M1: Introducción y Legalidad en el Hacking Ético

1. Introducción al Hacking Ético

1.1 ¿Qué es el hacking?

El **hacking** es la práctica de explorar sistemas informáticos y redes con el fin de comprender cómo funcionan, identificar fallos y, en algunos casos, manipularlos.

- Originalmente, el término *hacker* no tenía connotación negativa. En los años 60–70 se refería a personas creativas que encontraban soluciones ingeniosas a problemas técnicos.
- Con el tiempo, los medios de comunicación popularizaron el término como sinónimo de **ciberdelincuente**, aunque en realidad depende de la **intención** y del **marco legal** en el que actúe la persona.

Ejemplo histórico:

- En los años 80, el MIT usaba el término *hacker* para los estudiantes que inventaban soluciones técnicas innovadoras.
- En los 90, se asoció con los ataques a redes telefónicas y sistemas bancarios, lo que generó una visión negativa.

1.2 Definición de hacking ético

El **hacking ético** consiste en aplicar las mismas técnicas que utilizan los atacantes, pero con un propósito **defensivo, legal y autorizado**.

Características principales:

1. **Autorización previa**: solo se realiza con permiso expreso del propietario del sistema.
2. **Objetivo defensivo**: detectar vulnerabilidades para corregirlas antes de que las explote un ciberdelincuente.
3. **Metodología estructurada**: se siguen marcos reconocidos como OWASP o PTES.
4. **Responsabilidad legal y ética**: el trabajo queda documentado en informes oficiales.

Ejemplo: Una empresa de comercio electrónico contrata a un hacker ético para simular un ataque sobre su web. El especialista identifica una vulnerabilidad en el login que permitiría un ataque de *SQL Injection*. En lugar de explotarla con fines maliciosos, documenta la falla en un informe y recomienda cómo solucionarla.

1.3 Diferencia entre hacker ético y ciberdelincuente

Aspecto	Hacker Ético (White Hat)	Ciberdelincuente (Black Hat)
Autorización	Actúa con permiso legal	Actúa sin permiso
Objetivo	Mejorar la seguridad	Obtener beneficio o causar daño
Metodología	Documentada, transparente	Oculta, clandestina
Resultados	Informe de vulnerabilidades y recomendaciones	Robo de datos, fraude, sabotaje

"La técnica puede ser la misma, pero el contexto y la intención marcan la diferencia entre un acto legal y un delito."

1.4 Importancia del hacking ético en la ciberseguridad

Hoy en día, las organizaciones dependen de sistemas digitales: comercio electrónico, banca online, salud, servicios públicos. Esto genera una superficie de ataque cada vez mayor.

El hacking ético se vuelve imprescindible porque:

- Permite **detectar vulnerabilidades antes de que lo hagan los atacantes**.
- Ayuda a cumplir con **normativas de seguridad y protección de datos** (ej. RGPD, ISO 27001).
- Genera confianza en clientes y usuarios al demostrar un compromiso con la seguridad.
- Es una de las **profesiones más demandadas** en ciberseguridad (según ENISA, el déficit de profesionales en Europa supera los 200.000 en 2022).

1.5 Ámbitos de aplicación del hacking ético

Un hacker ético puede trabajar en diferentes entornos:

- **Aplicaciones web** → pruebas según OWASP Top 10.
- **Redes corporativas** → detección de configuraciones inseguras, segmentación, vulnerabilidades en routers/switches.
- **Sistemas operativos y servidores** → auditorías de parches y configuraciones.
- **Dispositivos móviles e IoT** → detección de problemas de seguridad en apps móviles o dispositivos conectados.
- **Ingeniería social** → simulaciones de phishing o pruebas de concienciación de usuarios (con autorización previa).
- **Otros**

1.6 Ejemplo práctico introductorio

Caso real simplificado:

1. Una entidad bancaria contrata a un equipo de hackers éticos.
2. Se establece un contrato que define el **alcance**: la aplicación de banca online, pero no la red interna.
3. Los hackers simulan ataques de **fuerza bruta** contra el sistema de autenticación.
4. Descubren que las cuentas no están protegidas contra múltiples intentos fallidos.

5. Resultado: entregan un informe detallando la vulnerabilidad y la recomendación de implementar un sistema de bloqueo temporal de cuentas.

Sin hacking ético, este fallo podría haber sido descubierto por un ciberdelincuente y explotado con fines fraudulentos.

1.7 Conclusiones

- El hacking no es en sí mismo ilegal: depende de la intención y autorización.
- El hacking ético usa técnicas de ataque con fines de defensa, siempre bajo permiso.
- Es esencial para proteger organizaciones frente a amenazas reales.
- La diferencia entre hacker ético y ciberdelincuente radica en la **legalidad, autorización y objetivos**.

2. Marco Legal en España y Europa

2.1 Importancia del marco legal en el hacking ético

El **hacking ético** solo es legal si se realiza **con autorización expresa** y dentro de los **límites definidos por contrato**.

- Actuar sin permiso, aunque sea con buenas intenciones (ej. descubrir una vulnerabilidad y avisar a la empresa), puede constituir un **delito penal** en España.
- La **normativa europea** añade obligaciones específicas para proteger los datos personales y reforzar la seguridad de las infraestructuras críticas.

Conclusión: el marco legal es el **pilar fundamental** que diferencia al **hacker ético** del **ciberdelincuente**.

2.2 Legislación en España

La legislación española considera los accesos no autorizados como delitos graves.

Código Penal (Ley Orgánica 10/1995, con reformas posteriores)

- **Artículo 197 – Descubrimiento y revelación de secretos**
  - Penaliza el acceso no autorizado a sistemas, datos o comunicaciones.
  - Incluye: copiar, interceptar, utilizar o divulgar datos sin permiso.
  - **Penas**: prisión de 1 a 4 años y multas.
- **Artículo 264 – Daños informáticos**
  - Penaliza la alteración, destrucción, supresión o inutilización de datos, programas o sistemas.
  - Incluye ataques de denegación de servicio (DoS/DDoS).
  - **Penas**: prisión de 1 a 5 años.

Ejemplo práctico: Un estudiante accede sin permiso a la red de su universidad para "probar la seguridad" y comparte capturas en un foro. Aunque no robe dinero ni datos sensibles, su acción estaría penada bajo el artículo 197 (acceso y difusión de datos).

2.3 Normativa europea

La Unión Europea ha creado un marco normativo que obliga a empresas y administraciones a **proteger datos personales** y **garantizar la seguridad de los servicios digitales**.

Reglamento General de Protección de Datos (RGPD, UE 2016/679)

- En vigor desde mayo de 2018, aplicable en todos los Estados miembros.
- Principales obligaciones:
  - **Protección de datos personales**: cualquier empresa que trate datos debe aplicar medidas de seguridad.
  - **Notificación de brechas**: si ocurre una fuga de datos, debe notificarse a la autoridad competente en un máximo de **72 horas**.
  - **Multas**: pueden alcanzar hasta **20 millones de € o el 4% de la facturación anual global**, la cantidad que sea mayor.

Ejemplo práctico: Un pentester autorizado descubre que una web almacena contraseñas en texto plano. La empresa debe corregirlo y, si los datos han estado expuestos, notificarlo según RGPD.

Directiva NIS y NIS2 (Network and Information Security)

- **Directiva NIS (2016/1148/UE):** primera ley europea sobre ciberseguridad.
- **NIS2 (2022/2555/UE):** refuerza los requisitos e incluye más sectores críticos.
- Principales aspectos:
  - Obliga a sectores esenciales (energía, banca, transporte, sanidad, digital) a implementar **medidas de seguridad robustas**.
  - Exige **planes de gestión de incidentes** y auditorías periódicas.
  - **Sanciones**: multas significativas por incumplimiento, similares al RGPD.

Ejemplo práctico: Un hospital sufre un ciberataque que deja inaccesible su sistema de historiales médicos. Bajo la NIS2, está obligado a notificar el incidente y demostrar que contaba con medidas de seguridad adecuadas.

2.4 Contratos y acuerdos de pentesting

Para garantizar la legalidad de una auditoría de seguridad, se firma un **contrato o autorización** que incluye:

- **Alcance**: qué sistemas, aplicaciones o redes pueden ser analizados.
- **Limitaciones**: qué pruebas están prohibidas (ej. ataques de denegación de servicio).
- **Responsabilidades**:
  - El pentester documenta vulnerabilidades.
  - La empresa se compromete a corregirlas y proteger los datos.
- **Confidencialidad**: obligación de no divulgar la información obtenida.

Sin contrato, cualquier acción de prueba puede ser considerada delito, aunque el objetivo sea “ayudar”.

2.5 Tabla comparativa: España vs UE

Aspecto	España (Código Penal)	Unión Europea (RGPD / NIS2)
Acceso sin autorización	Delito (art. 197 CP) → prisión y multa	Se considera incumplimiento grave de seguridad
Daños informáticos	Delito (art. 264 CP) → prisión	Se traduce en incumplimiento de protección de servicios esenciales
Protección de datos	Ley Orgánica 3/2018 (LOPDGDD, adaptación del RGPD)	RGPD: multas hasta 20 M€ o 4% facturación
Ciberseguridad sectores críticos	No específico en Código Penal	NIS2: obligaciones y sanciones a sectores esenciales

2.6 Conclusiones

- En España, el **Código Penal** castiga el acceso no autorizado y los daños informáticos.
- En Europa, el **RGPD** regula la protección de datos personales y la **NIS2** refuerza la ciberseguridad en infraestructuras críticas.
- El hacking ético **solo es legal** si existe autorización expresa y contrato firmado.
- Actuar sin permiso, incluso con buena intención, puede conllevar **prisión o multas millonarias**.

3. Tipos de Hackers y Metodologías

3.1 Tipos de hackers

El término **hacker** engloba perfiles muy diversos. No todos son ciberdelincuentes: la motivación, la ética y la legalidad determinan el tipo de hacker.

Tipo de hacker	Características	Motivación	Ejemplo práctico
White Hat (Sombrero blanco)	Hacker ético, actúa con autorización y dentro de la legalidad	Proteger sistemas, fortalecer la seguridad	Un pentester contratado para auditar la web de un banco
Black Hat (Sombrero negro)	Actúa de forma ilegal, explota vulnerabilidades sin permiso	Lucro económico, espionaje, sabotaje	Ciberdelincuente que roba tarjetas de crédito y las vende en foros clandestinos
Grey Hat (Sombrero gris)	Actúa sin autorización, pero no con fines maliciosos directos	Reconocimiento, prestigio, ego	Un investigador que descubre un fallo y lo publica sin permiso previo
Script Kiddie	Usuario con escasos conocimientos que usa herramientas hechas por otros	Diversión, reto, curiosidad	Adolescente que lanza un escaneo de puertos con Nmap sin saber interpretarlo
Hacktivista	Utiliza ataques para promover causas políticas o sociales	Activismo, protesta	Grupo que lanza un ataque DDoS contra una página gubernamental

Insider Threat (amenaza interna)	Persona con acceso legítimo a sistemas que lo usa maliciosamente	Venganza, beneficio económico	Empleado que filtra datos confidenciales de la empresa

No todos los hackers son iguales. El **white hat** es el referente profesional en el ámbito del hacking ético.

3.2 Metodologías en hacking ético

Para garantizar que un test de seguridad se realice de forma **estructurada, repetible y profesional**, los hackers éticos utilizan **metodologías reconocidas**.

Dos de las más importantes son **OWASP** (para aplicaciones web) y **PTES** (para auditorías integrales).

3.3 OWASP (Open Web Application Security Project)

- Organización internacional sin ánimo de lucro dedicada a mejorar la **seguridad en aplicaciones web** principalmente.
- Su documento más famoso es el **OWASP Top 10**, que lista los riesgos más críticos en aplicaciones web.

OWASP Top 10 (versión 2021, resumen de categorías)

1. **Broken Access Control** → fallos en control de accesos.
2. **Cryptographic Failures** → uso incorrecto de algoritmos criptográficos.
3. **Injection** → vulnerabilidades de inyección (ej. SQL Injection).
4. **Insecure Design** → fallos en el diseño de la aplicación.
5. **Security Misconfiguration** → configuraciones incorrectas en servidores o apps.
6. **Vulnerable and Outdated Components** → software sin actualizar.
7. **Identification and Authentication Failures** → problemas en autenticación (ej. contraseñas débiles).
8. **Software and Data Integrity Failures** → librerías no verificadas o código manipulado.
9. **Security Logging and Monitoring Failures** → falta de registro de eventos de seguridad.
10. **Server-Side Request Forgery (SSRF)** → posibilidad de forzar al servidor a realizar peticiones no autorizadas.

Esta es la versión vigente mientras OWASP trabaja en la **edición 2025.**

Ejemplo práctico OWASP

Un auditor realiza un test de una tienda online y encuentra que el formulario de login es vulnerable a **inyección SQL**.

- Riesgo: un atacante podría acceder a todas las cuentas de usuario.
- Acción del hacker ético: reportar el fallo y recomendar parametrización de consultas SQL.

OWASP se centra en **aplicaciones web y móviles**.

3.4 PTES (Penetration Testing Execution Standard)

- Estándar internacional que define cómo realizar pruebas de intrusión de forma completa y ordenada.
- Se aplica a redes, sistemas, aplicaciones, hardware y personas (ingeniería social).

Fases del PTES

1. **Pre-engagement (Preparación):**
   - Definición del alcance, objetivos, limitaciones.
   - Firma del contrato/autorización.
2. **Inteligencia y reconocimiento:**
   - Recopilar información sobre el objetivo.
   - Ejemplo: escaneo de subdominios, análisis de servicios expuestos.
3. **Modelado de amenazas:**
   - Identificar vectores de ataque posibles.
   - Ejemplo: sistemas con software obsoleto.
4. **Explotación:**
   - Intentar aprovechar vulnerabilidades de forma controlada.
   - Ejemplo: prueba de explotación de un fallo de autenticación.
5. **Post-explotación:**
   - Analizar el impacto real y el nivel de acceso conseguido.
   - Ejemplo: demostrar acceso a datos sensibles sin copiarlos ni difundirlos.
6. **Informe:**
   - Documentar las vulnerabilidades, pruebas realizadas y recomendaciones de mejora.

Ejemplo práctico PTES

Una empresa de telecomunicaciones pide una auditoría integral:

- Alcance: red interna y servidores.
- El auditor realiza reconocimiento, descubre un servidor con un sistema operativo sin parches y explota una vulnerabilidad de escalada de privilegios.
- Documenta el hallazgo y recomienda actualizar el servidor y reforzar controles de acceso.

PTES se usa en **auditorías completas de seguridad** (más allá de aplicaciones web).

3.5 Comparativa OWASP vs PTES

Aspecto	OWASP	PTES
Enfoque	Seguridad en aplicaciones web y móviles	Auditorías integrales (redes, sistemas, apps)
Metodología	Basada en riesgos y categorías (OWASP Top 10)	Basada en fases estructuradas de pruebas de intrusión
Aplicación típica	Test de aplicaciones web y APIs	Pruebas de penetración completas

Informe final	Riesgos según Top 10 + recomendaciones	Vulnerabilidades explotadas + análisis de impacto + roadmap de mitigación

3.6 Conclusiones

- Existen distintos tipos de hackers, desde los **white hat** (éticos) hasta los **black hat** (ilegales), pasando por perfiles intermedios como **grey hat, hacktivistas o script kiddies**.
- El **hacking ético** se diferencia por la **autorización, la legalidad y el propósito defensivo**.
- Las metodologías garantizan que las pruebas se realicen de forma **profesional y repetible**:
  - **OWASP** es la referencia en seguridad de aplicaciones web.
  - **PTES** cubre auditorías integrales con un proceso en fases.
- Un buen hacker ético debe conocer y aplicar ambas metodologías según el contexto del cliente.