



סילבוס



קורס סייבר האקינג

פרטי הקורס

תיאור הקורס

קורס זה מעמיק אל תוך החשיבה של האקרים זדוניים כדי לספק ללומדים בו הבנה מעמיקה לגבי האופן שבו חושבים האקרים מסוג כובעים שחורים. על ידי הבנת הסוגים השונים של השיטות והאסטרטגיות של התקפות האקרים, אנשי מקצוע בתחום אבטחת הסייבר יכולים לנצח אותם במשחק שלהם, ולהקדים תרופה למכה בהגנה מפני האיומים הקרבים. התלמידים יגלו כיצד לבצע ולהגן מפני מגוון מתקפות סייבר, כולל התקפות הנדסה חברתית, התקפות רשת, התקפות אפליקטיביות והתקפות קריפטוגרפיות. מעבודות מעשיות מספקות ללומדים את הכלים, הידע והמיומנויות הנדרשות כדי לגלות ולנצל את נקודות התורפה של המערכת.

יעדי הלמידה

- פיתוח כישורי סיור ועקיפה של מערכות הגנה שונות.
- אנומרציה של ארגונים וניצול שירותים ופורטים.
- פיתוח מיומנויות דיווח ייחודיות לענף, הכלולות המלצות הגנה, לאחר בדיקת חדירות.
- הרצת מתקפת העלאת הרשאות (רמת הרשאות גבוהה) במערכת הפעלה באמצעות שיטות מתקדמות כדי להפוך למנהל מערכת.
- להשתלט על אתרים, פלטפורמות אינטרנט ושרתי המארח שלהם.
- שימוש בטכניקות חדירה של יישומי אינטרנט כדי לגלות נקודות תורפה במערכות מבוססות ענן.

דרישות

דרישות השלמת הקורס

- שלמת הפרויקט המסכם
- שלמת המבחן המסכם בציון של 70% או יותר
- נוכחות ב-80% מהשיעורים לפחות

החומר הלימודי של הקורס

(זמין במערכת ניהול הלמידה)

החומר מכיל כמות לא מבוטלת של מידע שיש ללמוד. הלומדים נדרשים לעקוב אחר החומר הנלמד בכיתה ומצופה מהם לסקור מצגות ואת ספר הלימוד גם מחוץ לכותלי הכיתה. ספר הלימוד מכיל הפניות לחומרים חיצוניים והפניות למטלות מעבדה ספציפיות, המאפשרות לסטודנטים לבצע מטלות בבית, בזמן סקירת החומר בספר הלימוד.

חומרה

כדי להשלים את הקורס, הסטודנטים צריכים שיהיה ברשותם מחשב נייד עם דרישות המינימום הבאות:

- GB RAM 16
- GB HDD 256
- מעבד i5 core או גבוה יותר

תוכנה

כדי להשלים את הקורס, הסטודנטים צריכים שיהיו ברשותם את הבאים:

- Oracle VirtualBox 6 או גרסה מאוחרת יותר
- עורך טקסט (Word, OpenOffice, אחר)

תוכן הקורס

מספר שיעור	שם השיעור	נושאי השיעור	מעבדות
מבוא והכירות			
1	מבוא להאקינג	<ul style="list-style-type: none"> הכרות עם המדריך, תיאום ציפיות האקרים תוכנה זדונית 	<ul style="list-style-type: none"> מעבדה 1 - מחקר
2	מחזור מתקפת סייבר	<ul style="list-style-type: none"> השלבים בהתקפת סייבר החל מאיסוף מודיעין ועד מימוש ההתקפה. 	<ul style="list-style-type: none"> אין
יישור קו טכנולוגי - הקמת סביבת מעבדה			
3	יסודות הוירטואליזציה	<ul style="list-style-type: none"> התקנת VirtualBox 	<ul style="list-style-type: none"> מעבדה 1-התקנת VirtualBox
4	מערכת הפעלה ווינדוס	<ul style="list-style-type: none"> יצירת מכונה וירטואלית תרגול 	<ul style="list-style-type: none"> מעבדה 1- וירטואליזציה ב-Windows 10 מעבדה 2- תרגול CMD מעבדה 3- סוגי מתאמי רשת VirtualBox
5	מערכת הפעלה לינוקס	<ul style="list-style-type: none"> יצירת מכונה וירטואלית 	<ul style="list-style-type: none"> מעבדה 1- התקנת Kali Linux
התקפות תקשורת ורשת			
6	יסודות התקשורת	<ul style="list-style-type: none"> מבוא לרשתות יצירת כתובות רשת 	<ul style="list-style-type: none"> מעבדה 1- לוח קונפיגורציות רשת מעבדה 2- יצירת כתובות IP
7	פרוטוקולי תקשורת נתונים	<ul style="list-style-type: none"> נתבים ומתגים פרוטוקולים ותקשורת 	<ul style="list-style-type: none"> מעבדה 1- תרגול Ping ו-Traceroute
8	סריקת רשת	<ul style="list-style-type: none"> הגדרת רשת, סריקה סקירת Nmap סוגי סריקת Nmap 	<ul style="list-style-type: none"> מעבדה 1 - investigate the network מעבדה 2 - Scanning using Masscan מעבדה 3 - Zenmap Network Scanning מעבדה 4 - Python ARP Scanner

9	כלים לסריקת רשת	<ul style="list-style-type: none"> כלים נוספים 	אין
10	הכנה להתקפת MITM	<ul style="list-style-type: none"> MITM pfsense 	<ul style="list-style-type: none"> מעבדה 1 - Encrypt Decrypt Hashes
11	הרעלות - Poisoning	<ul style="list-style-type: none"> הרעלת ARP הרעלת DNS 	<ul style="list-style-type: none"> מעבדה 1 - Arp Spoofing מעבדה 2 - Bettercap DNS Poisoning
12	גניבת פורטים	<ul style="list-style-type: none"> גניבת פורט הפשטת SSL 	<ul style="list-style-type: none"> מעבדה 1 - SSL Strip
13	סייבר גיימינג – שיעור פתיחה והיכרות	<ul style="list-style-type: none"> הסבר על הפלטפורמה התקנת סביבה 	<ul style="list-style-type: none"> אתגר Basic HTML
התקפות הנדסה חברתית			
14	הנדסה חברתית	<ul style="list-style-type: none"> הנדסה חברתית (SE), כיצד ניתן לבצע אותה ואיך להתגונן מפני סוג זה של מתקפה. 	אין
15	פריצת סיסמאות	<ul style="list-style-type: none"> אתגרי פריצת סיסמאות באמצעות קוד מקור 	<ul style="list-style-type: none"> אתגרי פריצה מקוונים
16	עוגיות	<ul style="list-style-type: none"> עוגיות ונתוני אתרים 	<ul style="list-style-type: none"> פריצת משחק Cookie Clicker
17	התקפת Brute-Force	<ul style="list-style-type: none"> הצגת כלים לפיצוח סיסמאות וכיצד משתמשים בהם, בנוסף להגנות שונות נגדן 	<ul style="list-style-type: none"> מעבדה 1 - Encrypt Decrypt Hashes
18	פיצוח סיסמאות	<ul style="list-style-type: none"> פיצוח סיסמאות לא מקוון מתקפות סיסמה מקוונות 	<ul style="list-style-type: none"> מעבדה 1 - Rar and Hash Cracking מעבדה 2 - Brute Force Attacks
19	ערכת הכלים של מתקפות הנדסה חברתית	<ul style="list-style-type: none"> ערכת הכלים של מתקפות הנדסה חברתית כלים נוספים של הנדסה חברתית (SE) 	<ul style="list-style-type: none"> מעבדה 1 - SSL Strip מעבדה 2 - SFX Implementation
	סייבר גיימינג		<ul style="list-style-type: none"> אתגר Dictionary attack
התקפות תשתית ומערכות הפעלה			
20	מתקפות תשתיות	<ul style="list-style-type: none"> MetaSploit 	<ul style="list-style-type: none"> מעבדה 1 - SearchSploit מעבדה 2 - MetaSploit
21	הפיכת מעטפת	<ul style="list-style-type: none"> הפיכת מעטפת (Reverse Shell) 	<ul style="list-style-type: none"> מעבדה 1 - Metasploit Trojan
22	תנועה צדדית	<ul style="list-style-type: none"> Lateral Movement 	<ul style="list-style-type: none"> מעבדה 1 - EternalBlue

<ul style="list-style-type: none"> • מעבדה 1 - Windows Privilage Escalation • מעבדה 2 - Hiding The user • מעבדה 3 - Windows 10 Local PE 	<ul style="list-style-type: none"> • העלאת הרשאות ב-Windows • טכניקות מניעה 	<ul style="list-style-type: none"> • העלאת הרשאות ב-Windows 	23
<ul style="list-style-type: none"> • מעבדה 1 - Linux Local PE and Mitigation • מעבדה 2 - Linux Remote PE 	<ul style="list-style-type: none"> • PE מקומי ב-Linux • PE מרחוק ב-Linux 	<ul style="list-style-type: none"> • העלאת הרשאות ב-Linux 	24
התקפות אפליקטיביות			
<ul style="list-style-type: none"> • מעבדה 1 - Personal HTTP Server 	<ul style="list-style-type: none"> • התקפות אפליקטיביות • OWASP • הבנת טכנולוגיות רשת 	<ul style="list-style-type: none"> • התקפות אפליקטיביות 	25
<ul style="list-style-type: none"> • מעבדה 1 - Intercept and Access 	<ul style="list-style-type: none"> • פרוקסי אפליקטיבי • Burp Suit 	<ul style="list-style-type: none"> • פרוקסי אפליקטיבי • ובלי יירוט • אפליקטיביים 	26
<ul style="list-style-type: none"> • מעבדה 1 - Cross Site Scripting 	<ul style="list-style-type: none"> • שפות אינטרנט בצד הלקוח • Cross Site Scriptin • חטיפת הפעלה • צמצום XSS 	<ul style="list-style-type: none"> • התקפת XSS 	27
<ul style="list-style-type: none"> • אתגר 1 - Parameter tampering 		<ul style="list-style-type: none"> • סייבר גיימינג 	
<ul style="list-style-type: none"> • מעבדה 1 - Cross Site Scripting • מעבדה 2 - Local File Inclusion • מעבדה 3 - LFI within a PDF 	<ul style="list-style-type: none"> • התקפות של יישומי אינטרנט • בשיטת הכללת קבצים • מקומיים 	<ul style="list-style-type: none"> • הכללת קובץ מקומי 	28
<ul style="list-style-type: none"> • מעבדה 1 - Building a Database 	<ul style="list-style-type: none"> • יצירת מסד נתונים SQL • וקטורי התקפה נפוצים 	<ul style="list-style-type: none"> • מבוא למסדי נתונים 	29
<ul style="list-style-type: none"> • מעבדה 1 - SQLI Injection 	<ul style="list-style-type: none"> • SQL Injection 	<ul style="list-style-type: none"> • הזרקת SQL 	30
<ul style="list-style-type: none"> • אתגר SQL Injection 		<ul style="list-style-type: none"> • סייבר גיימינג 	
פרוייקט גמר וסיכום			
<ul style="list-style-type: none"> • אין 	<ul style="list-style-type: none"> • סקירת הבחינה 	<ul style="list-style-type: none"> • סיכום הקורס והבנה למבחן 	31
<ul style="list-style-type: none"> • מעבדה 1 - Final Project 	<ul style="list-style-type: none"> • תרחיש פרויקט גמר • פריסת סביבה • שלבי הפרוייקט 	<ul style="list-style-type: none"> • פרויקט גמר - האקינג 	32

חומר אקסטרה להעשרה			
	<ul style="list-style-type: none"> מבוא לאבטחת רשת ונקודת קצה תקלות וסיכונים 	אבטחת נקודת קצה	
<ul style="list-style-type: none"> עקיפת אנטי-וירוס 	<ul style="list-style-type: none"> רכיבים של אבטחת נקודת קצה איתור ותגובה של נקודת קצה מבוא ל-ClamAV 	רכיבי אבטחה לנקודות קצה	
<ul style="list-style-type: none"> יצירת כללי YARA 	<ul style="list-style-type: none"> מבוא לאבטחת רשת ונקודת קצה כללי YARA וחתימות 	חתימות וכללי YARA	
<ul style="list-style-type: none"> יצירת מסד נתונים לרשימת היתרים (Whitelist) 	<ul style="list-style-type: none"> מבוא לאבטחת רשת ונקודת קצה מסדי נתונים של רשימות היתרים 	יצירת מסדי נתונים ל-AV	
<ul style="list-style-type: none"> הצבת מלכודת דבש הגדרת רשת דבש מודרנית (MHN) 	<ul style="list-style-type: none"> מבוא למלכודות דבש אסטרטגיית מלכודת דבש Honeytokens מוצרי מלכודת דבש (HoneyPot) 	מלכודות דבש (Honeypots)	
<ul style="list-style-type: none"> פריסת מלכודת דבש Valhala 	<ul style="list-style-type: none"> מבוא למלכודות דבש מלכודת הדבש Valhala התחמקות 	מלכודת הדבש Valhala	
<ul style="list-style-type: none"> מקרה שימוש בדליפת נתונים תרגול ביטוי רגיל (Regex) 	<ul style="list-style-type: none"> מידע רגיש ערוצי הדלפת נתונים ביטויים שגורים 	מניעת אובדן נתונים	
<ul style="list-style-type: none"> התקנת OpenDLP מעקף DLP 	<ul style="list-style-type: none"> מבוא ל-DLP OpenDLP שיטות לעקוף DLP 	DLP	
<ul style="list-style-type: none"> nslookup תרגול פקודות POP3 	<ul style="list-style-type: none"> מבוא ל-DNS פרוטוקולים של דואר 	מבוא ל DNS ודוא"ל	
<ul style="list-style-type: none"> זיוף בדוא"ל 	<ul style="list-style-type: none"> הגנת DNS לדוא"ל כותרות דוא"ל מבוא לממסר דוא"ל מושגי ממסר דוא"ל מאפייני ממסר דוא"ל 	אבטחת דוא"ל	