# סילבוס

CYBER SCHOOL

## סדנת סייבר גיימינג

## Cyber Games

# פרטי הסדנה

## תיאור הסדנה

סדנה זו מספקת הצצה ייחודית ומעמיקה אל תוך עולם החשיבה של האקרים זדוניים, באמצעות שימוש בפלטפורמה חדשנית לתרגול מעשי של מתקפות סייבר בסביבה אמיתית ותחרותית. על ידי הבנת הסוגים השונים של השיטות והאסטרטגיות של התקפות האקרים, ותרגול מעשי שלהם בפלטפורמת המשחק, התלמידים יהפכו למעין אנשי מקצוע בתחום אבטחת הסייבר, אשר יכולים לנצח את ההאקרים במשחק שלהם.

במהלך הסדנה התלמידים יגלו כיצד לבצע ולהגן מפני מגוון מתקפות סייבר, כולל התקפות רשת, התקפות אפליקטיביות והתקפות קריפטוגרפיות. מעבדות מעשיות בתוך סביבת המשחק מספקות ללומדים את הכלים, הידע והמיומנויות הנדרשות כדי לגלות ולנצל את נקודות התורפה של מערכות ממוחשבות ואינטרנטיות, כל זאת תוך הנאה, תחרות ולמידה חווייתית.

הסדנה מיועדת לתלמידים בעלי רקע שליטה בסיסית באנגלית ורקע בסייבר (קורס מבוא לסייבר\סייבר באטל רויאל\סייבר האקינג).

## יעדי הלמידה

- פיתוח כישורי סיור ועקיפה של מערכות הגנה שונות.
- התגברות על הצפנות ומעקף טכניקות הסתרת מידע.
- הבנה ויישום של טכניקות הצפנה.
- למידת טכניקות התקפה מבוססות אפליקציה.
- הבנה ושימוש בכלי פרוקסי מתקדמים.
- ביצוע תקיפות פיצוח סיסמאות והבנת הסיכונים הרלוונטיים.
- הבנת דרך הפעולה של בסיסי נתונים, וביצוע של הזרקות מידע.
- ניתוח רשתות ותעבורה באמצעות כלי ניתוח מתקדמים.
- למידת התחום של על אתרים, פלטפורמות אינטרנט ושרתי המארח שלהם.
- שימוש בטכניקות חדירה של יישומי אינטרנט כדי לגלות נקודות תורפה במערכות מבוססות ענן.

# דרישות טכניות

## חומרה

**כדי להשתתף בסדנה, הסטודנטים צריכים שיהיה ברשותם מחשב עם דרישות המינימום הבאות:**

- 16 GB RAM
- כונן קשיח מסוג SSD עם GB30 פנויים.
- מעבד i5 core או גבוה יותר

## תוכנה

**הסטודנטים צריכים שיהיו ברשותם:**

- Oracle VirtualBox 6 או גרסה מאוחרת יותר
- מחשב מאופשר וירטואליזציה

# תוכן הסדנה

| מספר שיעור | שם השיעור | נושאי השיעור | מעבדות | אתגרים |
|---|---|---|---|---|
| **מבוא והיכרות, הקמת סביבה** | | | | |
| **1** | שיעור פתיחה | • הסבר על הפלטפורמה<br>• התקנת סביבה | • התקנת VBOX<br>• התקנת סייבר גיימס | |
| **2** | מבוא להתקפות אפליקטיביות | • מחקר קוד מקור | • פריצה ל-2048 | • Basic HTML<br>• URL Manipulation |
| **3** | קוד מקור | • שינוי ועריכת קוד מקור<br>• עוגיות | • פריצה ל- Cookie Clicker | • Parameter tampering 2 |
| **4** | התקפות אפליקטיביות בסיסיות | • מניפולציה על עמודי רשת | | • Parameter tampering 3<br>• Parameter tampering 4 |
| **הצפנות** | | | | |
| **5** | הצפנה וגיבוב | • גיבוב<br>• HASH | • אתגרי הצפנה<br>• Base64 Manual Encoding | • Basic crypto<br>• Crypto 2 |
| **6** | הסתרת מידע | • טכניקות הסתרה<br>• הסתרה דיגיטלית | • הסתרה בתוך קובץ | • Steganography<br>• Py decription |

| | | | | |
|---|---|---|---|---|
| **7** | הכנה לתקיפת Brute-Force | • התחמשות<br>• מילון | • יצירת מילון עם crunch | |
| **8** | תקיפות-Brute Force | • פיצוח סיסמאות אופליין<br>• פיצוח סיסמאות אונליין | • מעבדת פיצוח HASH | • Dictionary attack |
| **סייבר התקפי** | | | | |
| **9** | איסוף מודיעין וניצול חולשות | • מחזור מתקפה<br>• איסוף מידע<br>• ניצול חולשות | • ניצול robots.txt | • Robots.txt |
| **10** | התקפות רשת אלחוטית | • טכנולוגיות Wifi | • מחקר חולשות רשת | • WiFi Cracking |
| **11** | Wireshark | • שימוש ויישום Wireshark | • התקנת Wireshark | • Capturing passwords with WireShark |
| **12** | ניתוח רשת | • ניתוח תעבורה ברשת | • Advanced Analysis | |
| **התקפות אפליקטיביות** | | | | |
| **13** | התקפות אפליקטיביות | • פרוקסי אפליקטיבי<br>• BurpSuit | • Intercept and Access | • Parameter tampering 1 |
| **14** | התקפות אפליקטיביות מתקדמות | • BurpSuit מתקדם | | • Forced browsing |
| **15** | בסיס לעולם XSS | • שפות אינטרנט בצד הלקוח | | • XSS Attack |
| **16** | התקפות XSS | • Cross Site Scripting<br>• השלכות XSS | • תרגול XSS אונליין | • XSS Attack 2 |
| **17** | הכללת קובץ מקומי | • סוגי XSS<br>• העלאת קובץ זדוני | • bWapp | • LFI |
| **18** | מבוא ל- SQL | • בסיסי נתונים | • Building a Database | • SQL Injection |
| **19** | הזרקת SQL | • סכנות SQLi<br>• תקיפות | • bWapp | • SQL Injection 4 |
| **20** | סיכום ומבחן | • סיכום הקורס<br>• הצגת המנצחים | • מבחן סיכום | |