-סילבוס-

קורס סייבר סקיוריטי ואבטחת מידע

from zero to hero program

קהל יעד : לא נדרש רקע קודם בתחום (שער כניסה לתעשיית הסייבר)

היקף שעות : 400 שעות אקדמאיות (6 חודשים רצופים יומיים או 12 חודשים פעמיים בשבוע ערב)

רף כניסה לקורס : ידע בסיסי באנגלית , ידע ותפעול מחשב אישי , חשיבה יצירתית

הכרה והסמכה : מוכר משרד העבודה , תעודת סיום והסמכה, אפשרות להרחבת הסמכה בינלאומית

טכנולוגיות הכשרה : סימולטור תרחישי תקיפה , תוכן LMS , מעבדות אימון

www.cyberlabs-usa.com

סילבוס כללי – יחידות תוכן

פירוט מקצועות/נושאים	שעות לימוד		
	עיוני	מעשי	סה"כ
1. מבוא לאבטחת מידע והגנת הסייבר	16		16
2. תקני אבטחת מידע וניהול סיכונים	8	2	10
3. מבנה מחשב + יסודות מערכות הפעלה	14	4	18
4. יסודות תקשורת מחשבים-א' + ב'	16	12	28
5. הגנת גישה בתקשורת ואינטרנט	20	10	30
6. בידול והפרדת רשתות תקשורת	4	4	8
7. היבטי אבטחת מידע בציודי תקשורת (הקשחה) ואבטחת מידע	8	8	16
8. הצפנה ואימות	12	4	16
9. בקרת גישה	10	10	20
10. היבטי אבטחת מידע במערכות הפעלה והקשחות שרתים	20	20	40
11. היבטי אבטחת מידע במסדי נתונים	8	3	11
12. תוכנות זדוניות וזיהוי אנומליות	12	6	18
13. דלף מידע	4	2	6
14. ניהול ורישום אירועי אבטחת מידע (Audit)	6	2	8
15. טיפול באירועי אבטחת מידע	6	4	10
16. מחשוב ענן, שירותי אירוח, וירטואליזציה	4		4
17. שינוע מידע מ/אל הארגון	2		2
18. המשכיות עסקית (DRP/BCP)	4	4	8
19. אבטחה אפליקטיבית	8		8
20. מתודולוגית ביצוע ניסיונות חוסן (תשתית ואפליקציה)	8	10	18
21. חוק ואתיקה	8	1	9
22 אבטחה פיסית	2		2
23. ניתוח תעבורת רשת (Wireshark)	6	10	16
24. מערכות SIEM ותגובה לאירועים	6	10	16
25. מבוא ל-Penetration Testing	6	12	18
26. חקירה דיגיטלית בסיסית (Forensics)	8	4	12
27. הכנה להסמכה (Security+ / CEH)	14	2	16
28. פרויקט גמר (יישום כל הידע)	0	16	16
סה"כ שעות	**240**	**160**	**400**

סילבוס כללי – פירוט יחידות תוכן

1. **מבוא לאבטחת מידע והגנת הסייבר**
   - **שעות לימוד:** 16 שעות עיוני.
   - **חומר נלמד:** מושגי יסוד באבטחת מידע, איומים ופגיעויות, עקרונות הגנת סייבר, מודלים לאבטחת מידע (כגון CIA Triad), חשיבות האבטחה בעולם המודרני, סקירת תפקידים בתחום הסייבר, תעשיית הסייבר בעידן AI.
2. **תקני אבטחת מידע וניהול סיכונים**
   - **שעות לימוד:** 8 שעות עיוני, 2 שעות מעשי.
   - **חומר נלמד:** תקנים רלוונטיים (כגון ISO 27001, NIST), מתודולוגיות לניהול סיכונים (זיהוי, הערכה, טיפול), בניית תוכנית אבטחה.
   - **תרגול מעשי:** ניתוח מקרה בוחן של ניהול סיכונים בארגון, זיהוי נכסים, איומים ופגיעויות.
3. **מבנה מחשב + יסודות מערכות הפעלה**
   - **שעות לימוד:** 14 שעות עיוני, 4 שעות מעשי.
   - **חומר נלמד:** ארכיטקטורת מחשב (CPU, זיכרון, דיסק), סוגי מערכות הפעלה (Windows, Linux), תהליכים, קבצים, הרשאות, ניהול משתמשים.
   - **תרגול מעשי:** עבודה עם פקודות בסיסיות ב-CMD/Bash, ניהול קבצים והרשאות, יצירת משתמשים.
4. **יסודות תקשורת מחשבים-א' + ב'**
   - **שעות לימוד:** 16 שעות עיוני, 12 שעות מעשי.
   - **חומר נלמד:** מודל OSI/TCP/IP, פרוטוקולי תקשורת (IP, TCP, UDP, HTTP, DNS), כתובות IP, פורטים, ניתוב, מתגים, נתבים.
   - **תרגול מעשי:** הקמה וקונפיגורציה בסיסית של רשתות קטנות (Packet Tracer או מכונות וירטואליות), שימוש בפקודות רשת (ping, tracert, ipconfig/ifconfig, netstat).

5. **הגנת גישה בתקשורת ואינטרנט**
   - **שעות לימוד:** 20 שעות עיוני, 10 שעות מעשי.
   - **חומר נלמד:** Firewall (Packet Filtering, Stateful Inspection), IDS/IPS, VPN, NAT, proxies, אבטחת דוא"ל, אבטחת אינטרנט.
   - **תרגול מעשי:** הגדרת כללי Firewall בסיסיים (Windows Firewall / iptables), הדגמת פעולת VPN, ניתוח לוגים של אבטחה.
6. **בידול והפרדת רשתות תקשורת**
   - **שעות לימוד:** 4 שעות עיוני, 4 שעות מעשי.
   - **חומר נלמד:** VLANs, DMZ, עקרון ה-Least Privilege ברשת, פילוח רשתות.
   - **תרגול מעשי:** הגדרת VLANs בסיסיים (בסימולטור או במתגים וירטואליים), הקמת DMZ בסביבת מעבדה.
7. **היבטי אבטחת מידע בציודי תקשורת (הקשחה) ואבטחת מידע**
   - **שעות לימוד:** 8 שעות עיוני, 8 שעות מעשי.
   - **חומר נלמד:** הקשחת מתגים ונתבים (גישה מאובטחת, עדכונים, פרוטוקולים מאובטחים), אבטחת ציוד קצה.
   - **תרגול מעשי:** הגדרות אבטחה בסיסיות בציוד רשת (נתבים/מתגים וירטואליים), שימוש ב-SSH לגישה מאובטחת.
8. **הצפנה ואימות**
   - **שעות לימוד:** 12 שעות עיוני, 4 שעות מעשי.
   - **חומר נלמד:** עקרונות הצפנה (סימטרית, א-סימטרית), חתימה דיגיטלית, תעודות דיגיטליות (PKI), Hash functions, פרוטוקולי אבטחה (SSL/TLS).
   - **תרגול מעשי:** שימוש בכלי הצפנה בסיסיים (OpenSSL), יצירת זוג מפתחות ציבורי/פרטי, הדגמת חתימה דיגיטלית.

9. **בקרת גישה**
   - **שעות לימוד:** 10 שעות עיוני, 10 שעות מעשי.
   - **חומר נלמד:** מנגנוני בקרת גישה (DAC, MAC, RBAC), אימות רב-שלבי (MFA), Single Sign-On (SSO), LDAP/Active Directory.
   - **תרגול מעשי:** ניהול משתמשים וקבוצות ב-Active Directory, הגדרת הרשאות קבצים, הדגמת MFA.
10. **היבטי אבטחת מידע במערכות הפעלה והקשחות שרתים**
   - **שעות לימוד:** 20 שעות עיוני, 20 שעות מעשי.
   - **חומר נלמד:** הקשחת מערכות הפעלה (Windows/Linux), ניהול טלאים (Patch Management), אבטחת שירותים, מנגנוני ביקורת (Auditing).
   - **תרגול מעשי:** ביצוע הקשחה לשרת Windows/Linux (כיבוי שירותים מיותרים, שינוי סיסמאות ברירת מחדל, הגדרות אבטחה), סריקת פגיעויות בסיסית (לדוגמה עם OpenVAS/Nessus Community).
11. **היבטי אבטחת מידע במסדי נתונים**
   - **שעות לימוד:** 8 שעות עיוני, 3 שעות מעשי.
   - **חומר נלמד:** אבטחת מסדי נתונים (SQL Injection, הגדרות הרשאות, הצפנת נתונים במנוחה ובתעבורה), גיבוי ושחזור.
   - **תרגול מעשי:** הדגמת SQL Injection (בסביבת מעבדה מבוקרת), הגדרת הרשאות בסיסיות במסד נונים (MySQL/SQL Server Express).
12. **תוכנות זדוניות וזיהוי אנומליות**
   - **שעות לימוד:** 12 שעות עיוני, 6 שעות מעשי.
   - **חומר נלמד:** סוגי תוכנות זדוניות (וירוסים, תולעים, רוגלות, כופרות), מנגנוני הפצה, שיטות זיהוי (חתימות, התנהגותיות), סקירת כלי הגנה (אנטי-וירוס, EDR).
   - **תרגול מעשי:** ניתוח דוגמאות של קוד זדוני (בסביבה מבודדת), שימוש בכלי אנטי-וירוס וסריקה.
13. **דלף מידע**
   - **שעות לימוד:** 4 שעות עיוני, 2 שעות מעשי.
   - **חומר נלמד:** מושג ה-DLP (Data Loss Prevention), שיטות למניעת דלף מידע (טכנולוגיות, נהלים), סיווג מידע.
   - **תרגול מעשי:** הדגמת דלף מידע באמצעות כלים פשוטים, דיון על מדיניות DLP.

14. **ניהול ורישום אירועי אבטחת מידע (Audit)**
    - **שעות לימוד:** 6 שעות עיוני, 2 שעות מעשי.
    - **חומר נלמד:** חשיבות הלוגים, סוגי לוגים, ניטור לוגים, ניהול אירועים ותקריות (SIEM - נושא מורחב בפרקי ההשלמה).
    - **תרגול מעשי:** ניתוח לוגים של מערכת הפעלה ורשת, זיהוי אירועים חשודים.
15. **טיפול באירועי אבטחת מידע**
    - **שעות לימוד:** 6 שעות עיוני, 4 שעות מעשי.
    - **חומר נלמד:** שלבי תגובה לאירועים (זיהוי, הכלה, סילוק, שחזור, לקחים), בניית צוות תגובה (CSIRT).
    - **תרגול מעשי:** סימולציית אירוע אבטחה ויישום שלבי התגובה.
16. **מחשוב ענן, שירותי אירוח, וירטואליזציה**
    - **שעות לימוד:** 4 שעות עיוני.
    - **חומר נלמד:** מושגי יסוד בענן (IaaS, PaaS, SaaS), מודלי פריסה (ציבורי, פרטי, היברידי), אבטחה בענן (Shared Responsibility Model), וירטואליזציה.
17. **שינוע מידע מ/אל הארגון**
    - **שעות לימוד:** 2 שעות עיוני.
    - **חומר נלמד:** אבטחת העברת קבצים (SFTP, SCP), הצפנת נתונים בתעבורה, מדיניות העברת מידע.
18. **המשכיות עסקית (DRP/BCP)**
    - **שעות לימוד:** 4 שעות עיוני, 4 שעות מעשי.
    - **חומר נלמד:** מושגי DRP (Disaster Recovery Plan) ו- BCP (Business Continuity Plan), חשיבות הגיבוי והשחזור, תכנון התאוששות מאסון.
    - **תרגול מעשי:** בניית תוכנית גיבוי ושחזור לדוגמה, סימולציית תרחיש אסון.
19. **אבטחה אפליקטיבית**
    - **שעות לימוד:** 8 שעות עיוני.
    - **חומר נלמד:** עקרונות OWASP Top 10, פגיעויות נפוצות ביישומי ווב (XSS, CSRF, Broken Authentication), אבטחה בקוד.
    - **מערכות דרושות:** מצגות, חומרי קריאה.

20. **מתודולוגית ביצוע ניסיונות חוסן (תשתית ואפליקציה)**
    - **שעות לימוד:** 8 שעות עיוני, 10 שעות מעשי.
    - **חומר נלמד:** מבוא לבדיקות חדירה (Penetration Testing), סוגי בדיקות (Black Box, White Box), שלבי הבדיקה (איסוף מידע, סריקה, ניצול, דיווח).
    - **תרגול מעשי:** סריקת פורטים (Nmap), שימוש בכלים בסיסיים לזיהוי פגיעויות (כמו Nikto, OWASP ZAP).
21. **חוק ואתיקה**
    - **שעות לימוד:** 8 שעות עיוני, 1 שעה מעשי.
    - **חומר נלמד:** חוקי הגנת הפרטיות, חוק המחשבים, אחריות אתית של איש סייבר, קוד אתי.
    - **תרגול מעשי:** דיון בדילמות אתיות במקרי בוחן.
22. **אבטחה פיסית**
    - **שעות לימוד:** 2 שעות עיוני.
    - **חומר נלמד:** אמצעי אבטחה פיזיים (בקרת כניסה, מצלמות, גלאים), אבטחת חדרי שרתים.
23. **ניתוח תעבורת רשת (Wireshark)**
    - **שעות לימוד:** 6 שעות עיוני, 10 שעות מעשי.
    - **חומר נלמד:** עקרונות לכידת תעבורה, פרוטוקולים נפוצים, זיהוי אנומליות בתעבורה, פילטרים ב-Wireshark.
    - **תרגול מעשי:** לכידה וניתוח תעבורה באמצעות Wireshark, זיהוי התקפות בסיסיות (כגון ARP Spoofing) בניתוח חבילות.
24. **מערכות SIEM ותגובה לאירועים**
    - **שעות לימוד:** 6 שעות עיוני, 10 שעות מעשי.
    - **חומר נלמד:** עקרונות SIEM (Security Information and Event Management), איסוף, קורלציה וניתוח לוגים, בניית כללים והתראות, תגובה מתקדמת לאירועים.
    - **תרגול מעשי:** התקנה וקונפיגורציה בסיסית של SIEM (כגון - ELK Stack Elasticsearch, Logstash, Kibana), יצירת Dashboards והתראות.

25. **מבוא ל-Penetration Testing**

- **שעות לימוד:** 6 שעות עיוני, 12 שעות מעשי.
- **חומר נלמד:** שלבים מתקדמים בבדיקות חדירה, שימוש בכלי תקיפה (Metasploit, Nmap מתקדם, Burp Suite), פוסט-אקספלויטציה, הרחבת הרשאות.
- **תרגול מעשי:** ביצוע בדיקות חדירה מודרכות על סביבות פגיעות (כגון Metasploitable), שימוש ב-Metasploit לניצול פגיעויות.

26. **חקירה דיגיטלית בסיסית (Forensics)**

- **שעות לימוד:** 8 שעות עיוני, 4 שעות מעשי.
- **חומר נלמד:** עקרונות חקירה דיגיטלית, איסוף ראיות, שרשרת המשמורת, ניתוח זיכרון (Memory Forensics), ניתוח דיסקים.
- **תרגול מעשי:** שימוש בכלים בסיסיים לחקירה (כגון Autopsy/FTK Imager Lite), ניתוח קבצים חשודים.

27. **הכנה להסמכה (Security+)**

- **שעות לימוד:** 14 שעות עיוני, 2 שעות מעשי.
- **חומר נלמד:** סקירה מעמיקה של נושאי ההסמכה (Security+ של CompTIA), חזרה על נקודות מפתח, טיפים למבחן.
- **תרגול מעשי:** פתרון שאלות לדוגמה ממבחני הסמכה.

28. **פרויקט גמר (יישום כל הידע)**

- **שעות לימוד:** 0 שעות עיוני, 16 שעות מעשי.
- **חומר מתורגל:** יישום אינטגרטיבי של כלל הידע שנרכש בקורס על פרויקט סייבר מעשי (לדוגמה, אבטחת רשת ארגונית קטנה, הקמת סביבת SIEM, ביצוע בדיקת חדירה מלאה על יעד מוגדר).

תשתית טכנולוגית נדרשת לסביבת הכשרה

דרישות כלליות למערכות מעבדה:

- **תשתית וירטואליזציה:** VMware Workstation Pro / Oracle VirtualBox.
- **מערכות הפעלה:**
  - Windows Server (גרסאות 2022/2019/2016)
  - Windows Client (Windows 10/11)
  - Linux (Ubuntu Server/Desktop, Kali Linux)
  - Metasploitable (מכונה וירטואלית פגיעה)
- **כלי רשת וסימולציה:**
  - סימולטור הדמיית תרחישים מבית CYBERLABS
  - Cisco Packet Tracer / GNS3
  - Wireshark
  - Nmap
- **כלי אבטחה:**
  - OpenSSL
  - OWASP ZAP / Burp Suite Community Edition
  - כלי סריקת פגיעויות (OpenVAS / Nessus Community)
  - Metasploit Framework
  - כלי Forensic (Autopsy / FTK Imager Lite / Volatility Framework)
- **פלטפורמות SIEM:**
  - ELK Stack (Elasticsearch, Logstash, Kibana)
- **אחרים:**
  - יישומי וב פגיעים (DVWA, bWAPP)
  - תוכנות גיבוי (Replication Community Edition & Veeam Backup)
  - מגוון כלי שורת פקודה וסקריפטים.