

# ITSAFE

Cyber Security Trainings



# תשתית בודק חוסן





50 שעות תוכן ומעבדות

116 שיעורים

הכנה ל OSCP

מעבדות תירגול

# בדיקות חוסן תשתית

## 2. היכרות עם עולם בדיקות החוסן

- טרמינולוגיה בעולם התקיפה.
- סוגי טכנולוגיות בעולם ה-Pentest.
- תהליכי סריקה וזיהוי פגיעויות.
- השגת שליטה וחשיבותה.
- אחיזות על מכונה נתקפת.
- ניקוי עקבות.

## 4. איסוף מידע פאסיבי & אקטיבי

- חיפוש מידע על ידי Google Hacking
- איסוף ואיתור כתובות מיילים
- איסוף מידע פאסיבי OpenSource
- DNS Enumeration
- תקשורת מול שרתי DNS
- מחקר אוטומטי מול שרתי DNS
- DNS Forward Lookup
- DNS Reverse Lookup

## 1. הקמת סביבת מעבדות

- וירטואליזציה עם VirtualBox.
- טעינת Kali Linux.
- טעינת Windows.
- טעינת Metasploitable2.

## 3. כלי מפתח והבנה טכנולוגית

- שימוש ב-Netcat.
- התחברות בפרוטוקולים UDP/TCP.
- האזנה בפרוטוקולים UDP/TCP.
- תקשורת התקפית Reverse/Bind.
- העברת קבצים וסריקות על ידי Netcat.
- שימוש ב-Wireshark.
- פילטרים ב-Wireshark.
- חילוץ מידע מקבצי PCAP.

## 5. סריקת פורטים

- לחיצת יד משולשת ותקשורת TCP
- סריקות בפרוטוקול UDP
- טעויות נפוצות בסריקות פורטים.
- סריקות פורטים על ידי NMAP
- סריקות מתקדמות NMAP NSE
- עקיפת Firewalls ומוצרי הגנה.
- זיהוי מערכות הפעלה.
- Service Enumeration

"**מספר מקומות** העבודה

בתעשיית **הסייבר** עומד

**לזנק פי 10** בעשור הקרוב."

עיתון גלובס



## 8. הסלמת הרשאות Windows

- UAC Bypass User Interacion
- UAC Bypass No Interaction
- PE Suggester
- Patch Enumeration
- Unquoted Path
- Insecure Service
- Zero Click

## 9. הסלמת הרשאות Linux

- Basics Enumerations.
- Kernel Exploits.
- SUID Exploitation
- Sudo Abuse.
- Word Writable.
- CronTab PE.
- Sensitive Files.
- Http Methods.

## 6. Metasploit ואקספלוויטים

- היכרות עם Metasploit
- מודלים ב Metasploit
- Payloads
- Auxiliaries
- Exploits
- תקיפת FTP עם חולשת RCE
- SMB-Windows Brute Force
- Hydra Brute Force
- פרופילי סיסמאות
- Enumeration Tactics
- הזרקות Shellcode.
- מעבר בין תהליכים לאחר הזרקת קוד.
- עקיפות Firewall
- תקיפות Wordpress ו-Drupal
- LFI/RFI
- Log injections
- Environ & Fuzzing
- Remote Code Execution
- Command Injections
- יצירת סוסים טרויאנים.
- שליטה ב Meterpreter
- תקיפת Tomcat
- Backdooring
- Advanced Meterpreter
- Keylogging
- Download/Upload Functions
- SMTP Enumeration

## 7. העברת קבצים

- העברת קבצים באמצעות פייתון
- העברת קבצים ב-Windows ע"י Powershell
- העברת קבצים בין Windows ל Linux ע"י FTP
- העברת קבצים באמצעות שרת SMB
- שיטות נוספות למעבר קבצים





- Challenge Response מנגנון הזדהות
- גיבוב LM/NTLM
- SAM And Password Flow
- שליפת סיסמאות Mimikatz
- שליפת סיסמאות WCE
- Mimikatz Using Powershell
- Hash extraction SamDump
- Hash extraction SecretDump
- SecretDump Remoting
- Password Cracking Hashcat / Jhon
- Pass The Hash
- Responder introduction to LLMNR
- Responder Capture NTLMv2

- Introduction to X86 Architecture
- Understand Memory
- Program Memory
- CPU Registers
- Buffer Overflow Intro
- Introducing the ollydbg Debugger
- Overflowing the Buffer
- Fuzzing Tactics
- Dealing with the crash
- EIP control
- Shellcode space locating
- Bad Characters
- Execution flow redirection
- the return address
- Shellcoding with Metasploit
- Getting the Shell

