קורס Hacking Defined Experts
לתקיפה ומודיעין

יועץ אקדמי: מר אבי ויסמן *

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 יישומים ויישומי Web, ובתחום ה- Reverse Engineering.

על המרצים נמנים מובילי ההאקרים בישראל.

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

קהל יעד

הקורס מיועד לבעלי ידע מעשי בתחום התשתיות (מערכות הפעלה ותקשורת, ורצוי ידע בסיסי בכלי אבטחה בסיסיים ורצוי ידע בסיסי בפיתוח קוד) וכן בוגרי תואר ראשון או שני במדעי המחשב, הנדסת תוכנה\חומרה.

המסלול איננו מתאים למתחילים. מתחיל? פנה אל היועץ לקבל הכוונה לצורך התפתחות אישית לתחום זה.

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.

קורס טכניקות תקיפה לבעלי רקע בפיתוח או רקע בתשתיות טכנולוגיות

(ימי שלישי ושישי, תאריכים בעמוד הראשי של המכללה)

קורס Hacking Defined Experts
לתקיפה ומודיעין

see security colege

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

מתכונת הלימודים

משך התכנית כ- 24 מפגשים (ימים שלישי 17:30 עד 21:00 ושישי 09:00 עד 12:30). 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 ביה"ס.
- 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

תוכנית הלימודים

2003 – 2015:
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 2000 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.

Chapter A – Introduction

1 Introduction to Hacking
- 1.1 Methodology
- 1.2 Full Disclosure
- 1.3 Ethics
- 1.4 Hacking & the Law

2 Python for Penetration Testers
- 2.1 Working with Files
- 2.2 Sockets Handling
- 2.3 Web Client / Server
- 2.4 Parsing Web Sites
- 2.5 Web Brute Force Attack

3 Linux
- 3.1 Basic Commands
- 3.2 Users & Groups
- 3.3 Permissions
- 3.4 Working with terminal
- 3.5 Compile & Execute
- 3.6 full disk encryption
- 3.7 Build Linux from scratch - Gentoo
- 3.8 Bash Scripting

Chapter B – Reconnaissance

4 Introduction to Reconnaissance
- 4.1 Goals
- 4.2 General Understanding
- 4.3 Active vs Passive Information Gathering
- 4.4 Web Sources and On line Tools
- 4.5 Social Engineering Attacks
- 4.6 Social Network stalking
- 4.7 Creative Thinking – Think like the attacker

5 OSINT
- 5.1 Google Hacking And Dorking
- 5.2 Site Mapping
- 5.3 Maltego Framework Environment
- 5.4 General Relevant Information
- 5.5 Social Networking
- 5.6 Shodan
  - Data filtering
  - Scanning range for vulnerable servers
  - Finding Default Servers/Cams/Devices
- 5.7 DNS Interrogation
- 5.8 Whois Interrogation
  - IP Assignments With ARIN
  - Client
  - Methodology
- 5.9 Other Online Research
- 5.10 WhatCMS
- 5.11 Custom Tools Development

6 Organization Details
- 6.1 Organization general Information
- 6.2 Targeting Attacks
- 6.3 Public Sources
- 6.4 Searching for Metadata
- 6.5 Geolocation / Emails / Employees / Jobs
- 6.6 Foca
- 6.7 Creepy

7 Enumeration
- 7.1 SMTP Enumeration
- 7.2 SNTP Enumeration
- 7.3 NetBIOS Enumeration
- 7.4 MS Session Management
- 7.5 Listing Usernames on Windows XP Via Null Session
- 7.6 VRFY
- 7.7 EXPN
- 7.8 Banner Grabbing
- 7.9 Tracerouting
- 7.10 Whatweb
- 7.11 Fierce
- 7.12 DNS Interrogation
- 7.13 Reverse DNS Interrogation
- 7.14 MX/NS Enumeration
- 7.15 Zone Transferring
- 7.16 DNS Name Bruteforce
- 7.17 Port Scanning
  - Regular Scan
  - Decoy Scanning
  - XMAS Scan
  - Spoofed Scan
  - MAC Spoofing
  - Zombie Scan
  - SYN Scan
  - ACK Scan
  - UDP Scan
- 7.18 OS Fingerprinting
- 7.19 Service Fingerprinting
- 7.20 Load Balancer De-Multiplexing
- 7.21 Low Technology Reconnaissance
- 7.22 Path Determination
- 7.23 IDS / IPS Detection
- 7.24 Recon-ng / Osint

see security technologies ltd
InfoSec & Cyber Warfare College

Chapter C – Network Attacks & Penetration

8 Traffic Analysis
- 8.1 Subject Introduction
- 8.2 Recommended Tools

9 TCP Dump
- 9.1 Basic Usage
- 9.2 Working with filters
- 9.3 Analyzing PCAP Files

10 Wireshark
- 10.1 Introduction
- 10.2 Following Streams
- 10.3 Analyzing Data
- 10.4 Mining And Picking
- 10.5 Packet Structure
- 10.6 VOIP Building
- 10.7 Analyzing real world Attack

11 Traffic Interception and Manipulation
- 11.1 Subject Introduction
- 11.2 Open Source Tools on the Trade
- 11.3 From Cain to Bettercap
- 11.4 Building MITM Attack from scratch
- 11.5 Building ARP Reply Packets
- 11.6 Scripting File2Cable
- 11.7 Forging Packets
- 11.8 BeEF
- 11.9 MITM Framework
- 11.10 MITM Attacks
  - ARP Poisoning
  - ICMP redirection
  - DHPC spoofing
  - IPv6 DHCP Broadcast
  - Ettercap Manipulation
  - Scripting For Ettercap
  - SSLStrip
  - SSL Vania

12 Password Attacks
- 12.1 Online Brute Forcing

Attacks
12.2 Hydra + Hydra GTK
- Using Hydra
- CISCO Router / Switch Bruteforce
- SMB Password Bruteforce
- FTP Password Bruteforce
- POP3 Password Bruteforce
- HTTP Over SSL Bruteforce

12.3 Offline Attacks
12.4 Password Dumping
12.5 HashCat
12.6 Physical Access
12.7 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

13 RPC Enumeration
13.1 Open Source tools

14 PS Executable

15 VNC

16 BITS – Background Intelligent Transfer Protocol

17 Traffic Manipulation and Spoofing
17.1 Scappy
17.2 Etterfilter
17.3 DNS Crafting
17.4 DHCP Crafting
17.5 Packet Forging
17.6 Open Source

Chapter D – Wireless

18 Wi-Fi
18.1 Introduction
18.2 Chipset compatibility
18.3 Understanding 802.11x
18.4 Introduction to Tools
- airmon-ng
- airodump-ng
- aireplay-ng
- airebase-ng
- kismet

18.5 Cracking Encryptions
- WEP
- WPA
- WPA2
- WPS

18.6 WPS – reaver
18.7 Bypassing MAC filtering
18.8 Rouge Access Point
18.9 Evil Twin Attack
18.10 Netstumbler

19 RFID
19.1 Understanding RFID
19.2 Communication via RFID
19.3 Cracking and maintaining

20 Bluetooth
20.1 Enumeration
20.2 Basic tools
20.3 Bypassing security codes
20.4 False associations and connections

Chapter E – Web Application Penetration

21 Introduction

22 Tools
22.1 Firebug
22.2 Tamper Data
22.3 Paros
22.4 WebSCrab
22.5 Dirbuster
22.6 Fuzzers
22.7 Webshag
22.8 W3AF
22.9 Burp

23 Web Attacks
23.1 SQL Queries
23.2 Functions and Stored procedures
23.3 SQL Injection
- Introduction
- Blind
- Error based
- Union based
- Open Source Automated Tools
  - SQLMap
  - SQLNinja
  - Browser Addons

23.4 XSS
- DOM based
- Stored
- Reflected
- CSRF

23.5 Directory listing
23.6 Broken Authentication
23.7 Failure to restrict URLs
23.8 Insecure storage
23.9 Mal-configuration of Permissions
23.10 Changing User-Agent
23.11 File upload
23.12 Probing to find XSS
23.13 Chrome XSS Bypassing
23.14 Looking for XSS in PHP Files
23.15 LFIs
23.16 RFIs
23.17 PHP shell files
23.18 Sessions HiJacking
23.19 Sessions SideJacking
23.20 HTTP poisoning
23.21 Cross-Site Cooking
23.22 Session Fixation
23.23 Commercial Software
- 23.23.1 Accunetix
- 23.23.2 Shadow Security Scanner

Chapter F – Exploitation

24 Introduction
24.1 What Is Exploitation
24.2 Types Of Exploitation
24.3 0 Days

25 Buffer over Flows
25.1 Introduction
25.2 Finding Bugs
25.3 Case Studies
25.4 Verifying The Overflow
In The STOR
25.5 Which Bytes Overwritten EIP
25.6 Diving Deeper
25.7 Shell Codes

26 Metasploit Framework

26.1 MSF Console
26.2 MSF Web
26.3 MSF CLI
26.4 Meterpreter
26.5 Meterpreter Commands
26.6 Payloads
- Windows
- Linux
- Mobile

26.7 Auxillary
- Protocol Discovery
- Service Identification
- Server Modules

26.8 Modules
26.9 Exploits - Windows
26.10 Exploits - Linux
26.11 Exploits - Android/iOS
26.12 Write An Example In Python

Chapter G – Privilege Escalation

27 Permission Logic

27.1 Windows
- Task Scheduler – AT Command
- Windows RPC
- PS Exec Sysinternals

27.1.1 Local Password Crack

27.2 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 H – Reverse Engineering

28 Introduction

28.1 What is reverse engineering
28.2 Static analysis
28.3 Dynamic Analysis
28.4 Reverse Engineering Tools
- How to PMP in RE
- IDA
- ollyDebug
- WinDBG
- Cheat Engine
- IA-32 Instruction Set
- File formats

29 The Actual Deal

29.1 Reversing Introduction
29.2 How does Reversing Works
29.3 Assembly Basics
29.4 Registers and Flags
29.5 Process Memory Structure
29.6 Stack Section
29.7 Data Section
29.8 Code Section
29.9 Syntax And Instructions
29.10 Prologue
29.11 Memory Overwrite
29.12 Free after use
29.13 Infinite Loops
29.14 Searching for Strings
29.15 Bypassing Restrictions

Chapter I– Virology

30 Introduction

31 Types and Classes

31.1 Trojan Horse
31.2 Malware Today
31.3 Viruses Types

32 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

32.1 Windows Quirks
- Registry Bugs
- NTFS Alternate Data Stream

32.2 Anti-Virus Avoidance
32.3 Case Studies
- Stuxnet
- Flame
- Confiker
- Storm
- Packers
- Binders

33 Port Tunneling and Proxing

33.1 Reverse tunneling
33.2 Bind tunnel
33.3 Port Forwarding
33.4 Web Proxy
33.5 SOCK4/5
33.6 Proxy Tunneling
33.7 Proxy Chaining

see security technologies ltd
Cyber Warfare College

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

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 ו See 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