CyberPro 2026

תחום הסייבר החל להתפתח באופן מהיר מאוד. כיום, תחום הסייבר מהווה תחום מרכזי כמעט בכל מוסד, ארגון או חברה בעולם. לאור הגדילה המהירה בשוק הסייבר, נוצר מחסור גדול באנשי סייבר מקצועיים בשוק העבודה.
השילוב בין תחום מרכזי, שוק אשר גדל במהירות ומחסור גדול בעובדים מוסמכים יוצר הזדמנויות משמעותיות ביותר עבורכם, הסטודנטים ומאפשר לכם להיכנס לתחום המבוקש ביותר כיום בשוק ההייטק העולמי, להתפתח אישית ומקצועית ולהרוויח שכר מהטובים בשוק.
מכללת INT מציעה לכם את קורס הסייבר החדשני, הממוקד והאפקטיבי ביותר אשר יכין אתכם בצורה מושלמת לקריירה בתחום הסייבר.

חשוב לדעת!

היקף השעות
40 שעות אקדמיות | 8 מפגשים

קהל יעד
הקורס מיועד לבעלי רקע טכנולוגי בסיסי, שליטה טובה בשימושי מחשב, ידע ראשוני ברשתות תקשורת והיכרות עם מערכת ההפעלה Windows (רצוי גם Linux) נדרשת הבנה באנגלית טכנית לצורך עבודה עם כלים וסקריפטים. הקורס אינו דורש ניסיון קודם בסייבר, אך מתאים למועמדים בעלי אוריינטציה טכנית גבוהה ויכולת לימוד עצמית.

זכאות לתעודת גמר מטעם מכללת INT:
תעודת גמר מטעם מכללת iNT תוענק לעומדים בתקנון הלימודים, מעבר כל המבחנים בציון עובר ובעמידה בנוכחות של 85% מהשיעורים לפחות.

מטרות הקורס:

- הקניית כלים פרקטיים להבנת עולם הסייבר ההתקפי
- התנסות Hands-on בטכניקות פריצה, איסוף מידע, תקיפת רשתות ומערכות
- היכרות עם הכלים והמתודולוגיות המרכזיות של תוקפים בעולם האמיתי
- פיתוח חשיבה ביקורתית ויכולת אנליטית לזיהוי חולשות וניצולן

תוכנית לימודים:

מפגש 1: איסוף מידע מתקדם (OSINT) והנדסה חברתית

- מהו OSINT וכיצד משתמשים בו בהקשר סייבר
- כלים וטכניקות לאיסוף מידע גלוי
- שימוש ברשתות חברתיות ובמאגרים ציבוריים
- מבוא להנדסה חברתית: טכניקות שכנוע, התחזות ופישינג

מפגש 2: מתקפות Man in the Middle וניתוח תעבורת רשת

- מבנה התקשורת בין מחשבים ופרוטוקולים רלוונטיים (ARP, DNS וכו')
- מבוא ל־MITM: מהי וכיצד מתבצעת
- כלים ליירוט מידע: Wireshark, Ettercap, Bettercap
- הדגמות בזמן אמת וניתוח פקטות

מפגש 3: פריצת סיסמאות – תיאוריה, כלים ותרגול

- מבוא להצפנת סיסמאות ושיטות אחסון
- תקיפות brute-force, dictionary ו־rainbow tables
- כלים פופולריים: Hashcat, John the Ripper, Hydra
- שימוש ב־RockYou.txt ו־SecLists

מפגש 4: תקיפת רשתות אלחוטיות – WiFi Cracking

- סקירה של סוגי הצפנות(WEP, WPA, WPA2
- ניתוח חולשות בפרוטוקולים אלחוטיים
- שימוש ב־Aircrack-ng suite ו־Kismet
- תקיפות deauthentication ו־handshake capture

מפגש 5: עולם ה־VPN, פרוקסי וה־Darknet

- עקרונות אנונימיות והסוואת זהות ברשת
- מבוא ל־VPN, TOR, I2P ו־SOCKS Proxy
- סקירה של שווקים ופעילות ב־Darknet
- הדגמות ניתוח תעבורת Proxy וטכניקות מעקב

מפגש 6: מתקפותXSS – Cross Site Scripting

- מהי XSS? סוגים: Reflected, Stored, DOM-based
- שיטות זיהוי והזרקת קוד זדוני לדפדפן
- כלים: XSS Hunter, Burp Suite, OWASP ZAP
- הדגמות פרקטיות וסימולציות

מפגש 7 – SQL Injection: הזרקת קוד למסדי נתונים

- היכרות עם שפת SQL בסיסית
- ניצול חולשות במסדי נתונים, Authentication Bypass – מידע רגיש
- שימוש בכלים: SQLmap, Havij
- הגנה מפני SQLi – עקרונות בסיסיים

מפגש 8 – Steganography: הסתרת מידע בקבצים ומדיה

- עקרונות הסתרת מידע בתמונות, וידאו וקול
- כלים נפוצים: Steghide, zsteg, OpenStego
- שילוב ב־ICTF או־Red Teaming
- פרויקט מסכם: ניתוח קובץ והסתרת מסר

הערות:

- כל שיעור כולל הסבר תיאורטי, תרגול מודרך והתנסות עצמאית
- הסטודנטים יתבקשו לבצע תרגילי בית ולהגיש דוח קצר לאחר כל מפגש
- המפגש האחרון כולל פרויקט סיכום הכולל שילוב מספר טכניקות שנלמדו

תל אביב

המרץ 2