio impacto



Miguel Angel de Castro

SE At CrowdStrike, Especialista en Seguridad de la Información con más de 12 años de experiencia en Hacking Ético e Inteligencia de Amenazas. Amplia experiencia en reversing de malware, HUMINT y OSINT.



Manuel Urueña Pascual

Arquitecto de Seguridad en Telefónica Ingeniería de Seguridad, Investigador de Seguridad Senior. Tiene 16 años de experiencia docente en Grados y Másteres oficiales, impartiendo las asignaturas de Comunicaciones Seguras, Sistemas de Ciberdefensa.



**De los mejores
para los mejores**

Fórmate con los mejores en una de las disciplinas con mayor proyección dentro del mundo de la Seguridad Informática

Qué opinan nuestros alumnos



Jorge Gastón

El Máster en Reversing, Análisis de Malware y Bug Hunting tiene una orientación muy práctica, con unos contenidos técnicos actualizados al estado del arte, y que proporciona los conocimientos y las herramientas para poder adentrarse en el campo del análisis de malware. Al mismo tiempo nos da también las habilidades para que podamos profundizar en cada uno de los temas de forma autónoma. Por otro lado, la forma de impartirlo permite que los alumnos podamos estudiar a nuestro ritmo y compaginarlo con el trabajo.

El Máster

Un programa formativo de máximo nivel al servicio del Desarrollo de la Seguridad Informática

A continuación, presentamos un resumen con las características esenciales del Máster en Reversing, Análisis de Malware y Bug Hunting.



Importante

Certificación

UCAM (Universidad Católica San Antonio de Murcia)

Duración

El Máster, certifica 60 Créditos ECTS (European Credits Transfer System), equivalentes a 1.500 horas.

Impartido por:

El Campus Internacional de Ciberseguridad de ENIIT (Innova IT Business School), Campus de referencia de formación de Seguridad Informática.





Más información e Inscripciones

Campus Internacional de Ciberseguridad – ENIIT (Innova IT Business School)

<https://eniit.es/master-en-reversing-analisis-de-malware-y-bug-hunting/>

Responsable: Lidia Lobato

Teléfono: +34 673 163 878

E-mail: lidia.lobato@campusciberseguridad.com



ENIIT – CAMPUS INTERNACIONAL CIBERSEGURIDAD
Valladolid.
España.

+34 983 39 07 16

Responsable del Programa: Lidia Lobato

lidia.lobato@campusciberseguridad.com