המכללה ללימודי מקצועות הסייבר

התכנית ללימודי
מומחה בדיקות חדירות
(Penetration Tester)

תכנית זו מיועדת למתעלמי רקע
בתשתיות מחשוב או פיתוח תכנה,
וכוללת מעבדות ייחודיות מסוגל
למתרגל Hands-on.

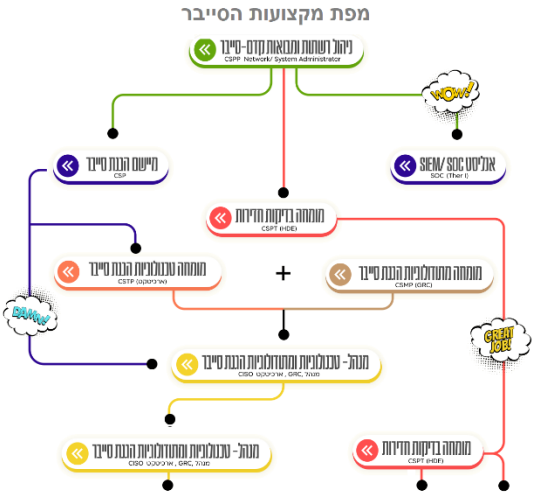
על-פי מערך הסייבר הלאומי
(אסדרת מקצועות הסייבר בישראל)

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, כולל הכנה למבחני מערך הסייבר, וכולל הכנה להסמכה OSCP.

* חוק חיילים משוחררים התשנ"ד

לטובתך! בקש מהמכללה ראיון ייעוץ אישי עם אבי ויסמן



להיות מומחה בדיקות חדירות בסייבר.

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

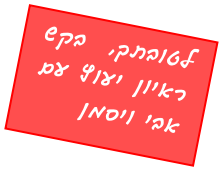
הלימודים בתכנית זו מחייבים רקע בתשתיות (System, Network, Python).

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 יוֹדַעַת לְלַמֵּד נכון, וְעִם הַלֵּב.

תכנית הסמכה רשמית ומעבדות ללימודי מקצוע בודק חדירות

התוכנית נבנתה לרגולציה של מערך הסייבר הלאומי (אסדרת מקצועות הסייבר בישראל)



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, אחת מ- 7 מכללות מסוגה בעולם ומהמוערכות שבהן, 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 ההסמכה למקצוע בודק חדירות צפוי להתקיים החל משנת 2020.

מאפייני תוכנית הלימודים	
עלות:	**15,500ש"ח + 400 ש"ח דמי הרשמה**
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית/ **טכנית / יישום**
מטרה:	הכשרת אנשי תקיפה ומודיעין, בתחומי תקיפתSystem, תקיפת Network, תקיפת Mobile, תקיפת יישומים ויישומי Web, ובתחום ה- Reverse Engineering.
שלב:	**מתחילים** ב-PT / בעלי רקע במחשבים/פיתוח
רוחב:	ממוקד / **רחב**
עומק:	סוקר / **עמוק**
הסמכות:	**HDE, CEH, OSCP**
שעות:	**152 שעות**
פתיחה:	ראה בעמוד הראשי של המכללה
מתכונת:	הלימודים בקמפוס המכללה ברמת גן, מתקיימים פעמיים בשבוע בימי א' + ד' בערב: 17:30 עד 21:30 (5 שעות אקדמיות למפגש), במשך כ-4 חודשים
תרגול בית:	**בהיקף 400 שעות**

אודות תכנית CSPT – 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 Hacking Defined Experts מרכזת מספר קורסי תקיפה הנהוגים במדינות מתקדמות, למערך הכשרה ארוך אחד, ועוסקת בכל השלבים הנדרשים: מאיסוף המודיעין, דרך שיטות החדירה, וכלה בניקוי ובמיסוד התקיפה. התוכנית פורטת לפרוטות את הטכניקות הקיימות על נדבכיהן, לרבות: System, Network, Mobile, 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 התשתיות, תקיפת אפליקציות Web, ותקיפת Mobile.

ב. להכינו לקראת מבחן OSCP (לא פחות מ- 6 חודשים מתום הלימודים).

ג. להכינו להסמכה הישראלית הרשמית של מערך הסייבר הלאומי לתפקיד "בודק חדירות מוסמך".

מכללת See Security היא הנציגה **היחידה** שמכינה כבר עתה את הבוגרים למבחן מערך הסייבר הלאומי. בכוונת מערך הסייבר למסד ב-2020 מבחן להסמכה ייחודית של מערך הסייבר בישראל, על-בסיס תכנית זו.

פחות מומלץ לגשת למבחן CEH כי מדובר בהסמכת "כניסה" שאינה מוערכת עבור אנשי מקצוע Penetration testing.

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.

תכנית CSPT ותוכניות Penetration Testing אחרות

לתחום ההאקינג/בדיקות חדירות, ידועות מספר הסמכות בינלאומיות:

1. הסמכת OSCP של Offensive Security (מבית היוצר של מתי אהרוני, יוצא מכללת See Security, אשר היה אחד המרצים בתכנית HDE זו). הסמכה זו ייעודית לעולם התקיפה, ממוקדת בפרק "תקיפת תשתיות", ואינה כוללת מיקוד על תקיפות Web, Mobile וסביבות אחרות.
   ההסמכה עמוקה ונחשבת לקשה וגבוהה, ובסיומה נדרש הנבחן לעמוד במטלת תקיפה רב-שלבית בת 24 שעות.
   ההסמכה אינה מתאימה למתחילים. OSCP מוכר במרבית מדינות העולם, לרבות על ידי משרד ההגנה בארה"ב.
2. הסמכת CEH (Certified Ethical Hacker) של EC-Council, . הסמכה זו איננה ממוקדת רק בתקיפה, אלא חורגת לעולם הגנת סייבר (כללית יותר), ומספקת הכשרה תיאורטית לעולם התקיפה, לצד תחומי הגנה כלליים, ברמת סקירה בלבד. גם CEH מוכר על ידי משרד ההגנה בארה"ב, לרמה נמוכה וראשונית של ידע.

מרבית הניגשים לתכנית HDE, מעוניינים (בהמשך הדרך) בהסמכת OSCP. מרבית הניגשים לתכנית, גם "דילגו" על הסמכת CEH.

זכאות לתעודה

- קיימת חובת נוכחות ב-80% מהמפגשים, ועמידה במבחנים/עבודות, בציון 70 (מבחן חוזר ללא תשלום).
- תיעוד: לעומדים בדרישות התכנית תוענק תעודת הסמכה מטעם See Security:

"מומחה בדיקות חדירות מוסמך - Hacking Defined Expert"

סגנון לימודי - טכני, תיאורטי ו- Hands On.

קהל יעד

למעוניינים להתמחות כבודקי חדירות (Penetration Testers), 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 כ- כ-4 חודשים. 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 רצופות לא תשכחו לעולם...

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

סגל המרצים

איציק משה, חוקר אבטחת מידע, בתחום האבטחת מידע קרוב לכ-20 שנה, מהחלוצים של קהילת האבטחת מידע הראשונה של ישראל. איציק נגע במגוון תחומים ועבד מול מספר רב של גופים פרטיים וביטחוניים בארץ ובעולם.

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

תכנית לימודים (מקוצר, ראה תכנית מלאה בדפים הבאים)

נושא	שעות
Preparation: Python	40
1. Introduction to Hacking	5
2. Cyber Security Fundamentals	5
3. Linux Essentials for HDE	5
4. Reconnaissance: Introduction	5
5. Reconnaissance: OSINT	10
6. Infrastructure Attacks: Introduction to Network Penetration	5
7. Infrastructure Attacks: Network Penetration	5
8. Infrastructure Attacks: Man in the Middle	5
9. Infrastructure Attacks: Exploitation: Metasploit	5
10. Infrastructure Attacks: Exploitation: Empire Framework	5
11. Infrastructure Attacks: Post Exploitation & Privilege Escalation	5
12. Infrastructure Attacks: Windows Domain Attack	5
13. Infrastructure Attacks: RF & WiFi	5
14. Web Application Penetration: Intro & OWASP top 10	10
15. Web Application Penetration: Additional findings q Scanners	5
16. Web Application EXAM	5
17. capture the flag: Full Day CTF - Hack & Beer	**12**
18. Reverse Engineering	10
סך הכל:	**152**

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.

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 Methodology
- 1.2 Full Disclosure
- 1.3 Ethics
- 1.4 Hacking & the Law

2 LINUX
- 2.1 Basic Commands
- 2.2 Users & Groups
- 2.3 Permissions
- 2.4 Working with terminal
- 2.5 Compile & Execute
- 2.6 full disk encryption
- 2.7 Build Linux from scratch - Gentoo
- 2.8 Bash Scripting

CHAPTER B – RECONNAISSANCE

3 INTRODUCTION TO RECONNAISSANCE
- 3.1 Goals
- 3.2 General Understanding
- 3.3 Active vs Passive Information Gathering
- 3.4 Web Sources
- 3.5 Social Network
- 3.6 Creative Thinking – Think like the attacker

4 OSINT
- 4.1 Google Hacking And Dorking
- 4.2 Site Mapping
- 4.3 Maltego Framework Environment
- 4.4 General Relevant Information
- 4.5 Social Networking
- 4.6 Shodan
  - Data filtering
  - Scanning range for vulnerable servers
  - Finding Default Servers/Cams/Devices
- 4.7 DNS Interrogation
- 4.8 Whois Interrogation
  - IP Assignments With ARIN
  - Client
  - Methodology
- 4.9 Other Online Research
- 4.10 WhatCMS
- 4.11 Custom Tools Development
- 4.12 Organization general Information
- 4.13 Targeting Attacks
- 4.14 Public Sources
- 4.15 Searching for Metadata
- 4.16 Geolocation / Emails / Employees / Jobs
- 4.17 Foca

CHAPTER C – NETWORK ATTACKS & PENETRATION

5 TRAFFIC ANALYSIS
- 5.1 Subject Introduction
- 5.2 Recommended Tools

6 TCP DUMP
- 6.1 Basic Usage
- 6.2 Working with filters
- 6.3 Analyzing PCAP Files

7 WIRESHARK
- 7.1 Introduction
- 7.2 Following Streams
- 7.3 Analyzing Data
- 7.4 Mining And Picking
- 7.5 Packet Structure
- 7.6 Analyzing real world Attack

8 TRAFFIC INTERCEPTION AND MANIPULATION
- 8.1 Subject Introduction
- 8.2 Open Source Tools on the Trade
- 8.3 Bettercap
- 8.4 Building MITM Attack from scratch
- 8.5 Building ARP Reply Packets
- 8.6 Scripting File2Cable
- 8.7 Forging Packets
- 8.8 BeEF
- 8.9 MITM Framework
- 8.10 MITM Attacks
  - ARP Poisoning
  - ICMP redirection
  - DHPC spoofing
  - IPv6 DHCP Broadcast
  - SSLStrip
  - SSL Vania

9 PASSWORD ATTACKS
- 9.1 Online Brute Forcing Attacks
- 9.2 Hydra + Hydra GTK
  - Using Hydra
  - CISCO Router / Switch Bruteforce
  - SMB Password Bruteforce
  - FTP Password Bruteforce
  - POP3 Password Bruteforce
  - HTTP Over SSL Bruteforce
- 9.3 Offline Attacks
- 9.4 Password Dumping
- 9.5 HashCat
- 9.6 Physical Access

9.7 NetCat
- Port Scanning With NetCat
- Port Forwarding With NetCat
- Backdoor (Bind Shell)
- Backdoor (Reverse Shell)
- Transferring Files With NetCat
- Using NetCat As a Honeypot
- Crypted Cats

9.8 PS Executable
9.9 BITS – Background Intelligent Transfer Protocol
9.10 Traffic Manipulation and Spoofing
9.11 Scappy
9.12 DNS Crafting
9.13 DHCP Crafting
9.14 Packet Forging
9.15 Open Source

CHAPTER D – EXPLOITATION

10 INTRODUCTION
10.1 What Is Exploitation
10.2 Types Of Exploitation
10.3 0 Days

11 BUFFER OVER FLOWS
11.1 Introduction
11.2 Finding Bugs
11.3 Case Studies
11.4 Verifying The Overflow In The STOR
11.5 Which Bytes Overwritten EIP
11.6 Diving Deeper
11.7 Shell Codes

12 METASPLOIT FRAMEWORK
12.1 MSF Console
12.2 MSF Web
12.3 MSF CLI
12.4 Meterpreter
12.5 Meterpreter Commands
12.6 Payloads
- Windows
- Linux
- Mobile

12.7 Auxillary
- Protocol Discovery
- Service Identification
- Server Modules

12.8 Modules
12.9 Exploits - Windows
12.10 Exploits - Linux
12.11 Exploits - Android/iOS
12.12 Write An Example In Python

13 ENUMERATION
13.1 SMTP Enumeration
13.2 SNTP Enumeration
13.3 NetBIOS Enumeration
13.4 MS Session Management
13.5 Listing Usernames on Windows XP Via Null Session
13.6 VRFY
13.7 EXPN
13.8 Banner Grabbing
13.9 Tracerouting
13.10 Whatweb
13.11 Fierce
13.12 DNS Interrogation
13.13 Reverse DNS Interrogation
13.14 MX/NS Enumeration
13.15 Zone Transferring
13.16 DNS Name Bruteforce
13.17 Port Scanning
- Regular Scan
- Decoy Scanning
- XMAS Scan
- Spoofed Scan
- MAC Spoofing
- Zombie Scan
- SYN Scan
- ACK Scan
- UDP Scan

13.18 OS Fingerprinting
13.19 Service Fingerprinting
13.20 Low Technology Reconnaissance
13.21 Path Determination
13.22 Detection
13.23 Recon-ng / Osint

CHAPTER E – PRIVILEGE ESCALATION

14 PERMISSION LOGIC
14.1 Windows
- Task Scheduler – AT Command
- Windows RPC
- PS Exec Sysinternals
- Local Password Crack

14.2 Linux
- Sudo
- Remote And Local Exploits
- Password & Files
- File Permissions And Attributes
- World Writable Files
- Set UID / SUID / SGID Bits
- Local Password Cracking
- Beef-browser exploitation
- DirtyCow Attack

CHAPTER F – WIRELESS

15 WI-FI

15.1 Introduction
15.2 Chipset compatibility
15.3 Understanding 802.11x
15.4 Introduction to Tools
- airmon-ng
- airodump-ng
- aireplay-ng
- airebase-ng
- kismet

15.5 Cracking Encryptions
- WEP
- WPA
- WPA2
- WPS

15.6 WPS – reaver
15.7 Bypassing MAC filtering
15.8 Rouge Access Point
15.9 Evil Twin Attack
15.10 Netstumbler

CHAPTER G – WEB APPLICATION PENETRATION

16 INTRODUCTION

17 TOOLS

17.1 Firebug
17.2 Tamper Data
17.3 Paros
17.4 WebSCrab
17.5 Dirbuster
17.6 Fuzzers
17.7 Webshag
17.8 W3AF
17.9 Burp

18 WEB ATTACKS

18.1 SQL Queries
18.2 Functions and Stored procedures
18.3 SQL Injection
- Introduction
- Blind
- Error based
- Union based
- Open Source Automated Tools
  - SQLMap
  - SQLNinja
  - Browser Addons

18.4 XSS
- DOM based
- Stored
- Reflected
- CSRF

18.5 Directory listing
18.6 Broken Authentication
18.7 Failure to restrict URLs
18.8 Insecure storage
18.9 Mal-configuration of Permissions
18.10 Changing User-Agent
18.11 File upload
18.12 Probing to find XSS
18.13 Chrome XSS Bypassing
18.14 Looking for XSS in PHP Files
18.15 LFIs
18.16 RFIs
18.17 PHP shell files
18.18 Sessions HiJacking
18.19 Sessions SideJacking
18.20 HTTP poisoning
18.21 Cross-Site Cooking
18.22 Session Fixiation
18.23 Commercial Software
- 18.23.1 Accunetix
- 18.23.2 Shadow Security Scanner

CHAPTER H – MOBILE ATTACK

CHAPTER I – REVERSE ENGINEERING

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.

לכבוד
המכללה לאבטחת מידע וללוחמת מידע
שיא סקיוריטי טכנולוגי'ז בע"מ
רמת-גן – פקס: 03-6122593

נא לרשום אותי לתוכנית הלימודים ברמת גן

קורס Hacking Defined Expert

<u>פרטים אישיים:</u>

שם משפחה _____ שם פרטי _____ ת.ז._____ שנת לידה _____

כתובת פרטית _____.

טל' בבית: _____ טל' נייד_____פקס_____ .

כתובת E –mail _____.

<u>מקום עבודה:</u>

שם החברה_____טל' _____ תפקיד_____.

<u>לתשלום (נא סמן בחירתך):</u>

☐ 400 ₪ - דמי רישום (חובה בכל מקרה) ☐ _____ ₪ - מקדמה (בגובה 10% משכר הלימוד)

☐ שכר לימוד בסך _____₪

☐ מצ"ב שיק מס' _____ע"ס _____ ₪ (ניתן לשלם עד ____תשלומים בהמחאות דחויות)

(את ההמחאות יש לרשום לפקודת שיא סקיוריטי בע"מ)

☐ מצ"ב מכתב התחייבות המעסיק, אם הינך ממומן על ידו. **(1)** יודפס ע"ג נייר לוגו **(2)** בציון מספר ח.פ של החברה, **(3)** לתשלום שוטף + 30 ממועד הפתיחה לכל היותר)

☐ נא לחייב כרטיס אשראי בתוקף עד:

☐ בתשלום אחד ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

☐ ב- _____ תשלומים (עד 18 תשלומים בקרדיט).

☐ ב- _____תשלומים ללא ריבית.

שם בעל הכרטיס _____ ת.ז. בעל הכרטיס _____תא' לידה של בעל הכרטיס _____.

כתובת בעל הכרטיס, המעודכנת בחברת האשראי _____.

טלפון בעל הכרטיס, המעודכן בחב' כרטיסי האשראי _____ .

שם בנק + סניף הבנק בו מנוהל חשבון כרטיס האשראי _____ .

- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכון וSee Security.
- דמי ההרשמה אינם כלולים בשכר הלימוד.
- יש לוודא כי התשלומים יסתיימו עד למועד סיום הקורס.

תאריך: _____ חתימה: _____.

שיא א. סקיוריטי טכנולוגי' בע"מ	ח.פ: 513431403	ספק משהב"ט: 83/168200