KERNELiOS
SIMULATING CYBER THREATS

Cyber Forensics Intro

SYLLABUS 2024

Ver. 1.5

תיאור הקורס

קורס מבוא לפורנזיקת סייבר מכסה נושאים עדכניים בתחום הפורנזי הדיגיטלי. הקורס יתאר את הכלים הפורנזיים, השיטות, הטכניקות ומה נדרש חוקר לחפש בעת חקירת אירוע מחשוב דיגיטלי.

המשתתף בקורס ילמד ביצד להעתיק, לנתח, לשחזר, לחפש ולחקור באופן פורנזי ארטיפקטים בארגון תחת תרחישים שונים.

הקורס גם יעסוק בשיטות לאיסוף ראיות שיהיו תקפות בבית המשפט.

הקורס נועד לתרגל את המשתתפים בתרחישים שונים בחיים האמיתיים עם דגש על הכשרה מעשית.

לכל תלמיד יהיו מעבדות וכלים משלו לתרגול.

קורס זה הוא הזדמנות מצוינת לקפוץ לתחום ההולך וגדל של תחום הפורנזי הדיגיטלי.

הקורס מקנה הסמכת בינלאומית של לינוקס LPI Linux Essentials (010-160)

קהל יעד

קורס זה מיועד לכל מי שרוצה ללמוד את תחום החקירות הפורנזיות ולהתחיל לעבוד בתחום זה בסיום הלימודים.

דרישות קדם

- הבנה בסיסית טובה בסביבת Windows
- קריאת אנגלית טכנית ברמה טובה
- 12 שנות לימוד / תעודת בגרות מלאה
- בגרות באנגלית עם מינימום 3 יח"ל + מתמטיקה עם מינימום 3 יח"ל
- מעבר מבחן סינון באנגלית עם ציון עובר של 70 + ראיון אישי

סילבוס קורס פורנזיקה

01

Linux Essentials (80 Hours)

Subject	Description
Lesson 1: LPI Exam and Virtual Machine	• LPI Exam • Computer Hardeware: Introduction • Benefits of Virtualization • Virtualization Type • Virtualizing Players – VMware \ Hyper-V \VirtualBox • Demo – Using VMware Workstations Exercise
Lesson 2: The Linux Operating System	• Introducing Linux • Why Linux? • Linux for Desktop • Open Source Licensing Models • History of Linux • Linux Hardware System • OS Commercial Restrictions • The Linux Layers • Software Package Manager Exercises
Lesson 4: Configuring the Linux Environment	• Introduction to the Linux Environment • Managing Linux Startup • The Linux File System Hierarchy Standard • Relative and Absolute modes Exercises

Lesson 5: Configuring the Linux Environment (continue)	• Learn and practice basic Linux commands Exercises
Lesson 6: Configuring the Linux Desktop Experience	• Working with Linux Software Repositories • Exploring Linux Desktop Applications • Understanding Linux Desktops Exercises
Lesson 7: Working with Linux Command Line Basics	• Using Linux Help Resources • The Linux Terminal • Linux Command Syntax Patterns and Shortcuts Exercises
Lesson 8: Navigating the Linux File System	• Working with Files and Directories • Searching the Linux File System Exercises
Lesson 9: Navigating the Linux File System (continue)	• Working with Archives • Linux Kernel Modules and Peripherals Exercises
Lesson 10: Linux Network Connectivity	• Network Configuration • Domain Name System (DNS) Configuration Exercises
Lesson 11: Linux Scripting	• A Shell variables • If, for, while Exercises
Lesson 12: Linux Scripting (continue)	• Writing advanced scripts

	Exercises
Lesson 13: Linux Network Connectivity	• Monitoring System Resources Exercises
Lesson 14: Working with Users and Groups in Linux	• Understanding Linux Users and Groups • Administrating Users and Groups Exercises
Lesson 15: Securing Linux Server	• Applying Object Permissions • Extending Object Usability Exercises
Lesson 16-20: Exam Preparation + Rehearsal	Exam Preparation + Rehearsal
LPI Exam	LPI Linux essentials exam

02

NETWORKING (40 Hours)

Subject	Description
Introduction to networking	Introduction to communication , types of equipment, OSI model , TCP/IP model
Layer 1	RJ45 , Cables STP/UTP , Fiber optics , RS232 , Serial , Computer architecture
Layer 2	LAN,WAN , Ethernet, MAC addresses , static/dynamic learning , unicast/broadcast/multicast, VLANs, Spanning tree
Layer 3 +Subnetting	IPv4, Public address/Private address , Subnets , CIDR , IPv6 , Decimal/Octal/Hex conversion , Network topology, Proxy , Routing (Static/Dynamic protocols)
Project	Final Project

03

SYSTEM (48 Hours)

Subject	Description
Windows 10/11 OS	• מבוא ל Windows 10-בסביבה ארגונית • מבוא בסיסי לממשקי פקודהRAM Dump + CMD, PowerShell • הגדרות משתמשים ופרופילים • הגדרות דיסק קשיח והרשאותNTFS • הכרות עם ה- Registry ומבוא ל-GROUP POLICY • הגדרות בסיסות של חומרה ב -Windows ודרייברים • התקנה והסרה של תוכנות ועבודה עם FILE HISTORY • Windows Firewall-אבטחת מידע במערכות הפעלה • BITLOCKER-מבוא הכרה בסיסית ושימוש עיקרי • הכרת cmd ופקודות בסיסיות

04

CYBER Forensics (40 Hours)

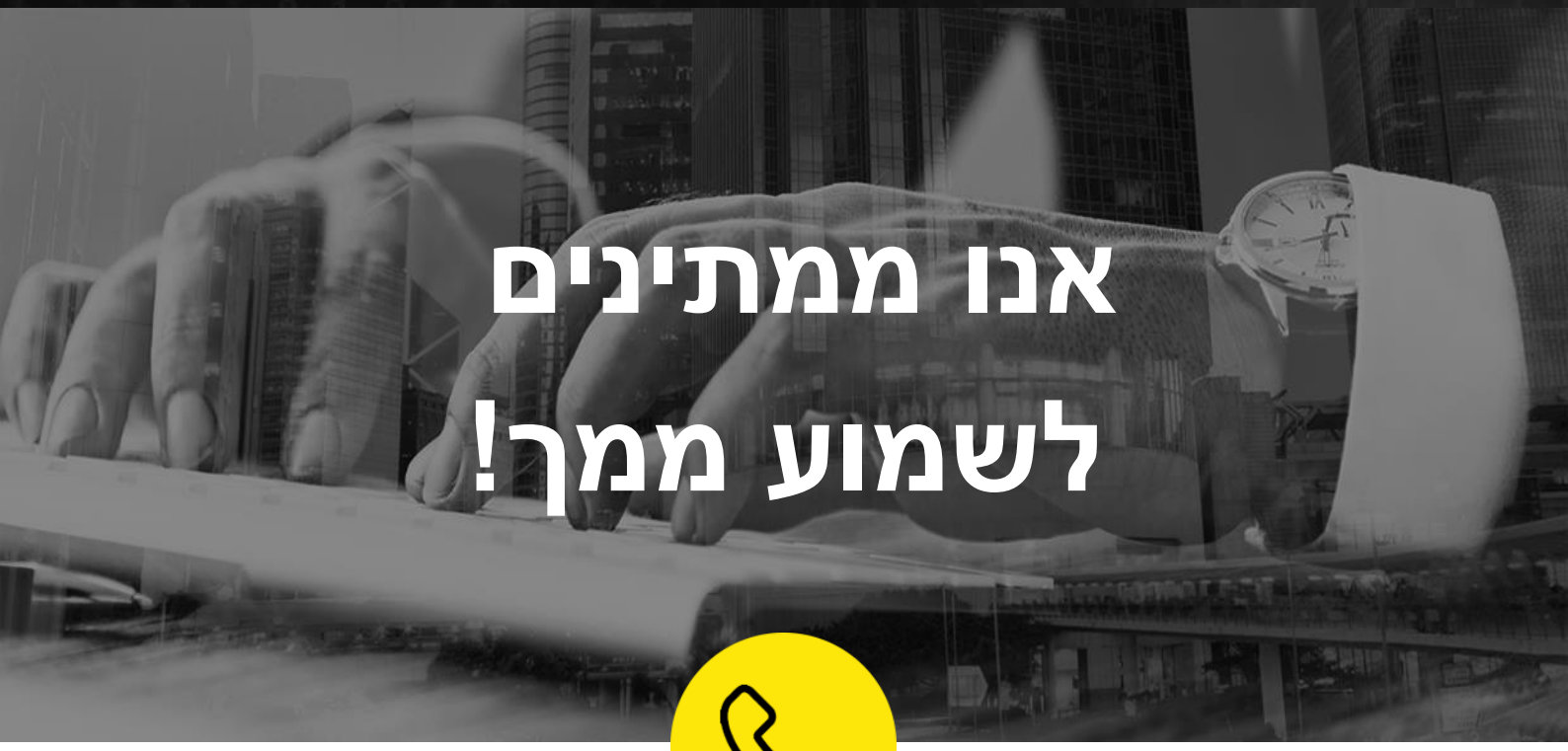
Subject	Description
Forensics Concepts and methods	• מבוא לניתוח מידע, הכרת כלים ושיטות • העתקת מידע ממחשב או מהתקן זיכרון בצורה פורנזית, סוגי העתקות • שחזור מידע, מבוא והכרת כלים בסיסיים • חקירת מידע דיגיטלי וארטיפקטים • חיפוש מידע, הכרת כלים ושיטות • שימור מידע דיגיטלי בצורה פורנזית • Metadata - מבוא, הכרה, שימוש וכלים בסיסיים בתחום • הכרת כלים פורנזיים מובנים בLinux
Security Cams and NVR/DVR	• מבוא, מושגי יסוד • מבוא בסיסי למקודדים ,המרות קבצים, הכרת סוגי קבצים • הכרה בסיסית של מכשירי dvr+nvr תפעול הגדרות ושליטה • חילוץ מידע ממערכות הקלטהcctv • ניתוח תוצרי וידאו

05

CYBER Security (40 Hours)

Subject	Description
Introduction to cyber security	Intro to cyber security and information security, Attack & Defense Concepts, examples.
Analyzing network traffic	Working with Wireshark ,Type of sniffers, installation, extracting credentials from network traffic, methods of extracting files and objects from network traffic. Follow sessions, and filters and statistics
Reconnaissance Methods	Port scanners, and working with Metasploit
Intro to Metasploit	Working with msfconsloe and msfvenom
Working with Metasploit	MSFConsole , MSFVenom , armitage , getting a shell/meterpreter
Static and Dynamic malware analysis	• Strings, exported and imported dlls , hash, PE structure etc.. • Using sandbox , sysinternals and other basic tools • Static & Dynamic Analysis, full report.
HD Forensics concepts	Concept, Create HD image and mem dump, Analyzing mem dump and HD image

Total Hours: 248 Academic Hours



אנו ממתינים לשמוע ממך!

03-566-3155

info@kernelios.com