קורס Malware Analysis Level I / II

יועץ אקדמי: מר אבי ויסמן, מרצה ראשי: אלכס מרגולין

תוכנית ממוקדת לאוכלוסיות טכנולוגיות, לבעלי רקע עמוק במחשבים

להבנה והכרת כלים וטכניקות זיהוי ופענוח נוזקה.

(תאריכים בעמוד הראשי של המכללה)

מבוא

נוֹזֶקָה (malware / malicious Software) היא תוכנה שמטרתה לחדור או להזיק למחשב ללא ידיעתו של המשתמש בו. הנוזקה בת זמננו הינה מערכת מבוססת תוכנה, לעיתים, מערך מקצועי ומושלם של תת-מערכות המשלימות זו את זו ופעולות יחד על-מנת להצליח במשימתן – הרס או איסוף מודיעין.

תחכומן ומורכבותן אינו מאפשר עוד לכלי הגנה וזיהוי לגלותן בטרם כניסתן, וקשה מאוד לאתרן גם לאחר חדירתן. לכן, מערך הכלים של מומחה ניתוח נוזקה הינו מורכב, מולטי-דיסציפלינרי, מחייב מיומנות רבה והיכרות עם שיטות התקיפה הנפוצות, על-מנת לפענחן, להצליח להסירן ולמנוע התפשטותן.

קורס זה מופיע בשתי מהדורות, קצרה (לא מחייבת שליטה בשפת C, ומורחבת: הרחבת הקורס עבור תכניתני C.

מאפייני תוכנית הלימודים	
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית / **טכנית** / **יישום**
שלב:	מתחילים / **מתקדמים**
רוחב:	**ממוקד** / רחב
עומק:	סוקר / **עמוק**
הסמכות:	Certified Malware Analyst-I/II
שעות:	**64/40 שעות**
פתיחה:	**ראה בעמוד הראשי של המכללה**
מתכונת:	**16/10 מפגשים ערב**
תרגול בית:	לא קיים / **קיים בהיקף 100 שעות**

מטרת התוכנית

קורס ניתוח תוכנות זדוניות Malware Analysis **Level I** מלמד כיצד לעשות שימוש בכלים קיימים. הקורס מיועד לבעלי רקע עשיר במערכות מידע שאינם שולטים בשפת C. הסטודנטים יוכשרו לבצע ניתוח נוזקות באמצעות מבחר כלים וטכניקות מובחרות.

קורס Malware Analysis **Level II** מיועד לשולטים בסביבת C, ורצוי - גם בסביבת אסמבלי כלשהי. מטרתו של קורס מתקדם זה, היא לחשוף את הסטודנט למגוון רחב של פלטפורמות ותרחישים, תוך התמקדות במיומנויות שונות, לרבות הנדסה לאחור, הן לניתוח לחומרה והן לניתוח תוכנה. זאת, בנוסף להכרה של כלים, טכנולוגיות ושיטות ניתוח מסורתיות.

היכולת תירכש מתוך היכרות עם הטכנולוגיות, הטכניקות , והוראות העבודה הנהוגות (Best Practice) בתחומים אלו, יכולת זו תוקנה לתלמיד בתוכנית הלימודים בין השאר, באמצעות הרצאות, התנסויות ותרגול.

קהל יעד

בעלי ידע מתחום תשתיות התקשוב: תקשורת, מערכות ההפעלה, שיטות תקיפה, נוזקות.

הסמכה

לעומדים בדרישות התוכנית, תוענק תעודה מטעם See-Security:

"מומחה ניתוח נוזקה" - "Certified Malware Analyst" Level I / II.

מי שאינם עומדים בדרישות, יהיו זכאים לתעודת השתתפות, ולהשלמת מחויבויותיהם (השתתפות חוזרת / עבודות ומשימות) ללא תשלום, לצורך קבלת ההסמכה.

הכרה

תוכנית הלימודים להכשרת מנתחי Malware, הינה הראשונה מסוגה בישראל, ונבנתה על-בסיס ההחלטות הרשמיות של מטה הסייבר הלאומי מינואר 2015 בנוגע לרשימת מקצועות הליבה באבטחת מידע וסייבר, ולצורך אספקת הביקוש לאנשי המקצוע המאיישים עמדות בקבוצת Incident Response או בחברות המייצרות טכנולוגיות אבטחת מידע.

תובל 30, רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593

www.see-security.com avi@see-security.com

קורס Malware Analysis Level I / II

תנאי קבלה

- Level I: חובה: ידע מתחום תשתיות התקשוב: תקשורת, מערכות ההפעלה, Windows internals, מבנה הזיכרון, תהליכים, ניהול מערכת קבצים במערכת הפעלה, שיטות תקיפה, נוזקות.
- Level II: חובה: ידע כנ"ל, וכן שליטה בשפת C בסביבת low level, וכן רצוי: היכרות עם Assembler, ועם Reverse Engineering.
- נכונות לעבודה עצמית מונחית.

מטלות תוכנית הלימודים

- קיימת חובת נוכחות בכל המפגשים.
- קיימת חובת עמידה בדרישות סיום (עבודה או מבחן).
- בנושאים הטכניים - תרגול (Hands-on) בכיתת מעבדת מחשבים.

מתכונת הלימודים

משך התכנית Level I: כ- 40 שעות, במתכונת של 10 מפגשי ערב (כ- 1.5 חודשים). משך התכנית Level II: כ- 64 שעות, במתכונת של 16 מפגשי ערב (כ- 2 חודשים). הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח פעמיים בשנה.

עלות הלימודים

Level I: סך 9,800 ₪ + 400 ₪ דמי רישום (כולל מע"מ)

Level II: סך 12,800 ₪ + 400 ₪ דמי רישום (כולל מע"מ) (כולל את level-I)

המרצים בתוכנית

על המרצים נמנים מובילי הענף, בהם מומחים מקצועיים המובילים בתחומם.

מידע נוסף

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

עיקרי התוכניות

Level I

• Sys-Internals • Honeypots • Unpackers • Static analysers • Dynamic analysers	• Hook Finders • Plain/Hidden data in formats (steganography, SQLite, etc.) • Network monitoring (PCAP viewers) • Anti-virus and virus total

Level II

• Level I topics, and: • IDC and IDA-python scripts • PE/ELF manipulation • Debugging user and kernel level code • Protocol analysis • Anti-reversing	• Rootkits and kernel-level reverse-engineering • Deciphering network protocols • Hardware inspection and reverse-engineering

קורס Malware Analysis Level I / II

תוכנית הלימודים (מקוצר)

* Only for level I
** Only for level II

- Catching malware
  - Anti-malware software
  - Sys-Internals suite
  - Honeypots and sandboxes – cuckoo
- PE and Packers
  - PE headers and sections
  - Windows process loading and execution
  - PE view and manipulation tools
  - Packer detection
  - Unpacking executable code
- Static analysis
  - Introduction to Assembly
  - Using IDA
  - Finding malicious code
  - Common malware practices
- Automated static analysis**
  - Using IDC scripts
  - Using IDA-python
  - Code exploration
  - Uncovering hidden code
- Dynamic analysis
  - Using ollydbg
  - Using x64dbg
  - Executable manipulation**
- Anti-malware software internals*
  - Signatures approach
  - Heuristic approach
  - Sandboxing
  - Signature generation with Yara
- Volatile malware*
  - Capturing volatile malware
  - Using Volatility to find and extract malicious code
  - Analysis of volatile malware
- Hooks and injection on Windows**
  - User-level API hooks
  - Kernel-level API hooks
  - Code injection into a process
  - DLL injection into a process
- Root-kit detection on Windows**
  - Using WinDBG
  - Using VirtualKD
  - Debugging the Windows kernel
- Linux-based malware
  - ELF format
  - Static analysis for ELF
  - Linux hooks**
  - Linux injection**
- Reverse engineering malware
  - Storage formats
  - Network access patterns
  - Communication protocols
- Anti-reversing methods
  - Obfuscation measures and counter-measures
  - Anti-debugging measures and counter-measures**
  - Other Anti-reversing measures and counter-measures**

הערות לתוכנית הלימודים

א. תוכנית הלימודים מחייבת בהכנת שיעורי בית להשגת יעדי הלימוד.
ב. משימות קריאה מהווים חובה לימודית.
ג. נושאי טכנאות/יישום אבטחת מידע (התקנות ותחזוקה) לא כלולים בתוכנית הלימודים (ראה תוכנית מתחילים)

הערות מינהל

- 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.

תובל 30, רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593
www.see-security.com avi@see-security.com

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 Malware Analysis Level I / II

<u>פרטים אישיים:</u>

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

כתובת פרטית _____.

טל' בבית:_____ טל' נייד_____פקס_____ .

כתובת E –mail _____.

<u>מקום עבודה:</u>

שם החברה_____טל' _____ תפקיד_____.

<u>לתשלום (נא סמן בחירתך):</u>

☐ 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 See Security.
- דמי ההרשמה אינם כלולים בשכר הלימוד.
- יש לוודא כי התשלומים יסתיימו עד למועד סיום הקורס.

תאריך: _____ חתימה:_____.