

Ethical Hacking Certified Associate (EHCA)

Código: JOIN-040

Propuesta de Valor: CERTJOIN

Duración: 24 Horas



El hacking está íntimamente ligado al nacimiento de Internet y a las oportunidades económicas, técnicas y sociales que supuso desde sus inicios en la década de los 60 y 70. Desde su origen militar, hasta su proliferación masiva a partir del año 2000 y su implantación global hoy en multitud de dispositivos electrónicos, Internet ha servido como vehículo de popularización, difusión e intercambio para este movimiento.

Por esta razón los hackers éticos, son fundamentales para asegurar que la información de las organizaciones esté lo más resguardada posible.



AUDIENCIA

- El curso está orientado a estudiantes y profesionales de informática que desean aprender cómo realizar Pruebas de Intrusión o Hacking Ético y que desean dar los pasos hacia su preparación para la certificación EHCA



PRE REQUISITOS

- El estudiante debe poseer sólidos conocimientos sobre redes TCP/IP
- Poseer conocimientos básicos de Linux y Windows



OBJETIVOS

- Al finalizar el curso los alumnos tendrán los conocimientos generales necesarios para poder llevar a cabo pruebas de intrusión de forma profesional sobre infraestructura informática, sin causar daños a la operatividad de esta.



CERTIFICACIÓN DISPONIBLE

- Este curso lo prepara par el exámen: **Ethical Hacking Certified Associate (EHCA)**.
- Certificado oficial de **CertJOIN**.



CONTENIDO

1. CAPÍTULO 1: INTRODUCCIÓN

- 1.1. ¿QUÉ ES HACKING?
- 1.2. ¿QUÉ ES UN HACKER?
- 1.3. CONCEPTOS BÁSICOS
- 1.4. HACKING ÉTICO
- 1.5. ÉTICA HACKER
- 1.6. VALORES FUNDAMENTALES
- 1.7. HACKING ÉTICO
- 1.8. VULNERABILIDADES
- 1.9. VENTAJAS DEL HACKING ÉTICO
- 1.10. DESVENTAJAS DEL HACKING ÉTICO
- 1.11. FASES DEL HACKING
- 1.12. TEST DE PENETRACIÓN
- 1.13. ¿QUÉ ES UN PENTESTER O HACKER ÉTICO?
- 1.14. ¿POR QUÉ SE NECESITAN PENTESTERS?
- 1.15. ¿POR QUÉ CONVERTIRTE EN PENTESTER?
- 1.16. PEN-TEST (PENETRATION TEST)
- 1.17. HERRAMIENTAS PENTESTING

2. CAPÍTULO 2: RECONOCIMIENTO

- 2.1. TIPOS DE RECONOCIMIENTO
- 2.2. GOOGLE HACKING
- 2.3. WHO-IS
- 2.4. NSLOOKUP
- 2.5. MALTEGO
- 2.6. INGENIERÍA SOCIAL

3. CAPÍTULO 3: ESCANEEO

- 3.1. CLASES DE ESCANEEO
- 3.2. ESTADOS DE PUERTOS
- 3.3. EL ESCÁNER NMAP
- 3.4. ANALIZADORES DE
- 3.5. VULNERABILIDADES

4. CAPÍTULO 4: ENUMERACIÓN

- 4.1. PROTOCOLOS NETBIOS Y CIFS/SMB
- 4.2. OTROS PROTOCOLOS DE RED
- 4.3. ENUMERACIÓN DE WINDOWS
- 4.4. HERRAMIENTAS DE ENUMERACIÓN

5. CAPÍTULO 5: HACKING

- 5.1. MECANISMOS DE HACKING
- 5.2. FRAMEWORKS DE HACKING
- 5.3. METASPLOIT
- 5.4. ATAQUES DE CLAVES
- 5.5. ATAQUES DE MALWARE
- 5.6. ATAQUES DOS
- 5.7. ATAQUES MITM
- 5.8. HACKING WEB Y WIFI
- 5.9. HACKING WEB Y WIFI

6. CAPÍTULO 6: ESCRIBIENDO EL INFORME

- 6.1. PASOS SUGERIDOS
- 6.2. TIPS PARA NO SUFRIR UN COLAPSO MENTAL
- 6.3. HERRAMIENTAS DE DOCUMENTACIÓN
- 6.4. INFORMES DE EJEMPLO

7. LABORATORIO PRÁCTICO

- 7.1. HACKEANDO METASPLOITABLE 2
- 7.2. CREACIÓN DE CORREOS FALSOS CON
- 7.3. CREACIÓN DE CORREOS FALSOS CON
- 7.4. SENDEMAIL Y ATAQUES DEL LADO DEL CLIENTE CON SET TOOL
- 7.5. CRACKEANDO CLAVES CON MEDUSA
- 7.6. ATAQUE MITM CON ETTERCAP Y WIRESHARK
- 7.7. HACKEANDO WEP CON AIRCRACK
- 7.8. ATAQUE DE CLAVES A WPA/WPA2



BENEFICIOS

- Al finalizar el curso, los participantes tendrán los conocimientos generales necesarios para poder llevar a cabo pruebas de intrusión de forma profesional sobre infraestructura informática.