



סילבוס



קורס סייבר באטל רויאל

Cyber Battle Royale

פרטי הקורס

תיאור הקורס

זהו קורס מבוא לעולם הסייבר. הקורס מעניק נקודת פתיחה לעולם הסייבר, דרך למידה של מושגי מחשוב, רשתות ואבטחת מידע, וכיצד הם מתייחסים לעולם המודרני שלנו. השיעורים מציגים בפניכם את יסודות הרשת והפעילות בה, מערכות ההפעלה Linux ו-Windows ומושגי וירטואליזציה. תלמדו גם כיצד להריץ פקודות בסיסיות ופרוטוקולי תקשורת מחשבים, תפתחו הבנה מוצקה של מבני מערכת ההפעלה הבסיסיים ותלמדו על המחזור של התקפת סייבר. גישת החינוך החווייתי לאורך כל הקורס מספקת תרגול מעשי כדי לאפשר להבין טוב יותר את אמצעי הנגד של אבטחת הסייבר וטכניקות ההגנה. הקורס גם נוגע בעולם של הכלים והטכנולוגיות להגנה על מגוון סוגי ארגונים.

יעדי הלמידה

- ללמוד אודות פריצות ידועות ותוצאותיהן.
- ללמוד על הגישה ברשת האינטרנט: כתובות, דומיין ו-Proxy.
- להשתמש במיומנויות ושיטות חיפוש כדי לאתר מידע.
- ללמוד על אתיקה ופרטיות ברשת.
- ללמוד על רכיבי החומרה והתוכנה במערכת של מחשב Windows.
- ללמוד על טכניקות העלאת הרשאות בלינוקס ו-Windows.
- לסקור ולנתח מגוון ספקי שירות מודעות ואת השירותים שהם מציעים.
- לזהות רכיבי רשת ופרוטוקולים של רשתות.
- להבין את רכיבי התוכנה של מערכת ההפעלה Linux.
- לזהות נקודות תורפה של מחשבים ורשתות.
- ללמוד על הצפנה והסתרת מידע באינטרנט, ועל גיבוב (Hash).
- ללמוד על מחזור מתקפת סייבר ועל תפקידו במתקפות סייבר.
- לנתח תעבורת רשתות ושימוש ב-Wireshark.
- להבין את רכיבי אבטחה לנקודות קצה.

דרישות

דרישות השלמת הקורס:

➤ השלמת המבחן המסכם בציון של 70% או יותר

➤ נוכחות של 80% ומעלה בשיעורים

החומר הלימודי של הקורס (זמין במערכת ניהול הלמידה)

החומר מכיל כמות לא מבוטלת של מידע שהתלמידים צריכים ללמוד. סטודנטים נדרשים לעקוב אחר החומר הנלמד בכיתה ומצופה מהם לחזור על מצגות ועל ספר הלימוד גם מחוץ לכותלי הכיתה. ספר הלימוד מכיל הפניות לחומרים חיצוניים והפניות למטלות מעבדה ספציפיות, המאפשרות לתלמידים לבצע מטלות בבית.

דרישות חומרה

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

➤ RAM 16GB ומעלה

➤ 50GB זיכרון פנוי בדיסק הקשיח

➤ מעבד i5 core או גבוה יותר

דרישות תוכנה

כדי להשלים את הקורס, סטודנטים צריכים שיהיה ברשותם את הכלים הבאים:

➤ עורך טקסט (Word, OpenOffice, אחר)

➤ דפדפן רשת (IE, Chrome)

חלוקת שיעורי הקורס:

מודול	שם המודול	נושא	מעבדות
מבוא והכירות			
1	שיעור פתיחה	<ul style="list-style-type: none"> הצגה עצמית נושאי הקורס הדגמת פריצה למשחק 2048 	<ul style="list-style-type: none"> פריצת משחק 2048
2	עקרונות הגנת סייבר	<ul style="list-style-type: none"> עקרונות אבטחת הסייבר שיטות הגנה באבטחת סייבר 	<ul style="list-style-type: none"> תכנון בסיסי של DiD
מחקר סייבר			
3	מחקר סייבר באינטרנט	<ul style="list-style-type: none"> מה נדרש כדי להצליח? האינטרנט כמקור מידע 	<ul style="list-style-type: none"> חיפוש מסווג ב-Google
4	הסוואה וגישה	<ul style="list-style-type: none"> דומיין, כתובת IP מה אתרים יודעים עלינו Proxy, גלישה בסתר, Captcha, ארכיון 	<ul style="list-style-type: none"> תרגול שימוש בארכיון האינטרנט מציאת מיקום כתובות IP
5	מחקר נקודות תורפה (CVE)	<ul style="list-style-type: none"> מחקר נקודות תורפה (CVE) 	<ul style="list-style-type: none"> אין
6	אתיקה ופרטיות	<ul style="list-style-type: none"> אתיקה ומוסר ברשת פרטיות ברשת דרכים לשמירה על הפרטיות 	<ul style="list-style-type: none"> אימות דו שלבי
7	שפה זרה	<ul style="list-style-type: none"> האתגר בתרגום ותרגום מכונה Google Translate, מורפיקס מקלדת וירטואלית לשפות זרות 	<ul style="list-style-type: none"> פענוח מסר זר
8	דרכי חשיבה במידענות	<ul style="list-style-type: none"> חשיבה מידענית מחקר אינטרנטי 	<ul style="list-style-type: none"> תרגול חיפוש מידעני

9	מודיעין סייבר	<ul style="list-style-type: none"> סוגי המודיעין מודיעין תקיפה והגנה 	<ul style="list-style-type: none"> תרגול איסוף מודיעין
יישור קו טכנולוגי - תקשורת נתונים, וירטואליזציה ומערכות הפעלה			
10	יסודות התקשורת	<ul style="list-style-type: none"> מבוא לרשתות יצירת כתובות רשת 	<ul style="list-style-type: none"> לוח קונפיגורציית רשת יצירת כתובות IP
11	פרוטוקולי תקשורת נתונים	<ul style="list-style-type: none"> נתבים ומתגים פרוטוקולים ותקשורת 	<ul style="list-style-type: none"> תרגול Ping ו-Traceroute
12	יסודות הוירטואליזציה	<ul style="list-style-type: none"> יסודות הוירטואליזציה 	<ul style="list-style-type: none"> התקנת VirtualBox
13	מערכת הפעלה חלונות (Windows)	<ul style="list-style-type: none"> מחשבים - חומרה ותוכנה יסודות מערכת ההפעלה Window 	<ul style="list-style-type: none"> וירטואליזציה ב-Windows 10 תרגול CMD סוגי מתאמי רשת VirtualBox
14	העלאת הרשאות ב-Windows	<ul style="list-style-type: none"> הרשאות Windows Windows Local PE Post Exploitation 	<ul style="list-style-type: none"> העלאת הרשאות מקומית עם קובץ ISO הצפנת כונן
15	מבוא למערכת ההפעלה לינוקס	<ul style="list-style-type: none"> מבוא המבנה של מערכת ההפעלה Linux 	<ul style="list-style-type: none"> התקנת Kali Linux
16	ניווט ופקודות בלינוקס	<ul style="list-style-type: none"> ניווט ומניפולציית תוכן 	<ul style="list-style-type: none"> מסוף Linux
17	העלאת הרשאות בלינוקס	<ul style="list-style-type: none"> תהליך האתחול עריכת GRUB 	<ul style="list-style-type: none"> העלאת הרשאות מקומית הצפנת GRUB
בטיחות ברשת			
18	משתמשים פיקטיביים	<ul style="list-style-type: none"> זיהוי משתמשים פיקטיביים ההשפעות על הרשת 	<ul style="list-style-type: none"> תרגול פתיחה ותחזוקה – משתמש פיקטיבי

<ul style="list-style-type: none"> • זיהוי וירוס באמצעות VirusTotal • תרגול הזרקת SQL 	<ul style="list-style-type: none"> • מהי נזקה, סוגי נזקות • אנטי וירוס, VirusTotal • תקיפות רשת 	<ul style="list-style-type: none"> • וירוסים ואיומים ברשת 	19
<ul style="list-style-type: none"> • תרגול הרשאות יישומים 	<ul style="list-style-type: none"> • בריונות ושיימינג • סוגי הפגיעה השונים • כלים להתמודדות 	<ul style="list-style-type: none"> • גלישה בטוחה 	20
סייבר התקפי			
<ul style="list-style-type: none"> • תרגול MITM 	<ul style="list-style-type: none"> • מונחים ומושגים • On-Path 	<ul style="list-style-type: none"> • התקפת תקשורת - On-Path 	21
<ul style="list-style-type: none"> • Apache DoS • הרצת Dos 	<ul style="list-style-type: none"> • מונחים ומושגים • DoS/DDoS 	<ul style="list-style-type: none"> • התקפת תקשורת - DoS/DDoS 	22
<ul style="list-style-type: none"> • חילוץ סיסמת WPA2 Handshake 	<ul style="list-style-type: none"> • מונחים ומושגים • מתקפות אלחוטיות 	<ul style="list-style-type: none"> • התקפות תקשורת - רשת אלחוטית 	23
<ul style="list-style-type: none"> • Reconnaissance (סיור) מערכת 	<ul style="list-style-type: none"> • Cyber Kill Chain • Reconnaissance (איסוף מידע) 	<ul style="list-style-type: none"> • מחזור התקפת סייבר - איסוף מודיעין טכני 	24
<ul style="list-style-type: none"> • התחמשות עם Crunch 	<ul style="list-style-type: none"> • Cyber Kill Chain • Weaponization (התחמשות) 	<ul style="list-style-type: none"> • מחזור התקפת סייבר - התחמשות 	25
<ul style="list-style-type: none"> • פשינג ושכפול אתר 	<ul style="list-style-type: none"> • Cyber Kill Chain • Delivery (העברה) • Exploitation (ניצול) 	<ul style="list-style-type: none"> • מחזור התקפת סייבר - העברה וניצול פגיעויות 	26
<ul style="list-style-type: none"> • תרגול אתגרי פריצת סיסמאות 	<ul style="list-style-type: none"> • פרצות אבטחה • קובץ מקור 	<ul style="list-style-type: none"> • פריצת סיסמאות 	27
<ul style="list-style-type: none"> • Cookie clicker – פריצה לנתוני עוגיות על ידי שימוש בקונסולה 	<ul style="list-style-type: none"> • מהן עוגיות (Cookies) • שמירה ואחזור מידע, נתוני אתרים 	<ul style="list-style-type: none"> • עוגיות 	28

29	סייבר גיימינג	<ul style="list-style-type: none"> הכירות עם הפלטפורמה 	<ul style="list-style-type: none"> התקנת סביבה 2 אתגרים ראשונים
סייבר הגנתי			
30	אמצעי נגד והגנה	<ul style="list-style-type: none"> הגנה - סקירה כללית מקרה בוחן: NotPetya הגנות מתקפות סייבר 	<ul style="list-style-type: none"> זיהוי תוכנה זדונית חסימת גלשיה ברשת קטגוריות בקרה
31	גיבוב HASH	<ul style="list-style-type: none"> מושגים בהצפנה אלגוריתמים לפונקציית גיבוב 	<ul style="list-style-type: none"> Base64 Manual Encoding Rainbow Table
32	הצפנה	<ul style="list-style-type: none"> הצפנה חתימות דיגיטליות ותעודות אבטחה (certificates) 	<ul style="list-style-type: none"> Encryption Games
33	התקנת Wireshark	<ul style="list-style-type: none"> Wireshark למתקדמים 	<ul style="list-style-type: none"> Installing Wireshark
34	שימוש ויישום ב Wireshark	<ul style="list-style-type: none"> סטטיסטיקות Wireshark חילוץ קבצים 	<ul style="list-style-type: none"> Advanced Analysis Extracting Files
35	ניתוח תעבורה ברשת	<ul style="list-style-type: none"> Network Miner Network Monitor 	<ul style="list-style-type: none"> Network Monitor
36	חומת אש (Firewall)	<ul style="list-style-type: none"> מבוא ל-Firewall pfSense 	<ul style="list-style-type: none"> Pass or Block pfSense Installation
37	הגנת רשת עם FW	<ul style="list-style-type: none"> סוגי Firewal תכונות נוספות של Firewalls 	<ul style="list-style-type: none"> pfSense Rule Port Forwarding
טכנולוגיות אבטחת מידע וסייבר			
38	וירוס VBS	<ul style="list-style-type: none"> מערכת הפעלה שפת התכנות VBS 	<ul style="list-style-type: none"> בניית וירוס
39	אבטחת נקודת קצה	<ul style="list-style-type: none"> מבוא לאבטחת רשת ונקודת קצה תקלות וסיכונים 	<ul style="list-style-type: none"> Bypassing an Antivirus Application

Update ClamAV Signature Database	<ul style="list-style-type: none"> רכיבים של אבטחת נקודת קצה איתור ותגובה של נקודת קצה מבוא ל-ClamAV 	רכיבי אבטחה לנקודות קצה	40
Creating YARA Rules	<ul style="list-style-type: none"> מבוא לאבטחת רשת ונקודת קצה כללי YARA וחתימות 	חתימות וכללי YARA	41
Create a Whitelist Database	<ul style="list-style-type: none"> מבוא לאבטחת רשת ונקודת קצה מסדי נתונים של רשימות היתרים 	יצירת מסדי נתונים ל-AV	42
Searching Shodan Mirai Botnet Research	<ul style="list-style-type: none"> מבוא ל-IoT-האינטרנט של דברים סיכונים פוטנציאליים אבטחת IoT 	IoT - האינטרנט של הדברים	43
Stuxnet Worm Research Analyzing Firmware	<ul style="list-style-type: none"> מערכות בקרה תעשייתיות קושחה 	ICS - מערכות בקרה תעשייתיות	44
מבחן סיכום	<ul style="list-style-type: none"> תרגול וחזרה על החומר 	תרגול וחזרה על החומר	45
חומר אקסטרה להעשרה			
NW Investigator Challenge	<ul style="list-style-type: none"> Deep Packet Inspection Protocol Analyzer NW Investigator 	ניתוח עמוק של תעבורת רשת (DPI)	
Suricata Installation	<ul style="list-style-type: none"> גילוי ומניעת חדירות פתרונות נפוצים 	גילוי ומניעת חדירות לרשת	
IP Investigation Anomaly Detection	<ul style="list-style-type: none"> שיטות לגילוי עבודה עם IDS ו-IPS תפקיד האנליסטים 	כלי IDS ו-IPS	

<ul style="list-style-type: none"> • Regular Expression • Data Leak Use Case 	<ul style="list-style-type: none"> • מידע רגיש • ערוצי הדלפת נתונים • ביטויים שגורים 	מניעת אובדן נתונים	
<ul style="list-style-type: none"> • OpenDLP Installation • Bypassing DLP 	<ul style="list-style-type: none"> • מבוא לDLP • OpenDLP • שיטות לעקוף DLP 	DLP	
<ul style="list-style-type: none"> • Honeypot Placement • Set Up a Modern 	<ul style="list-style-type: none"> • מבוא למלכודת דבש • אסטרטגיית מלכודת דבש • Honeytokens • מוצרי מלכודת דבש (Honeypot) 	מלכודות דבש (Honeypots)	
<ul style="list-style-type: none"> • Valhala Honeypot 	<ul style="list-style-type: none"> • מבוא למלכודת דבש • מלכודת הדבש Valhala • התחמקות 	מלכודת הדבש Valhala	