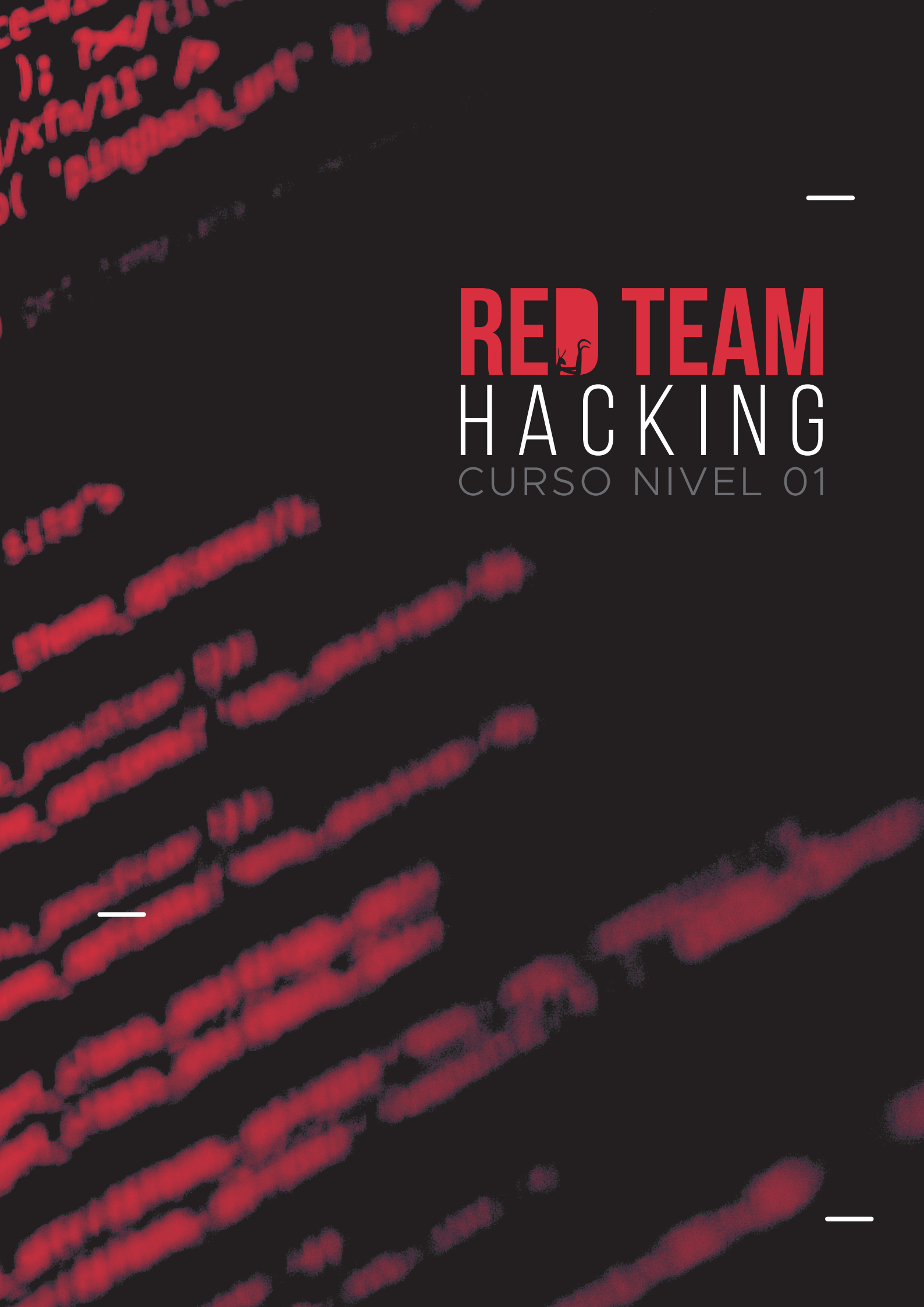

RED TEAM HACKING

CURSO NIVEL 01

RED TEAM HACKING

CURSO NIVEL 01

El curso de **Red Team Nivel I Hacking Fundamentals** es un curso de dos días intensivos que busca un equilibrio entre la persona que quiere iniciarse en el mundo del Hacking y aquellas personas que ya cuentan con algunos conceptos y conocimientos técnicos básicos, pero que quiere profundizar en el mismo.

El curso está orientado a Estudiantes de Sistemas, Analistas de Seguridad Informática, Jefes y/o CISOs de Seguridad informática que quieran profundizar sus conocimientos y cualquier persona con curiosidad y pasión por la tecnología y la seguridad.

Es un curso orientado netamente a la práctica por lo que está diseñado para que sea 30% de Teoría y un 70 % de Práctica, generando un enfoque en dónde el alumno, al terminar el mismo, conozca y pueda poner rápidamente los conocimientos adquiridos en práctica.

En el curso, y dentro de la fase netamente práctica, el alumno tendrá la oportunidad de realizar ejercicios y prácticas con laboratorios provistos por el instructor, los cuales estarán conformados tanto por máquinas virtuales que se entregarán a los alumnos, como así también, a través de una serie de web sites específicos para las mismas, y en dónde se usarán una variedad de herramientas para todas las diferentes fases.

MÓDULOS

01

INTRODUCCIÓN AL HACKING Y SUS FASES

- Diferencias entre un ejercicio de Penetration test de un Red Team.
- Diferencias entre un servicio de Pentest y un vulnerability scanning.
- Principales Frameworks y Metodologías de Penetration Test.

02

FASE DE RECONOCIMIENTO Y ENUMERACIÓN PASIVA

- Técnicas de OSINT y Enumeración Pasiva.
- Google hacking y Censys.io
- Sitios y buscadores on line especializados.
- Escaneos SSL.
- Búsqueda de metadatos en documentos públicos.
- Enumeración Pasiva a través de Command Line Interface (CLI).
- Buscadores IoT (Shodan)
- Herramientas All in One para la automatización.
- El mundo de las APIs para la automatización.

Laboratorios varios y prácticas del Módulo 1

ENUMERACIÓN ACTIVAY VULNERABILITY SCANNING

03

- Fingerprintingde servicios comunes a través de línea de comando (Whois, nslookup, dig, etc).
- Identificación de rangos IP e IPs vivas a través de técnicas de barridos de ping.
- Port scanning a través de Nmap y ZenMap.
- Nmap Port states (Estados de puertos).
- Técnicas de escaneo con Nmap.
- Nmap Scripting.
- Laboratorios de CLI y Nmap.
- Vulnerability Scanning.
- Conceptos fundamentales de Vulnerability Scanning.
- Tipos de escaneos.
- Introducción a Nessus.
- Laboratorios de Nessus.
- Introducción a OpenVAS.
- Administración de OpenVAS.
- Laboratorios de OpenVAS.
- Introducción a NMAP Scripting para Vulnerability Scanning.
- Laboratorio y uso de NMAP scripting para Vulnerability Scanning.

EXPLOTACIÓN Y POST EXPLOTACIÓN

04

- Introducción y conceptos de fase de explotación.
- Cenceptos de exploit.
- Introducción a Metasploit.
- Arquitectura de Metasploit.
- Comandos básicos de Metasploit.
- Integración de NMAP y OpenVAS desde Metasploit.
- Integración y uso de Nessus desde Metasploit.
- Escaneo y explotación de servicios con módulos auxiliares de metasploit.
- Introducción y conceptos de fase de Post Explotación.
- Introducción a Meterpreter.
- Comandos de Meterpreter.
- Usando Meterpreter.

Laboratorios varios de Explotación y Post Explotación.

HACKING WIRELESS

05

- Estándares Relevantes.
- Conceptos de modo de operación.
- Modos y tipos de Infraestructura.
- Autenticación.
- Cifrado.
- Hardware.
- Fases de ataque.
- Rogue Access Points.

Demos y Laboratorios varios de hacking Wifi.

CONOCIMIENTOS NECESARIOS

Se requiere que el participante, para poder aprovechar al máximo el curso, tenga conocimientos básicos y mínimos de fundamentos de Redes, modelo OSI y protocolo TCP/IP, cómo así también un manejo, al menos básico, de Windows y de Linux (poder trabajar en una consola CMD o Bash Shell). Si bien se iniciará, en una primera instancia, con un fuerte repaso a los conceptos del pentest y sus fases implícitas desde cero, el curso luego pasará directamente a prácticas sobre máquinas virtuales y sitios web.

EQUIPAMIENTO

El alumno deberá concurrir con su propio equipo portátil o laptop, el cual debería tener como configuración recomendada un procesador de tipo Intel I5 o I7 con al menos 8GB de memoria RAM y unos 90GB de espacio libre en disco, para poder instalar las virtuales con las que se trabajará.

CONTACTO

dgbruno@blackmantisecurity.com

+54 911 58101244

@BlackMantisSeg

BLACKMANTISECURITY

Porto . Trentalance
Antúnez & asociados

Gestión de la Información
Seguridad . Calidad . Tecnología