CSPT: Cyber security Penetration Tester
לתקיפה ומודיעין (Hacking Defined Expert)

see security colege

יועץ אקדמי: מר אבי ויסמן *

קורס טכניקות תקיפה לבעלי רקע בפיתוח או רקע בתשתיות טכנולוגיות

אודות התוכנית

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.

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: System, Network, Mobile, Web, Application, ועד האדם – Social Engineering.

מאפייני תוכנית הלימודים	
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית/ **טכנית** / יישום
שלב:	מתחילים / **מתקדמים**
רוחב:	ממוקד / **רחב**
עומק:	סוקר / **עמוק**
הסמכות:	**HDE, CEH**
שעות:	**96 שעות**
פתיחה:	**ראה בעמוד הראשי של המכללה**
מתכונת:	**24 מפגשי ערב, כ-3 חודשים**
תרגול בית:	לא קיים / **בהיקף 400 שעות**

מטרת התוכנית

להכשיר אנשי מקצוע לעולם התקיפה האתית, בתחומי תקיפת System, תקיפת Network, תקיפת Mobile, תקיפת יישומי ויישומי Web, ובתחום ה- Reverse Engineering.

על המרצים נמנים מובילי ההאקרים בישראל.

הקורס נחשב נכס צאן ברזל במיטב הגופים העוסקים בנושא תקיפה ויעוץ.

תנאי קבלה

- ידע מעשי בתחום תשתיות, מערכות הפעלה ותקשורת
- ידע בסיסי בפיתוח קוד וכלי אבטחה
- ראיון אישי

תעודה

- קיימת חובת נוכחות ב-80% מהמפגשים, ועמידה במבחנים/עבודות, בציון 70.
- תיעוד: לעומדים בדרישות התכנית תוענק תעודת הסמכה מטעם See Security: **"Hacking Defined Expert"**

הכרה

קורס Hacking Defined Experts הינו המהדורה "השחורה" של תוכנית CEH, וידוע כסטנדרט דה-פקטו בתעשיית הסייבר בישראל. בוגרי התוכנית יכולים לגשת ולהצליח מאוד במבחן CEH.

(ימי שלישי ושישי, תאריכים בעמוד הראשי של המכללה)

לעבוד קשה, להיכנס עמוק אל תוך הלילה, ליהנות מכל רגע של ערנות,
ולעסוק במה שהכי אוהבים...

ז'בוטינסקי 1, בית הדר-די מול קומה 1', רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593
www.see-security.com avi@see-security.com

CSPT: Cyber security Penetration Tester
לתקיפה ומודיעין (Hacking Defined Expert)

see security colege

מתכונת הלימודים

משך התכנית כ- 24 מפגשים. הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח כ- 3 פעמים בשנה.

עלות הלימודים

סך 13,500 ₪ + 400 ₪ דמי רישום. ~~סך 15,000 ₪ + 400 ₪ דמי רישום.~~

הערות

- התוכנית נבנתה לצרכי ידע מעשי.
- התוכנית מוכרת להסמכת Cyber Warfare level-2.
- פתיחת כל תכנית מותנית במספר הנרשמים.
- דמי ההרשמה אינם מוחזרים, אלא במקרה של אי פתיחת התכנית על ידי המכללה.
- דמי ההרשמה ומבחנים חיצוניים כלשהם אינם כלולים בשכר הלימוד.
- ייתכנו שינויים במערך התכנית, במועדי הלימודים והבחינות או בכל נושא אחר. הודעה על כל שינוי תימסר למשתתפים.
- רשימת תת הנושאים, עומקם ורוחבם עשויה להשתנות בהתאם לשליטת התלמידים בחומר.

מידע נוסף

- **מידע מינהלי:** אלוירה אליסייב,03-6122831 , 052-8787889, elvira@see-security.com.
- **יועץ אקדמי:** אבי ויסמן, 054-5222305, avi@see-security.com

Hacking Defined - חווית לימוד שונה
ההסמכה דה-פקטו המוערכת בישראל

:2015 – 2003
עשור של בכורה מקצועית

כאשר מסלול HDE הושק לראשונה, ניתן דגש להרכשת טכניקה, במקום ללימוד כלים קיימים. בתחילת העשור הקודם, בימיהן של מערכות Windows Server ,XP ומערכות ה- Linux של הדור הקודם, היו המערכות חדירות מאוד, שכן יצרניהן השקיעו מאמץ ירוד יחסית בהגנתן. הדור הנוכחי של המערכות מחד, והתפתחות כלי ההגנה ואבטחת המידע, הביאו לכך שהשימוש ב"כלים אוטומטיים לתקיפה" נעשה לא רלבנטי, או "פחות יעיל", לשון המעטה.

ההאקר נדרש להפעלת גישה מולטי-דיסציפלינארית המשלבת ידע ויצירתיות רבה בפעילותו. לכלים אוטומטיים קיימת "חתימה", כשם שלמטוס קיימת "חתימת מכ"ם" ייחודית לדגם שלו. כלי ההגנה של הדור הנוכחי לומדים במהירות את החתימות של הכלים, ולכן – מאפשרים חסימת התקפות המבוצעות באמצעותם.

בתולדות התקיפה הקיברנטית, זכו "מומחי תקיפה" המבוססת רק על הפעלת "ערכות כלים" לכינוי הגנאי "Script Kiddies" או "Skiddies".

קורס Hacking Defined Experts מלמד "כיצד לדוג", ולא "באיזה כלים משתמשים לאכילת דג". הקורס עתיר תרגילים לסביבת הכיתה והבית, ומחייב השקעה כוללת בת 400 שעות לכל הפחות.

גישה זו מחייבת השקעה ריטואלית ויקרה בפיתוח התרגילים, אך הוכיחה עצמה כגישה היחידה לפיתוח "ראש חושב".

מאז הקמת הסדרה, הוכשרו מאות רבות של מומחי תקיפה ומומחי אבטחה, במסגרת קורסי סידרת Hacking Defined.

אינך רשאי להרשם? בדוק גם את תוכנית Ethical Hacking הפתוחה לכל ומיועדת להכנה למבחני CEH בלבד.

פנה אל היועץ להכוונה.

תוכנית הלימודים

CSPT: Cyber security Penetration Tester
לתקיפה ומודיעין (Hacking Defined Expert)

see security colege

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 and On line Tools
- 3.5 Social Engineering Attacks
- 3.6 Social Network stalking
- 3.7 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
- 4.18 Creepy

5 Enumeration
- 5.1 SMTP Enumeration
- 5.2 SNTP Enumeration
- 5.3 NetBIOS Enumeration
- 5.4 MS Session Management
- 5.5 Listing Usernames on Windows XP Via Null Session
- 5.6 VRFY
- 5.7 EXPN
- 5.8 Banner Grabbing
- 5.9 Tracerouting
- 5.10 Whatweb
- 5.11 Fierce
- 5.12 DNS Interrogation
- 5.13 Reverse DNS Interrogation
- 5.14 MX/NS Enumeration
- 5.15 Zone Transferring
- 5.16 DNS Name Bruteforce
- 5.17 Port Scanning
  - Regular Scan
  - Decoy Scanning
  - XMAS Scan
  - Spoofed Scan
  - MAC Spoofing
  - Zombie Scan
  - SYN Scan
  - ACK Scan
  - UDP Scan
- 5.18 OS Fingerprinting
- 5.19 Service Fingerprinting
- 5.20 Load Balancer De-Multiplexing
- 5.21 Low Technology Reconnaissance
- 5.22 Path Determination
- 5.23 IDS / IPS Detection
- 5.24 Recon-ng / Osint

Chapter C – Network Attacks & Penetration

6 Traffic Analysis
- 6.1 Subject Introduction
- 6.2 Recommended Tools

7 TCP Dump
- 7.1 Basic Usage
- 7.2 Working with filters
- 7.3 Analyzing PCAP Files

8 Wireshark
- 8.1 Introduction
- 8.2 Following Streams
- 8.3 Analyzing Data
- 8.4 Mining And Picking
- 8.5 Packet Structure
- 8.6 VOIP Building
- 8.7 Analyzing real world Attack

9 Traffic Interception and Manipulation
- 9.1 Subject Introduction
- 9.2 Open Source Tools on the Trade
- 9.3 From Cain to Bettercap
- 9.4 Building MITM Attack from scratch
- 9.5 Building ARP Reply Packets
- 9.6 Scripting File2Cable
- 9.7 Forging Packets
- 9.8 BeEF
- 9.9 MITM Framework
- 9.10 MITM Attacks
  - ARP Poisoning
  - ICMP redirection
  - DHPC spoofing
  - IPv6 DHCP Broadcast
  - Ettercap Manipulation
  - Scripting For Ettercap
  - SSLStrip
  - SSL Vania

ז'בוטינסקי 1, בית הדר-די מול קומה 1', רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593
www.see-security.com avi@see-security.com

10 Password Attacks
- 10.1 Online Brute Forcing Attacks
- 10.2 Hydra + Hydra GTK
  - Using Hydra
  - CISCO Router / Switch Bruteforce
  - SMB Password Bruteforce
  - FTP Password Bruteforce
  - POP3 Password Bruteforce
  - HTTP Over SSL Bruteforce
- 10.3 Offline Attacks
- 10.4 Password Dumping
- 10.5 HashCat
- 10.6 Physical Access
- 10.7 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
- 10.8 PS Executable
- 10.9 BITS – Background Intelligent Transfer Protocol
- 10.10 Traffic Manipulation and Spoofing
- 10.11 Scappy
- 10.12 Etterfilter
- 10.13 DNS Crafting
- 10.14 DHCP Crafting
- 10.15 Packet Forging
- 10.16 Open Source

Chapter D – Reverse Engineering

11 Introduction
- 11.1 What is reverse engineering
- 11.2 Static analysis
- 11.3 Dynamic Analysis
- 11.4 Reverse Engineering Tools
  - How to PMP in RE
  - IDA
  - ollyDebug
  - WinDBG
  - Cheat Engine
  - IA-32 Instruction Set
  - File formats

12 The Actual Deal
- 12.1 Reversing Introduction
- 12.2 How does Reversing Works
- 12.3 Assembly Basics
- 12.4 Registers and Flags
- 12.5 Process Memory Structure
- 12.6 Stack Section
- 12.7 Data Section
- 12.8 Code Section
- 12.9 Syntax And Instructions
- 12.10 Prologue
- 12.11 Memory Overwrite
- 12.12 Free after use
- 12.13 Infinite Loops
- 12.14 Searching for Strings
- 12.15 Bypassing Restrictions

Chapter E – Exploitation

13 Introduction
- 13.1 What Is Exploitation
- 13.2 Types Of Exploitation
- 13.3 0 Days

14 Buffer over Flows
- 14.1 Introduction
- 14.2 Finding Bugs
- 14.3 Case Studies
- 14.4 Verifying The Overflow In The STOR
- 14.5 Which Bytes Overwritten EIP
- 14.6 Diving Deeper
- 14.7 Shell Codes

15 Metasploit Framework
- 15.1 MSF Console
- 15.2 MSF Web
- 15.3 MSF CLI
- 15.4 Meterpreter
- 15.5 Meterpreter Commands
- 15.6 Payloads
  - Windows
  - Linux
  - Mobile
- 15.7 Auxillary
  - Protocol Discovery
  - Service Identification
  - Server Modules
- 15.8 Modules
- 15.9 Exploits - Windows
- 15.10 Exploits - Linux
- 15.11 Exploits - Android/iOS
- 15.12 Write An Example In Python

Chapter F – 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 Fixation
18.23 Commercial Software
- 18.23.1 Accunetix
- 18.23.2 Shadow Security Scanner

Chapter G – Wireless

19 Wi-Fi

19.1 Introduction
19.2 Chipset compatibility
19.3 Understanding 802.11x
19.4 Introduction to Tools
- airmon-ng
- airodump-ng
- aireplay-ng
- airebase-ng
- kismet

19.5 Cracking Encryptions
- WEP
- WPA
- WPA2
- WPS

19.6 WPS – reaver
19.7 Bypassing MAC filtering
19.8 Rouge Access Point
19.9 Evil Twin Attack
19.10 Netstumbler

Chapter H – Privilege Escalation

20 Permission Logic

20.1 Windows
- Task Scheduler – AT Command
- Windows RPC
- PS Exec Sysinternals
- Local Password Crack

20.2 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 I– Virology

21 Introduction

22 Types and Classes

22.1 Trojan Horse
22.2 Malware Today
22.3 Viruses Types

23 Malware features
- Physical Keyloggers
- Software Keyloggers
- Rubber Ducky
- Root Kits
- Memory Based RootKit
- User Mode Root Kit
- Kernel Mode RootKit
- BIOS Root Kit
- Root Kit In Action: HXDEF

23.1 Windows Quirks
- Registry Bugs
- NTFS Alternate Data Stream

23.2 Anti-Virus Avoidance
23.3 Case Studies
- Stuxnet
- Flame
- Confiker
- Storm
- Packers
- Binders

24 Port Tunneling and Proxing

24.1 Reverse tunneling
24.2 Bind tunnel
24.3 Port Forwarding
24.4 Web Proxy
24.5 SOCK4/5
24.6 Proxy Tunneling
24.7 Proxy Chaining

הצהרת תלמיד בלימודי HDE

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

שם הנרשם: _____ תאריך: _____ חתימה _____

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

נא לרשום אותי לתוכנית הלימודים ברמת גן

קורס Hacking Defined Expert

פרטים אישיים:

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

כתובת פרטית _____.

טל' בבית: _____ טל' נייד _____ פקס _____.

כתובת E –mail _____.

מקום עבודה:

שם החברה _____ טל' _____ תפקיד _____.

לתשלום (נא סמן בחירתך):

☐ 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