KERNELiOS
SIMULATING CYBER THREATS

CHCSS

Certified Hands-on Cyber Security Specialist (310)+ Linux LPI (140)

SYLLABUS 2021

Ver. 4.2

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: מבינה לעולם הסייבר המקנה הסמכת לינוקס LPI Linux Essentials (010-160)

חלק שני: קורס מיישם הגנת סייבר מעשי המקנה הסמכות של קרנליוס ומערך הסייבר הלאומי.

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

Linux Essentials Syllabus

Subject	Description
Intro: Introduction to Virtualization	• Virtual Machine • Benefits of Virtualization • Virtualization Type • Virtualizing Players – VMware \ Hyper-V \VirtualBox \ Citrix
Module 1: Introduction to the Linux Essentials 010-160 Exam	Using the Linux Essentials Path to Pass the Exam
Module 2: Introducing Open Source Software	• Introducing Linux • Why Linux? • Linux for Desktop • Open Source Licensing Models
Module 3: The Linux Operating System	• History of Linux • Linux Hardware System • OS Commercial Restrictions • The Linux Layers • Software Package Manager
Module 4: Linux Distribution	• Linux Distribution Families • Linux in Cloud • Linux for Cloud • Long-Term Support (LTS)
Module 5: Installing Linux	• Introduction to Linux Installation • Installation-time Decisions • LVM Volume

Module 6: Installing Ubuntu	• Pre-Installation Steps • Min. System Requirements • Ubuntu Multipass
Module 7: Configuring the Linux Environment	• Introduction to the Linux Environment • Managing Linux Startup • The Linux File System Hierarchy Standard • Managing Linux Environments
Module 8: Managing System Hardware	• CPU, PSU, Motherboard, RAM and Disks • Server vs. workstations • Managing Devices • Creating Virtual Addresses
Module 9: Configuring the Linux Desktop Experience	• Working with Linux Software Repositories • Exploring Linux Desktop Applications • Understanding Linux Desktops
Module 10: Working with the Linux Server	• Introduction to the Linux Server • Using Linux Containers • Installing and Working with Server Apps: Apache • Installing and Working with Server Apps: Nextcloud • Compiling Code in Linux
Module 11: Working with Linux Command Line Basics	• Using Linux Help Resources • The Linux Terminal • Linux Command Syntax Patterns and Shortcuts
Module 12: Navigating the Linux File System	• Working with Files and Directories • Searching the Linux File System • Working with Archives • Linux Kernel Modules and Peripherals

Module 13: Linux Network Connectivity	• Network Configuration • Domain Name System (DNS) Configuration • Remote Connections and Secure Shell (SSH)
Module 14: Linux Scripting	• A Simple Calculator Script • Working with Loops and Flow Controls
Module 15: Optimizing Linux Systems	• Monitoring System Resources • Managing System Processes • Managing Process Priorities
Module 16: Working with Users and Groups in Linux	• Understanding Linux Users and Groups • Administrating Users and Groups
Module 17: Securing Linux Server	• Applying Object Permissions • Extending Object Usability • Hardening Servers • Data Encryption

Total Hours: 140

CHCSS Syllabus

01

INTRODUCTION (5 Hours)

Subject	Description	Hours
Introduction to the Cyber world	What is the Cyber world, Players in the cyber world, Motivation, Pros and Cons,CIA triad,The life cycle of an attack,Types of malwares,Basic concepts, etc.	5

02

NETWORKING (50 Hours)

Subject	Description	Hours
Introduction to network	Introduction to communication, types of equipment, OSI model , TCP/IP model	5
Layer 1	RJ45, Cables STP/UTP, Fiber optics, RS232, Serial, Computer architecture	5
Layer 2	LAN,WAN , Ethernet, MAC addresses , static/dynamic learning , unicast/broadcast/multicast, VLANs, Spanning tree	5
Layer 3	IPv4, Public address/Private address , Subnets , CIDR , IPv6 , Decimal/Octal/Hex conversion , Network topology, Proxy , Routing (Static/Dynamic protocols)	10
Layer 4 – Network Protocols	BGP, HTTP, HTTPS, Telnet, SSH, DNS, DHCP, SNMP, SMTP, FTP	5
Basic configuration of Switches and routers	Working with packet tracer, Configure VLANs, Port mirroring, Trunk/Access, Routing on stick, CLI commands, port security, Access lists, users,	10

with the CLI	logins , line VTY	
Final Project	Hands on Labs Project	10

03

SYSTEM (100 Hours)

Subject	Description	Hours
Introduction to Virtual environment	VMware\Hyper-V	5
Introduction to Operating System	Windows 10 - Install And Configure	5
Workgroup \ Domain \ Troubleshoot		5
Server 2012 R2\Server 2016	Installation Roles & Features – Tools	10
Active Directory Introduction		5
Active Directory	Installation & Configure	5
Active Directory Users & Computers	Users \ Security Group \ OU Design	5
File Management	NTFS\Share Permissions (Shadow Copy)	5
Registry + Group Policy		5
Password Policy / Auditing Policy / Fine Grained Password Policy / Security Policy		5
Securing Windows Server by Using Group Policy Objects		5
Patch Management	WSUS	5

Storage + Data transition methods	RAID Levels (openfiler) Data transitions methods + Audit	5
Windows Backup		5
Business continuity and DR	BCD Methods	5
Cloud computing	Office 365, Azure, AWS	5
Final Project (System)	Hands-On Labs Project	10

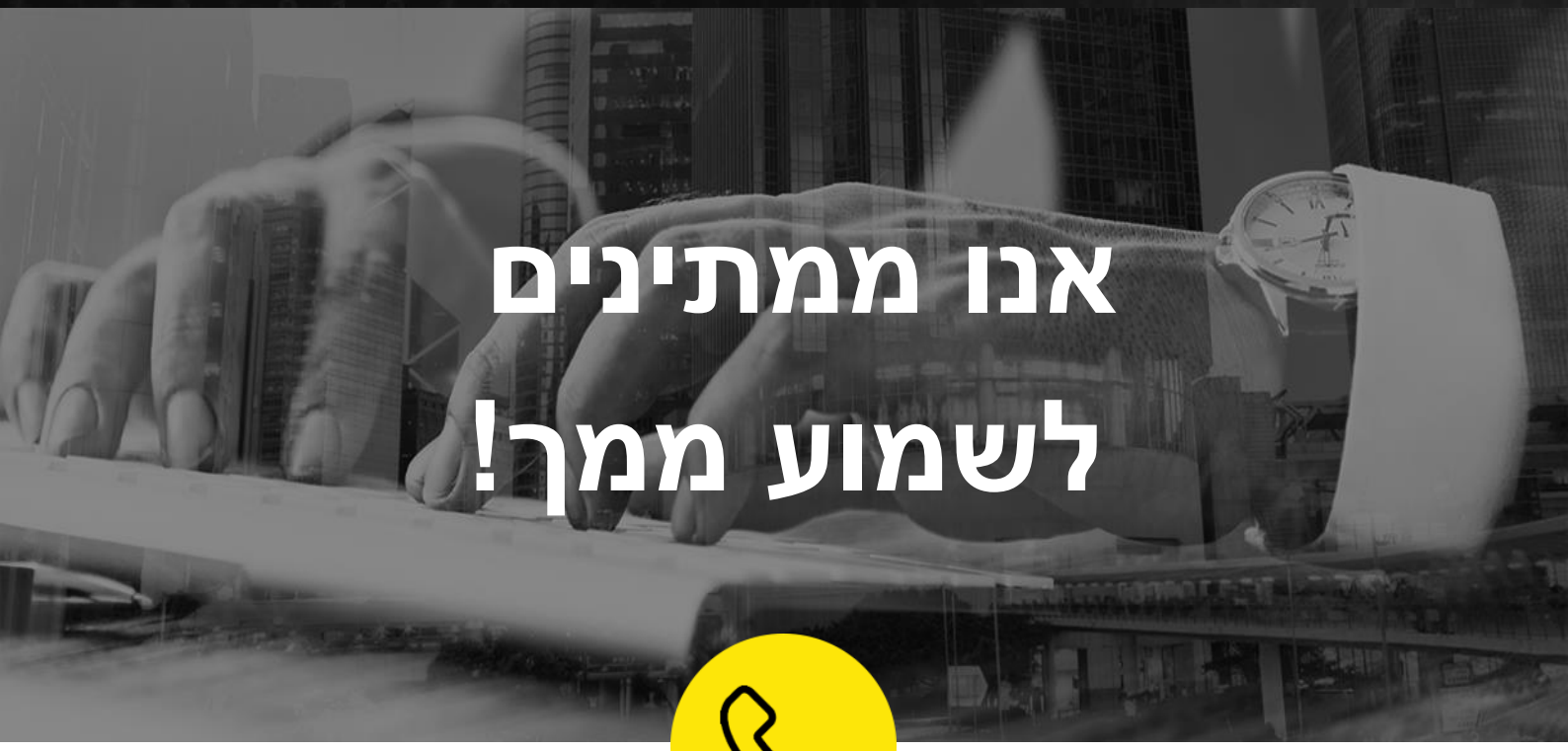
04

CYBER SECURITY (155 Hours)

Subject	Description	Hours
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	5
Working with Python	What is programming language, open new project in pycharm, operators, basic I\O commands, if else, conditions, loops.	5
Introduction to KALI Linux	Installation, Linux's concept, working with the Terminal, tools etc.	15
Reconnaissance Methods	Google Hacking (with regex), Social Engineering	5
Infrastructure attacks	UDP Flood, SYN Flood, DDOS, ARP poisoning, ARP spoofing and MAC spoofing, MITM	5
Mitigation of Infrastructure attacks	Encryption, Digital Certificate, NAC, etc.	5
Password cracking and Mitigation	Cryptographic Hash functions, Brute Force, Rainbow tables, Password Hijacking	5

Application security - hacking and mitigation	Databases and SQL, SQL injection. CSRF, Path Traversal, XSS, Session Hijacking, Buffer Overflow, Privilege escalation	20
Exploits and Working with Metasploit		5
From Cyber-attack to Cyber security	Concept of cyber defense vs hacking etc.	5
End Point security	EMMET (including DEP, ASLR, SEH), HIPS, DLP, AV, app-lockers	10
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.	15
Patch management and vulnerability assessment	The process of risk management and vulnerability Assessment	5
Forensics concepts	Concept, Create HD image and mem dump, Analyzing mem dump and HD image	5
Audit Concepts		5
Static and Dynamic malware analysis	Strings, exported and imported DLLs , hash, PE structure etc. Using sandbox , Sysinternals and other basic tools	10
Data encryption and authentication		10
Law and Ethics/ Physical Security		10
Final exam	Hands-On Labs and simulator	10

Total Hours: 310



אנו ממתינים לשמוע ממך!

03-566-3155

info@kernelios.com