CYBERIUM ARENA

**Descripción**

Sumérgete en el ámbito de la Forense de Linux con este curso integral, diseñado para equipar a los participantes con habilidades prácticas en adquisición de datos, análisis de memoria, detección de malware y más. Explora escenarios del mundo real, comprende las complejidades del sistema de archivos de Linux y domina técnicas forenses avanzadas. Este curso combina teoría con prácticas de laboratorio, asegurando una comprensión holística de las investigaciones digitales basadas en Linux.

# NX215 - FORENSE DE LINUX

## Módulo 1: Fundamentos de Linux

Este módulo proporciona una introducción comprensiva a los fundamentos de Linux, luego profundiza en los detalles de los servicios de Linux, incluyendo cómo son gestionados y configurados. Finalmente, equipa a los aprendices con habilidades de scripting, vitales para la automatización y tareas avanzadas en entornos Linux.

**Introducción a Linux**
Virtualización
Comandos Básicos
Archivos del Sistema
**Servicios**
Instalación
Archivos de Configuración
Archivos de Log
**Scripting**
Permisos de Archivos
Automatización de Linux

## Módulo 2: Análisis

Análisis de Logs, detalla cómo inspeccionar logs de Linux en busca de pistas vitales durante una investigación. La sección de Análisis de Archivos enseña métodos para diseccionar sistemas de archivos de Linux y extraer datos significativos. Finalmente, Análisis de Red imparte técnicas para inspeccionar el tráfico de red e identificar patrones sospechosos o anomalías, esenciales para investigaciones cibernéticas.

**Análisis de Logs**
Manipulación de Texto
Logs Integrados
Mejores Prácticas de Logs
Análisis de Archivos
Metadatos
Carving
Esteganografía
Llamadas
**Análisis de Red**
Wireshark
Herramientas Generales de Red
Automatización de TShark

## Módulo 3: Recolección de Evidencia

La sección de Artefactos instruye cómo localizar e interpretar artefactos del sistema Linux, invaluables en investigaciones post-violación. Análisis en Vivo imparte habilidades para escrutar sistemas activos, identificando amenazas en curso. La porción de Análisis de Imágenes discute métodos para inspeccionar e interpretar imágenes de disco, revelando datos ocultos o evidencia.

**Artefactos**
Hashes y Codificaciones
Archivos de Usuario
Entendimiento de Shells
Archivos del Sistema
Información de Usuario Sospechosa
**Análisis en Vivo**
Montaje de Particiones
Volcado de Memoria
Clonación de HDD
Búsqueda Avanzada en Archivos de Log
**Imágenes Capturadas**
Trabajando con FTK
Detectando Archivos y Directorios Ocultos

## Módulo 4: Ciberseguridad

Este módulo cubre Protocolos de Red esenciales, proporcionando una comprensión de su operación y vulnerabilidades potenciales. Luego explora Ataques de Red, discutiendo diversos vectores de ataque y estrategias. Finalmente, el módulo introduce el concepto de endurecimiento, enseñando a los aprendices cómo fortalecer un sistema Linux contra posibles amenazas.

**Netcat**
Diferentes Usos
**Protocolos de Red**
MiTM
Análisis de Tráfico
**Ataques de Red**
SSH
FTP
**Endurecimiento**

**Defensa NX | NIVEL: 4 | DURACIÓN: 40h**