תוכנית Cyber +16

יועץ אקדמי: מר אבי ויסמן *

קורס טכניקות תקיפה לבעלי רקע בפיתוח או רקע בתשתיות טכנולוגיות

אודות התוכנית

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 הגיאו-חברתית. 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.

מאפייני תוכנית הלימודים	
קהל:	מנהלים / סביבתיים / **מקצוענים**
אוריינטציה:	מנהלית/ **טכנית** / **יישום**
שלב:	**מתחילים** / **מתקדמים**
רוחב:	ממוקד / **רחב**
עומק:	סוקר / **עמוק**
הסמכות:	**Hacking Defined Experts**
שעות:	**467 שעות**
פתיחה:	**פעם בחודש**
מתכונת:	**92 מפגשי ערב, כ-13 חודשים**
תרגול בית:	**בהיקף 700 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 System, Network, Mobile, 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 הבגרות המתקיימות בבתי הספר התיכוניים במקביל.

תעודות

- קיימת חובת נוכחות ב-80% מהמפגשים, ועמידה במבחנים/עבודות, בציון 70.
- תיעוד: לעומדים בדרישות התכנית תוענק תעודת הסמכה מטעם See Security:
- **Cyber Security Preparation Program Certification**
- **SOC Analyst Certification**
- **Hacking Defined Experts Certification**

הכרה

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

תובל 30, רמת-גן – 5252242, טל': 03-6122831, 03-5799555, 054-5222305, פקס: 03-6122593
www.see-security.com avi@see-security.com

אודות המכללה

מכללת See-Security הינה מוסד לימודים ייעודי לתחום אבטחת מידע, לוחמת סייבר ותשתיות, היחידה בישראל, ייחודית ברחבי העולם, אשר עוסקת בלעדית רק באבטחת מידע וסייבר, 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 מופַרים, ולעיתים - בכירים מאוד בענף הסייבר בישראל.

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

מבואות הסייבר ו-SOC: 18,500₪ שכר לימוד + 400 ₪ דמי רישום.

Hacking Defined Experts: סה"כ 10,500 ₪ .

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.

פרק 1': מבוא להגנת סייבר

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

מושגים והכוונה

1. מחשב אישי
2. שרת
3. מערכת משובצת
4. רשת
5. רשת פנימית
6. DoS/DDoS
7. נוזקה (Malware)
8. סוס טרויאני (Trojan Horse).
9. תולעת מחשבים (Computer Worm)
10. וירוס מחשבים (Computer Virus)
11. Adware
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
2. Script Kids
3. White Hat
4. Black Hat
5. VPN – Virtual Private Network
6. חומת אש Firewall
7. חומת אש לאפליקציות Web – WAF Application Firewall
8. Antivirus
9. Black Box Scanner
10. White Source Code Analysis – BoxScanner

פרק 3: מבוא לתוכנית הלימודים

מטרת הפרק: הבנת תכולת הלימודים במקצוע.

מושגים והכוונה

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

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
2. תווך תקשורת
3. תקשורת קווית
4. תקשורת אלחוטית
5. תת מערכות תקשורת וחיבוריות ביניהם (רשת ביתית, הרשת הגלובלית)
6. כתובת וניתוב
7. פרוטוקול תקשורת
8. טופולוגיות תקשורת
9. תקשורת סינכרונית/אסינכרונית
10. קצב שידור
11. אפנון
12. ריבוב
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
2. פרוטוקול
3. תקן
1. כימוס (Encapsulation)
2. Protocol Tunneling
3. השכבה הפיזית (Physical Layer)
4. שכבת הקו (Data Link Layer)
5. שכבת הרשת (Network Layer)
6. שכבת התעבורה (Transport Layer)
1. שכבת ניהול השיחה (Session Layer)
7. שכבת התצוגה (Presentation Layer)
8. שכבת האפליקציה (Application Layer)
9. תקורה (Overhead)

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

פרק 7: טכנולוגיות LAN (Local Area Network)

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

מושגים והכוונה

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

פרק 8: יסודות רכיבי תקשורת

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

מושגים והכוונה

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

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

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

פרק 11: תכנות ב-Soket-ים

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

מושגים והכוונה

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

פרק 12: אבטחת מידע בפרוטוקולי TCP/IP

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

מושגים והכוונה

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

פרק 13: scapy

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

מושגים והכוונה

1. Python
   א. list
   ב. dict
   ג. גישה לשדות
   ד. list comprehensions
2. scapy
   א. פרוטוקולים: IP, TCP, ARP, Ether, DNS, ICMP
   ב. פקודות : lsc, ls, hexdump, rdpcap, 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)
2. DNS (Domain Name System)
3. TLD (Top-Level Domains)
4. Zone Transfer
5. SMTP (Simple Mail Transfer Protocol)
6. SMTP spoofing

פרק 15: תרגיל סיכום

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

מושגים והכוונה

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

חלק ג' - הגנת אפליקציות (בדגש Web)

פרק 16: מבוא לאפליקציות Web

(לאלו 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
2. JavaScript
3. Ajax
4. Client-Server
5. Cache

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)
2. Credentials
3. Session
4. Cookies
5. Same Origin Policy
6. Cross Site Scripting

פרק 18: SQL Injection

מטרת הפרק: התלמיד יכיר תקיפת SQL Injection והגנה מפניה.

מושגים והכוונה

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

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

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

פרק 20: שירותי מערכת ההפעלה

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

מושגים והכוונה

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

פרק 21: תהליכים

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

מושגים והכוונה

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

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

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

פרק 23: מחקר תהליכים ב- Windows

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

see security technologies ltd
InfoSec & Cyber Warfare College

פרק 25: Windows כמערכת מוכוונת אירועים

מטרת הפרק: הבנת Event Driven programming והארכיטקטורה שעומדת מאחוריו.

מושגים והכוונה

1. חלונות
2. הודעות
3. מערכת ניתוב ההודעות ב-windows
   - א. Message Pool
   - ב. Message Pump
   - ג. GetMessage
   - ד. DispatchMessage
   - ה. תור ההודעות
4. אירועים שגורמים לקבלת הודעה
   - א. אירוע חומרה
   - ב. שליחת הודעה מתהליך אחר
   - ג. Windows Hooks
   - ד. Keyboard sniffer
   - 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: התלמיד 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
2. בעיית תיאום המפתחות
3. צופן א-סימטרי
4. פונקצית Hash
5. PKI (Public Key Infrastructure)
6. CA (Certificate Authority)
7. חתימה דיגיטלית
8. Challenge Response
9. SSL
10. Kerberos

פרק 28: הגורם האנושי

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

מושגים והכוונה

1. Bugs
2. Phishing
3. Spam Mail
4. Social Engineering
5. Shoulder Sniffing
6. Captcha
7. brute force תקיפת
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