KERNELiOS
SIMULATING CYBER THREATS

CHCSS

Certified Hands-on Cyber Security Specialist + Linux LPI(506)

SYLLABUS 2024

Ver. 1.7

תיאור הקורס

קורס סייבר פרקטי ברמת בסיס המיועד למי שמבקש להכנס לעולם אבטחת המידע וסייבר או לחילופין למי שמעוניין לבצע שינוי קריירה.

הסטודנטים בקורס ייחשפו למגוון רחב של נושאים , שיטות הגנה ותקיפה מעולם הסייבר ויתרגלו החומר במעבדות ייחודיות ועם כלים המדמים את מה שמתרחש בעולם האמיתי, כלים הדרושים לעבודה השוטפת של מגן הסייבר בעולם האבטחה המשתנה.

קורס הכשרה ייחודי זה פותח על ידי מומחי הסייבר המובילים בישראל והוא מורכב ממגוון נושאים הנדרשים בתעשייה, עם דגש רב על הקניית ידע **מעשי** בהגנה בסייבר.

הסטודנטים מתרגלים גם באמצעות סימולטור הסייבר הייחודי שלנו המסמלץ תקיפות סייבר שונות וזאת במטרה לתרגל התגוננות בפני ההתקפות השונות.

מטרת הקורס היא לחשוף את הסטודנט למגוון רחב של תיאוריות וכלים מעשיים על מנת ליצור מאגר ידע רחב שיאפשר לסטודנט להשתלב בהצלחה בתעשיית הסייבר. הקורס מכיל גם שיעורי בית לתלמידים כחומר עזר נוסף.

הקורס מחולק לשני חלקים עיקריים:

חלק ראשון: מכינה לעולם הסייבר המקנה הסמכת לינוקס בינלאומית LPI Linux Essentials (010-160)

חלק שני: קורס מיישם הגנת סייבר מעשי המקנה הסמכות של קרנליוס ומדינת ישראל.

קהל יעד

קורס זה מיועד לכל מי שרוצה ללמוד אבטחת מידע וסייבר ולהתחיל לעבוד בתחום זה.

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

Cyber Security Specialist

01

Linux Essentials (98 Hours)

Subject	Description
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
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 • Linux Distribution Families • Linux in Cloud • Linux for Cloud • Long-Term Support (LTS) • Introduction to Linux Installation • Installation-time Decisions • Installing Ubuntu: Pre-Installation Steps • Min. System Requirements
Configuring the Linux Environment	• Introduction to the Linux Environment • Managing Linux Startup • The Linux File System Hierarchy Standard • Relative and Absolute modes •Learn and practice basic Linux commands

Configuring the Linux Desktop Experience	• Working with Linux Software Repositories • Exploring Linux Desktop Applications • Understanding Linux Desktops
Working with Linux Command Line Basics	• Using Linux Help Resources • The Linux Terminal • Linux Command Syntax Patterns and Shortcuts
Navigating the Linux File System	• Working with Files and Directories • Searching the Linux File System • Working with Archives • Linux Kernel Modules and Peripherals
Linux Network Connectivity	• Network Configuration • Domain Name System (DNS) Configuration
Linux Scripting	• A Shell variables • If, for, while • Writing advanced scripts
Optimizing Linux Systems	• Monitoring System Resources
Working with Users and Groups in Linux	• Understanding Linux Users and Groups • Administrating Users and Groups
Securing Linux Server	• Applying Object Permissions • Extending Object Usability
Exam Preparation	Preparation for LPI Linux Essentials exam

02

NETWORKING (80 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	IPv4, Public address/Private address , Subnets , CIDR , IPv6 , Decimal/Octal/Hex conversion , Network topology, Proxy , Routing (Static/Dynamic protocols)
Layer 4 - Network Protocols	HTTP , HTTPS, Telnet , SSH, DNS, DHCP, SNMP, SMTP FTP
Routing	Static and Dynamic routing (EIGRP , OSPF,BGP)
Basic configuration of Switches and routers with the CLI	Working with packet tracer , Configure VLANs, Port mirroring , Trunk/Access , Routing on stick , CLI commands, port security, Access lists , users , logins , line VTY
Final Project	CLI, Basic switch and end device configuration, console cable, Telnet & SSH (On Router)

03

SYSTEM (128 Hours)

Subject	Description
Introduction to Virtual environment	VMware\Hyper-V
Introduction to Operating System	Windows 10 - Install And Configure
Workgroup \ Domain \ Troubleshoot	
Server 2016\2019	Installation Roles & Features – Tools
Active Directory Introduction	
Active Directory	Installation & Configure
Active Directory Users & Computers	Users \ Security Group \ OU Design
File Management	NTFS\Share Permissions (Shadow Copy)
Registry + Group Policy	
Password Policy / Auditing Policy / Fine Grained Password Policy / Security Policy	
Securing Windows Server by Using Group Policy Objects	
Patch Management	WSUS
Storage + Data transition methods	RAID Levels (openfiler) Data transitions methods + Audit
Windows Backup	

Business continuity and DR	BCD Methods
Cloud computing	Office 365, Azure, AWS
Material Recap	Material Recap
Final Project (System)	Hands-On Labs Project

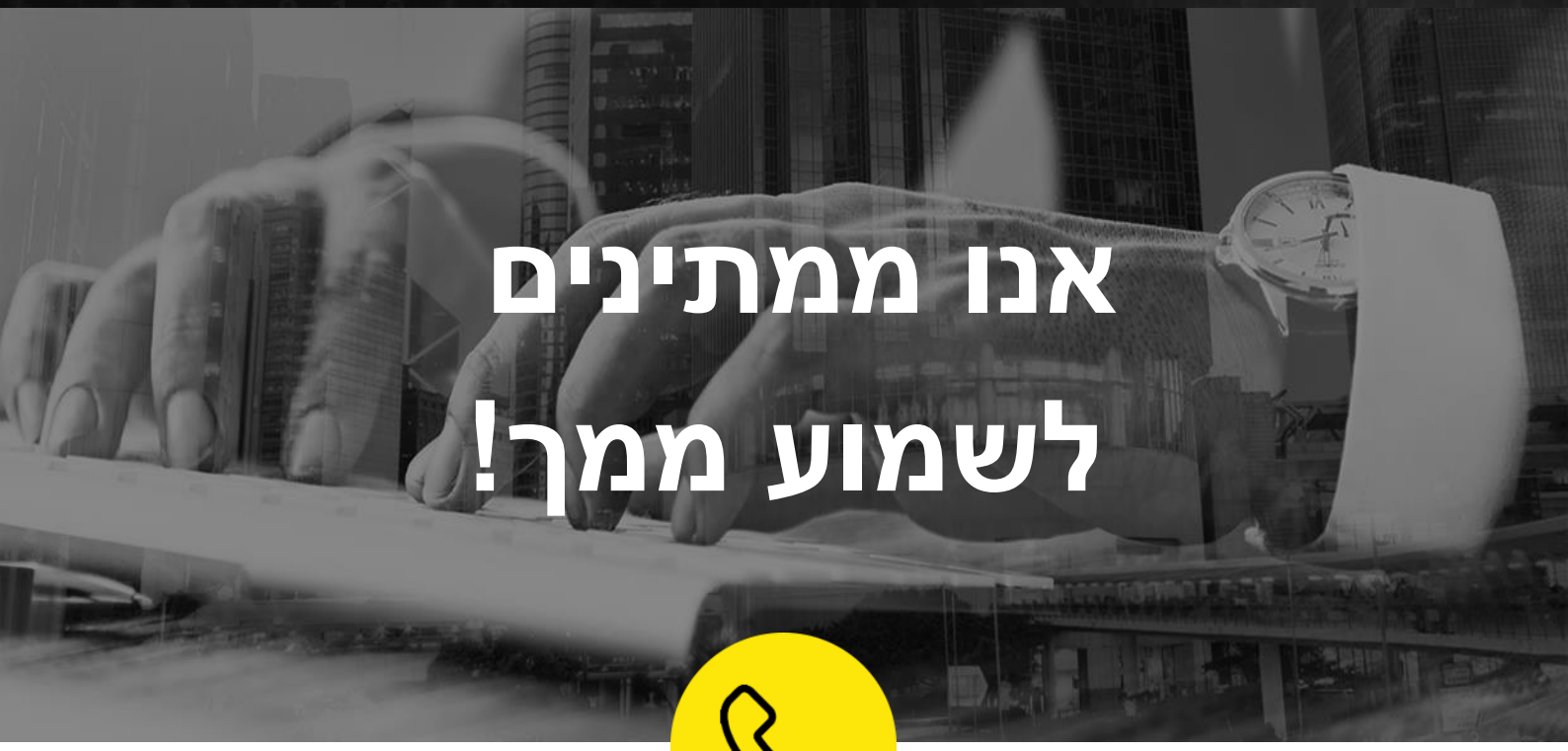
04

CYBER SECURITY (200 Hours)

Subject	Description
Network traffic Analyzing	Working with Wireshark , NMAP, Type of sniffers, installation, extracting credentials from network traffic, methods of extracting files and objects from network traffic. Follow sessions, and filters and statistics
Working with Python	What is programming language, open new project in pycharm, operators, basic I\O commands, if else, conditions, loops.
Introduction to KALI Linux	Installation, Linux's concept, working with the Terminal, tools etc.
Reconnaissance Methods	Google Hacking (with regex), Social Engineering
Infrastructure attacks	UDP Flood, SYN Flood, DDOS, ARP poisoning, ARP spoofing and MAC spoofing, MITM
Mitigation of Infrastructure attacks	Encryption, Digital Certificate, NAC, etc.
Password cracking and Mitigation	Cryptographic Hash functions, Brute Force, Rainbow tables, Password Hijacking
Application security - hacking and mitigation	Databases and SQL, SQL injection. CSRF, Path Traversal, XSS, Session Hijacking, Buffer Overflow, Privilege escalation
Exploits and Working with Metasploit	
From Cyber-attack to Cyber security	Concept of cyber defense vs hacking etc.

End Point security	EMMET (including DEP, ASLR, SEH), HIPS, DLP, AV, app-lockers
Organization network security	FW and ACL, IPS, NAC, Web Application Control, VPN, DNS Sec, IPsec, Content Disarm and Reconstruction, Waterfalls, SIEM. Information security and risk assessment standards.
Patch management and vulnerability assessment	The process of risk management and vulnerability Assessment
Forensics concepts	Concept, Create HD image and mem dump, Analyzing mem dump and HD image
Audit Concepts	
Static and Dynamic malware analysis	Strings, exported and imported DLLs , hash, PE structure etc. Using sandbox , Sysinternals and other basic tools
Data encryption and authentication	
Law and Ethics/ Physical Security	
Final exam	Hands-On Labs and simulator

Total Academic Hours: 506



אנו ממתינים לשמוע ממך!

03-566-3155

info@kernelios.com