

# Certified Network Defense Professional

## Ethical Hacker



### ➤ Descripción del curso

EL curso para la certificación CNDP tiene como objetivo enseñarnos como proteger a nuestra organización de ataques externos o internos a nuestros sistemas. Mediante una metodología de estudio practica, aprenderemos las técnicas y herramientas de última generación que utilizan los hackers para vulnerar la seguridad de los sistemas de información, comprenderemos el cómo y el porqué de los diferentes tipos de ataques y lo mas importante como crear una estructura de defensa eficiente y proactiva.

El curso CNDP permite aplicar los conocimientos adquiridos mediante prácticas de laboratorios en ambiente que simula la realidad y al finalizar el curso será capaz de redactar un informe completo de lo obtenido en sus tareas, de forma analítica y completa. Es por esto que la certificación CNDP representa un esquema diferente en lo que se refiere a las certificaciones existentes en el mercado. El CNDP se prepara con dos enfoques: Funcional y Técnico. Por lo que nuestro CNDP no solo tendrá las herramientas necesarias para aplicar los conocimientos técnicos en su organización sino que será capaz de desarrollar un plan de trabajo basado en el análisis de la información obtenida.



Certified Network  
Defense Professional

E T H I C A L H A C K E R

### ➤ Examen de Certificación

Nuestro proceso de certificación consta de dos fases.

Fase I: Examen en Línea (1020V1-GLC). El estudiante deberá contestar un numero de preguntas teórico/prácticas de lo aprendido en el curso.

Fase II: Examen práctico. Luego de la aprobación del examen en línea se le otorgara una clave especial para acceder remotamente a nuestros servidores de laboratorio en el cual deberá realizar un ejercicio de PenTest, posteriormente deberá generar un informe técnico con la información generada en su ejercicio. El cual será evaluado por un jurado de expertos internacionales.

La puntuación mínima para la aprobación de cada Fase deberá ser de 700 / 1000 Puntos. Para la Fase II (examen práctico) el alumno tendrá 45 días luego de la aprobación del examen en línea, para acceder a los servidores asignados y lograr los objetivos requeridos por GLCCORP al estudiante certificado. Los servidores estarán equipado con las protecciones estándar del mercado, el objetivo será acceder a dicha información, vulnerar el sistema y obtener los datos que se soliciten para elaborar un informe, entre ellos, Password, data confidencial, pruebas de accesos. Con esto garantizara los Jueces Hacker Éticos que el participante posee los conocimientos necesarios para obtener dicha certificación, en el proceso enviaremos el reconociendo escrito de la certificación CNDP y será publicada en el site de GLCCORP la información de los diferentes logros obtenidos según el informe. Finalmente se hara entrega de la certificación y el crédito obtenido para completar CMSE (Certified Master Security Engineer).

### ➤ A quien va dirigido

Jefes, Administradores, Oficiales y Responsables de Seguridad Informática y Sistemas de información, Auditores, Técnicos y toda persona interesada en la seguridad de los sistemas de información.

### ➤ Duración

5 días.

### ➤ Requerimientos

El alumno debe poseer fuertes conocimientos técnicos en Redes, Hardware, Sistemas Operativos GNU/Linux y Microsoft Windows, Programación y Seguridad Informática en general.



## > Contenido del curso

### Modulo 1: Introducción

- Introducción al curso.
- 

### Modulo 2: Ethical Hacking

- Que es EH.
  - Tipos de Hackers.
  - Diferencias entre EH, VA y Pentest.
- 

### Modulo 3: Footprinting

- Definición de Footprinting.
  - Metodologías para obtener información.
  - Footprinting Countermeasures.
- 

### Modulo 4: Scanning

- Definición de Scanning.
  - Tipos de Scanning.
  - Técnicas de Scanning.
  - Scanning Countermeasures.
- 

### Modulo 5: Enumeration

- Definición de Enumeration.
  - Técnicas de Enumeration.
  - Enumeration Countermeasures.
- 

### Modulo 6: Buffer Overflow

- Que es un Buffer Overflow.
  - Tipos de Buffer Overflow.
  - ShellCode.
  - Buffer Overflow Countermeasures.
- 

### Modulo 7: Hackeando Sistemas

- Explotando vulnerabilidades.
  - Escalando privilegios.
  - Password Cracking.
  - Countermeasures.
- 

### Modulo 8: Vulnerabilidades en Aplicaciones y Servidores Web.

- Vulnerabilidades en aplicaciones Web.
  - Vulnerabilidades en IIS y Apache.
  - Countermeasures.
- 

### Modulo 9: Anonimato, evasión y borrado de huellas.

- Navegando anónimamente.
- Evadiendo IDS, IPS y Honeypot.
- Borrando rastros.
- Countermeasures.

### Modulo 10: Ingeniería Social.

- Que es Ingeniería Social.
  - Tipos de Ingeniería Social.
  - Phishing.
  - Countermeasures.
- 

### Modulo 11: Hacking Wireless y Bluetooth.

- Introducción a las redes Wireless.
  - Hacking Wireless.
  - Hacking Bluetooth.
  - Countermeasures.
- 

### Modulo 12: Seguridad Física.

- Seguridad Fisica.
  - Perdida de equipos.
  - Countermeasures.
- 

### Modulo 13: Denial of Service.

- Tipos de DOS.
  - DDOS.
  - Countermeasures.
- 

### Modulo 14: Introducción a la Criptografía.

- Criptografía simétrica.
  - Criptografía asimétrica.
  - Esteganografía.
- 

### Modulo 15: Password Cracking.

- Password Cracking en Sistemas Operativos.
  - Password Cracking en aplicaciones.
  - Countermeasures.
- 

### Modulo 16: Sniffers y Session Hijacking.

- Tipos de Sniffers.
  - Ataques MID.
  - Countermeasures.
- 

### Modulo 17: Trojans, Back-Doors y Root Kits.

- Definición de Trojans, Back-Doors y Root Kits
  - Countermeasures.
- 

### Modulo 18: Redacción de un reporte final.

- Redacción de un reporte de EH.