Aspectos Éticos y Legales

Hacking Ético

©Ismael Ripoll &
Hector Marco

Universidad Politècnica de València

March 21, 2021

Índice

Lo que vamos a trabajar

- Cuál es la legislación aplicable.
- Qué se puede hacer y qué no se puede hacer.
- Cómo tener una actitud profesional.

BOE-A-2015-3439 (I)

Ley Orgánica del Código Penal:
https://www.boe.es/buscar/act.php?id=BOE-A-2015-3439

Articulo 197:
1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, ***intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación****, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.*

BOE-A-2015-3439 (II)

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen ***registrados en ficheros o soportes informáticos, electrónicos o telemáticos****, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.*

BOE-A-2015-3439 (III)

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

BOE-A-2015-3439 (IV)

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por ***las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros****; o*

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. … Penas más altas para cierto tipo de datos (religión[1],…)

6. … Penas más altas si hay fines lucrativos.

7. … Sobre imagenes privadas.

BOE-A-2015-3439 (V)

Artículo 197 bis:

1.- El que por cualquier medio o procedimiento, ***vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él*** *en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.*

2.- El que mediante la utilización de ***artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información****, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.*

BOE-A-2015-3439 (VI)

Artículo 197 ter:

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, ***sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros****, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:*

a) ***un programa informático, concebido o adaptado principalmente para cometer dichos delitos****; o*

b) ***una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información****.*

etc....

---

[1] En Suiza, la religión no es ningún secreto.

Comentarios a la ley

- Las leyes las hacen los políticos. Con mayor o menor acierto.
- Esta ley ha sido muy criticada por los ciber investigadores, porque dejar sin amparo su labor.
- Si un investigador que descubre una vulnerabilidad y se la notifica al propietario, el propietario puede emprender acciones legales.
- La ley no contempla el trabajo del hacker ético.
- Cualquier trabajo que “puediera” ser usado por terceros para cometer delitos, podría ser sancionable.
- Muchos libros de hacking dejan claro que lo que se presentan como ejemplos son “pruebas de concepto”, nunca exploits.
- Parece asumir que las capacidades de los hackers éticos aparecen de la nada (generación espontánea, no es necesario practicar).

Fair use

- En USA, existe el concepto de “uso justo” (fair use), que permite utilizar material con copyright en cirtos casos: https://en.wikibooks.org/wiki/Reverse_Engineering/Legal_Aspects

*“ Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, **teaching (including multiple copies for classroom use), scholarship, or research**, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include: ... ”*

Ingeniería inversa (I)

- La mayoría de los programa privativos prohíben explícitamente hacer cualquier tipo de análisis (desemsamblado, reverseing, etc.).
- Las GPL sí que lo permite. No todas la licencias de “open source” permiten el desensamblado. Cuidado con el BSD License!
- Pero en la EU, es posible en ciertos supuestos, independientemente de lo que diga la licencia o el fabricante.
- DIRECTIVE 2009/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 April 2009 on the legal protection of computer programs: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF

Ingeniería inversa (II)

Article 5 Exceptions to the restricted acts

1. In the absence of specific contractual provisions, the acts referred to in points (a) and (b) of Article 4(1) shall not require authorisation by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including ***for error correction****.*

2. The making of a back-up copy by a person having a right to use the computer program may not be prevented by contract in so far as it is necessary for that use.

3. The person having a right to use a copy of a computer program shall be entitled, ***without the authorisation of the rightholder, to observe, study or test the functioning of the program*** *in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading,*

Ingeniería inversa (III)

displaying, running, transmitting or storing the program which he is entitled to do.

Article 6 Decompilation

1. The authorisation of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of points (a) and (b) of Article 4(1) are ***indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs****, provided that the following conditions are met:*

(a) those acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorised to do so;

(b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in point (a); and

Ingeniería inversa (IV)

(c) those acts are confined to the parts of the original program which are necessary in order to achieve interoperability.

2. The provisions of paragraph 1 shall not permit the information obtained through its application:

(a) to be used for goals other than to achieve the interoperability of the independently created computer program;

(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or

(c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

Pentesting (I)

Antes de hacer ninguna acción de análisis de seguridad, y de pentesting en especial, debéis dejar muy claras las condiciones del trabajo para proteger tanto a la empresa como a vosotros:

- Firmar con la empresa un contrato de confidencialidad (NDA, Non Disclosure Agreement). Nada de lo encontrado debe ser revelado a terceros.
- Debéis obtener la autorización por escrito de la tarea a realizar.
- Debéis informar sobre los posibles incidentes que se pudieran producir durante el análisis.
- Dejar claro que el testeo "**demuestra la presencia de fallos pero no la ausencia de los mismos**".
- Debéis ser especialmente cuidadosos protegiendo la información que obtenéis.

Codigo ético (I)

Código de Ética Profesional de Pen Testers: 10 Principios Éticos, **Aury M. Curbelo** www.expresionbinaria.com

1. Independencia: Cuando se trabaja de forma independiente se mantiene la objetividad del trabajo. Independencia es que el hacker ético no esté comprometido con algún vendedor comercial o proveedor de servicios profesionales que posea alguna solución de informática relacionada a la seguridad. Ejemplo, una compañía dueña de un producto que asegura detecta vulnerabilidades e intenta vender el producto como parte de las soluciones para proteger a la empresa que le contrató para hacer las pruebas de vulnerabilidad.
2. Prohibición de aceptar dinero por compañías de la competencia para realizar pruebas en otras compañías: La compañía X me contrata para hacer un análisis de vulnerabilidad de la compañía competidora.

Codigo ético (II)

3. Cuidado del cliente: Se le debe informar sobre los posibles riesgos de realizar algunas pruebas de vulnerabilidad
4. Profesionalismo y calidad en la operación
5. Responsabilidad corporativa, establecer bien claro las responsabilidades de las consecuencias de las pruebas
6. Imparcialidad, neutralidad y transparencia de procesos
7. Evitar el conflicto de intereses
8. Obediencia estricta a las leyes
9. Respeto por los humanos: Ingeniería social
10. Dar los créditos correctos en el informe final

Vulnerability disclosure (I)

Cuando un hacker descubre una vulnerabilidad (sin haber sido contratado para realizar un pentesting), existen varias alternativas para publicar/notificar la vulnerabilidad.
Este es un tema muy controvertido con intereses muy encontrados.
[Definiciones de la Wikipedia]

Responsive disclosure: A vulnerability or an issue is disclosed only after a period of time that allows for the vulnerability or issue to be patched or mended.

Coordinate disclosure: The primary tenet of coordinated disclosure is that nobody should be informed about a vulnerability until the software vendor gives their permission.

Vulnerability disclosure (II)

Full disclosure: The practice of publishing analysis of software vulnerabilities as early as possible, making the data accessible to everyone without restriction. The primary purpose of widely disseminating information about vulnerabilities is so that potential victims are as knowledgeable as those who attack them.

Bruce Schneier stated "Full disclosure – the practice of making the details of security vulnerabilities public – is a damned good idea. Public scrutiny is the only reliable way to improve security, while secrecy only makes us less secure".

Non disclosure: No vulnerability information should be shared, or should only be shared under non-disclosure agreement (either contractually or informally). Common proponents of non-disclosure include commercial exploit vendors, researchers who intend to exploit the flaws they find

Vulnerability disclosure (III)

Impact disclosure: Se hace público (no se comunica con antelación al fabricante) únicamente el impacto que tienen las vulnerabilidades, pero no los detalles que permitirían explotarlas.

Este modelo se ha empezado a utilizar en 2018 a raíz del caso de los fallos en placas de AMD:

amd-has-a-spectre-meltdown-like-security-flaw-of-its-own