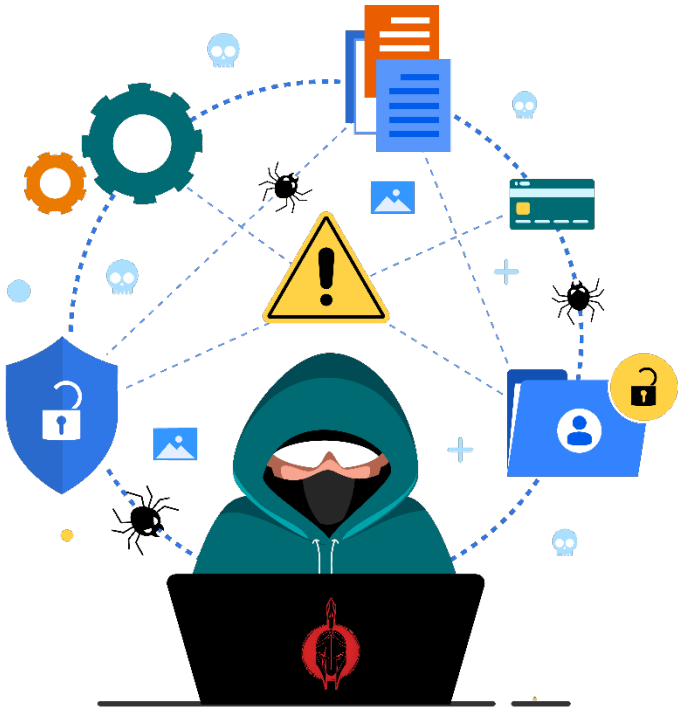
# CURSO PROFESIONAL DE PENTESTING PARA JUNIORS

## Spartan-Cybersecurity



# ADVERTENCIA

Todos los derechos reservados. Ninguna parte de esta publicación, en su totalidad o en parte, puede ser reproducida copiada, transferida o cualquier otro derecho reservado a su propietario, incluyendo la fotocopia y cualquier otra copia, cualquier transferencia o transmisión utilizando cualquier red u otros medios de comunicación, cualquier emisión para el aprendizaje a distancia, en cualquier forma o por cualquier medio, como cualquier sistema de almacenamiento, transmisión o recuperación de información, sin autorización escrita del autor.

TODO nuestro contenido publicado se realiza con fines educativos, informativos y éticos.

TODAS las técnicas expuestas en este curso son desarrolladas y ejecutadas en entornos controlados.

¡NO SOMOS RESPONSABLES DEL MAL USO QUE LE PUEDAN DAR!

# TABLA DE CONTENIDO

9) Enumeración SMB
    a) Caso practico
        i) Comprometiendo un Windows 10 con SMBGhost – (CVE-2020-0796)
        ii) Accediendo a información sensible en un SMB publico
10) Enumeración FTP
    a) Caso practico
        i) Acceso a información sensible por medio de FTP anonimo
11) Enumeración Web
    a) Descubrimiento de directorios y ficheros
    b) Identificación de vulnerabilidades
    c) Reconocimiento de vulnerabilidades
    d) Explotación de vulnerabilidades
        i) XSS
        ii) SQLI
            (1) Troubleshooting vulnerabilidades (Blind Injection)
        iii) RCE y WebShell
            (1) Caso practico
                (a) Abusando de controles mal configurados para subir webshells sobre uploaders
        iv) Utilizando CVE
            (1) Caso practico
                (a) Explotación de Log4Shell – (CVE-2021-44228)
        v) Encadenamiento de vulnerabilidades
            (1) Caso practico
                (a) SSRF + SSTI
    e) Detectando vulnerabilidades en CMS
        i) Comprometiendo Wordpress
    f) Obteniendo RCE sobre un Jenkins
12) Escalamiento de privilegios
    a) Linux
        i) Caso practico
            (1) Abusando de NOPASSWD sobre SUDO
            (2) Abusando de CRONTABS mal configurados

- b) Windows
  - i) Caso practico
    - (1) Explotación de CVE-2017-7344 – (FortiClient)

13) Introducción a Active Directory
- a) Enumeración con AdPEAS.ps1
- b) Creación de macros maliciosas para Microsoft Word
- c) Caso practico
  - i) Comprometiendo un Windows Server con ZeroLogon

14) Introducción a la evasión de antivirus
- a) Bypass AMSI

15) Ataques de fuerza bruta
- a) Password Cracking
- b) Caso practico
  - i) Fuerza bruta sobre login de aplicativo web en NodeJs
  - ii) Fuerza bruta sobre archivos con contraseña

16) Tunneling
- a) Local Port Forward
- b) Remote Port Forward
- c) Socks Proxies
- d) Caso practico
  - i) Pivoting utilizando SSH dinámico con Proxychains

17) Introducción al buffer Overflow
- a) Explotación de un buffer overflow en Windows

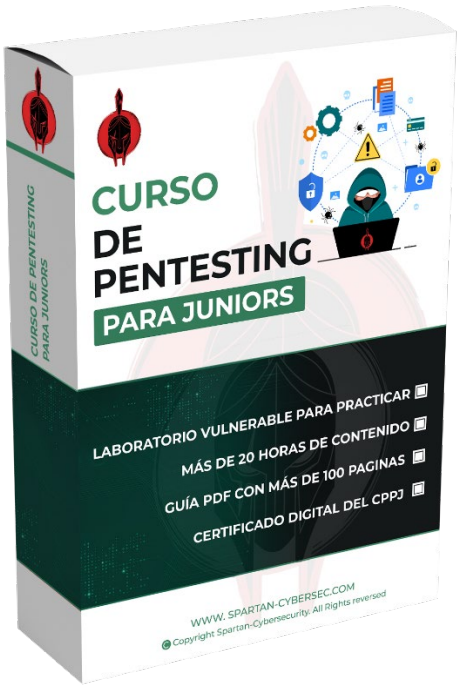
18) Introducción al pentesting cloud
- a) Caso Practico
  - i) Post-explotacion en EC2

19) Conociendo un HoneyPot

20) Introducción a Command & Control – (C2)
- a) Utilizando Metasploit

21) Desarrollo de informes técnicos

# DETALLES DEL CURSO




**Material entregable:**

- ✓ Acceso a más de 20 horas de contenido en MATERIAL GRABADO.
- ✓ Libro PDF de 130 páginas.
- ✓ Acceso a laboratorio vulnerable para hackear una infraestructura de 10 servidores.
- ✓ Acceso a un grupo exclusivo del curso para interactuar con los demás estudiantes y el profesor.
- ✓ Certificado del CPPJ por parte de Spartan-Cybersecurity.

**Costo del curso:** $200 USD

**Comunícate con el área de ventas para conocer nuestros descuentos:**

**WhatsApp:** https://wa.link/j265a0

**Telegram:** https://t.me/Spartan_Cybersecurity

**Te esperamos** 😎