

We invented a Methodology for Cyber Education because nobody else did it.

# קורס Cyber16+

פתיחה: \_\_\_\_\_ ימים ראשון ורביעי (ערב)

## יועץ אקדמי: מר אבי ויסמן \*

קורס טכניקות תקיפה לבעלי רקע בפיתוח או רקע בתשתיות טכנולוגיות

מאפייני תוכנית הלימודים		אודות התוכנית
קהל:	מנהלים / סביבתיים / מקצוענים	<p>למרחב הסייבר יש השפעה על חיי היום יום של כל אחד מאיתנו, ולכן פגיעה בהן עלולה להפריע למהלך החיים התקין. לכן, ישנה חשיבות ללימוד הגנת כסייבר כמקצוע. "מגשימים לאומית" הינה תוכנית מצוינות המתמקדת בהכשרה ובפיתוח המתמקדת בהכשרה ובפיתוח מומחיות בתחום הסייבר והמחשבים בקרב בני נוער מצטיינים בגילאי 15 עד 18 בפריפריה הגיאוגרפית. התוכנית מתפרסת על פני שלוש שנים ובנויה מקורסים מקצועיים. התוכנית נערכת במתכונת של שני מפגשים בשבוע בני 3 שעות אחר הצהריים במשך 5-6 סמסטרים הפרוסים בין הכיתות י' עד י"ב. בכל קבוצת למידה משתתפים כ-25 תלמידים. תוכנית Cyber16+ נחשבת נכס צאן ברזל במיטב הגופים העוסקים בנושא תקיפה ויעוץ, ומהווה העתק משודרג לתוכנית הרשמית "מגשימים", המיועדת להכשרת בני נוער לעולם הסייבר הצבאי.</p>
אוריינטציה:	מנהלית/ טכנית / יישום	
שלב:	מתחילים / מתקדמים	
רוחב:	ממוקד / רחב	
עומק:	סוקר / עמוק	
הסמכות:	Cyber Warfare Defense level-II	
שעות:	280 שעות	
פתיחה:	2015	
מתכונת:	70 מפגשי ערב, כ-10 חודשים	
תרגול בית:	בהיקף 620 שעות	

## מטרת התוכנית

תוכנית Cyber16+ מיועדת להכין תלמידי תיכון המעוניינים בהתמחות במרחב המקוון (Cyber), להכשירם כאנשי מקצוע לכל עולמות ההגנה הדיגיטלית, ולעולם התקיפה האתית, בתחומי Mobile, Network, System, ותקיפת יישומים ויישומי Web.

## קהל יעד

בני נוער מגיל 15 ואילך, בעלי רקע לימודי טכנולוגי, עם עדיפות למגמות המחשב. התוכנית פרוסה על-פני שנתיים, בהתחשב בדרישות מבחני הברגרות המתקיימות בבתי הספר התיכוניים במקביל.

## תעודה



- קיימת חובת נוכחות ב-80% מהמפגשים, ועמידה במבחנים/עבודות, בציון 70.
  - תיעוד: לעומדים בדרישות התכנית תוענק תעודת הסמכה מטעם See Security
- "Cyber Warfare Defense level-II Professional"**

## הכרה

תוכנית Cyber16+ מהווה העתק משודרג לתוכנית הרשמית "מגשימים", המיועדת להכשרת בני נוער לעולם הסייבר הצבאי.

## אודות המכללה

מכללת See-Security הינה מוסד לימודים ייעודי לתחום אבטחת מידע, לוחמת סייבר ותשתיות, היחידה בישראל, אחת מ-7 מכללות ייעודיות ברחבי העולם, אשר עוסקת בלעדית רק באבטחת מידע, לוחמת מידע ותשתיות. ההתמחות העמוקה של המכללה הציבה אותה ואת אנשיה במעמד יוצא דופן בעולם. המוניטין שיצא למכללה נובע מתוקף עבודתה בצמוד למערכת הבטחון בישראל מזה 12 שנה, ומהעומק המקצועי, הגישה הפדגוגית והרמה הגבוהה של המרצים - כולם מופרים, ולעיתים - בכירים מאוד בענף הסייבר בישראל.

### 2014 – 2003:

#### עשור של בכורה מקצועית

זמן רב לפני שהושקו תוכניות ללימודי Cyber, בתקופה בה הושק לראשונה מסלול HDE, כבר ניתן דגש להרכשת טכניקה, במקום ללימוד כלים קיימים. בתחילת העשור הקודם, בימיהן של מערכות XP, Windows Server 2000 ומערכות ה-Linux של הדור הקודם, היו המערכות חדירות מאוד, שכן יצרניהן השקיעו מאמץ ירוד יחסית בהגנתן. הדור הנוכחי של המערכות מחד, והתפתחות כלי ההגנה ואבטחת המידע, הביאו לכך שהשימוש ב"כלים אוטומטיים לתקיפה" נעשה לא רלבנטי, או "פחות יעיל", לשון המעטה.

ההאקר נדרש להפעלת גישה מולטי-דיסציפלינארית המשלבת ידע ויצירתיות רבה בפעילותו. לכלים אוטומטיים קיימת "חתימה", כשם שלמטוס קיימת "חתימת מכ"ם" ייחודית לדגם שלו. כלי ההגנה של הדור הנוכחי לומדים במהירות את החתימות של הכלים, ולכן – מאפשרים חסימת התקפות המבוצעות באמצעותם.

בתולדות התקיפה הקיברנטית, זכו "מומחי תקיפה" המבוססת רק על הפעלת "ערכות כלים" לכינוי הגנאי "Script Kiddies" או "Skiddies".

כיום, קיימת דרישה רשמית למומחי סייבר שונים, במגוון מקצועות ותפקידים, בכל מגזרי המשק, וכמובן – בסקטור הבטחוני בראשם. הביקוש הגואה מחד, והרבגוניות המקצועית המתחייבת מאידך, מחייבים מענה מקצועי, יסודי, ארוך-טווח, ואינם יכולים להתממש באמצעות קורסים נקודתיים.

תוכנית הלימודים Cyber16+ מלמדת "כיצד לדוג", ולא "באיזה כלים משתמשים לאכילת דג". התוכנית הינה שפול של תוכנית "מגשימים לאומית", עתירת תרגילים לסביבת הכיתה והבית, ומחייבת השקעה כוללת בת 900 שעות לכל הפחות.

גישה זו מחייבת השקעה ריטואלית ויקרה בפיתוח התרגילים, אך הוכיחה עצמה כגישה היחידה לפיתוח "ראש חושב".

התוכנית מופעלת בשלוחות באר שבע ורמת גן בלבד.

פנה אל היועץ להכוונה.

## מתכונת הלימודים

משך התכנית כ-70 מפגשים (ימים ראשון ורביעי 17:30 עד 21:00). הלימודים מתקיימים בקמפוס See Security ברמת-גן, ובקמפוס Cyber7 בבאר שבע. המסלול נפתח פעמיים בשנה.

### עקרונות מנחים בלימוד ההתמחות:

1. Hands-on - עבודה באופן ישיר, בלתי-אמצעי ומעשי עם המערכות השונות בתכנית הלימודים.
2. Low level - הבנה מעמיקה ויסודית עם המערכות השונות. יש להבין את המנגנונים הפנימיים של המערכות.

### המלצות לבחירה במסגרת הבגרות במדעי המחשב

1. יחידה חמישית – מערכות מחשב ואסמבלי
2. יחידה שלישית – מבוא לתכנות בסביבת אינטרנט

## עלות הלימודים

סך 19,400 ₪ + 400 ₪ דמי רישום.

## הערות

- התוכנית נבנתה לצרכי ידע מעשי, ובהתאמה לדרישות הטיפוסיות של צה"ל.
- 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.
- רשימת תת הנושאים, עומקם ורוחבם עשויה להשתנות בהתאם לשליטת התלמידים בחומר, או בהתאם לדרישות מתחדשות של משרד הביטחון, במידה שתימסרנה.

## מידע נוסף

◦ מידע מינהלי: אלירה אליסייב, 03-6122831, 052-8787889, [elvira@see-security.com](mailto:elvira@see-security.com)

◦ יועץ אקדמי: אבי ויסמן, 054-5222305, [avi@see-security.com](mailto:avi@see-security.com)

## תוכנית הלימודים

ההתמחות בנויה משישה חלקים:

עבודת גמר	משימות בית	סה"כ כיתה	שעות כיתה מעשיות	שעות כיתה עיוניות	חלק	
	12	12	0	12	מבוא להגנת סייבר	1
	88	88	48	40	הגנת רשתות	2
	60	40	24	16	הגנת אפליקציות (בדגש Web)	3
	120	80	32	48	הגנת מערכות הפעלה (בדגש Windows)	4
	20	20	4	16	הגנת סייבר בעולם מורכב	5
	80	40	16	24	השלמות Hacking Defined	6
220					עבודת גמר	7
<b>220</b>	<b>400</b>	<b>280</b>	<b>124</b>	<b>156</b>	<b>סך הכל</b>	

### חלק א' - מבוא להגנת סייבר

#### פרק 1: מבוא להגנת סייבר

מטרת הפרק: להבין את משמעות המונח "סייבר" ומהי "הגנת סייבר".

##### מושגים והכוונה

- |                 |                                   |
|-----------------|-----------------------------------|
| 1. מחשב אישי    | 7. נזקה (Malware)                 |
| 2. שרת          | 8. סוס טרויאני (Trojan Horse).    |
| 3. מערכת משובצת | 9. תולעת מחשבים (Computer Worm)   |
| 4. רשת          | 10. וירוס מחשבים (Computer Virus) |
| 5. רשת פנימית   | 11. Adware                        |
| 6. DoS/DDoS     | 12. Spyware                       |

#### פרק 2: אינטרסים ושחקנים מרכזיים בעולם הסייבר

מטרת הפרק: להכיר מה הם האינטרסים בעולם הגנת הסייבר ומיהם השחקנים המרכזיים.

##### מושגים והכוונה

- |                                  |   |
|----------------------------------|---|
| 1. ארגוני ביון                   | 7. חומת אש לאפליקציות Web – WAF             |
| 2. Script Kids                   | 8. Application Firewall                     |
| 3. White Hat                     | 9. Antivirus                                |
| 4. Black Hat                     | 10. Black Box Scanner                       |
| 5. VPN – Virtual Private Network | 10. Source Code Analysis – White BoxScanner |
| 6. חומת אש Firewall              |   |

#### פרק 3: מבוא לתוכנית הלימודים

מטרת הפרק: הבנת תכולת הלימודים במקצוע.

##### מושגים והכוונה

- |                |                  |
|----------------|------------------|
| 1. רשת         | 4. החוק הישראלי  |
| 2. מערכת הפעלה | 5. החוק האמריקאי |
| 3. אפליקציה    |                  |

## חלק ב' - הגנת רשתות

### פרק 4: מבוא לתקשורת

**מטרת הפרק:** לבצע הכרות ראשונית עם עולם התקשורת תוך הדגמה על רשת האינטרנט.

#### מושגים והכוונה

- |   |                                |
|---|--------------------------------|
| 1. הודעה בתור יחידת מידע בסיסית           | 7. פרוטוקול תקשורת             |
| 2. תווך תקשורת                            | 8. טופולוגיות תקשורת           |
| 3. תקשורת קוויית                          | 9. תקשורת סינכרונית/אסינכרונית |
| 4. תקשורת אלחוטית                         | 10. קצב שידור                  |
| 5. תת מערכות תקשורת וחיבוריות ביניהם (רשת | 11. אפנון                      |
| ביתית, הרשת הגלובלית)                     | 12. ריבוב                      |
| 6. כתובת וניתוב                           | 13. RFC (Request for Comment)  |

### פרק 5: מודל 7 השכבות

**מטרת הפרק:** להבין את העיקרון של חלוקה לשכבות בעת ביצוע תקשורת בין שני Hosts/Nodes ברשת, להציג את מטרת השכבות, הפעולות אותן הן נדרשות לבצע והסדר בניהן.

#### מושגים והכוונה

- |                                  |                                       |
|----------------------------------|---------------------------------------|
| 1. שכבת תקשורת                   | 5. שכבת הרשת (Network Layer)          |
| 2. פרוטוקול                      | 6. שכבת התעבורה (Transport Layer)     |
| 3. תקן                           | 1. שכבת ניהול השיחה (Session Layer)   |
| 1. כימוס (Encapsulation)         | 7. שכבת התצוגה (Presentation Layer)   |
| 2. Protocol Tunneling            | 8. שכבת האפליקציה (Application Layer) |
| 3. השכבה הפיזית (Physical Layer) | 9. תקורה (Overhead)                   |
| 4. שכבת הקו (Data Link Layer)    |                                       |

### פרק 6: עבודה עם Sniffer

**מטרת הפרק:** להכיר את המטרה של שימוש ברכיב Sniffer (הן תוכנתי והן חומרתי). התנסות ועבודה עם Sniffer תוכנתי בשם Wireshark. להכיר את בעיות האבטחה בנוגע ל-Sniffer.

#### מושגים והכוונה

- |                            |                              |
|----------------------------|------------------------------|
| 1. Sniffer Promiscues Mode | 6. Transport Name Resolution |
| 2. Non-Promiscues Mode     | 7. Transport                 |
| 3. Display Filter          | 8. Dissector                 |
| 4. Capture Filter          | 9. (Man In The Middle) MITM  |
| 5. MAC Resolving           |                              |

### פרק 7: טכנולוגיות LAN (Local Area Network)

**מטרת הפרק:** הכרות עם אופן זרימת התקשורת ברשתות LAN (Local Area Network).

#### מושגים והכוונה

- |               |                    |
|---------------|--------------------|
| 1. MAC כתובות | 7. Broadcast       |
| 2. CRC        | 8. Multicast       |
| 3. CSMA/CD    | 9. Collisions      |
| 4. CSMA/CA    | 10. VLAN (רשות)    |
| 5. Ethernet   | 11. Tagging (רשות) |
| 6. Unicast    |                    |

## פרק 8: יסודות רכיבי תקשורת

**מטרת הפרק:** לבצע הכרות ראשונית עם ציוד תקשורת ואופן פעולתו.

### מושגים והכוונה

- |                                    |                     |
|------------------------------------|---------------------|
| 7. נתב (Router)                    | 1. Broadcast Domain |
| 8. Table CAM (Content Addressable) | 2. Collision Domain |
| (Memory)                           | 3. משחזר (Repeater) |
| 9. טבלת ניתוב (Routing Table)      | 4. גשר (Bridge)     |
| 10. מודם (Modem)                   | 5. רכזת (HUB)       |
|                                    | 6. מתג (Switch)     |

## פרק 9: ניתוח תעבורת רשת בסיסית עם Python

**מטרת הפרק:** התלמידים יכירו את שפת Python שתשמש אותם ככלי scripting מחקרי-אינטראקטיבי בהקשר להגנת סייבר. בפרק הזה הכלי ישמש לניתוח בסיסי של תעבורת רשת.

## פרק 10: חבילת הפרוטוקולים TCP/IP

**מטרת הפרק:** ללמוד על חבילת הפרוטוקולים TCP/IP גרסה 4, להציג את הפרוטוקולים, מטרתם ואופן פעולתם.

### מושגים והכוונה

- |   |  |
|---|--|
| 5. IP Address                                 | 1. IP (Internet Protocol)              |
| 6. Port                                       | 2. UDP (User Datagram Protocol)        |
| 7. NAT/PAT (Network/Port Address Translation) | 3. TCP (Transmission Control Protocol) |
|   | 4. ARP (Address Resolution Protocol)   |

## פרק 11: תכנות ב-Socket-ים

**מטרת הפרק:** ללמוד על אופן פיתוח תוכניות בסביבת הרשת באמצעות Socket-ים.

### מושגים והכוונה

- |                        |                     |
|------------------------|---------------------|
| 7. send הפונקציה       | 1. Socket           |
| 8. sendto הפונקציה     | 2. Import socket    |
| 9. recvfrom הפונקציה   | 3. bind הפונקציה    |
| 10. Blocking Functions | 4. listen הפונקציה  |
| 11. Stream Protocols   | 5. connect הפונקציה |
| 12. Datagram Protocols | 6. recv הפונקציה    |

## פרק 12: אבטחת מידע בפרוטוקולי TCP/IP

**מטרת הפרק:** להכיר היבטים אבטחתיים ותקיפות בחבילת הפרוטוקולים TCP/IP ודרכי ההתמודדות איתם.

### מושגים והכוונה

- |                           |                     |
|---------------------------|---------------------|
| 6. ARP Spoofing           | 1. פורט פתוח / סגור |
| 7. Smurf Attack (רשות)    | 2. nmap             |
| 8. Teardrop Attack (רשות) | 3. Firewall         |
| 9. SYN Attack (רשות)      | 4. Proxy            |
| 10. TCP SYN Cookie (רשות) | 5. IDS              |



We invented a Methodology for Cyber Education because nobody else did it.

### פרק 13: scapy

**מטרת הפרק:** לנתח ולייצר תעבורת רשת בעזרת חבילת scapy של Python.

**מושגים והכוונה**

- |                        |                                      |
|------------------------|--------------------------------------|
| Python .1              | scapy .2                             |
| א. list                | א. פרוטוקולים: IP, TCP, ARP, Ether,  |
| ב. dict                | DNS, ICMP                            |
| ג. גישה לשדות          | ב. פקודות: lsc, ls, hexdump, rdpcap, |
| ד. list comprehensions | send, sendp, sr, sr1, wireshark      |

### פרק 14: פרוטוקולים בשכבת האפליקציה

**מטרת הפרק:** ללמוד ולהכיר פרוטוקולים נפוצים בשכבת האפליקציה.

**מושגים והכוונה**

- |  |   |
|--|---|
| .1 HTTP (Hyper Text Transfer Protocol) | .4 Zone Transfer                        |
| .2 DNS (Domain Name System)            | .5 SMTP (Simple Mail Transfer Protocol) |
| .3 TLD (Top-Level Domains)             | .6 SMTP spoofing                        |

### פרק 15: תרגיל סיכום

**מטרת הפרק:** לתכנן, לתעד ולממש פרוטוקול תקשורת ברמת האפליקציה.

**מושגים והכוונה**

- |                          |           |
|--------------------------|-----------|
| .1 שלבים בפיתוח פרוטוקול | .2 Python |
| א. תכנון                 | ד. def    |
| ב. תיעוד                 |           |
| ג. מימוש                 |           |

## חלק ג' - הגנת אפליקציות (בדגש Web)

### פרק 16: מבוא לאפליקציות Web

(לאילו שלמדו תכנות בסביבת אינטרנט הפרק הוא חזרה קצרה. ואפשר להפחית את כמות השעות לטובת נושאים אחרים והגשת עבודת הגמר)

**מטרת הפרק:** להכיר ולהבין מהי אפליקציית web.

**מושגים והכוונה**

- |               |                  |
|---------------|------------------|
| .1 HTML       | .4 Client-Server |
| .2 JavaScript | .5 Cache         |
| .3 Ajax       |                  |

### פרק 17: הגנה מפני Cross Site Scripting

**מטרת הפרק:** התלמיד יבין מהן התקפות וההגנות ברמת האפליקציה ולהכיר התקפת XSS והגנה מפניה.

**מושגים והכוונה**

- |  |                         |
|--|-------------------------|
| .1 OWASP (Open Web Application Security Project) | .4 Cookies              |
| .2 Credentials                                   | .5 Same Origin Policy   |
| .3 Session                                       | .6 Cross Site Scripting |



## פרק 18: SQL Injection

מטרת הפרק: התלמיד יכיר תקיפת SQL Injection והגנה מפניה.

### מושגים והכוונה

- |                       |    |                     |    |
|-----------------------|----|---------------------|----|
| Escape character      | .6 | מסד נתונים          | .1 |
| Stored Procedures     | .7 | SQL                 | .2 |
| Parameterized Queries | .8 | SQL Injection       | .3 |
| Error Pages           | .9 | Blind SQL Injection | .4 |
|                       |    | Input Validation    | .5 |

## חלק ד' – הגנת מערכות הפעלה

### פרק 19: מבוא למערכות הפעלה

מטרת הפרק: לפרט את מטרת מערכת ההפעלה ותפקידיה העיקריים, ולהסביר בקווים כלליים את מבנה המחשב. להוות מבוא כללי, בו התלמידים אמורים להבין בקווים כלליים איך המחשב בנוי, ומהם התפקידים של מערכת ההפעלה במחשב.

### מושגים והכוונה

- |                                  |      |                     |      |
|----------------------------------|------|---------------------|------|
| (write back) (4                  |      | מבנה מחשב           | .1   |
| פסיקה                            | .iii | א. רכיבים           |      |
| מימוש במחשב האמיתי               | .ג   | א. שעון             |      |
| CPU                              | .i   | א. זיכרון           |      |
| Instruction pointer              | .ii  | אוגרים (1           |      |
| מחסנית                           | .iii | RAM (2              |      |
| תפקידי מערכת ההפעלה              | .2   | פעולות אריתמטיות    | .iii |
| א. ניהול מערכת קבצים             | .א   | ב. מושגים נוספים    |      |
| ב. ניהול תהליכים וחוסים          | .ב   | א. קוד לעומת נתונים |      |
| ג. ניהול זיכרון וזיכרון וירטואלי | .ג   | א. מעגל ביצוע       |      |
| ד. ממשקים חיצוניים               | .ד   | fetch (1            |      |
| ה. ניהול משתמשים והרשאות         | .ה   | decode (2           |      |
|                                  |      | execute (3          |      |

### פרק 20: שירותי מערכת ההפעלה

מטרת הפרק: הכרת Windows API, הצגת הספריות המשותפות (DLL-ים) ופיתוח יכולות מחקריות ב-win32api.

### מושגים והכוונה

- |             |    |                |    |
|-------------|----|----------------|----|
| MessageBox  | .ד | קובץ הרצה      | .1 |
| socket      | .6 | PE             | .2 |
| send        | .א | DLL            | .3 |
| recv        | .ב | Export Table   | .4 |
| syscalls    | .7 | WinAPI         | .5 |
| kernel mode | .א | LoadLibrary    | .א |
| user mode   | .ב | GetProcAddress | .ב |
| MSDN        | .8 | ShellExecute   | .ג |

### פרק 21: תהליכים

מטרת הפרק: הבנת מהו תהליך במערכת ההפעלה ומהם המשאבים הקשורים אליו.

### מושגים והכוונה

- |   |    |                 |    |
|---|----|-----------------|----|
| ניהול תהליכים ו-Thread-ים ב-Windows (רשות):               | .4 | תהליך (Process) | .1 |
| א. ה- Process Control Block וה- Process Environment Block |    | Thread          | .2 |
|   |    | scheduler       | .3 |

ג. היררכיית ריצה של תהליכים  
ב. ה- Thread Environment Block וה- Thread Control Block.

### פרק 22: ניהול הזיכרון

מטרת הפרק: הבנה כיצד מערכת ההפעלה מאפשרת לתהליכים רבים להשתמש במשותף בזיכרון הדינאמי (RAM) של המחשב.

מושגים והכוונה

- |                     |                               |
|---------------------|-------------------------------|
| 1. זיכרון וירטואלי  | 5. page table                 |
| 2. flat memory      | 6. page file                  |
| 3. Page – דף זיכרון | 7. protected mode             |
| 4. page fault       | 8. memory mapped file (העשרה) |

### פרק 23: מחקר תהליכים ב- Windows

מטרת הפרק: הבנה וניתוח ניתוח תהליכים שקורים "מאחרי הקלעים" ב-Windows, פיתוח מיומנויות חקר פעילות זדונית לצורך אבטחת המערכות.

מושגים והכוונה

1. hooking

### פרק 24: ניהול משאבים והרשאות

מטרת הפרק: הכרת תהליך ניהול המשאבים שנעשה במערכת ההפעלה, זיהוי בעיות אבטחה נפוצות שנובעות משיתוף המשאבים, ודרכים להתמודד עמם.

מושגים והכוונה

- |                             |                              |
|-----------------------------|------------------------------|
| 1. משאבים משותפים ב-Windows | ג. תהליך וידוא ההרשאות       |
| ב. מערכת הקבצים             | ד. הרשאות משתמש, תהליך וקובץ |
| י. ספריות מערכת             | ה. ירושת הרשאות              |
| ii. (path) מיקום.           | ו. security token            |
| ג. Registry                 | 3. בעיות אבטחה נפוצות        |
| ד. Handle                   | א. Directory traversal       |
| ה. סקירת משאבים נוספים:     | ב. Temp directory            |
| ו. socket                   | ג. DLL Hijacking             |
| ז. חלון                     | י. סדר טעינת DLL-ים          |
| ח. התקני חומרה              | ד. Privilege Escalation      |
| 2. מערכת ההרשאות            | ה. Race Conditions           |
| א. Object manager           | ו. Security Domains          |
| ב. kernel mode              |                              |

### פרק 25: Windows כמערכת מוכוונת אירועים

מטרת הפרק: הבנת Event Driven programming והארכיטקטורה שעומדת מאחוריו.

מושגים והכוונה

- |                                   |                                |
|-----------------------------------|--------------------------------|
| 1. חלונות                         | ה. תור ההודעות                 |
| 2. הודעות                         | 4. אירועים שגורמים לקבלת הודעה |
| 3. מערכת ניתוב ההודעות ב-windowns | א. אירוע חומרה                 |
| א. Message Pool                   | ב. שליחת הודעה מתהליך אחר      |
| ב. Message Pump                   | ג. Windows Hooks               |
| ג. GetMessage                     | ד. Keyboard sniffer            |
| ד. DispatchMessage                | ה. SendMessage                 |



## חלק ה' - הגנת סייבר בעולם מורכב

### פרק 26: סיכום ההגנות הדרושות בעולם הסייבר

מטרת הפרק: לסכם את סוגי ההגנות והתקיפות שהכרנו במהלך לימודי המערך.

מושגים והכוונה

חזרה על מושגים מהמערך כולו.

### פרק 27: מבוא לקריפטוגרפיה (הצפנה)

מטרת הפרק: התלימיד יכיר את השימוש בקריפטוגרפיה כאבן יסוד בהגנת סייבר.

1. PKI
2. להסביר את מודל PKI – מפתחות פרטים ומפתחות ציבוריים, RSA.
3. בתיאור מודל PKI כדאי לספר על חלקו של Shamir ב- RSA.
4. בתיאור PKI לא כדאי להכנס לפרטים המתמטיים אלא את הרעיונות ותוצאותיהן.

מושגים והכוונה

- |                                    |                               |
|------------------------------------|-------------------------------|
| 1. צופן סימטרי                     | 6. (Certificate Authority) CA |
| 2. בעיית תיאום המפתחות             | 7. חתימה דיגיטלית             |
| 3. צופן א-סימטרי                   | 8. Challenge Response         |
| 4. פונקצית Hash                    | 9. SSL                        |
| 5. (Public Key Infrastructure) PKI | 10. Kerberos                  |

### פרק 28: הגורם האנושי

מטרת הפרק: להבין את גבולות ההגנות המובנות מול טעויות אנוש.

מושגים והכוונה

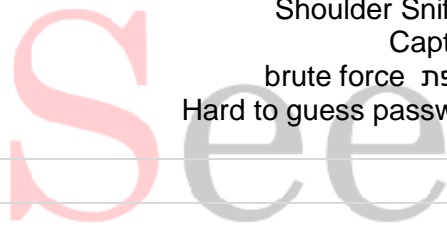
- |                       |                           |
|-----------------------|---------------------------|
| 1. Bugs               | 5. Shoulder Sniffing      |
| 2. Phishing           | 6. Captcha                |
| 3. Spam Mail          | 7. תקיפת brute force      |
| 4. Social Engineering | 8. Hard to guess password |

### פרק 29: ניתוח מקרה תקיפה

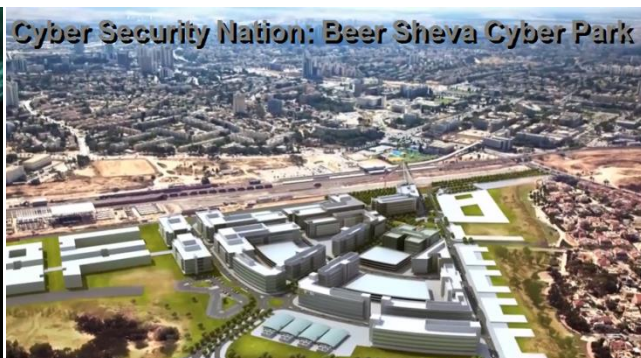
מטרת הפרק: להבין לעומק מקרה תקיפה מורכב.

מושגים והכוונה

חזרה על מושגים מהמערך כולו.



see security technologies ltd  
InfoSec & Cyber Warfare College



לכבוד  
המכללה לאבטחת מידע וללוחמת מידע  
שיא סקויריטי טכנולוגיז בע"מ  
רמת-גן – פקס : 03-6122593

**נא לרשום אותי לתוכנית הלימודים במכללת Cyber7 בבאר שבע**  
**קורס Cyber16+**

**פרטים אישיים:**

שם משפחה \_\_\_\_\_ שם פרטי \_\_\_\_\_ ת.ז. \_\_\_\_\_ שנת לידה \_\_\_\_\_  
כתובת פרטית \_\_\_\_\_  
טל' בבית: \_\_\_\_\_ טל' נייד \_\_\_\_\_ פקס \_\_\_\_\_  
כתובת E-mail \_\_\_\_\_

**מקום עבודה:**

שם החברה \_\_\_\_\_ טל' \_\_\_\_\_ תפקיד \_\_\_\_\_

**לתשלום (נא סמן בחירתך):**

- 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 סקויריטי 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 המכון וSee Security.
- דמי ההרשמה אינם כלולים בשכר הלימוד.
- יש לוודא כי התשלומים יסתיימו עד למועד סיום הקורס.

תאריך: \_\_\_\_\_ חתימה: \_\_\_\_\_

שיא א. סקויריטי טכנולוגיז בע"מ	ח.פ: 513431403	ספק משהב"ט: 83/168200
--------------------------------	----------------	-----------------------