סייבר מתקדם הגנה ותקיפה 2026

על הקורס

בקורס זה, נתמקד בטכניקות פריצה והגנה, ביצוע בדיקות חדירות (Penetration Testing) ניתוח פרצות אבטחה מתרחישים אמיתיים והבנת מנגנוני הגנה במערכות.

בימינו כשכל העולם הפך ממוחשב, אין זה פלא שהאנושות הגיעה למקום שבו גם המלחמות מתנהלות בזירה הטכנולוגית והממוחשבת.
עם התפתחות הטכנולוגיה והאפשרויות שהיא מציעה, גדלו עמה גם האפשרויות ללוחמה מסוג חדש, משוכללת ומתוחכמת יותר , מפחידה בהרבה מכל סוגי הלוחמה שהכרנו עד העת הזו. מדובר כמובן על תחום לוחמת המידע המתרחש במרחבים הממוחשבים ובמרחבים הווירטואליים ברשת האינטרנט.

לוחמה מסוג זה מתבצעת באמצעים טכנולוגיים משוכללים ומורכבים ועיקרה הוא חדירה למערכות ממוחשבות של גופים שונים. לוחמת סייבר הוא שמה הנפוץ, ולאחרונה אנו עדים למתקפות לא מעטות של האקרים ושל ארגוני פשע שונים הפועלים במרחב הסייבר – על מדינות, על ארגונים ועל עסקים שונים שבהם מבקשים אותם ארגונים או אנשים לפגוע.

לפיכך, ההגנה הנדרשת בעידן זה גם היא הולכת ומשתכללת – בהתאם לפשעים החדשים המתבצעים כיום ולשיטות הפגיעה הקיימות. תחום לוחמת המידע, לוחמת הסייבר, הוא תחום הנמצא בהתפתחות מטאורית כיום, ונדרשים בו אנשים מיומנים המכירים אותו לעומק.

לוחמה והגנת סייבר הינה כלל המקרים בהם ישנם ניסיונות חדירה למערכות ממוחשבות על ידי האקרים וארגוני פשע במטרה לפגוע במידע השמור במערכות אלה.

קהל יעד

בוגרי קורס אבטחת מידע וסייבר.

דרישות קדם

- ראיון מקדים
- בוגר קורס סייבר במכללה
- רצון ללמוד את התחום ולהתקדם

לאחר השתתפות ומעבר הקורס נכיר ונוכל לבצע את הפעולות הבאות

- What is cyber and the digital universe?
- What is denial of service and how it is performed?
- How is information gathering performed?
- How to gain privileges (with brute-forcing and without)?
- How to inject code into interpreted context?
- How to exploit vulnerable code?
- What are blacklists and how are they implemented?
- What are whitelists and how are they implemented?
- How to improve authentication mechanisms?
- How to better manage your current assets?
- How to create baselines and detect anomalies?
- How to use and improve the human factor?
- What are APTs?
- What is security by design?

סילבוס

- cmd OS injections
- data-store injections
- file injections
- remote file and resource inclusion
- injecting web clients (browsers)
- injecting client applications (office, pdf, etc)
- Buffer, stack and heap overflows
- Browser and plugin exploitation
- Code execution
- Flooding
- Spoofing
- Scanning, fingerprinting and enumeration
- Manual vs. Automated spidering
- Credential harvesting
- Resource mapping
- Brute-force logins and passwords
- Password hashes and password dictionaries
- Custom dictionaries and password complexity
- Bypass authentication mechanisms
- Bypass session management
- Bypass OS user and fs permissions
  Bypass security software
- What is defense all about

- IP blacklists
- Anti-malware defenses
- URL filtering
- Block mail SPAM and spoofs
- Application firewalls (proxies and reverse-proxies, WAFs, DB-fw)
- IDS/IPS/HIPS
- NAC
- backup and disaster recovery
- Honeypots and decoys
- Exploit mitigation tools
- Centralized log collection and analysis (aka SIEM)
- Network/host-based anomaly detection
- Heuristic A/V and HIPS
- New profession: security analyst
- User education
- Skill assessment and training
- Penetration testing
- Firewalls and access-lists
- Application whitelisting
- Application firewalls (positive proxies and reverse-proxies)
- strong passphrases
- cryptography
- multi-factor authentication
- permissions and the 'need to know' rule
- admins (locale & domain) and roots
- audit
- patch operating systems and applications
- perform vulnerability scans
- harden OS and application configurations