סילבוס הקורס

חומר לימוד

1 יחידות

תוכן העניינים

1. סילבוס הקורס: האקינג אתי מהיסוד (Ethical Hacking from Zero)

סילבוס הקורס: האקינג אתי מהיסוד (Ethical Hacking from Zero)

היקף: כ-30 שעות וידאו · 8 מודולים · מבוסס על מתודולוגיית *Practical Ethical Hacking* של TCM Security **קהל יעד:** מתחילים ללא רקע קודם באבטחת מידע **דרישות קדם:** היכרות בסיסית עם מחשב; אין צורך בידע מוקדם בתכנות או ברשתות

מטרות הקורס

בסיום הקורס הלומד יוכל:

- להסביר את חמשת שלבי ההאקינג האתי (Five Stages of Ethical Hacking) וליישם אותם בסדר הנכון.
- להקים סביבת מעבדה (Lab) מבודדת ובטוחה עם Kali Linux ומכונות מטרה.
- לבצע איסוף מידע (Reconnaissance) פסיבי ואקטיבי על יעד.
- לסרוק ולמנות (Scanning & Enumeration) שירותים, פורטים וחולשות.
- לנצל חולשות (Exploitation) ולהשיג גישה למערכת בעזרת Metasploit וכלים נוספים.
- להבין ולבצע Buffer Overflow בסיסי מקצה לקצה.
- לתקוף סביבת Active Directory ולבצע פעולות Post-Exploitation.
- לתעד ממצאים ולכתוב דוח בדיקת חדירות (Penetration Test Report).

הערת אתיקה וחוק ⚠️

כל הטכניקות בקורס מיועדות **אך ורק** לבדיקות מורשות: מעבדה פרטית, מכונות תרגול ייעודיות (למשל TryHackMe, HackTheBox), או יעד שקיבלת ממנו **אישור בכתב**. תקיפה של מערכת ללא רשות היא עבירה פלילית לפי חוק המחשבים, התשנ"ה-1995. הידע כאן נועד להגנה — לא לתקיפה.

מבנה הקורס

#	מודול	נושאים עיקריים	שיעורי מקור
1	**מבוא, המעבדה ו-Kali Linux**	התקנת VMware/VirtualBox, Kali Linux, סקירת הכלים, ניווט בסיסי	1–13
2	**יסודות רשתות (Networking)**	מודל OSI, TCP/IP, פורטים ופרוטוקולים, כתובות IP ו-Subnetting	(רוחבי)
3	**Python להאקרים**	משתנים, מבני נתונים, לולאות, פונקציות, כתיבת Port Scanner	14–31
4	**איסוף מידע (Reconnaissance)**	OSINT, איתור דומיינים, כתובות מייל, טכנולוגיות אתר, Burp Suite	32–39
5	**סריקה ומיפוי (Scanning & Enumeration)**	Nmap, מניית HTTP/SMB/SSH, Nessus, חקר חולשות	40–48
6	**ניצול והשגת גישה (Exploitation)**	Reverse/Bind Shells, Payloads, Metasploit, Brute Force	49–53
7	**Buffer Overflow**	Fuzzing, EIP, Bad Characters, Shellcode, השגת Root	54–59
8	**Active Directory**	בניית מעבדת AD, וקטורי תקיפה, Post-Compromise, Pass-the-Hash	60–73

שיטת ההוראה

כל מודול כולל:

1. **חומר לימוד (Material)** — מסמך PDF מובנה בעברית עם מושגי מפתח, פקודות ודוגמאות.
2. **מצגת (Slides)** — סיכום ויזואלי לחזרה ולהוראה.
3. **מונחים דו-לשוניים** — כל מונח טכני בעברית עם המקור באנגלית בסוגריים, ושמות כלים (nmap, Metasploit) נשמרים באנגלית.
4. **תרגול מומלץ** — הפניה למכונות תרגול חוקיות.

הערכה מומלצת

- תרגול מעשי בכל מודול על מכונה חוקית.
- פרויקט מסכם: בדיקת חדירות מלאה על מכונת תרגול (Capstone) עם כתיבת דוח.