קורס Hacking Defined Advanced

מחזור מס' 32

יועץ אקדמי: מר אבי ויסמן *

קורס טכניקות תקיפה לבעלי רקע ברשתות או בפיתוח

פתיחת קורס בתל-אביב: ~~19 במאי 2011, יומיים בשבוע (בוקר)~~

* יו"ר הפורום הישראלי לאבטחת מידע IFIS ומנכ"ל המכללה לאבטחת מידע ולוחמת מידע See Security

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 – מהחשובים מבין חמשת עולמות אבטחת המידע, מיועד לבעלי כשרון טכני ויצירתיות.

מטרת התכנית

להכשיר אנשי מקצוע בתחום אבטחת המידע לצורך התמודדות עם תוקפים בתחומי תקיפת System, תקיפת Network, תקיפת Mobile, תקיפת יישומים ויישומי Web.

על המרצים נמנים מובילי ההאקרים בישראל.

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

משפחת קורסי Hacking Defined נוסדה ב- 2003.

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

אחדים מהקורסים מיועדים למומחי אבטחת מידע, ואחרים – לתקיפה אתית.

פנה אל היועץ להכוונה.

קהל היעד

בעלי ידע מעשי בתחום התשתיות (מערכות הפעלה ותקשורת) וכן בוגרי תואר ראשון או שני במדעי המחשב, הנדסת תוכנה\חומרה, עם עדיפות לבעלי יכולת פיתוח קוד.

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

תנאי הקבלה

- מיועד לבעלי רקע קודם בניהול רשתות Windows או Linux או באבטחת מידע או בפיתוח תכנה. נדרשת הכרת Windows, Linux, TCP/IP, Web ושירותים כגון:, DNS, FTP, TELNET, SMTP, HTTP.
- נכונות לעבודה עצמית מונחית רבת היקף (כ- 400 שעות לימוד ביתי).
- ראיון אישי.

מתכונת הלימודים

משך התכנית כ- 60 שעות, במתכונת של לימודי ערב (17:30 עד 21:00), פעמיים בשבוע במסגרת 15 מפגשים. הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח כ- 3 פעמים בשנה.

עלות התכנית

סך 10,000 ₪ + 400 ₪ דמי רישום.

זכאות לתעודה

- קיימת חובת נוכחות ב-80% מהמפגשים, ועמידה במבחנים/עבודות, בציון 70.

4 Maale' Hshachar St. Ramat-Gan 52383, Israel. Tel: +(972)-3-6122831, Fax: +(972)-3-6122593
avi@see-security.com http://www.see-security.com

- לעומדים בדרישות התכנית תוענק תעודת הסמכה מטעם See Security:
  "Hacking Defined Advanced"
- התוכנית נבנתה לצרכי **ידע מעשי**.

ה ע ר ו ת :

- 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.
- המכללה מביאה לידיעת הנרשמים והתלמידים כי ייתכנו שינויים במערך התכנית, במועדי הלימודים והבחינות או בכל נושא אחר. הודעה על כל שינוי תימסר למשתתפים.

לכל מידע נוסף או לתיאום ראיון אישי או פגישת יעוץ:

מידע מינהלי: אלוירה אליסייב, 03-6122831, 052-8787889, elvira@see-security.com

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

סילבוס מקוצר

Chapter A - Introduction

1. General Introduction to Hacking Defined Course
2. Hacking Today
3. Hacking History
4. Hacking Terminology
5. Hackers Status
6. Characteristics of Attackers
7. Ethical Hacking
8. Attackers thinking

Chapter B - Course Tool Kit

9. BackTrack
   - BackTrack Basic Commands
   - BackTrack Networking
     - Automatic Configuration DHCP
   - BackTrack Services
10. Development Environments
11. Visual Studio
12. Python
13. Perl

Chapter C - Reconnaissance

14. Reconnaissance - General
    - Goals
      - Real World Scenario
      - Real World Scenario - Example
    - Low Technology Reconnaissance
      - Methods for low technology Reconnaissance
      - Gathering relevant target information
      - Network enumeration
15. Social Engineering Reconnaissance
    - Organization Details
    - Social Engineering Handles
16. Phishing
    - Socially aware attacks
    - Context-aware attacks
17. Web-based Reconnaissance
    - Whois Interrogation
      - IP address assignments through ARIN
      - Clients
      - Whois enumeration methodology
      - Whois Exercise
    - WotWeb
      - Installation
    - Google Enumeration / Hacks
      - Google / Web Based Reconnaissance Exercise
    - Other Online Reconnaissance Resources
18. Network Reconnaissance
    - Enumeration Services
      - DNS Interrogation
      - Nslookup
      - MX/NS enumeration
      - Reverse DNS enumeration
      - Zone Transfers
      - Zone Transfer Example

- DNS Name Bruteforce
- CDNS Enumeration Exercises
- SNMP Enumeration
  - SNSCAN
  - SNMPEnum
  - SNMP Enumeration Exercises
- SMTP Enumeration
  - VRFY
  - EXPN
  - SMTP Enumeration Exercises
- Netbios Enumeration
  - Null Sessions
  - SamSpade
  - MS Session Management
  - Listing usernames via a null session on Windows XP
  - Netbios Enumeration Exercises
- Trace-routing
- Countermeasures and defenses
- Banner grabbing
  - Banner Grabbing Examples
- Port Scanning
- NMAP Scanner
  - Port Scanning Exercises
  - Fingerprinting OS
  - Load balancer demultiplexing

19. Application Reconnaissance
- Application dependesies
  - .net Framework
  - java
  - scripts (py,perl, etc..)
  - cygwin
- Processes
  - find app process, service, executable
  - find app registry entries

Chapter D - System Penetration

20. Windows
- Windows XP
  - Manipulating Remote Services
  - local privileges escalation basics
  - local password cracking
  - coldboot attack

21. Linux
- ubuntu
  - Manipulating Remote Services
  - local privileges escalation basics

Chapter E - Network Penetration

22. Getting Interactive
- Netcat
  - Port Scanning With NetCat
  - Banner Grabbing With NetCat
  - NetCat as a BackDoor (Connect / Bind Shell)
  - NetCat as a Reverse Back Door (Reverse Shell)
  - Transferring Files using NetCat
  - NetCat as a mini Honey pot
  - Netcat Exercises
- RPC Enumeration and remote code execution
  - PSExec
  - PSExec Usage
  - PSExec Advanced Usage
  - PSExec Exercise
- Other Remote Control Techniques
  - Dameware
  - VNC
  - Radmin
- Transferring Files
  - TFTP
  - FTP
  - Interactive Shell vs. Non Interactive Shell
  - Inline File Transfer
  - BITS – Background Intelligent Transfer Service

23. Traffic Interception and Analysis
- Capturing Packets
  - WireShark (Ethereal)
  - Analyzing Traffic Exercise
- Additional Sniffers
  - TCPDump
  - Commview

24. Traffic Interception and Manipulation
- Building your own Packets
- ARP spoofing
  - ARP Spoofing MITM Attacks
  - ARP Spoofing - MITM the Hard Way
- Advanced MITM - the Easy Way
  - Ettercap

25. DOS / DDOS
- Methods of attack
- Nuke Attacks
- Buffer Overflows DOS
- Flooding the target
- SYN Floods
- Smurf Attacks
- Banana Attack
- Flood Attacks
- Effects of DoS
- DDOS – Exercise

26. Password Attacks
- Password Brute force Attacks (online)
- Hydra
  - Using Hydra
  - Cisco Router / Switch Brute force
  - SMB Password Brute force
  - FTP Password Brute force
  - POP3 Password Brute force
  - htpasswd over SSL Password Brute force:
  - Password Attacks (online) – Exercise
- Password Brute force Attacks (offline)

- Password Dumping
- Physical Access

27. Vulnerability Scanners
    - Command Line Vulnerability Scanners
    - Shadow Security Scanner
    - Nessus Vulnerability Scanner
    - Accunetix Vulnerability Scanner
    - Core Impact

Chapter F - Wireless & Mobile Penetration

28. Wireless Hacking
    - Netstumbler / EEYE Wireless Scanner
    - Kismet
    - Cracking WEP
    - Overcoming MAC Address Restrictions
    - Cracking WPA
    - Cracking WPA – II
29. Mobile Hacking
    - Bluetooth
    - Smartphones

Chapter G - Web Applications Penetration

30. Web Applications
31. Introduction
32. Web Based Vulnerabilities
    - OWASP Top 10 Application Security Risks - 2010
33. Java Script
34. TOOLS
    - FIREBUG
    - PAROS
    - WEBSCRAB
    - TAMPER DATA
    - DirBuster
35. SQL
    - Injection
36. XSS Cross-Site Scripting
37. CSRF
38. Broken Authentication and Session Management
39. Insecure Direct Object References
40. Failure to Restrict URL Access
41. Security Misconfiguration
42. Insecure Cryptographic Storage
43. Insufficient Transport Layer Protection
44. Unvalidated Redirects and Forwards
45. User Agent
46. Different User Agent
47. Directory Listing
48. Directory Traversal
49. File Upload Vulnerability
50. PHP Shell Files
51. Remote File Inclusion Vulnerability
52. Regular Expressions
    - Attacking Web Sessions
    - Session Hijacking
    - Session Sidejacking
    - Session Fixation
    - Cross-Site Cooking
    - Session Hijacking
    - Session Hijacking - Protection
53. HTTP Poisoning

Chapter H - Vulnerability World

54. Buffer Overflows
55. MetaSploit
56. Client Side Attacks
57. WMF Client Side

Chapter I - Virology & House Keeping

58. Thinking Security
59. Key Loggers
60. Native Backdoors
61. Trojan horse Attacks
62. What is Trojan horse?Installing Services
63. Windows QuirksAnti Virus Avoidance
64. Root kitsNTFS Alternate Data Streams

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

נא לרשום אותי לתוכנית הלימודים ברמת גן

קורס Hacking Defined Advanced

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 כרט☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

☐ 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:_____.

4 Maale' Hshachar St. Ramat-Gan 52383, Israel. Tel: +(972)-3-6122831, Fax: +(972)-3-6122593
avi@see-security.com http://www.see-security.com