**Introduccion al hacking ético**

# **Introducción**

## ¡Bienvenidos al curso!

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu2ol3ri57dcbr62o6s0?&autoplay=true&crosstime=296>

### **Recomendaciones/Notas**

Servidor de discord : <https://discord.gg/u3dsh9M>

Youtube : <https://youtube.com/s4vitar>

Twitter : <https://twitter.com/s4vitar>

## Requisitos antes de empezar

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu2qj2eje35bt9chblbg?&autoplay=true&crosstime=138>

### **Recomendaciones/Notas**

Descargar :

Kali linux

Parrot OS

# **Conceptos básicos**

## Creación y gestión de usuarios

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu2r44ri57dcbr62od0g?&autoplay=true&crosstime=413>

### **Recomendaciones/Notas**

Material de apoyo

Guia de creacion de usuarios en Linux: <https://culturacion.com/como-crear-cuentas-de-usuario-en-linux/>

Administracion de usuarios en Linux: <https://www.pedroventura.com/linux/administracion-de-usuarios-en-linux-crear-borrar-modificar-usuarios-y-grupos/>

## Asignación e interpretación de permisos

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu2vue6je35bt9chc6h0?&autoplay=true&crosstime=359>

### **Recomendaciones/Notas**

Material de apoyo

Permisos básicos en GNU/Linux con chmod: <https://blog.desdelinux.net/permisos-basicos-en-gnulinux-con-chmod/>

Permisos y derechos en Linux: <https://blog.desdelinux.net/permisos-y-derechos-en-linux/>

## Ejemplos prácticos de asignación e interpretación de permisos

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu30ohri57dcbr62ovog?&autoplay=true&crosstime=338>

### **Recomendaciones/Notas**

Material de apoyo

Permisos básicos en GNU/Linux con chmod: <https://blog.desdelinux.net/permisos-basicos-en-gnulinux-con-chmod/>

Permisos y derechos en Linux: <https://blog.desdelinux.net/permisos-y-derechos-en-linux/>

## Lectura e interpretación numérica de permisos

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu3adpeje35bt9chcuag?&autoplay=true&crosstime=331>

### **Recomendaciones/Notas**

Permisos y atributos: <http://mural.uv.es/oshuso/8339_permisos_y_atributos.html>

## Explotación de permisos SUID

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu3beqbi57dcbr62pltg?&autoplay=true&crosstime=215>

### **Recomendaciones/Notas**

Material de apoyo:

Permisos especiales en Linux: Sticky Bit, SUID, SGID: <https://www.ochobitshacenunbyte.com/2019/06/17/permisos-especiales-en-linux-sticky-bit-suid-y-sgid/>

El permiso SUID; <http://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/doc-curso-salamanca-admin-avanzada/html/ch08s06.html>

GTFOBins: <https://gtfobins.github.io/>

### **Ejercicios**

**EJERCICIO DE EXPLOTACION DE PRIVILEGIOS :**

Os animamos a nos enviéis un reporte PDF explotando otro binario del sistema con privilegios SUID, mostrando como partiendo de un usuario no privilegiado, es posible convertirse en un usuario (root)

**IMPORTANTE:** No es necesario enviar los ejercicios. En caso de dudas enviar el ejercicio a través del soporte.

## Explotación y abuso de los privilegios

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu3cl4bi57dcbr62pntg?time=1&autoplay=true&crosstime=566>

### **Ejercicio**

**EJERCICIO DE EXPLOTACION DE PRIVILEGIOS :**

Os animamos a que realicéis el ejercicio explotando otra mala configuración definida en el sistema, mostrando como partiendo de un usuario no privilegiado, es posible convertirse en un usuario (root)

posible convertirse en un usuario privilegiado (root).

En nuestro caso, hemos estado tocando el archivo ‘/etc/passwd’ para que otros puedan escribir, pero no es el único archivo que supone un riesgo.

¡A investigar!

**IMPORTANTE:** No es necesario enviar el ejercicio.

## Explotación de tareas Cron

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu3i2tri57dcbr62q7lg?&autoplay=true&crosstime=191>

### **Recomendaciones/Notas**

Material para profundizar acerca de las tareas de Cron

Como utilizar Cron y Contrab en Linux: <https://www.redeszone.net/tutoriales/servidores/cron-crontab-linux-programar-tareas/>

## Detección de tareas Cron a través de un script Bash

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu3ipl3i57dcbr62q9s0?&autoplay=true&crosstime=565>

## Explotación de un PATH, hijacking frente a un binario SUID

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu3vpmmje35bt9chem90?&autoplay=true&crosstime=326>

## Explotación de un PATH, hijacking frente a un binario SUID 2

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu41cn3i57dcbr62re90?&autoplay=true&crosstime=427>

## Explotación y abusos de las capabilities en Linux

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu46t0ji57dcbr62rts0?&autoplay=true&crosstime=311>

### **Recomendaciones/Notas**

Material de apoyo:

Capabilities – Linux Manual Page : <https://www.incibe-cert.es/blog/linux-capabilities>

Linux Kernel capabilities – No solo de sudo vive el root: <https://www.incibe-cert.es/blog/linux-capabilities>

### **Ejercicio**

**EJERCICIO DE EXPLOTACION DE LAS CAPABILITIES :**

Os animamos a que practiquéis explotando otro binario del sistema al que previamente le hayais asignado una Capabilities tal que, tras su explotación, sea posible partiendo de un usuario no privilegiado, convertirse en un usuario (root).

Os hacemos recordar que en la página de GFTFObins, contáis con distintos

**EJEMPLOS**: <https://gtfobins.github.io/>

**IMPORTANTE:** No es necesario enviar el ejercicio

# **Pentesting**

## ¿Qué es el pentesting?

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu3iag3i57dcbr62q8bg?&autoplay=true&crosstime=329>

## Fase de reconocimiento inicial: Enumeración de puertos con nmap

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu48cd6je35bt9chfe60?&autoplay=true&crosstime=627>

### **Recomendaciones/Notas**

Material de apoyo

Nmap: Descarga, instalación y manual de uso paso a paso: <https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/>

## Creando una pequeña utilidad en Bash para filtrado de puertos

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu4b1iri57dcbr62sbag?&autoplay=true&crosstime=833>

## Detección de versión y servicios con Nmap

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu4bll6je35bt9chfof0?&autoplay=true&crosstime=269>

### **Recomendaciones/Notas**

Material de apoyo

Tutorial y listado de comandos más útiles para nmap: <https://protegermipc.net/2018/11/07/tutorial-y-listado-de-comandos-mas-utiles-para-nmap/>

## Técnicas para agilizar nuestros escaneos con nmap

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu60nquje35bt9chj03g?&autoplay=true&crosstime=237>

### **Recomendaciones/Notas**

Material de apoyo

Como usar Nmap, tutorial para principiantes: <https://esgeeks.com/como-usar-nmap-con-comandos/#:~:text=Nmap%20es%20una%20utilidad%20muy,puerto%20correspondiente%20(detecci%C3%B3n%20de%20servicios)>

## Creación de herramientas en Bash para detección de puertos TCP abiertos

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6143mje35bt9chj0l0?&autoplay=true&crosstime=553>

### **Recomendaciones/Notas**

Material de apoyo

Guia de Scripting en Bash : <https://www.hostinger.es/tutoriales/bash-script-linux/>

## Creación de herramientas en Bash para el descubrimiento de equipos en la red

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu61b9uje35bt9chj0r0?&autoplay=true&crosstime=230>

### **Recomendaciones/Notas**

Material de apoyo

Scripting en Bash paso a paso: <https://likegeeks.com/es/script-de-bash-tutorial/>

## Reconocimiento a través de los scripts que incorporan Nmap por categoría

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6225ji57dcbr62vl6g?&autoplay=true&crosstime=548>

### **Recomendaciones/Notas**

Ejercicio :

Os animo a que probéis categorías de Nmap, asi como scripts específicos de utilidad que aporten información de valor para un atacante.

Estos scripts puedes probar a lanzarlos sobre los servicios que esten activos en tu router, o en su defecto, sobre algún equipo que forme parte de tu segmento de red (también puedes ser sobre tu propio equipo).

## Uso de scripts específicos de Nmap y uso de analizadores de trafico

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu630cji57dcbr62vmig?&autoplay=true&crosstime=855>

### **Recomendaciones/Notas**

Material de apoyo

Ejemplos de uso con tcpdump: <https://rm-rf.es/tcpdump-ejemplos/>

Ejemplos de uso con tshark: <https://webimprints.medium.com/un-analizador-de-paquetes-ligero-y-f%C3%A1cil-de-usar-tshark-372e4b5854e0>

Ejercicio :

Con la herramienta ‘tcdump’ captura tráfico proveniente de una traza ICMP enviada desde tu equipo.  
A través de ‘tshark’, filtra en formato JSON haciendo uso de los parámetros de la propia herramienta, por el campo que corresponde a la dirección IP origen y destino.

## Uso de WireShark para el análisis del trafico de red

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu63iqmje35bt9chj3v0?&autoplay=true&crosstime=353>

### **Recomendaciones/Notas**

Material de apoyo

Ejemplos de uso de WireShark: <https://sites.google.com/site/practicasuptxabraham/3-3practica-de-laboratorio-uso-de-wireshark-para-ver-el-trafico-de-la-red>

Ejercicio practica:

En base a lo visto en la clase anterios, os animo a probar a interceptar una petición donde se esten tramitando datos a través del motodo POST.  
Esto puede ser en un panel Login o en algún formulario donde posteriormente se emitan los datos a través de este método.

## Creación de script en Pyhton3 para identificar el sistema operativo

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu646cji57dcbr62vo6g?&autoplay=true&crosstime=642>

### **Recomendaciones/Notas**

Material de apoyo

Curso de Python de Nate G.

## Terminamos el script en Python3 para identifica el OS

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu65ue6je35bt9chj82g?&autoplay=true&crosstime=369>

### **Recomendaciones/Notas**

Material de apoyo

Curso de python de Nate G.

Ejercicio práctico con Python:

En base al script elaborado en la clase anterior, trata de incorporar un manejo de excepciones de forma que se tenga control del input que el usuario esta introduciendo a la hora de proporcionar un argumento al programa.

## Uso de Wfuzz para hacer fuzzing

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6bh26je35bt9chjklg?&autoplay=true&crosstime=656>

### **Recomendaciones/Notas**

Material de apoyo

Wfuzz – The Web Fuzzer : <https://wfuzz.readthedocs.io/en/latest/>

Fuzzing con Wfuzz: <https://blog.hackingcodeschool.net/fuzzing-con-wfuzz/>

## Fuzzing de extensiones de archivo con Wfuzz (Uso de múltiples payloads)

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6jgpeje35bt9chk19g?&autoplay=true&crosstime=320>

### **Recomendaciones/Notas**

Material de apoyo

Como hacer pruebas de penetración con Wfuzz: <https://noticiasseguridad.com/importantes/como-hacer-pruebas-de-penetracion-de-con-wfuzz/>

Wfuzz (navaja suiza de pentesting) [1/3]: <https://www.pinguytaz.net/index.php/2019/10/18/wfuzz-navaja-suiza-del-pentesting-web-1-3/>

Wfuzz (navaja suiza de pentesting) [2/3]: <https://www.pinguytaz.net/index.php/2019/10/22/wfuzz-navaja-suiza-del-pentesting-web-2-3/>

Wfuzz (navaja suiza de pentesting) [3/3]: <https://www.pinguytaz.net/index.php/2019/10/28/wfuzz-navaja-suiza-del-pentesting-web-3-3/>

## Uso de Dirbuster para hacer Fuzzing

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6kplri57dcbr630lmg?&autoplay=true&crosstime=296>

### **Recomendaciones/Notas**

Material de apoyo

Escaneando contenido web con Dirbuster: <https://byte-mind.net/escaneando-contenido-web-con-dirbuster/>

Como listar directorios y archivos de un sitio web usando Dirbuster: <https://ourcodeworld.co/articulos/leer/417/como-listar-directorios-y-archivos-de-un-sitio-web-utilizando-dirbuster-en-kali-linux>

## Uso de Dirb para hacer Fuzzing

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6m0lri57dcbr630nu0?&autoplay=true&crosstime=169>

### **Recomendaciones/Notas**

Material de apoyo

Dirb – documentacion : <https://kali-linux.net/article/dirb/#:~:text=El%20objetivo%20principal%20de%20DIRB,otros%20scanner%20CGI%20no%20encuentran>

## Uso de GoBuster para hacer Fuzzing

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6m8dmje35bt9chk6a0?&autoplay=true&crosstime=228>

### **Recomendaciones/Notas**

Material de apoyo

Escanear paginas web y sus directorios con GoBuster: <https://comandoit.com/escanear-paginas-web-y-sus-directorios-con-gobuster/>

## Uso de DirSearch para hacer Fuzzing

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6mtgji57dcbr630qa0?&autoplay=true&crosstime=258>

### **Recomendaciones/Notas**

Material de apoyo

DirSearch – Brute Force a directorios y archivos en sitios web: <https://hackingenvivo.blogspot.com/2017/08/dirsearch-brute-force-directorios-y.html>

## Técnicas de enumeración bajo un servidor web

### **Vidéo**

<https://platform.thinkific.com/videoproxy/v1/play/bu6ngs6je35bt9chk95g?&autoplay=true&crosstime=716>

### **Recomendaciones/Notas**

Material de apoyo

Escanear un siervidor usando Nikto: <http://www.reydes.com/d/?q=Escanear_un_Servidor_Web_utilizando_Nikto>

WPScan – Escaner de vulnerabilidades para WordPress: <https://byte-mind.net/wpscan-escaner-de-vulnerabilidades-para-wordpress/>

Identificar la existencia de un FireWall para aplicaciones web usando WafW00f: <http://www.reydes.com/d/?q=Identificar_la_Existencia_de_un_Firewall_para_Aplicaciones_Web_utilizando_wafw00f>

## Técnicas de enumeración bajo un servidor web 2

### **Vidéo**

<https://platform.thinkific.com/videoproxy/v1/play/bu6nu2uje35bt9chka50?&autoplay=true&crosstime=251>

## Hackeando nuestra primera maquina

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6q5hbi57dcbr6311h0?&autoplay=true&crosstime=788>

## Hackeando nuestra primera máquina 2

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6r99ji57dcbr6315j0?&autoplay=true&crosstime=753>

## Tratamiento de la TTY tras una intrusión

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu6rks3i57dcbr6316sg?&autoplay=true&crosstime=218>

## ¿Cómo identificar una vulnerabilidad?

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu7hofeje35bt9chme2g?&autoplay=true&crosstime=57>

## Uso de searchploit y exploit-db para la búsqueda de vulnerabilidades

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu7vusri57dcbr6341rg?&autoplay=true&crosstime=539>

### **Recomendaciones/Notas**

Material de apoyo

Como usar SearchPloit para encontrar exploits: <https://blog.ehcgroup.io/2018/11/27/01/00/39/4198/como-usar-searchsploit-para-encontrar-exploits/hacking/ehacking/>

## Diferencias entre vulnerabilidades locales y remotas

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu80ekuje35bt9chnffg?&autoplay=true&crosstime=73>

## Uso de la herramienta Metasploit

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu80v2ri57dcbr6343e0?&autoplay=true&crosstime=382>

### **Recomendaciones/Notas**

Material de apoyo

Como utilizar Metasploit con Kali Linux: <https://comandoit.com/como-utilizar-metasploit-con-kali-linux/>

Explotando una vulnerabilidad con Metasploit Framework: <https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra>

## Creación de un Listener desde Metasploit y acceso al equipo comprometido

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu8987ri57dcbr634rdg?&autoplay=true&crosstime=242>

### **Recomendaciones/Notas**

Material de apoyo

Como utilizar Metasploit con Kali Linux: <https://comandoit.com/como-utilizar-metasploit-con-kali-linux/>

Explotando ua vulnerabilidad con Metasploit Framework: <https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra>

## Explotación manual de la vulnerabilidad anteriormente encontrada

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu89nqbi57dcbr634sv0?&autoplay=true&crosstime=400>

## Uso de la herramienta BurpSuite

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu8uacmje35bt9chpqv0?&autoplay=true&crosstime=478>

### **Recomendaciones/Notas**

Material de apoyo

Tutorial de BurpSuite desde cero paso a paso: <https://www.manusoft.es/tutorial-burp-suite/>

## BurpSuite – Definicion del Scope y comprometiendo un servidor web

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu98t7eje35bt9chqj8g?&autoplay=true&crosstime=713>

### **Recomendaciones/Notas**

Material de apoyo

Traget Scope – PortSwigger : <https://portswigger.net/burp/documentation/desktop/tools/target/scope>

## BurpSuite – Comprometemos el servidor web y accedemos al sistema

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu9aegri57dcbr637asg?&autoplay=true&crosstime=335>

### **Recomendaciones/Notas**

Material de apoyo

BurpSuite – La navaja Suiza del Pentester : <https://fwhibbit.es/burp-suite-i-la-navaja-suiza-del-pentester>

## BurpSuite – Uso de Repeater y explotando un caso práctico

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu9afbbi57dcbr637atg?&autoplay=true&crosstime=283>

### **Recomendaciones/Notas**

Material de apoyo

Using Burp Repeater – PortSwigger : <https://portswigger.net/burp/documentation/desktop/tools/repeater/using>

## BurpSuite – Uso del Intruder y explotando un caso practico

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu9aut6je35bt9chqoe0?&autoplay=true&crosstime=267>

### **Recomendaciones/Notas**

Material de apoyo

Using Burp Intruder – PortSwigger : <https://portswigger.net/burp/documentation/desktop/tools/intruder/using>

## ¿Qué es HackTheBox?

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bu9clbmje35bt9chqrrg?&autoplay=true&crosstime=517>

## Explotando vulnerabilidad Local File Inclusión (LFI)

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bua0pkmje35bt9chs32g?&autoplay=true&crosstime=567>

### **Recomendaciones/Notas**

Material de apoyo

¿Como funciona la vulnerabilidad Local File Inclusion?: <https://www.welivesecurity.com/la-es/2015/01/12/como-funciona-vulnerabilidad-local-file-inclusion/>

## Explotando vulnerabilidad Local File Inclusion (LFI) 2

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bua112eje35bt9chs3b0?&autoplay=true&crosstime=378>

### **Recomendaciones/Notas**

Material de apoyo

Local File Inclusion – Cheat Sheet (Wrappers): <https://ironhackers.es/herramientas/lfi-cheat-sheet/>

## Explotando vulnerabilidad Log Poisoning – LFI to RCE

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buac0tji57dcbr639b50?&autoplay=true&crosstime=702>

### **Recomendaciones/Notas**

Material de apoyo

From LFI to RCE : <https://platform.thinkific.com/videoproxy/v1/play/buac0tji57dcbr639b50?&autoplay=true&crosstime=702>

## Explotando vulnerabilidad Remote File inclusión (RFI)

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bua1h3bi57dcbr638nj0?&autoplay=true&crosstime=428>

### **Recomendaciones/Notas**

Material de apoyo

Inclusion de ficheros remotos (RFI): <https://www.cyberseguridad.net/inclusion-de-ficheros-remotos-rfi-remote-file-inclusion->

## Explotando vulnerabilidad HTML injection y XSS (Cross-Site Scripting)

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bua2123i57dcbr638o60?&autoplay=true&crosstime=699>

### **Recomendaciones/Notas**

Material de apoyo

Excess XSS: A comprehensive tutorial on cross-site Scripting: <https://excess-xss.com/>

XSS: ¿qué es y cómo funciona el Cross-Site Scripting?: <https://blogs.imf-formacion.com/blog/tecnologia/xss-que-es-y-como-funciona-201805/>

## Explotando vulnerabilidad Cross-Site Request Forgery(CSRF)

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bua27g6je35bt9chs4u0?&autoplay=true&crosstime=316>

### **Recomendaciones/Notas**

Material de apoyo

CSRF ¿Como funcionan los ataques Cross-Site Request Forgery?: <https://www.ionos.es/digitalguide/servidores/seguridad/cross-site-request-forgery/>

## Explotando vulnerabilidad Server-Side Request Forgery (SSRF)

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bua379ri57dcbr638r2g?&autoplay=true&crosstime=707>

### **Recomendaciones/Notas**

Material de apoyo

Como explotar un SSRF : <https://www.elladodelmal.com/2015/04/ssrf-server-side-request-forgery-xspa.html>

Como funciona un Server Side Request Forgery: <https://empresas.blogthinkbig.com/como-funciona-server-side-reques/>

## Explotando vulnerabilidad SQL injection – SQLmap

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buabcsji57dcbr639aag?&autoplay=true&crosstime=954>

### **Recomendaciones/Notas**

Material de apoyo

SQLMap – Herramienta de inyeccion SQL: <https://www.solvetic.com/tutoriales/article/1615-sqlmap-herramienta-de-inyecci%C3%B3n-de-sql-y-ethical-hacking-de-bases-de-datos/#:~:text=Esta%20herramienta%20sirve%20para%20testear,de%20una%20base%20de%20datos>.

## Explotando vulnerabilidad SQL injection – Método manual

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buacckbi57dcbr639bc0?&autoplay=true&crosstime=394>

### **Recomendaciones/Notas**

Material de apoyo

MYSQL por linea de comandos: <https://desarrolloweb.com/articulos/2408.php>

## Explotando vulnerabilidad SQL injection – Método manual 2

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bual4ebi57dcbr639la0?&autoplay=true&crosstime=715>

## Explotando vulnerabilidad SQL injection – Método manual 3

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buam2buje35bt9cht21g?&autoplay=true&crosstime=445>

### **Recomendaciones/Notas**

Material de apoyo

Inyección SQL – Manual básico : <https://www.redeszone.net/seguridad-informatica/inyeccion-sql-manual-basico/>

## Explotando vulnerabilidad Padding Oracle Attack – Padbuster

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buamdf3i57dcbr639me0?&autoplay=true&crosstime=482>

### **Recomendaciones/Notas**

Material de apoyo

Explotar Padding Oracle para obtener claves de cifrado: <https://www.hackplayers.com/2018/10/explotar-padding-oracle-para-obtener-clave.html>

## Explotando vulnerabilidad Padding Oracle Attack – BurpSuite Bit Flipper Attack

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buamlnmje35bt9cht2mg?&autoplay=true&crosstime=404>

### **Recomendaciones/Notas**

Material de apoyo

Breaking excrypted data using BurpSuite: <https://portswigger.net/blog/breaking-encrypted-data-using-burp>

## Explotando vulnerabilidad ShellShock

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buamtvji57dcbr639n70?&autoplay=true&crosstime=250>

### **Recomendaciones/Notas**

Material de apoyo

ShellShock – Error de Software : <https://es.wikipedia.org/wiki/Shellshock_(error_de_software)>

## Explotando vulnerabilidad XML External Entity Injection (XXE)

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buana06je35bt9cht3ig?&autoplay=true&crosstime=541>

### **Recomendaciones/Notas**

Material de apoyo

Explorando la vulnerabilidad XXE : <https://backtrackacademy.com/articulo/explorando-la-vulnerabilidad-xxe-xml-external-entity>

Entendiendo y explotando XXE: <https://underc0de.org/foro/bugs-y-exploits/entendiendo-y-explotando-xxe-(external-xml-entities)/>

## Explotando vulnerabilidad Domain Zone Transfer

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buankd6je35bt9cht3ug?&autoplay=true&crosstime=248>

### **Recomendaciones/Notas**

Material de apoyo

Transferencia de Zona DNS : <https://es.wikipedia.org/wiki/Transferencia_de_zona_DNS>

¿De que se trata un ataque de transferencia de zona?: <https://www.welivesecurity.com/la-es/2015/06/17/trata-ataque-transferencia-zona-dns/>

## Explotando vulnerabilidades de tipo Insecure Deserialization

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bubbtgbi57dcbr63aujg?&autoplay=true&crosstime=620>

### **Recomendaciones/Notas**

Material de apoyo

What is insecure Deserialization ?: <https://www.acunetix.com/blog/articles/what-is-insecure-deserialization/>

## Explotando vulnerabilidad Type Juggling sobre panel Login

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bubteg3i57dcbr63cg00?&autoplay=true&crosstime=820>

## Concepto de escalada de privilegios

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bubu8lri57dcbr63ci3g?&autoplay=true&crosstime=106>

## Abuso del Sudoers para escalar privilegios

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bubugsuje35bt9chvv9g?&autoplay=true&crosstime=168>

## Abuso de permisos SUID para escalar privilegios

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bubus9eje35bt9ci00dg?&autoplay=true&crosstime=142>

### **Recomendaciones/Notas**

¿Como funcionan los permisos SUID?: <https://www.luisguillen.com/posts/2017/12/como-funcionan-permisos-suid/>

## Avuso de las Capabilities para escalar privilegios

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bubv4cuje35bt9ci011g?&autoplay=true&crosstime=135>

### **Recomendaciones/Notas**

Material de apoyo

Linux Kernel Capabilities : <https://www.incibe-cert.es/blog/linux-capabilities>

## PATH Hijacking/Library Hijacking

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bubvdlbi57dcbr63cl20?&autoplay=true&crosstime=293>

## Abuso del Kernel para escalar privilegios

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/bubvqomje35bt9ci02pg?&autoplay=true&crosstime=247>

## Reconocimiento del sistema

### **Video**

<https://platform.thinkific.com/videoproxy/v1/play/buc03p6je35bt9ci037g?&autoplay=true&crosstime=161>