Introducción

Hacking Ético

©Ismael Ripoll &
Hector Marco

Universidad Politècnica de València

February 1, 2022

Índice

Qué vamos a trabajar (I)

Para evitar confusiones, esta asignatura **no va de**:

- Uso de exploits. Eso lo hacen los script kiddies.
- Ni de entrar en sistemas.
- Tampoco es un manual de metaexploit, ni kali, ni IDA, ni...

¿Qué aprenderéis?:

- Los problemas de la seguridad desde el lado del atacante.
- Conceptos fundamentales de cómo funciona la informática.
- Cómo los fallos de programación se transforman en un problema de seguridad.
- Que la ignorancia es la madre de la felicidad[1].
- Apreciar la dificultad de la seguridad avanzada.

[1] Y espero haceros un menos felices.

La Ética (I)

Real Academia Española

La palabra ética proviene de "Ethos" que significa: "Conjunto de rasgos y modos de comportamiento que conforman el carácter o la identidad de una persona o una comunidad."

- Un gran poder conlleva una gran responsabilidad.
- Existen varios tipos de hackers en función del uso que hagan de sus conocimientos:

  Black Hat: Hacker que está fuera de la ley y utiliza las vulnerabilidades que encuentra en su propio beneficio. También conocido como *cracker*.

  Grey Hat: Las leyes no son precisas y caben varias interpretaciones. Hacen cosas que están en el borde de la ley o sin legislar.

La Ética (II)

Blue Hat: Hackers contratados por el propietario para estudiar la seguridad de su sistema, siguiendo la filosofía black hat.

White Hat: Cybersecurity researcher. Hacker que estudia fallos y propone soluciones.

- Excelete entrada de blog de **Aury M. Curbelo**: "Hacking ético: sus claroscuros, implicaciones y beneficios" www.expresionbinaria.com. Extraeré partes de este blog:
- Qué consideramos como un comportamiento ético en nuestra sociedad: "*Si una acción al menos contiene cualquiera de estas características es considerada una acción ética por ejemplo: promover la salud general de la sociedad, mantener o incrementar los derechos de los individuos, proteger las libertades, preservar a los individuos de daño, tratar a todos los humanos con valor dignidad y respeto, así como mantener el valor social, cultural y respetar las leyes.*"

La Ética (III)

- El objetivo fundamental del hacking ético consiste en:
  - "**Explotar las vulnerabilidades**" existentes en el sistema de interés, valiéndose de una prueba de intrusión, verificar o evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etcétera.
  - "**Con la intención de ganar acceso y demostrar**" las vulnerabilidades en el sistema. Esta información es de gran ayuda a las organizaciones para adoptar las medidas preventivas en contra de posibles ataques malintencionados.
- Algunos autores reducen el hacking a la realización de "pentesting" (tests de penetración).

La ética en la Universidad

- La ética se demuestra TODOS los días.
- No solo hay que ser bueno, sino que hay que demostrarlo.
- Un momento excelente para demostrar vuestra integridad ética van a ser los **exámenes** y las **prácticas**.
- **No se tolerará ningún tipo de trampa en la evaluación.**[2]
- Esto no es el instituto. La "copia" o el "intento de copia" tendrá bonificación especial, cero en examen y cero en asignatura, respectivamente.
- Es fácil detectar a los copiones, todos hemos sido estudiantes.

[2] Suena como una amenaza, cuando es una obviedad. ¿No?

Contexto social (I)

- La seguridad en el mundo:
  - ECHELON.
  - Stuxnet.
  - Robo a Sony.
  - Ataque Mirai.
  - Robo de 81M$ al Banco central de Bangladesh.
  - RamsomWare.
  - HeartBleeding.
  - ShellShock.
  - KrackAttack (WAP2).
  - Adobe reader.
  - Meltdown, Spectre, Ryzenfall, ...
- Pero no hay que ir tan lejos, aquí en la universidad ya pasan bastantes fiestas ¿No?

Glosario de términos (I)

Algunos términos que se suelen utilizar en seguridad.

Debilidad: Tipo de defecto o fallo de diseño, programación, o configuración. Por ejemplo: "no comprobar el valor retornado por las syscalls".

Vulnerabilidad: Fallo (de diseño, programación o configuración) que afecta a la seguridad del sistema y que puede ser utilizado directamente para ganar acceso a un sistema.

Exploit: Programa o método para subvertir la seguridad de un sistema a partir de una o más vulnerabilidades.

Hacker: Persona extremadamente curiosa que sabe cómo funcionan las cosas.

Cracker: Individuo que usa los ordenadores fuera de la ley.

RCE: Remote Code Execution. Forzar a un sistema remoto a ejecutar el código que el atacante quiere.

Glosario de términos (II)

ROP: Return Oriented Programming. Estilo de programación que permite crear programas mas allá de la funcionalidad del programa atacado.

API: Application Programming Interface. This is the set of public types/variables/functions that you expose from your application/library.

ABI: Application Binary Interface. This is how the compiler builds an application. It defines things (but is not limited to):

- How parameters are passed to functions (registers/stack).
- Who cleans parameters from the stack (caller/callee).
- Where the return value is placed for return.
- How exceptions propagate.

Glosario de términos (III)

0-day: Vulnerabilidad con exploit asociado que a fecha de publicación no ha sido resuelta por el fabricante.

1-day: Vulnerabilidad que ha sido resuelta por el fabricante pero usada por los atacantes en sistemas no actualizados.

Ingeniería social: Utilizar las personas para, sin su conocimiento o consentimiento, obtener información o realizar acciones que impacten en la seguridad.

Antivirus: Tecnología básica utilizada para detección de software malicioso.

Vector de ataque: Método que utilizado para tener acceso al activo objetivo de ataque. Ej. *Email con javascript malicioso*.

APT: Advanced Persitent Threat. Amenaza persistente y avanzada. Típicamente es una nación o grupo patrocinado por un estado.

Glosario de términos (IV)

Sandbox: Entorno de ejecución aislado y monitorizado usado para ejecutar aplicaciones "expuestas" (Ej. *servidores*).

Pentesting: Penetration testing. Análisis de seguridad consistente en tratar de realizar una intrusión (solicitada por el propietario) lo más realista posible sobre un objetivo. Lo que suelen llevar a cabo los blue hats.

Hacker Ético: Se suele confundir con Pentester. Un hacker desarrolla sus propias herramientas y PoCs (es un científico de la seguridad), mientras que el pentester utiliza las herramientas (es un ingeniero de la seguridad). Un tipo de white hat.

Glosario de términos (V)

Offensive security: Investigador que estudia las técnicas de ataque empleando las mismas estrategias que los crackers. La diferencia está en el uso que se hace de los resultados. Un tipo de white hat. La seguridad no tiene porqué limitarse a la defensa.

Keylogger: Captura las pulsaciones introducidas por un usuario. Puede ser físico (USB) o un programa que intercepta los eventos del sistema.

RAM scraper: Inspeccionan la memoria de los procesos en búsqueda de información útil.

Ransomware: Malware que cifra los datos de los discos y pide un rescate para su recuperación.

Glosario de términos (VI)

Banking trojans: Typically include a keylogger component, which is used to sniff out the passwords as the user is using them to log into the bank.

Bots: Toma el control de una máquina y permite ser controlada con comandos remotos. El control de bots se suele realizar de forma colectiva, enviado un comando a muchos bots simultáneamente.

RATs: Remote Access Trojan. Es un malware que se instala en un sistema target y permite el control individualizado. Se parece a un Bot, pero permite el control fino del sistema. Mientras el Bot está pensado para ser usado como puente para realizar ataques a terceros, el RAT se centra en la explotación.

The big picture (I)

Actores: En función del interés: Estados, grupos empresariales, grupos terroristas, cyber delincuentes y activistas.

Objetivos: Cada grupo tiene objetivos y estrategias diferentes. Pero en general se busca el beneficio propio o del grupo al que pertenecen.

Metodologías: Ingeniería social (phishing), insiders, 0-days, 1-days, backdoors, etc. El hacking o del desarrollo de exploits es una más de las herramientas que se usan en los ataques informáticos. No hay que subestimar otros vectores de ataque.

Contramedidas: NDIS, firewalls, planes de contingencias, pen testing, etc.

The big picture (II)

- Aunque la ciberseguridad comprende muchas áreas de conocimiento: **De no existir los crackers $\rightarrow$ no existiría la ciberseguridad**.
- El problema no son las vulnerabilidades, sino el uso que se haga de ellas.
- Las vulnerabilidades son el medio para cometer delitos.
- Las vulnerabilidades SIEMPRE existirán.