

קורס Exploit Writing (for level-3)

המכללה לאבטחת מידע ולוחמת מידע See Security מזמינה אותך להשתתף בקורס Exploit Writing המיועד למתקדמים בלוחמת סייבר.

מחזור ראשון מתקיים בתאריכים 8 עד 12 באפריל 2012
(5 ימי לימוד משעה 09:00 עד 16:00), ברמת-גן.

מבוא

קורס Exploit Writing הינו "השלב הבא" עבור מומחי תקיפה המצוידים בידע אודות שיטות התקפה, וביכולת פיתוח. הקורס נבנה בעיקרו עבור מערכת הבטחון באמצעות בוגרי מערכת הבטחון העוסקים בפיתוח "נוצלות", ונועד לחשוף את הסטודנטים למונחים ולשיטות מתקדמות בלוחמת מידע, באמצעות מרצים אשר פעילים בתחום זה, מהבכירים בענף.

קורס זה נועד לספק למומחי תקיפה ובודקי חדירות רמה חדשה של יכולות, ולהכשירם לפתח בעצמם את כליהם, במקום כלים נפוצים שנבנו בידי אחרים.

תחום תקיפת Cyber (או לוחמת מידע או לוחמה קיברנטית) הינו מן התחומים הטכנולוגיים המרתקים בעולם אבטחת המידע וה-Cyber Warfare.

מטרת התכנית

לספק יכולת לפיתוח עצמי של exploits למטרות מקצועיות.

קהל היעד

בעלי רקע בתחומי ה-Penetration Testing, ניסיון בפיתוח קוד, ורקע בסיסי ב-Debugging, בסביבת לוחמת מידע, Cyber, מודיעין.

* הקורס אינו פתוח לקהל הרחב. כל מועמד יאושר ע"י See Security.

מתכונת הלימודים

משך התכנית כ- 40 שעות אקדמיות, במתכונת של לימודי יום (09:00 עד 16:00).

זכאות לתעודה

- ° קיימת חובת נוכחות ב-80% מהמפגשים, ועמידה במבחן סיום, בציון 70 לפחות.
- ° תיעוד: בוגרי הקורס אשר יעמדו במבחן הסיום בציון 70 לכל הפחות, יזכו מטעם מכללת See Security ו-Cyberia בתעודת בוגר קורס:

Exploit Writing: level-3

Cyber Warfare & Cyber Crime

עלות התכנית (למחזור דצמבר 2011)

עלות למשתתף: 8,800 ש"ח (כולל מע"מ). ניתן להירשם עד 15 במרץ 2011.

הזמנות, אל שיא סקיריטי טכנולוג'ז בע"מ: ספק משרד הבטחון: 83/168200, ח.פ: 513431403, לכתובת: מעלה השחר 4, רמת-גן – 52383. טלפון: 03-6122831, פקס: 03-6122593.



הערות:

- 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.
- רשימת תת הנושאים, עומקם ורוחבם עשויה להשתנות בהתאם לשליטת התלמידים בחומר.

לכל מידע נוסף או לתיאום ראיון אישי או פגישת יעוץ:

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

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

תוכנית הלימודים

Day 1:

1. Introduction to exploit writing

- Operating Systems differences
- Windows for Exploit writing
- Linux for Exploit writing
- Setting up an Exploit writing lab

2. Programming Intro

- The ASM language
- Intel ASM syntax
- AT&T ASM syntax
- C language for XW
- Script languages
- Python script language for XW

Day 2:

3. Exploits in the wild

- How to find exploits on the internet

4. Shellcode

- How to write shellcodes
- How to find shellcodes

5. Overflows

- What are overflows?
- Buffer overflows
- Stack overflows in windows
- Stack overflows in linux

6. Debuggers

- Windows debuggers
- Linux debuggers

Day 3:

7. Overflows

- Heap overflows in windows
- Heap overflows in linux
- Format string attacks

8. Fuzzing

- Manual and automated fuzzing
- Fault Injection
- How to build a fuzzer

Day 4:

9. Reverse engineering

- Using IDA
- Reversing a windows application
- .Net applications
- Anti debuggers
- Software cracking

Day 5:

10. Writing real world exploits

- Writing a real buffer overflow exploit
- Writing a real heap overflow exploit
- Writing a real format string exploit
- Conclusive lab

דף רישום ללימודים בעמוד הבא

