IL Hack Institute

See security technologies ltd

קורס Reverse Engineering (for level-3)

המכללה לאבטחת מידע ולוחמת מידע See Security מזמינה אותך להשתתף בקורס Reverse Engineering המיועד למתקדמים בלוחמת סייבר.

מחזור ראשון מתקיים בתאריכים 22 עד 27 באפריל 2012
(5 ימי לימוד משעה 09:00 עד 16:00), ברמת-גן.

מבוא

קורס Reverse Engineering 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.

במקרים רבים של אירועי אבטחת מידע לא יכול צוות התגובה והחקירות להשלים במדויק את תהליך הניתוח, מבלי להבין היטב את התהליך של Runtime. האקרים מתקדמים עושים שימוש בטרויאנים מתוחכמים שאינם מזוהים על ידי אנטי וירוס, ולפיכך – ניתן לזהותם ולפענח את פעולתם רק באמצעות הנדסה לאחור.

כלי הנדסה לאחור משמשים גם כדי לפענח את הקוד המעורבל של ספקי הגנות שונות על תוכנה, ועל-מנת לזהות נקודות תורפה בקוד המפותח על-ידי תכניתני הארגון.

הנדסה לאחור נועדה לאפשר ניתוח מדוקדק של מערכת תוכנה, לשם בנייתה באופן משוער הקרוב ככל הניתן למקור, במטרה למצוא את נקודות התורפה שלה לצורך תקיפתה.

טכניקה זו מנפצת את המיתוס כי קוד בינארי מייצג ערכים הקסדצימליים ולכן הוא לא מובן ובלתי ניתן לשינוי.

קיימות שיטות אחדות של הנדסה לאחור, אך היעילה והנפוצה ביותר, מתבססת על זוית הראייה של מפתחי התוכנה המקורית. ניתוח מסוג זה, מתבסס על העובדה שמפתחים נוהגים לפתח מערכות על-בסיס מתודה קבועה, זרימת חשיבה הגיונית, ובדרך כלל מוכרת וניתנת להבנה על-ידי המנתח, כך שתהליך הניתוח נעשה קל ומובן יותר. אחד ממודלי הנדסה לאחור הנפוצים מכונה "מודל המפל" (Waterfall Model).

בתהליך זה, אשר כולל ניתוח דינמי וסטטי, ניתן, בין השאר, דגש על זיהוי רכיבים ופונקציות שפותחו בשלב מאוחר יותר והתווספו למערכת, שכן הניסיון מלמד שרמת האבטחה של "רכיבים מאוחרים" נמוכה יותר.

ההגנה כנגד הנדסה לאחור נחשבת קשה מאוד, שכן "בהנתן מספיק זמן ומשאבים", כל קוד, יהא מוגן ככל שיהיה, ייכנע בסופו של דבר למשחזרים.

עם זאת, אין הדבר אומר שעל המפתחים להקל על המשחזרים. סדרת צעדי הגנה נדרשת מהמפתחים על מנת להקשות מאוד על מבצעי ההנדסה לאחור. בראש השיטה – ערפול מושגים וערפול של הלוגיקה המובילה את המפתחים.

הנדסה לאחור הינו כלי חיוני של חוקרי פגיעויות (Vulnerability researcher).

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

IL Hack Institute

See security technologies ltd

לספק יכולת לניתוח נוזקות / קוד עוין למטרות מקצועיות.

קהל היעד

בעלי רקע בתחומי הסיסטם ופרוטוקולי תקשורת ורקע בסיסי ב- Debugging, בסביבת לוחמת מידע, Cyber, מודיעין. רקע ב-Penetration Testing , וניסיון בפיתוח קוד מהווים יתרון,

* הקורס איננו 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-IL-Hack בתעודת בוגר קורס:

Reverse Engineering: level-3

Cyber Warfare & Cyber Crime

עלות התכנית (למחזור אפריל 2012)

עלות למשתתף: 11,800 שח (כולל מע"מ). ניתן להירשם עד 15 במרץ 2011.

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

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

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

תוכנית הלימודים בעמוד הבא.

IL Hack Institute

see security technologies ltd

תוכנית הלימודים

Day 1:

1. Introduction to Reverse Engineering

- Operating Systems differences
- Hashing functions
- Encrypted binaries
- Reversing compression types
- Stack overflows
- Heap overflows
- Isolating malware
- Unpacking malware
- Monitoring registry changes
- Identifying communication channels
- Digital Rights Management (DRM) implementations
- Thwarting anti-debugger code
- Debugging multi-threaded programs
- Recursive traversal dissasemblers
- Reversing .NET bytecode
- CREA Review
- Conditional branching statements

Day 2:

- Virtual machines and bytecode
- System vs. Code Level reversing
- Identifying variables
- Compilers and branch prediction
- Memory management
- Win32 executable formats and image
- sections
- IDA configuration, scripts & Plugin architecture
- Windows Kernel & API
- Rootkits types

Day 3:

- WinDBG & kernel Debugging
- Rootkit Reverse Engineering
- Warm Reverse Engineering
- IDA Plugins
- Runtime analysis
- device drivers Reverse Engineering
- kernel malware Analyzing

Day 4:

- PECOFF File Format
- PE Anti-Reverse Engineering techniques
- Packers
- Storm kernel Reverse Engineering
- Process & DLL injection
- VM Based Packers Unpacking
- Obfuscation methods
- physical memory Analyzing
- 64bit packers
- Tracking Program Process Injection
- Unpacking examples

Day 5:

- Remote debugging
- reversing binary protocols
- Botnet Reverse Engineering
- C&C protocol Reverse Engineering
- Identifying common algorithms inside worms
- Linux Malware Reverse Engineering

דף רישום ללימודים בעמוד הבא

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

IL Hack Institute

See security technologies ltd

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 Reverse Engineering

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 ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

☐ 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