IMECAF®

www.imecaf.com

CURSO DE HACKING ÉTICO

TI

INVERSIÓN
$3,999.00 + IVA

DURACIÓN
40 HRS.

MODALIDAD
En Linea

Tel. 55 1085 1515 / 800 236 0800 | info@imecaf.com

CURSO DE HACKING ÉTICO

TI

OBJETIVO

El curso de Hacking Ético se enfoca en los conceptos básicos de las Pruebas de Penetración. También ayuda al estudiante a estar consciente de estrategias de ataque de redes y de contramedidas comunes. El Hacking Ético prepara a los estudiantes para usar varias herramientas de pruebas de penetración para analizar las redes en búsqueda de vulnerabilidades. El conocimiento de estas vulnerabilidades también ayuda a los estudiantes a entender como contrarrestarlaras y mejorar la seguridad de la red.

TEMARIO

I. **INTRODUCTION TO ETHICAL HACKING**
   a. Introduction
      i. Introduction to Ethical Hacker Pro (5:13)
      ii. Use the Simulator (14:55)
      iii. Explore the New Lab Features (10:17)

II. **INTRODUCTION TO PENETRATION TESTING**
   a. Penetration Testing Process and Types
      i. Penetration Test Process and Types (4:42)
      ii. Penetration Test Process and Types Facts
      iii. Practice Questions
   b. Threat Actors
      i. Threat Actor Types (6:35)
      ii. Threat Actor Type Facts
      iii. Practice Questions
   c. Target Selection
      i. Choose a Target (3:41)
      ii. Additional Scoping Considerations (5:05)

iii. Target Selection Facts
iv. Practice Questions

d. Assessment Types
   i. Assessment Types (4:49)
   ii. Special Considerations (2:08)
   iii. Assessment Type Facts
   iv. Practice Questions

e. Legal and Ethical Compliance
   i. Legal Compliance (5:54)
   ii. Ethics (2:37)
   iii. Authorization and Corporate Policies (3:52)
   iv. Legal and Ethical Compliance Facts
   v. Engagement Contracts (4:18)
   vi. Engagement Contract Facts
   vii. Practice Questions

III. SOCIAL ENGINEERING AND PHYSICAL SECURITY

a. Social Engineering
   i. Social Engineering Overview (4:46)
   ii. Social Engineering Overview Facts
   iii. Social Engineering Motivation (10:18)
   iv. Social Engineering Motivation Facts
   v. Social Engineering Techniques (10:16)
   vi. Social Engineering Technique Facts
   vii. Phishing and Internet-Based Techniques (4:59)
   viii. Phishing and Internet-Based Technique Facts
   ix. Use the Social Engineer Toolkit (SET) (4:24)
   x. Identify Social Engineering
   xi. Practice Questions

b. Physical Security
   i. Physical Security Overview (11:25)
   ii. Physical Security Facts

iii. Physical Security Attacks (6:32)
iv. Physical Security Attack Facts
v. Practice Questions

c. Countermeasures and Prevention
i. Countermeasures and Prevention (8:13)
ii. Countermeasures and Prevention Facts
iii. Implement Physical Security Countermeasures
iv. Practice Questions

IV. RECONNAISSANCE

a. Reconnaissance Overview
i. Reconnaissance Processes (4:56)
ii. Reconnaissance Process Facts
iii. Reconnaissance Tool Facts
iv. Google Hacking for Office Documents (4:19)
v. Perform Reconnaissance with theHarvester (4:51)
vi. Perform Reconnaissance with Nmap (4:14)
vii. Perform Reconnaissance with Nmap
viii. Practice Questions

b. Reconnaissance Countermeasures
i. Reconnaissance Countermeasures (3:01)
ii. View Windows Services (5:11)
iii. Disable Windows Services
iv. View Linux Services (4:14)
v. Manage Linux Services
vi. Enable and Disable Linux Services
vii. Reconnaissance Countermeasure Facts
viii. Disable IIS Banner Broadcasting (1:47)
ix. Hide the IIS Banner Broadcast
x. Practice Questions

V. SCANNING

a. Scanning Overview

i. Scanning Processes (5:54)
ii. Scanning Process Facts
iii. Scanning Tool Facts
iv. Perform a Scan with Nmap (4:36)
v. Perform an Internal Scan
vi. Perform an External Scan Using Zenmap
vii. Perform a Scan with Nmap Scripts (4:36)
viii. Scanning Considerations (5:38)
ix. Scanning Considerations Facts
x. Practice Questions

b. Banner Grabbing
i. Banner Grabbing (4:19)
ii. Banner Grabbing Facts
iii. Practice Questions

VI. ENUMERATION

a. Enumeration Overview
i. Enumeration (5:11)
ii. Enumerate a Windows System (4:00)
iii. Enumerate Windows (4:09)
iv. Enumerate a Linux System (6:55)
v. Enumeration Facts
vi. Enumerate with SuperScan (4:41)
vii. Enumerate with NetBIOS Enumerator (2:52)
viii. Enumerate Ports and Services Facts
ix. Perform Enumeration with Nmap
x. Enumerate with SoftPerfect (3:50)
xi. Perform Enumeration with Metasploit
xii. Perform Enumeration of MSSQL with Metasploit
xiii. Practice Questions

b. Enumeration Countermeasures
i. Enumeration Countermeasures (1:53)

ii. Enumeration Countermeasure Facts
iii. Disable DNS Zone Transfers (5:07)
iv. Prevent Zone Transfer
v. Practice Questions

VII. ANALYZE VULNERABILITIES

a. Vulnerability Assessment
   i. Vulnerability Assessment (8:41)
   ii. Vulnerability Assessment Facts
   iii. Conduct Vulnerability Scans (4:01)
   iv. Practice Questions
b. Vulnerability Management Life Cycle
   i. Vulnerability Management Life Cycle (6:20)
   ii. Vulnerability Management Life Cycle Facts
   iii. Vulnerability Solutions (2:20)
   iv. Vulnerability Solution Facts
   v. Practice Questions
c. Vulnerability Scoring Systems
   i. Vulnerability Scoring Systems (5:41)
   ii. Vulnerability Scoring System Facts
   iii. Practice Questions
d. Vulnerability Assessment Tools
   i. Vulnerability Assessment Tools (4:52)
   ii. Vulnerability Assessment Tool Facts
   iii. Scan a Network with Retina (7:16)
   iv. Scan a Network with Nessus (3:16)
   v. Scan for Vulnerabilities on a Windows Workstation
   vi. Scan for Vulnerabilities on a Linux Server
   vii. Scan for Vulnerabilities on a Domain Controller
   viii. Scan for Vulnerabilities on a Security Appliance
   ix. Scan for Vulnerabilities on a WAP
   x. Practice Questions

VIII. SYSTEM HACKING

a. System Hacking
   i. Introduction to Hacking (7:05)
   ii. Introduction to Hacking Facts
   iii. Keylogger Attack (5:18)
   iv. Analyze a USB Keylogger Attack
   v. Analyze a USB Keylogger Attack 2
   vi. Use Rainbow Tables (3:33)
   vii. Crack a Password with Rainbow Tables
   viii. Crack Passwords (8:02)
   ix. Crack Password Protected Files (3:22)
   x. Crack a Password with John the Ripper
   xi. Crack a Router Password (6:35)
   xii. Use L0phtCrack to Audit Passwords (2:46)
   xiii. Configure Password Policies (10:41)
   xiv. Configure Account Password Policies
   xv. Practice Questions

b. Privilege Escalation
   i. Privilege Escalation in Windows (7:15)
   ii. Use Bootable Media to Modify User Accounts (6:29)
   iii. Crack the SAM Database (4:17)
   iv. Change a Windows Password (3:03)
   v. Privilege Escalation in Windows Facts
   vi. Crack the SAM Database with John the Ripper
   vii. Configure User Account Control (6:57)
   viii. Enforce User Account Control
   ix. Practice Questions

c. Maintain Access
   i. Exploit Systems to Maintain Access (4:01)
   ii. Establish an Unauthorized SSH Connection (4:20)
   iii. Create a Backdoor with Metasploit (5:22)

iv. Create a Backdoor with Metasploit
v. Exploit Systems to Maintain Access Facts
vi. Create a Backdoor with Netcat
vii. Practice Questions

d. Cover Your Tracks
i. Cover Your Tracks (4:57)
ii. Clear Logs In Windows (3:01)
iii. Use CCleaner to Hide Tracks (4:41)
iv. Cover Your Tracks Facts
v. Clear Windows Log Files on Server 2016
vi. Clear Audit Policies
vii. Hide Programs (7:48)
viii. Use NTFS Data Stream to Hide Files (3:14)
ix. Use Steganography to Hide a File (3:20)
x. Hide Programs Facts
xi. Hide Files with OpenStego
xii. Practice Questions

IX. MALWARE

a. Malware
i. Malware Overview (9:40)
ii. Malware Overview Facts
iii. Trojans and Backdoors (5:36)
iv. Trojan and Backdoor Facts
v. Malware Concerns (3:51)
vi. Malware Concern Facts
vii. Malware Analysis (4:25)
viii. Create a Virus (2:34)
ix. Create a HTTP Trojan (3:12)
x. Use ProRat to Create a Trojan (3:14)
xi. Practice Questions

b. Combat Malware

i. Anti-Malware Software (5:04)
ii. Scan for Open Ports with Netstat (3:09)
iii. Track Port Usage with TCPView (2:31)
iv. Anti-Malware Software Facts
v. Detect Open Ports with Nmap
vi. View Open Ports with netstat
vii. Scan for Open Ports from a Remote Computer
viii. Counter Malware with Windows Defender
ix. Practice Questions

X. **SNIFFERS, SESSION HIJACKING, AND DENIAL OF SERVICE**

a. Sniffing
i. Sniffing (6:38)
ii. Sniffer Facts
iii. Sniff Network Traffic with Wireshark (6:49)
iv. Capture Traffic with TCPDump (5:40)
v. Use SMAC to Spoof MAC Addresses (3:45)
vi. Spoof MAC Addresses with SMAC
vii. Poison ARP (5:13)
viii. Poison ARP and Analyze with Wireshark
ix. Poison DNS (6:17)
x. Poison DNS
xi. Filter and Analyze Traffic with Wireshark
xii. Analyze Email Traffic for Sensitive Data
xiii. Analyze Email Traffic for Sensitive Data 2
xiv. Sniffing Countermeasures and Detection (2:54)
xv. Detect Promiscuous Mode (3:16)
xvi. Sniffing Countermeasure and Detection Facts
xvii. Practice Questions

b. Session Hijacking
i. Session Hijacking Overview (2:36)
ii. Session Hijacking Facts

iii. Client-Side and Network Attacks (8:02)
iv. Client-Side and Network Attack Facts
v. Perform a Man-in-the-Middle DHCP Attack (6:55)
vi. Perform a DHCP Spoofing Man-in-the-Middle Attack
vii. Perform an MITM Attack from a Remote Computer
viii. Capture HTTP POST Packets with Wireshark
ix. Use Burp Suite (5:36)
x. Hijack a Web Session (3:33)
xi. Hijack a Web Session
xii. Session Hijacking Countermeasures (3:56)
xiii. Session Hijacking Countermeasure Facts
xiv. Practice Questions

c. Denial of Service
i. Denial of Service (DoS) Overview (6:44)
ii. Denial of Service (DoS) Facts
iii. DoS Attack Types (5:12)
iv. DoS Attack Type Facts
v. Perform a SYN Flood (6:18)
vi. Perform and Analyze a SYN Flood Attack
vii. Analyze ICMP Traffic in Wireshark
viii. Launch a DoS and DDoS Attack (5:42)
ix. Perform a DoS Attack
x. Analyze a DDoS Attack
xi. DoS Countermeasures (3:42)
xii. DoS Countermeasure Facts
xiii. Practice Questions

XI. IDS, FIREWALLS, AND HONEYPOTS

a. Intrusion Detection Systems
i. Intrusion Detection Systems (5:15)
ii. Intrusion Detection System Facts
iii. Avoid IDS Detection (9:36)

iv. Avoid IDS Detection Facts
v. Evade IDS (11:25)
vi. Evade IDS Facts
vii. IDS Penetration Testing Facts
viii. Detect IDS Intrusion with Snort (9:16)
ix. Implement Intrusion Detection (5:58)
x. Implement Intrusion Detection
xi. Practice Questions

b. Firewalls
i. Firewalls (10:07)
ii. Firewall Facts
iii. Evade Firewalls (6:38)
iv. Evade Firewalls Facts
v. Firewall Penetration Testing Facts
vi. Configure a Perimeter Firewall (7:53)
vii. Configure a Perimeter Firewall
viii. Avoid Firewall Detection (5:26)
ix. Perform a Decoy Scan
x. Perform a Decoy Scan with Zenmap
xi. Bypass Windows Firewall with Metasploit (3:45)
xii. Bypass Windows Firewall with Metasploit
xiii. Practice Questions

c. Honeypots
i. Honeypots (4:36)
ii. Honeypot Facts
iii. Evade Honeypots (4:35)
iv. Evade Honeypots Facts
v. Detect Malicious Network Traffic with a Honeypot (3:23)
vi. Create a Honeypot with Pentbox
vii. Practice Questions

XII. **WEB SERVERS, WEB APPLICATIONS, AND SQL INJECTIONS**

a. Web Servers
    i. Web Server Hacking (3:38)
    ii. Web Server Hacking Facts
    iii. Web Server Attacks (5:05)
    iv. Web Server Attack Facts
    v. Mirror a Website with HTTrack (2:13)
    vi. Extract Web Server Information (4:30)
    vii. Extract Web Server Information with Nmap
    viii. Crack FTP Credentials with Wireshark
    ix. Web Server Countermeasures (4:58)
    x. Web Server Countermeasures Facts
    xi. Practice Questions
b. Web Applications
    i. Web Applications (4:39)
    ii. Web Application Facts
    iii. Web Application Hacking (5:32)
    iv. Web Application Hacking Facts
    v. Hidden Field Manipulation Attacks (2:36)
    vi. Exploit Cross-Site Scripting Vulnerabilities (2:57)
    vii. Web Application Countermeasures (6:43)
    viii. Scan a Website with Acunetix (4:17)
    ix. Web Application Countermeasure Facts
    x. Practice Questions
c. SQL Injections
    i. SQL Injection (5:52)
    ii. SQL Injection Facts
    iii. SQL Injection Attack Types (4:32)
    iv. SQL Injection Attack Facts
    v. Exploit SQL on a Web Page (3:57)
    vi. Perform an SQL Injection Attack
    vii. SQL Injection Countermeasures (2:26)
    viii. SQL Injection Countermeasure Facts

ix. Practice Questions

XIII. WI-FI, BLUETOOTH, AND MOBILE DEVICES

a. Wi-Fi
   i. Wireless Overview (9:31)
   ii. Wireless Facts
   iii. Wireless Encryption and Authentication (8:56)
   iv. Wireless Encryption and Authentication Facts
   v. Wireless Hacking (10:51)
   vi. Wireless Hacking Facts
   vii. Wi-Fi Packet Analysis (5:33)
   viii. Crack Wi-Fi Encryption with Aircrack-ng (5:40)
   ix. Discover a Hidden Network
   x. Wireless Hacking Countermeasure Tools (11:12)
   xi. Wireless Hacking Countermeasures Tool Facts
   xii. Detect a Rogue Device (5:53)
   xiii. Discover a Rogue DHCP Server
   xiv. Locate a Rogue Wireless Access Point
   xv. Practice Questions

b. Bluetooth Hacking
   i. Bluetooth Hacking (6:45)
   ii. Bluetooth Hacking Facts
   iii. Discover Vulnerable Bluetooth Devices (3:28)
   iv. Discover Bluetooth Devices
   v. Practice Questions

c. Mobile Devices
   i. Mobile Device Attacks (7:52)
   ii. Mobile Device Attack Facts
   iii. Mobile Device Operating Systems (8:58)
   iv. Mobile Device Operating System Facts
   v. Secure a Device (5:43)
   vi. Secure a Mobile Device

vii. Mobile Device Hacking (7:54)
viii. Hack Android with Binary Payloads (7:18)
ix. Mobile Device Hacking Facts
x. Mobile Device Management (6:00)
xi. Mobile Device Management Facts
xii. Practice Questions

XIV. CLOUD COMPUTING AND INTERNET OF THINGS

a. Cloud Computing
   i. Cloud Computing (13:06)
   ii. Cloud Computing Facts
   iii. Cloud Computing Threats (6:13)
   iv. Cloud Threats Facts
   v. Cloud Computing Attacks (9:04)
   vi. Cloud Attacks Facts
   vii. Cloud Security (6:40)
   viii. Cloud Security Facts
   ix. Secure Files in the Cloud (3:52)
   x. Practice Questions
b. Internet of Things
   i. Internet of Things (6:40)
   ii. Internet of Things Facts
   iii. IoT Technologies and Protocols (8:37)
   iv. IoT Technologies and Protocols Facts
   v. IoT Security Challenges (7:17)
   vi. IoT Security Challenge Facts
   vii. IoT Hacking (6:14)
   viii. IoT Hacking Facts
   ix. Search for IoT with Shodan (4:38)
   x. Scan for IoT with Nmap (3:23)
   xi. Scan for IoT Devices
   xii. Practice Questions

XV. CRYPTOGRAPHY

a. Cryptography
   i. Cryptography (5:22)
   ii. Cryptography Facts
   iii. Symmetric Encryption (4:11)
   iv. Symmetric Encryption Facts
   v. Asymmetric Encryption (5:40)
   vi. Asymmetric Encryption Facts
   vii. Verify MD5 Hash Integrity (2:50)
   viii. Compare an MD5 Hash
   ix. Practice Questions
b. Public Key Infrastructure
   i. Public Key Infrastructure (6:49)
   ii. Public Key Infrastructure Facts
   iii. Practice Questions
c. Cryptography Implementations
   i. Disk and Email Encryption (5:58)
   ii. PGP and GPG (4:22)
   iii. Disk and Email Encryption Facts
   iv. Encrypt Files with GPG (5:46)
   v. Encrypt a Hard Disk (6:01)
   vi. Encrypt a Hard Drive
   vii. Practice Questions
d. Cryptanalysis and Cryptographic Attack Countermeasures
   i. Cryptanalysis and Cryptographic Attack Countermeasures (5:56)
   ii. Cryptanalysis and Cryptographic Attack Countermeasures Facts
   iii. Data Encryption (4:31)
   iv. Practice Questions

XVI. TESTOUT ETHICAL HACKER PRO - PRACTICE EXAMS

a. Prepare for Certification
   i. TestOut Ethical Hacker Pro Exam Objectives

ii. TestOut Ethical Hacker Pro Objectives by Course Section
iii. How to Take the Certification Exam
iv. Certification FAQs

b. TestOut Ethical Hacker Pro Domain Review
i. Domain 1: Prepare
ii. Domain 2: Gain Access
iii. Domain 3: Attack
iv. Domain 4: Cover Up
v. Domain 5: Defend a System

c. TestOut Ethical Hacker Pro Certification Practice Exam

XVII. EC-COUNCIL CERTIFIED ETHICAL HACKER - PRACTICE EXAMS

a. Prepare for Certification
i. EC-Council EH Objectives
ii. EC-Council EH Objectives by Course Section
iii. How to Register for an Exam
iv. Exam FAQs
v. Exam-Taking Hints and Tips

b. EC-Council CEH Practice Exams (20 Questions)
i. EC-Council CEH Domain 1: Background
ii. EC-Council CEH Domain 2: Analysis/Assessment
iii. EC-Council CEH Domain 3: Security
iv. EC-Council CEH Domain 4: Tools/Systems/Programs
v. EC-Council CEH Domain 5: Procedures/Methodology
vi. EC-Council CEH Domain 6: Regulation/Policy
vii. EC-Council CEH Domain 7: Ethics

c. EC-Council CEH Practice Exams (All Questions)
i. EC-Council CEH Domain 1: Background
ii. EC-Council CEH Domain 2: Analysis/Assessment
iii. EC-Council CEH Domain 3: Security
iv. EC-Council CEH Domain 4: Tools/Systems/Programs
v. EC-Council CEH Domain 5: Procedures/Methodology

vi. EC-Council CEH Domain 6: Regulation/Policy
vii. EC-Council CEH Domain 7: Ethics

d. EC-Council CEH Practice Exam

CURSO DE HACKING ÉTICO

TI

POLÍTICAS DE PAGO

• Precios en **Pesos Mexicanos** - Excepto casos que se indique en otra moneda de manera expresa
• **LIQUIDACIÓN TOTAL** – Aplica previa al inicio del evento
• **DESCUENTO POR PRONTO PAGO** - Aplica liquidando el total de la inversión hasta 5 días hábiles previos al evento
• **POLÍTICAS DE PRECIOS Y DESCUENTOS** - Sujetas a términos y condiciones de IMECAF
• **FINANCIAMIENTO** – NO aplica

MÉTODOS DE PAGO

TARJETA DE CRÉDITO / DÉBITO
• VISA y MASTER CARD - No requiere presentación física
• AMERICAN EXPRESS - Si no es por PayPal, requiere presentación física
MESES SIN INTERESES
•3, 6, 9 Y 12 MSI – Tarjetas Banamex
•PayPal (Según las opciones disponibles en la plataforma)
TRANSFERENCIA INTERBANCARIA
• BANAMEX - Clabe 002180414600184021
DEPÓSITO BANCARIO
• BANAMEX - Cuenta 18402
• Sucursal 4146
TRANSFERENCIA O DEPÓSITO REQUIERE REFERENCIA
• Colocar cualquiera de los siguientes datos como referencia:
• Nombre, razón social, RFC o número de factura
BENEFICIARIO
• IMECAF México, SC

IMECAF®

Arquímedes 130
Dpcho. 205
Col. Polanco,
CDMX 11570

TEL. **55 1085 1515**
800 236 0800
info@imecaf.com

www.imecaf.com

CURSO DE HACKING ÉTICO

TI

POLÍTICAS DE CONFIRMACIÓN Y CANCELACIÓN

PENALIZACIONES
NO APLICA - Notificando hasta 6 días hábiles previos al evento
• **20%** - Notificando con menos de 6 días hábiles previos al evento - Se podrá elegir otro Curso pagando la diferencia. En caso de reincidencia, aplica penalización del **100%**
• **100%** - NO SHOW (No Asistencia) o notificando con menos de 72 hrs. hábiles previas al evento
• **CANCELACIONES CON TARJETA DE CRÉDITO / DÉBITO** - Se les descontarán las comisiones efectuadas por el banco emisor (incluyendo la opción de meses sin intereses, en su caso)

CONFIRMACIÓN OFICIAL

IMECAF notificará **5 días hábiles previos** al evento vía e-mail y/o teléfono del contacto proporcionado por la empresa contratante y ésta deberá confirmar por el mismo medio su asistencia.

Se sugiere realizar la gestión de **viáticos**, en su caso, una vez recibida | IMECAF no se hace responsable por gastos incurridos en este rubro.

IMECAF se reserva la posibilidad de cambios sin previo aviso por causas ajenas a su voluntad - Cursos sujetos a **QUÓRUM MÍNIMO**