המכללה ללימודי מקצועות הסייבר

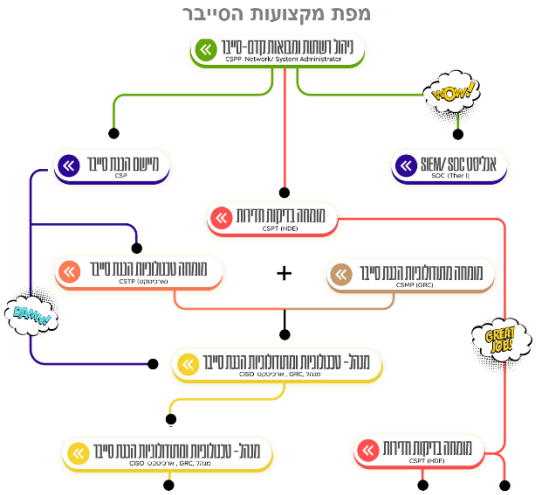
התכנית ללימודי
מומחה בדיקות חדירות
(WEB Application attacks)

תכנית זו אינה מקנה רקע
במשפטים אינשוק או פיתוח תכנה,
וכוללת מעבדות ייחודיות מסוגל
לתרגול Hands-on.

על-פי מערך הסייבר הלאומי
(אסדרת מקצועות הסייבר בישראל)

https://www.gov.il/he/Departments/israel_national_cyber_directorate

מקצוע מפוקח על-ידי מדינת ישראל*, שיכלול בקרוב תעודה רשמית של מדינת ישראל למקצוע מומחה בדיקות חדירות בתחום האפליקטיבי.



מומחה בדיקות חדירות (האקר, בלשון העם), הוא אחד ממקצועות הליבה היוקרתיים בעולם הדיגיטלי בכלל, וענף הסייבר בפרט.

הלימודים בתכנית זו מחייבים רקע בתשתיות (System, Network, Python).

חוק הסייבר והרגולציה הממשלתית (אסדרת מקצועות הסייבר בישראל, מערך הסייבר הלאומי, משרד ראש הממשלה), מחילים פיקוח ממשלתי על מקצוע זה, על-מנת למנוע הפצת תכניות לימוד מסחריות בלתי מאושרות. דרוש אישור משרד העבודה לתכנית הלימודים למקצוע בודק חדירות!

וְלֹא פָּחוֹת חָשׁוּב: נִלְמָד כְּפִי שֶׁרַק שִׁיא סֶקְיוּרִיטִי יוֹדֵעַת לָלַמֵּד **נכון**, וְעִם **הַלֵּב**.

תכנית הסמכה רשמית ומעבדות ללימודי מקצוע בודק חדירות בתחום האפליקטיבי

מבוא

תחום תקיפת Cyber (או לוחמת מידע או לוחמה קיברנטית או מבחני חדירה) הינו מן התחומים הטכנולוגיים המרתקים בעולם אבטחת המידע וה- Cyber Warfare. התחום הינו מהחשובים מבין חמשת עולמות אבטחת המידע, מיועד לבעלי כשרון טכני ויצירתיות.

אודות המכללה

מכללת See Security הנה מכללה **בינלאומית** התמחותית למקצועות ניהול רשתות וסייבר, ועוסקת בלעדית בתחום זה בכל זמנה, במתודולוגית הדרכה שנבנתה עבור גורמים ממלכתיים.

המכללה מייצאת את תכניות הלימודים לכל רחבי העולם, באמצעות המותג *See Security International*, ובאמצעות גופי סייבר ישראליים ידועי-שם העוסקים ביצוא בטחוני.

מנהל הקבוצה שבה משולבת המכללה, מר אבי ויסמן, הינו ממובילי ענף הסייבר, יועץ לממשלת ישראל בנושא "אסדרת מקצועות הגנת הסייבר" בישראל, פרשן בערוצי השידור בארץ ובחו"ל, מקימו של הפורום הלאומי לאבטחת מידע IFIS יחד עם האלוף במיל' וראש המל"ל לשעבר, יעקב עמידרור, מנכ"ל משותף בחברה להשמת כוח אדם בענף הסייבר - *SeeHR*, בחברה לייעוץ *See Consulting – Cyber*, בחברה לפתרונות Managed SEIM/SOC – *See Events*, ובמכללה הבינלאומית לסייבר *See Security College International*.

אודות מערך הסייבר הלאומי: רגולציה רשמית למקצועות הסייבר בישראל (תחת פיקוח ממשלתי והסמכה ממשלתית)

מערך הסייבר הלאומי אשר פועל במשרד ראש הממשלה כיחידה עצמאית (מקביל למשרד ממשלתי), החליט להפעיל אסדרה (רגולציה) מחייבת בנושא הגדרתם של המקצועות השונים בעולם הסייבר, ומפעיל המלצות ברורות בנוגע לתכני הידע לכל מקצוע, וזאת, על מנת להפסיק את הכאוס הקיים בלימודים במוסדות מסחריים. בחלק ממקצועות הסייבר כבר נקבעה תכנית לימודים מחייבת, וקיימים מבחני הסמכה. מבחן

מאפייני תוכנית הלימודים	
עלות:	**8,000 ש"ח + 400 ש"ח דמי הרשמה**
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית/ **טכנית / יישום**
מטרה:	הכשרת אנשי תקיפה ומודיעין, , תקיפת יישומים ויישומי Web.
שלב:	**מתחילים** ב-PT / בעלי רקע במחשבים/פיתוח
רוחב:	ממוקד / **רחב**
עומק:	סוקר / **עמוק**
שעות:	**40 שעות**
פתיחה:	ראה בעמוד הראשי של המכללה
מתכונת:	Bootcamp או לפי הזמנת הלקוח.
תרגול בית:	**בהיקף 120 שעות**

אודות תכנית WEB Application Attacks – בודקי חדירות

מדינת ישראל באמצעות מערך הסייבר הלאומי מיסדו בחוק את נושא לימודי סייבר בכלל, ואת לימודי מקצוע Penetration Testing בפרט.

תכנית זו נבנתה בשים לב לרגולציה של מקצוע Penetration Tester וכוללת עבודת Hands-on רבה.

תוכנית WEB Application Attacks מרכזת מספר תחומי תקיפה הנהוגים במדינות מתקדמות, למערך הכשרה אחד, ועוסקת בכל השלבים הנדרשים: מאיסוף המודיעין, דרך שיטות החדירה, וכלה בניקוי ובמיסוד התקיפה. התוכנית פורטת לפרוטות את הטכניקות הקיימות על נדביכהן, לרבות: Web Application, ועד האדם – Social Engineering.

התכנית עתירת תרגול עצמי ומשימות אישיות, מעבדות, לרבות מעבדות המונגשות לבית התלמיד.

תכנית CSPT מיועדת להשיג את שלשת היעדים הבאים:

א. להנגיש לתלמיד (המנוסה ב-IT או בפיתוח, אך "מתחיל" בהאקינג) את הידע, את המעבדות ואת התרגול עצמו, לעולם תקיפת אפליקציות Web.

מעבדות תרגול בינלאומיות

תכנית זו הינה עתירת תרגול מעשי, על-גבי מעבדות מוכחות וותיקות של See Security, לצד תשתיות מעבדתיות בינלאומיות ידועות:

1. HDE Labs
2. Hack the Box
3. Over the Wire
4. HDE-Hack & Beer CTF (Capture The Flag). זהו פרויקט מרתק (רווי בירה ומגשי פיצה), שבו התלמידים שקועים עד צווארם מבוקר עד לילה במבחן שמהותו -תקיפה אמיתית, רב-שלבית, המשלבת דיסציפלינות ושיטות תקיפה שנלמדו במהלך התכנית, עד להשגת היעד הסופי.

סגנון לימודי - טכני, תיאורטי ו- Hands On.

קהל יעד

למעוניינים להתמחות כבודקי חדירות בתחומים האפליקטיביים, או להמשיך למקצועות חקירת פוגענים. ראה בסוף המסמך – מפת התפתחות.

דרישות סף

- ידע מעשי בתחום תשתיות, מערכות הפעלה ותקשורת
- ידע בסיסי בפיתוח קוד וכלי אבטחה, עם דגש על שפת Python, ו/או סיום מכינת Python לפי החלטת היועץ האקדמי.
- בוגרי 12 שנות לימוד, (או: תנאי הקבלה לחרדים מבחן מיון והתאמה למקצוע: ישיבה קטנה / ישיבה גדולה).
- ראיון אישי עם אבי ויסמן / וועדת קבלה / ועדת חריגים.

מתכונת לימודים

- משך התכנית כחודש. הלימודים מתקיימים בקמפוס See Security ברמת-גן (צמוד לתחנת רכבת מרכז), והמסלול נפתח כ- 3 פעמים בשנה.
- יתכן כי מועמד יחויב לעבור מכינת Python בת 3 מפגשים לפני הקורס, לשיקול דעתו הבלעדי של היועץ האקדמי.

את מבחן הסיכום בן 12 שעות בדופות לא תשכחו לעולם...

HDE: Hack & Beer ...האתגר, הפיזות, הבירה, המשחק

סגל המרצים

תומר חדד מוביל את קורס HDE במכללת שיא סקיוריטי. תומר משמש כ- Tech lead & appsec offensive researcher בחברת Hacktics, והוא ממחה בכל הנוגע ל- desktop apps, mobile, embedded, IoT and Reversing. תומר מנוסה מאוד בפיתוח חומרי למידה וקורסים כמו גם בהוראה. בנוסף, תומר מרצה בכנסים בינלאומיים כמו OWASP ו- BSides.

למידע נוסף / פגישת יעוץ:

מידע מינהלי: אלוירה אליסייב, 03-6122831, elvira@see-security.com

יועץ אקדמי: אבי ויסמן, 03-6122831, 054-5222305, avi@see-security.com

כיצד נבנה המוניטין של המכללה?

מנקודת המבט של הנהלת המכללה, תלמיד מצליח אך ורק אם הצליח להשתלב אצל מעסיק בתפקיד רלוונטי. לכן הגדרת תכני הקורס נבנתה בהתאם לדרישת המעסיקים.

המעסיק דורש ומצפה כי בוגר של מכללה ייעודית לסייבר כמו See Security יגיע בוגר יותר, עשיר יותר ובעל ידע רב תחומי, ויחזיק ברשותו גם הסמכה בינלאומית מוכרת באופן רשמי.

"המתחרה" של המועמד איננו המעסיק. להיפך: הוא מבקש את הטוב ביותר לעצמו. כאשר הוא מבקש לקלוט מועמד של מכללה מקצועית-ייעודית, הוא מצפה לפחות שיהיה בעל ידע רב יותר ממועמד המגיע מחברות אחרות המשווקות קורסים.

עובד משרד הבטחון / צה"ל / משרד ראש הממשלה / מטה הסייבר / מערך הסייבר / בוגר מכללת שיא סקיוריטי

בדוק עם הנהלת המכללה דרכי ההרשמה ומחירי משהב"ט/ראה"מ לגבי המסלול.

מה אנחנו מצפים מבוגר התכנית?

1. בתקופת הלימודים תשקיע את כל הזמן כדי לקיים את הנחיות המרצה, אינך הראשון ולא תהיה האחרון שימצא עצמו בעבודה מאומצת, בודק חדירות בלב התעשייה.
2. בסיום לימודיך היעזר בהנהלת המוסד לבניית טופס קורות חיים ההולם את מאמצייך.
3. הסתפק בתחילת דרכך במשרה רלבנטית מכל סוג שהוא כדי לצבור ניסיון, והרבה להתאמן לבד.
4. בדוק עם היועץ האקדמי את איכות עמידתך בריאיון אישי לקראת ראיונות העבודה האמיתיים, במקרים מסויימים אפילו תלמיד מצטיין זקוק לתיקונים (פשוטים יחסית) שמשביחים מאוד את יכולתו למצוא משרה איכותית.
5. צא לדרכך, אל תשכח להמשיך ללמוד, דאג תמיד להיות מבחינת ידע רמה אחת יותר מהאחרים, כי ככל שתגביה כך יהיו לך פחות מתחרים, שכר גבוה יותר, וסיפוק רב יותר.

הערות

- ההרשמה לכל מבחן חיצוני, הנה בתשלום ותבוצע באחריות הסטודנט בלבד.
- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכללה.
- המכללה מביאה לידיעת הנרשמים והסטודנטים כי ייתכנו שינויים במערך התכנית, במועדי הלימוד והבחינות או בכל נושא אחר. הודעה על שינוי תימסר למשתתפים.

תכנית לימודים:

CHAPTER A – INTRODUCTION

1 INTRODUCTION TO HACKING
- 1.1 Hackers & motivations
- 1.2 Targets
- 1.3 Attack lifecycle
- 1.4 Goals

2 DIGITAL INFORMATION
- 2.1 Ways of representing data
- 2.2 Binary representation
- 2.3 Hashing
- 2.4 Cryptography
- 2.5 Data Integrity

3 WEB APPLICATIONS INTRO
- 3.1 HTML, CSS, JS
- 3.2 The browser
- 3.3 HTTP
- 3.4 Client-server
- 3.5 Common architectures

CHAPTER B – RECONNAISSANCE

4 INTRODUCTION TO RECONNAISSANCE
- 4.1 Goals
- 4.2 Active vs Passive Information Gathering

5 KNOW YOUR TARGET
- 5.1 Using the app
- 5.2 Mapping opportunities
- 5.3 Deciding on focus

6 AUTOMATIC SCANNING
- 6.1 Dirsbusting
- 6.2 Versions
- 6.3 Libraries
- 6.4 Technologies
- 6.5 CMSs and frameworks
- 6.6 Automatic vulnerability identification

7 MANUAL RECON
- 7.1 Footprinting
- 7.2 Misconfigurations
- 7.3 Important headers
- 7.4 Client-side leads

CHAPTER C – AUTHENTICATION & AUTHORIZATION

8 INTRO
- 8.1 Common authentication methods
- 8.2 Authorization & permissions – vertical vs horizontal

9 AUTH BYPASS
- 9.1 Forceful browsing
- 9.2 Parameter tampering

10 ACCOUNT TAKEOVER
- 10.1 User enumeration
- 10.2 Brute force & dictionary attacks
- 10.3 Session management issues

11 SOCIAL ENGINEERING ATTACKS
- 11.1 Same Origin Policy & CORS
- 11.2 CSRF
- 11.3 Clickjacking
- 11.4 Open Redirect

CHAPTER D – DATA IN TRANSIT

12 HTTP/S
- 12.1 Man-in-the-Middle and HTTP
- 12.2 HTTPs scanning
- 12.3 Important security headers

CHAPTER E – INJECTION & RCE

13 CRLF

14 OS COMMANDS INJECTION

15 XSS
- 15.1 Persistent XSS
- 15.2 Reflected XSS
- 15.3 DOM-XSS

16 SQL INJECTION
- 16.1 UNION based
- 16.2 Blind
- 16.3 Automatic tools

17 FILE UPLOAD
- 17.1 Viruses
- 17.2 Web shell
- 17.3 Malicious downloadable

CHAPTER F – OTHER WEB APPLICATION ATTACKS

18 INCLUSION

18.1 Local file inclusion
18.2 Remote file inclusion

19 SSRF

20 SERIALIZATOIN

CHAPTER G – CTF (CAPTURE THE FLAG) FINAL EXAM

A vulnerable web application with hidden “flags”.

Flags are exposed by exploiting vulnerabilities learned during the course.

הצהרת תלמיד בלימודי HDE

הריני מאשר בזאת כי קיבלתי דף מידע זה, הבנתי את תכנו והסכמתי לתנאים המפורטים בו.

שם הנרשם: _____ תאריך: _____ חתימה _____

We invented a methodology for cyber education,
because nobody else did it.