קורס פרקטיקום לחקירות Forensics

See Security College

יועץ אקדמי: מר אבי ויסמן, מרצה ראשי: אורן אלימלך

תוכנית ממוקדת לאוכלוסיות טכנולוגיות, לבעלי רקע במחשבים להכשרת מומחי חקירות.

מבוא

תוכנית הלימודים "מומחי חקירה", הינה תוכנית אשר נבנתה בישראל בשיתוף גורמים ממלכתיים ביטחוניים ועל-בסיס דרישות מטה הסייבר הלאומי במשרד ראש הממשלה, במטרה להכשיר מומחי Forensics להפעיל ולשלוט באמצעים לפענוח אירועי מחשב, לצורך שחזור ופענוח כשלי תוכנה וחומרה, וכמובן - לצורך מניעתם בעתיד.

סט כלי Forensics נועד לספק אמצעים לפענוח אירועי פשיעת מחשב.

השימוש בכלים מסוג זה מבוצע בדרך כלל במקרים הבאים:

1. במסגרת משפטית – לצורך בחינת מערכות מחשב אשר שימוש את הנאשמים, הנתבעים או את התובעים.
2. לצורך שחזור מידע על-גבי מדיות שניזוקו עקב כשל חומרה או תוכנה.
3. על-מנת להבין את התהליכים המתקיימים במערכת לצורך שיפור ביצועים, או לצורך שחזור תקלה לצורך מניעתה בעתיד.
4. על-מנת להבין את התהליכים המתקיימים במערכת בעת חדירת תוקף, לצורך הבנת ההתקפה ומניעתה בעתיד, או לצורך זיהוי התוקף.

מאפייני תוכנית הלימודים	
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית/ **טכנית** / יישום
שלב:	מתחילים / **מתקדמים**
רוחב:	**ממוקד** / רחב
עומק:	סוקר / **עמוק**
הסמכות:	See Security - Certified **Forensics Professional**
שעות:	**48 שעות**
מתכונת:	12 מפגשי ערב, כ- 1.5 חודשים
תרגול בית:	לא קיים / **קיים**

מטה הסייבר הגדיר את דרישות המקצוע כך: אדם בעל ידע עדכני ויכולת מעשית גבוהה בנושאי תחקור אירועים (Forensics) בעל ידע וכישורים כדלקמן:

1. בסיס ידע כמו של מיישם הגנת סייבר.
2. יכולת שחזור מידע ונתונים.
3. יכולת פענוח אירועים.
4. הכרה בסיסית של Reverse Engineering.
5. יכולת שימור ראייתי.
6. הכרת חקירת זמן אמת לעומת חקירת אקס פוסט.
7. הכרת כלים וטכנולוגיות רלבנטיות.
8. הכרת ההיבט המשפטי.
9. הכרת גופי חקירה רלוונטיים בישראל וסמכויותיהם.
10. כושר לכתיבת דו"ח בדיקה מסכם.

מטרת התוכנית

הכשרת אנשי מקצוע כמומחי Forensics לצורך שליטה והפעלה נכונים של כלי פענוח אירועי מחשב.

קהל יעד

בעלי ידע מעשי בתחום התשתיות (מערכות הפעלה ותקשורת, ורצוי ידע בסיסי בכלי אבטחה בסיסיים) וכן בוגרי תואר ראשון או שני במדעי המחשב, הנדסת תוכנה\חומרה. המסלול לא מתאים למתחילים.

הסמכה

התוכנית נבנתה לצרכי ידע מעשי. לעומדים בדרישות התוכנית, תוענק תעודה מטעם See-Security:

"מוסמך חקירות אירועי מחשב"

."Certified Forensics Professional"

מי שאינם עומדים בדרישות יהיו זכאים לתעודת השתתפות, ולהשלמת מחויבויותיהם (השתתפות חוזרת / עבודות ומשימות) ללא תשלום. בעלי רקע בחקירות מחשב יכולים לגשת למבחני CCFP של (ISC)^2 בכפוף להנחיות הארגון.

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

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

קורס פרקטיקום לחקירות Forensics

הכרה

הסמכות מכללת See Security נעשו סטנדרט דה-פקטו בישראל.

תנאי קבלה

- רקע קודם בניהול רשתות Windows או Linux או באבטחת מידע. התלמיד נדרש להכיר מערכות הפעלה כגון Windows ו-Linux, פרוטוקולי תקשורת ומודל TCP/IP ואת עולם ה-WEB.
- נכונות לעבודה עצמית מונחית (כ- 100 שעות לימוד ביתי).
- ראיון אישי.

מטלות תוכנית הלימודים

- קיימת חובת נוכחות ב-80% מהמפגשים.
- כל מודול נלמד מחייב עמידה במבחן פנימי ו/או בעבודות בציון 70 לפחות (ראה תקנון קורס במכללה).
- בנושאים הטכניים - תרגול (Hands-on) בכיתה (מעבדת מחשבים).

מתכונת הלימודים

משך התכנית כ- 48 שעות, במתכונת של 12 מפגשי ערב (כ- 2 חודשים). הלימודים מתקיימים בקמפוס See Security ברמת-גן. המסלול נפתח פעמיים בשנה.

עלות

סך 9,400 ₪ + 400 ₪ דמי רישום (כולל מע"מ)

מתודולוגיה

מסלול Forensics נבנה על סמך היכרות המכללה עם עולם אבטחת המידע והסייבר בישראל ובעולם. התכנים נבנו בסיוע אנשי מקצוע מהמעולים בתחום הנושאים על גבם ניסיון ארוך טווח והיכרות עם טכנולוגית מגוונת בתחומי הלימוד.

תוכנית הלימודים

1. Module 1 - Introduction

- The Goals of Forensics
- Relevant Israeli Digital Investigation Bodies
- Rulings and precedents by the Law of Evidence
- Digital Investigations
- Forensics Methodologies & Legal Issues
- Digital Forensics Importance
- Forensically Sound & Write Blockers
- Chain of Custody Importance
- Common types of Forensics cases
- Types of Evidence
- Stages of the Forensics Process
- The Limits of Forensics
- The Israeli Law
- Preparing for Forensics
- Forensics and SIRT
- Data Acquisition Process
- Order of Volatility
- Volatile Data Order
- Specific Forensic Techniques
  - Disk Forensics
  - File Carving
  - Using Autopsy (aka: The Sleuth Kit GUI)
  - Network Forensics
  - Document Forensics
  - Memory Forensics – Basics
  - Cell Phone Forensics
- Storage Acquisition
- Duplicating Hard-drives
- Exercise 1

2. Module 2 – Storage & File Systems Fundamentals

- RAID
- RAID Levels
- Duplicating RAID
- Storage Types
- Hard Disks Interfaces: SCSI, IDE/EIDS, ATA/SATA, USB, Fibre Channel
- Digital Media: Floppy, CD-ROM, DVD, HD-DVD, Blu-Ray, USB Flash Drive, SD/CF/MMC/MS/SM
- Boot Sequence: BIOS, CMOS, UEFI, Secure Boot
- File Systems: Windows, Linux, OSX – Clusters ,Sectors, Partitions
- GPT vs MBR
- FAT 32 Filesystem
- ExFAT Filesystem
- NTFS Filesystem Internals
  - NTFS Alternate Data Streams
  - NTFS Junctions
  - File Encryption
- Virtual File System
- Importance of Indexing
- Exercise 2

3. Module 3 – Data Extraction & Investigation

- Open Source Tools : WinHex, HxD, Neo, Pattern, WFT, Plaso, Galetta, NirSoft
- Commercial Tools: FTK, EnCase, R-Studio
- Remote Data Acquisition: LinEn, Helix
- Recovering Deleted files
- Recovering from Slack Space
- Start-up files
- Filesystem Times Analysis
- Logs Analysis
- Event Log Analysis
- LNK gathering
- Log File Investigation
- Web-Server Log Analysis
- Data-Base Log Analysis
- Windows Registry Analysis
  - Registry Structure
  - Auto start Locations
  - User Activity
  - MRU Lists
  - User Assist
  - USB Removable Storage
  - Wireless SSIDs
- Triage Analysis Execution
- Internet Forensics
  - Browser Activity
  - Important Folders
  - Cache, Favorites, History, Database
  - Internet Explorer, Firefox, Chrome,
- Exercise 3

4. Module 4 – File System Triage & Analysis

- Linux Forensics
  - System Artifacts
  - System Profiling
  - Time Zone
  - User Accounts
  - Login History
  - Web Browser Artifacts
  - SSH
  - Syslog
- Triage Analysis Execution
- Hash Functions (Message Digests)
- Hash Extraction
- Signature Check
- Mime Type and EOF
- NSRL: Hash Database
- File Metadata Gathering
- Entropy
- PE Analysis
- Sysinternals: Sysmon, Process Explorer, Process Monitor, SigCheck, Autoruns
- Tools: Process Hacker, Apate-DNS, VirusTotal, TeamCymru
- Things to Watch out for:
  - Persistence mechanisms
  - Back doors
  - Suspicious file and Directories
- Exercise 4

5. Module 5 – Advanced & Compounded Data Triage

- Image Analysis
- Steganography
- Password Cracking
- Software Analysis and Reverse Engineering
- Network Traffic Acquisition
- Network Traffic Analysis
- Tracking Email: PST, EDB, OST, EML, MSG
- Email Message Structure
- Exercise 5

6. Module 6 – Reverse Engineering Basics

- Volatile RAM Acquisition: Windows, Linux
- Extract Memory for Hibernation File,
- Process Snapshot
- Memory Analysis
- Windows Anomalies Detection
  - Rogue Process Identification
  - Tools
  - Known & Unknown Services
  - Anomaly Detection & Rootkit Behavior
  - Unusual OS Artifacts
  - Suspicious Network Activity
  - Evidence of Persistence
- Volatility Workshop: peinfo, svcscan, netscan, Malfind, psxview, apihooks
- Process Analysis
- Dynamic analysis
- Static analysis
- Exercise 6

7. Module 7 – Reporting & CleanUp

- Writing a Forensic Report
- Data Destruction
- Anti-Forensics: Techniques, Detection & Countermeasures
- Final Exercise

הערות לתוכנית הלימודים

- תוכנית הלימודים מחייבת בהכנת שיעורי בית להשגת יעדי הלימוד.
- משימות קריאה מהווים חובה לימודית.
- תכנים, נושאים ו/או יצרנים עשויים להשתנות במהלך הרצת התוכנית כתוצאה ממגבלות שיווקיות / אחרות.

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.

מידע נוסף

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

פרקטיקה בחקירות – Forensics Practicum

<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:_____.