Formación en Hacking Ético e Certificación Red Team Certified Professional

Descrición

Trátase dunha completa formación en Hacking Ético que contén os seguintes módulos:

- Hacking en Sistemas (20 horas)
- Entrenamento Hacking Ético Vol. 1 (20 horas)
- Hacking Ético Web (20 horas)
- Hacking Windows Vol.1 (20 horas)
- Hacking Windows Vol.2 (20 horas)
- Entrenamento Hacking Ético Vol.2 (20 horas)
- Exame de certificación RTCP (Red Team Certified Professional) (8 horas)

HORARIO DO CURSO: de luns a xoves de 16:00 a 21:00 horas os seguintes días:

- Marzo: os días 1 a 4, 15 a 18

- Abril: 5 a 8 e 19 a 22

- Maio: 3 a 6, 13 e 18 a 20

Exame de certificación presencial o 2 de xuño de 14:00 a 22:00 horas.

Obxectivos

Facilitar ao alumnado puntos de partida sólidos en Hacking Ético, tanto a nivel sistemas en xeral (Windows ou UNIX), web, así como un alto nivel de especialización en ataques a redes Microsoft modernas. Todo esto realizado dende un punto de vista que incide no práctico, apoiado en laboratorios específicos para replicar o explicado polo profesor.

Dirixido a

Profesionais do hacking ético, auditoras/es de ciberseguridade ou administradoras/es de sistemas con curiosidade en hacking ético con interese en mellorar as súas cualificacións e especializarse no mundo do Hacking Ético.

Debe terse en conta que:

- Os cursos requiren traballo adicional ás horas adicadas na clase.
- A realización dos cursos esize adicación plena durante as horas de clase.
- As formacións, documentación, titorías, forma de comunicación cos profesores e o exame será únicamente en idioma castelán.

BENEFICIOS Opción gratuita dun exame de certificación oficial

Diploma de asistencia

Perfil do docente

Enxeñeira/o en sistemas pola UNAL (Universidad Nacional de Colombia), Master oficial en software libre. Offensive Security Certified Professional (OSCP). Profesional con 14 anos de experiencia en desenvolvemento, sistemas, auditorías de código, así como execución de auditorías de seguridade, pentesting e hacking ético.

PROGRAMA Programación 2026/27

TIPO CURSO

MATRÍCULA Gratuíta

PERIODO INSCRICIÓN 01/02/2027 - 15/02/2027

PROBA DE SELECCIÓN 16/02/2027 (00:00)

CRITERIOS DE SELECCIÓN Proba técnica presencial no CNTG en Santiago de Compostela

Nº PRAZAS	20 (Mínimo 10)
METODOLOXÍA	Virtual
TIPO DE EDICIÓN	Edición única tarde (desempregados/as e ocupados/as)
DURACIÓN	120 horas
DATA INICIO	01/03/2027
DATA FIN	20/05/2027
HORARIO	De luns a xoves de 16:00 a 21:00 horas. Días de docencia:
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	RTCP: Red Team Certified Professional
MÓDULOS TRANSVERSAIS	Igualdade de 10 horas
TECNOLOXÍA	Ciberseguridade/Ciberseguridad Securízame
PERIODO DOCENCIA	01/03/2027 - 20/05/2027

Temario

HACKING DE SISTEMAS

- Estrutura dun ataque e procedemento – metodoloxía para un pentest ofensivo
- Recolección de info en fontes abertas OSINT
- Uso completo de Nmap
- Detección e enumeración de servizos e de vulnerabilidades
- Uso escáneres de vulnerabilidades para a detección de vulnerabilidades

- Explotación con Metasploit Framework
- Introdución a exploits, shellcodes e payloads
- Creación manual de payloads para evasión de AVs
- Procesos de post-explotación en sistemas Linux e Windows
- Outras técnicas e ferramentas

HACKING WEB

- Introdución ao protocolo HTTP
- Introdución á construción de aplicacións web
- Configuración dun contorno de probas para pentesting web
- Uso de ferramentas para a análise de aplicacións web no lado do cliente
- Uso de servidores proxy web para pentesting
- Descrición do proxecto OWASP
- Aplicacións prácticas
- Exemplos prácticos
- Explotación de aplicacións web vulnerables
- Detección e explotación doutras vulnerabilidades e scripting para a automatización de ataques web

HACKING PRÁCTICO: EXPLOTACIÓN E POST-EXPLOTACIÓN EN WINDOWS

- Enumeración completa dun contorno AD: Usuarios, grupos, estacións de traballo, propiedades de usuarios existentes, controladores de dominio dispoñibles, relacións de confianza "intra-forest" e "inter-forest", políticas de grupo, ACLs etc.
- Explotación e elevación de privilexios en workstations. Elevación de privilexios en sistemas Windows, mecanismos de evasión de AVs e movementos laterais a outras máquinas do contorno
- Elevación de privilexios no dominio
- Técnicas para o descubrimento e extracción de credenciais e sesións de contas de dominio con privilexios altos e execución de ataques de repetición
- Técnicas de Kerberoasting e as súas variantes
- Técnicas de persistencia e ataques de confianza cruzada: Uso de técnicas que permitan executar e/ou modificar obxectos no dominio
- Enumeración completa de estacións de traballo e dominio utilizando GhostPack, Impacket e ferramentas do tipo C2
- Ataques IPv6 en contornos de Active Directory
- Técnicas de post-explotación avanzadas utilizando utilidades tales como PingCastle, BloodHound, CrackMapExec, Empire Framework entre outras
- Técnicas para executar movementos laterais. WMI Event Subscription, DCOM, DLL Hijacking, entre outras
- Técnicas de persistencia en estacións de traballo
- Técnicas de persistencia no dominio

ADESTRAMENTO 100% PRÁCTICO

- Neste adestramento poderás poñer en práctica os teus coñecementos sobre hacking, así como adquirir e aprender novos, mediante a práctica sobre plataformas reais, preparadas en laboratorio.

PROBA DE CERTIFICACIÓN

- O obxectivo desta certificación é que o alumnado demostre que é capaz de vulnerar sistemas nun contorno corporativo.