# סילבוס

# Penetration Testing Expert

Version 1

OnlineSecurity
CYBER SECURITY TRAINING COURSES

# על הקורס

ישראל נחשבת למעצמת סייבר. השקעות חסרות תקדים, מאות חברות המתעסקות בתחום הסייבר ואבטחת המידע, וכתוצאה מכך חברות המשוואות לעובדים מקצוענים בתחום. כשאנחנו מביטים אל העולם המרתק הזה אנחנו מבינים שיש צורך בהכשרה מקצועית שמגיעה מתוך התעשייה ומתוך היכרות חזקה עם הדרישות העדכניות בתחום.

קורס PTE הינו קורס Hands-On 100% בתחום בדיקות החדירה והאקינג.
הקורס משלב סרטוני וידאו מעמיקים בעולמות ההתקפה לצד מעבדות מתקדמות וריאליסטיות המדמות חברת Enterprise שאליה תצטרכו לחדור כחלק מהאתגרים והתרחישים במעבדות.

במהלך הקורס תרכשו כישורי תקיפה הנחוצים במיוחד בתעשיית אבטחת המידע, ובעזרתם תוכלו לסלול לעצמכם את הדרך לתפקידי מפתח בתחום. שמנו דגש על שילוב של ידע תיאורטי חזק לצד תרגול תרחישים מהעולם האמיתי וזאת על-מנת שתהיו מוכנים לתפקידים מאתגרים בתחום.

מעבדות ה- CyberAction שלנו יהיו נגישות לכם לכל אורך הקורס בכדי שתוכלו לממש כל טכניקה שתלמדו, לחוש סביבה ריאליסטית של חברת Enterprise, לשבור מכונות ולחדד את כישורי התקיפה שלכם. תוכלו לשלוט במכונות המעבדה, לצפות בהתקדמות שלכם באתגרים ועוד... באמצעות ממשק המעבדות המתקדם שלנו.

בסיום הקורס תגשו למבחן ההסמכה PTE Certified.
המבחן הוא 100% מעשי ובמהלכו תנסו לחדור 4 מכונות לפי רמות קושי שונות.
אורך המבחן המעשי הוא כ- 6 שעות ובמהלכו תדרשו להציג יכולות Hands-On גבוהות.
המחזיקים בהסמכת PTE Certified מוכיחים הבנה ויכולות מעשיות גבוהות בתחום המבוקש ביותר בעולם אבטחת המידע.

# תכני הקורס

**1. – Course Overview**
1.1 - Welcome
1.2 - Career Opportunities \ Motivation
1.3 - Setting up your Environment
1.4 - Labs Environment - CyberAction

**2. – Core Skills**
2.1 - Linux Overview
2.2 - The Bash Environment
2.3 - Kali Linux
2.4 - Databases
2.5 - Wireshark
2.6 - TCPdump
2.7 - Netcat
2.8 - Encoding,Encryption, Hashing and Obfuscation
2.9 - Botnet, Malwares etc.

**3. – Metasploit**
3.1 - Introduction
3.2 - Metasploit Interfaces
3.3 - Know the System
3.4 - Metasploit Database
3.5 - Exploits
3.6 - Payloads
3.7 - Multi Handler
3.8 - Preparing Your Report

**4. – Information Gathering and scanning**
4.1 - Introduction
4.2 - Popular system and Services
4.3 - DNS Enumeration
4.4 - Email Harvesting
4.5 - NMAP
4.6 - Maltego
4.7 - Vulnerabilities Scanning

**5. – Stay Anonymous**
5.1 - Introduction
5.2 - Proxy Chains
5.3 - VPN
5.4 - Changing MAC Address

**6. – Bypassing Security systems**
6.1 - Introduction
6.2 - Scripting and Administrative Tools
6.3 - Msfvenum
6.4 - Veil-Evasion
6.5 - Shellter
6.6 - PowerShell Empire

**7. – Exploits the System**
7.1 - Introduction
7.2 - Windows Exploitation
7.3 - Bypass UAC
7.4 - Linux Exploitation

**9. – Network Attacks**
9.1 - MITM Attack
9.2 - LLMNR / NetBIOS Spoofing Attack
**9.3 - Denial of Service Attack**
9.3.1 - Introduction
9.3.2 - Spoofed User-agent
9.3.2 - Slowloris

**10. - Using Credentials**
10.1 - Introduction
10.2 - Windows Credentials
10.3 - Linux Credentials
10.4 - Get the Hash
10.5 - Pass the Hash
10.6 - Using PSExec
10.7 - Invoke-TheHash

**11. – Password Cracking**
11.1 - Introduction
11.2 - Brute Force Attack
11.3 - Dictionary Attack
11.4 - Rainbow table

**12. - Post Exploitation**
12.1 - Privilege Escalation
12.2 - Migrate the Process
12.3 - Search for Valuable Content
12.4 - File Transfers
12.5 - Create Backdoor Access
12.6 - Clear logs and evidence
12.7 - Add New User to Administrators
12.8 - Disable FW

**13. - Web Applications**
13.1 – Introduction
**13.2 - Web Application Structure**
13.2.1 - HTTP Protocol
13.2.2 - URL Structure
13.2.3 - Encoding
13.2.4 - HTML Forms
13.2.5 - Cookies and Sessions
**13.3 - Fingerprinting**
13.3.1 - Web Spider
13.3.2 - Server Information
13.3.3 - Hidden Content
13.3.4 - Scanners
**13.6 - Web Application Attacks**
13.6.1 - Input Validation and Fuzzing
13.6.2 - XSS - Cross Site Scripting
13.6.3 - LFI and RFI
13.6.4 - Injection
13.6.5 - SQL Injection
13.6.6 - Automated SQL Injection

# מידע נוסף

## למי הקורס מתאים

- אנשי IT
- בעלי תשוקה לעולם אבטחת המידע, עם רקע במחשבים
- אנשי Testing Penetration מתחילים
- בעלי אורנטציה טכנית המעוניינים להשתלב בתחום

**הקורס מתקיים בשפה העברית אך אנגלית בסיסית נדרשת.**

## חומר לקורס ועזרים

- 5 שעות של סרטוני וידאו בשפה העברית.
- הורדת הוידאו ישירות למחשב.
- גישה למעבדות ה- CyberAction באמצעות VPN.

## הסמכת PTE Certified -

- אורך מבחן ההסמכה הינו בן 6 שעות.
- ניתן לגשת למבחן עד חצי שנה מסיום הקורס.
- מעבר מלא של האתגרים בסביבת המעבדות יזכה אתכם ב10- נקודות בונוס.
- הגשת דו"ח מלא של האתגרים במעבדות יזכה אתכם ב-5 נקודות בונוס נוספות.
- מעבר המבחן יזכה את התלמיד בתעודת הסמכה PTE-Certified.

# הסיפור שלנו

ישראל נחשבת למעצמת סייבר .השקעות חסרות תקדים ,מאות חברות המתעסקות בתחום הסייבר ואבטחת מידע ,ובתוצאה מכך חברות המשוואות לעובדים מקצוענים בתחום .כשאנחנו מביטים אל העולם המרתק הזה אנחנו מבינים שיש צורך בהכשרה מקצועית שמגיעה מתוך התעשייה ומתוך היכרות חזקה עם הדרישות העדכניות בתחום .אנחנו ב OnlineSecurityמציעים הכשרה והדרכה מקוונת למקצועות אבטחת המידע הכוללת תרגולים פרקטיים במעבדות מתקדמות ,הסמכה וליווי במציאת עבודה בתחום .איתנו תהיו בטוחים שהכניסה שלכם לתחום תהיה חלקה ומהנה.

יצירת קשר:

www.onlinesecurity.co.il/contact_us

support@onlinesecurity.co.il

OnlineSecurity
CYBER SECURITY TRAINING COURSES