CYBERIUM ARENA

Description

Dive deep into the realm of Linux Forensics with this comprehensive course, designed to equip participants with hands-on skills in data acquisition, memory analysis, malware detection, and more. Explore real-world scenarios, understand the intricacies of the Linux file system, and master advanced forensic techniques. This course combines theory with practical labs, ensuring a holistic understanding of Linux-based digital investigations.

LINUX FORENSICS

Module 1: Linux Fundamentals

This module provides a comprehensive introduction to Linux fundamentals, then delves into the details of Linux services, including how they are managed and configured. Finally, it equips learners with scripting skills, vital for automation and advanced tasks in Linux environments.

Intro to Linux
Virtualization
Basic Commands
System Files
Services
Installation
Configuration Files
Logs Files
Scripting
File Permissions
Linux Automation

Module 2: Analysis

Log Analysis, it details how to inspect Linux logs for vital clues during an investigation. The File Analysis section teaches methods to dissect Linux file systems and extract meaningful data. Finally, Network Analysis imparts techniques for inspecting network traffic and identifying suspicious patterns or anomalies, essential for cyber investigations.

Log Analysis
Text Manipulation
Built-in Logs
Logs Best Practice
File Analysis
Metadata
Carving
Steganography
Calls
Network Analysis
Wireshark
General Network Tools
TShark Automation

Module 3: Collecting Evidence

The Artifact section instructs how to locate and interpret Linux system artifacts, invaluable in post-breach investigations. Live Analysis imparts skills to scrutinize active systems, identifying ongoing threats. The Analyzing Images portion discusses methods to inspect and interpret disk images, revealing concealed data or evidence.

Artifacts
Hashes and Encodings
User Files
Understanding Shells
System Files
Suspicious User-Info
Live Analysis
Mounting Partitions
Dumping Memory
Cloning HDD
Log File Advance Search
Captured Images
Working with FTK
Detecting Hidden Files and Directories

Module 4: Cyber Security

This module covers essential Network Protocols, providing an understanding of their operations and potential vulnerabilities. It then explores Network Attacks, discussing various attack vectors and strategies. Lastly, the module introduces the concept of hardening, teaching learners how to strengthen a Linux system against possible threats.

Netcat
Different Uses
Network Protocols
MiTM
Analyzing Traffic
Network Attacks
SSH
FTP
Hardening

NX Defense | LEVEL: 4 | DURATION: 40h