ספר קורס

CYBER SCHOOL

מבוא להאקינג

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

מידע על ספר לימוד זה

מסמך זה הוא ספר לימוד עבור הקורס המלא של האקינג אתי. הוא מכיל את כל המידע שהמנחה יציג בכיתה.

ספר הלימוד מלווה את הקורס כולו, לפי סדר כרונולוגי, משלב ההתחלה ועד לחומר המתקדם של הקורס.

מקרא

קטעי טקסט צבעוניים מופיעים לאורך מסמך זה כדי להפנות את הקורא למקור ספציפי, או להעשיר אותו במידע נוסף.

קטעי הטקסט הצבעוניים כוללים את הנושאים הבאים:

משימת מעבדה
יש לעיין בקבצי המעבדה התואמים כדי לתרגל את מה שנלמד עד כה. תיבת טקסט זו כוללת גם שאלות ספציפיות לתרגול.

טוב לדעת
מידע נוסף או תובנות לגבי הנושא. מידע זה נועד לצורך העשרה בלבד ואינו חלק מהחומרים עליהם תיבחנו.

טיפ
מידע שימושי שיש בו כדי לסייע לתלמידים ללמוד את החומר או לעבוד עם כלים מסוימים.

מידע נוסף
קישורים או הפניות לחומר חיצוני שניתן להשתמש בהם כדי להרחיב את הידיעות שלכם לגבי הנושא.

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

האקרים

להאקינג יש משמעויות שונות בהקשרים שונים. יחד עם זאת, הוא קשור בדרך כלל לשינוי הפונקציונליות או ההתנהגות של המוצר כדי לגרום לו לפעול בצורה שונה מהאופן שבו הוא נועד לפעול. בעולם אבטחת הסייבר, המונח קשור בדרך כלל בהשגת גישה בלתי מורשית למערכת מקומית או מרוחקת.

המשפט שמבטא את רוח ההאקינג בצורה הטובה ביותר הוא "תמיד יש דרך להיכנס", ומרבית מתכוני ההאקרים יכללו את המרכיבים הבאים:

- הכל אפשרי
- תחרותיות
- חשיבה יצירתית
- חיפוש אחר Bug Bounties (פרסים על מציאת באגים)
- קבלת אתגרים

סוגי האקרים

ניתן לקבץ האקרים לפי החלוקה הבאה:

כובעים לבנים: האקרים אתיים, שהתמחותם היא פגיעה ברשתות אבטחה. כובעים לבנים משתמשים ביכולותיהם למטרות טובות (משפטיות), כגון זיהוי נקודות תורפה של מערכת או רשת לפני שייפגעו על ידי האקרים בעלי כוונות זדוניות.

כובעים שחורים: האקרים זדוניים המפרים את אבטחת המחשב בעיקר מתוך מניעים של רווח אישי, כגון כסף, כוח, פוליטיקה, נקמה, או אפילו רק לשם גרימת נזק. האקרים כאלה עשויים לפעול לבד או בקבוצות, ולעתים קרובות פעילותם אינה חוקית ואף פלילית.

כובעים אפורים: האקרים שנמצאים על הרצף בין כובעים לבנים לכובעים שחורים. האקרים מסוג כובעים אפורים אולי לא מונעים מרווח אישי או גרימת נזק, אך הם עלולים בכל זאת לבצע פעולות בלתי חוקיות מבחינה טכנית.

צוות האקרים

אנשי מקצוע האחראים על אבטחת הסייבר מקובצים לשלושה צוותים עיקריים:

חברי **הצוות האדום** הם מומחי אבטחה האחראים על חקירה פעילה וגישוש (האקינג) של מערכות. הם מפתחים בדיקות טרום-שימוש כמו גם בדיקות על מערכות חיות. מומחי הצוות האדום ידועים גם כבודקי חדירות.

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

חברי **הצוות הכחול** הם מומחי אבטחת מידע (InfoSec) ואבטחת סייבר שמעורבים בעיקר בהגנה על המערכות דרך הגדרות וקונפיגורציות, ודרך הטמעת אמצעי אבטחה אחרים ברחבי המערכת כולה.

חברי **הצוות הסגול** מנסים למזג בין היתרונות והשיטות של שני הצוותים האחרים - הצוות האדום והצוות הכחול. ההכרעה באשר לכדאיות העסקת צוות סגול עדיין נדונה בענף אבטחת הסייבר.

מפת מתקפות חיות

כישורי האקינג המשמשים למטרות זדוניות הם תופעה שכיחה בעידן המודרני. מוערך היא כי בממוצע יותר מ-40 מיליון מתקפות מתבצעות מדי יום ברחבי העולם.

כמות מתקפות הסייבר היומית עולה כל הזמן, בין אם מסיבות כלכליות או בשל אינטרסים אחרים. ארגונים מממנים האקרים זדוניים כדי להשיג מידע רגיש מהמתחרים שלהם. מדינות מממנות אנשים בעלי כישורי האקינג זדוניים לאיסוף מודיעין או כדי לגרום נזק למערכות של מדינות אחרות.

האקרים מקצועיים זדוניים לרוב מונעים על ידי כסף ומשתמשים בכישורים שלהם כדי לסחוט את קורבנותיהם באמצעות תוכנת כופר, או כדי לגנוב מספרי כרטיסי אשראי באמצעות תוכנות זדוניות.

לצורך ניטור בזמן אמת, ספקי אבטחה רבים יוצרים מפות מתקפות סייבר מבוססות אינטרנט. מפות רבות כאלה מציגות התקפות באופן גרפי, ולמרות שהן עשויות להוות מצגת מכירות טובה עבור החברות, הן גם חושפות את המציאות העגומה של פעילות סייבר זדונית בלתי פוסקת.

מפת מתקפות חיות של צ'ק פוינט

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

מידע נוסף

דף האינטרנט הבא מפרט אתרים המארחים מפות מתקפות חיות:
https://www.secureworldexpo.com/industry-news/6-live-cyber-attack-maps
כדי לעיין במפת איומי הסייבר החיים של צ'ק פוינט, יש לעבור אל דף האינטרנט הבא:
https://threatmap.checkpoint.com
כדי לעיין במפת איומי הסייבר החיים של פורטנייט, יש לעבור אל דף האינטרנט הבא:
https://threatmap.fortiguard.com

תרגול קצר: חיפוש ב-Talos

יש לעבור אל האתר: **https://talosintelligence.com**
יש להזין את כתובות ה-IP הבאות כדי לבדוק אם הן חשודות:

- 209.141.40.58
- 162.144.45.185
- 104.168.253.225
- 102.130.114.195

הסמכות

- **CEH**: Certified Ethical Hacker - האקר אתי מוסמך הסמכה המוצעת על ידי מועצת ה-EC אשר נדרשת עבורה הוכחת ידע בהערכת רמת האבטחה של מערכות המחשב, ויש להשיב על שאלות לגבי שיטות לבדיקת חדירות.
- **OSCP**: Offensive Security Certified Professional - בעל מקצוע מוסמך בתחום האבטחה ההתקפית. אנשי מקצוע מוסמכים המסוגלים להשתמש בשיטות וכלים לבדיקת חדירות. כדי לקבל הסמכה זו, על המועמדים לתקוף בהצלחה מכונות חיות בסביבת מעבדה סגורה.
- **OSCE**: Offensive Security Certified Expert - מומחה בתחום האבטחה ההתקפית. אנשי מקצוע מוסמכים המסוגלים לזהות נקודות תורפה שקשה למצוא אותן ותצורות שגויות. בחינת ה-OSCE כוללת רשת וירטואלית המתארחת מרחוק המכילה תצורות ומערכות הפעלה שונות.

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

- **CISA**: Certified Information System Auditor - מבקר מערכות מידע מוסמך. הסמכה המוצעת על ידי ISACA. הבחינה מסמיכה את האדם בידע ובמיומנויות של מקצועות האבטחה.
- **CISM**: Certified Information Security Manager - מנהל מערכות מידע מוסמך. הסמכה המוצעת על ידי ISACA. הבחינה מסמיכה את האדם בידע ובניסיון הדרושים כדי לפתח ולנהל תוכנית אבטחת מידע ארגונית.

אתיקה: בודקי חדירות

בעולם הסייבר, האתיקה מונעת על ידי הציפיות והדרישות של התנהגות מקצועית בקרב אנשי אבטחה, הן כיחידים והן כחלק מארגון.

ארגונים רבים המבוססים על טכנולוגיה מגדירים ציפיות מקצועיות באמצעות כללי התנהגות וכללי אתיקה.

בתחום בדיקת החדירות (PT), אבן הבניין הבסיסית היא בחירתו של הפרט להשתמש בכלים רבי עוצמה הקשורים לסייבר למטרה הנכונה.

אם כלים כאלה נמצאים בידיים הנכונות, הם יכולים לשמש ככוח-נגד להאקרים שבוחרים בדרך הזדונית, בכל מקום ברחבי העולם.

חלק בוחרים להגן, בעוד שאחרים מבקשים גישה בלתי מורשית, מניעת שירותים והשמדת נתונים חשובים, כדי לקדם את המטרות שלהם.

לכל בודק חדירות המועסק בתעשיית הסייבר חייב להיות קוד אתי שבו הוא דבק, ואשר מבטיח כי הוא פועל במסגרת החוק.

- הקוד האתי שמציית לו בודק חדירות בענף אבטחת המידע, אמור לזכות באמון של לקוחות וארגונים ולהבטיח את בטיחות הנתונים.
- מטרתו של קוד אתי אישי צריכה להיות הימנעות משימוש באמצעים בלתי חוקיים כשיטה להשגת מטרות אבטחת המידע.
- בחברות העוסקות בבדיקת חדירות, מתבקשים הבוחנים לחתום על הסכם סודיות להגנה על הלקוחות ולפעול בגבולות החוק הציבורי והפרטי כאחד.
- בודקי חדירות צריכים לשקול את מיקומו של הלקוח, שכן החוקים עשויים להשתנות במדינות ובארצות השונות.
- בודקי חדירות חייבים להיות מעודכנים בנוגע לחוקים החלים ועליהם לשמור על יושרה אתית ומקצועית בכל עת.
- בודקי חדירות לא אמורים כלל לבצע פעולות שיגרמו נזק ממשי למערכת.
- בודקי חדירות צריכים הרשאה בכתב כדי להיכנס אל המערכות שהם אמורים לבדוק.

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

תוכנה זדונית

הגדרה של תוכנה זדונית

המונח תוכנה זדונית מתאר תכניות המעוצבות לגרום נזק למערכות או להפעיל אותן באופן לא חוקי.

מטרת התוכנה הזדונית היא לרוב לסכן מחשבים אישיים, רשתות שלמות או מכשירים ניידים על ידי שליטה על הפעלתם.

רוב מתקפות הסייבר הקשורות לתוכנות זדוניות כוללות גניבה, הצפנה או מחיקה של נתונים, שינוי או חטיפה של פונקציות מחשב מרכזיות וריגול אחר פעילות מחשב ללא ידיעתו או רשותו של המשתמש.

טוב לדעת
ברוב המקרים, תוכנה זדונית אינה פוגעת בחומרה פיזית אלא מכוונת לפגוע במערכת ההפעלה.

סוגי תוכנה זדונית

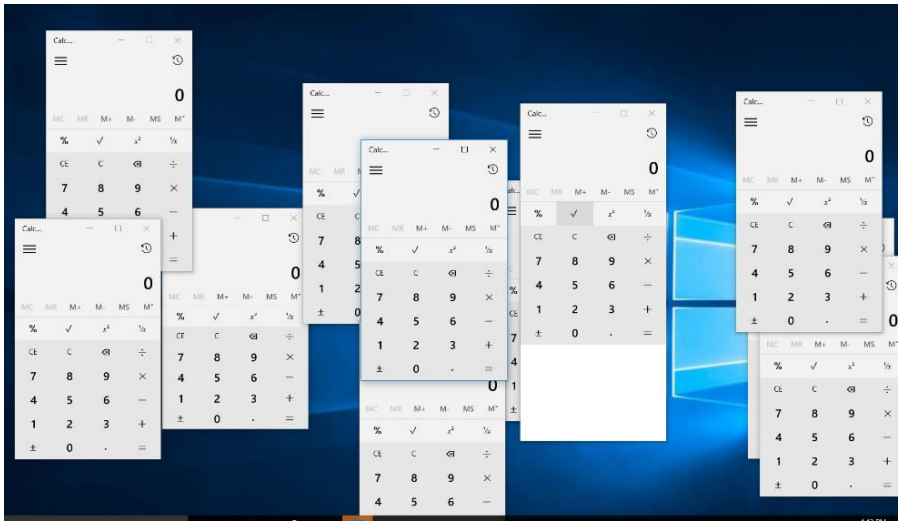
וירוס

וירוס מחשב הוא סוג של תוכנה זדונית המשכפלת את עצמה כאשר היא מופעלת. הוא משנה תוכנות מחשב אחרות ומוסיפה קוד שמדביק קבצים אחרים.

תוקפים שמשתמשים בווירוסים ישקיעו זמן רב בהונאות וניצול של הנדסה חברתית שיסייעו בהפצת הווירוס.

רוב הווירוסים לא נועדו לגנוב מידע. הם נועדו להתמקד בעיקר במערכת ההפעלה, לפגוע בה וברכיבי מחשב אחרים.

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383



חלוקת מחשבון לאחר הפעלת וירוס.

כופרה

תוכנת כופר היא סוג של תוכנה זדונית שמצפינה את נתוני המערכת ומחזיקה אותם כבני ערובה כשהיא ממתינה לקריפטו בתמורה (בדרך כלל נדרש מטבע דיגיטלי, כדי למנוע מעקב אחר כסף אמיתי).

הנדסה חברתית היא לרוב השיטה הנבחרת. המטרה היא בדרך כלל ארגון או אדם בעלי שפע אמצעים כלכליים.

חברות ידועות רבות ברחבי העולם חוו התקפות של תוכנת כופר, וחלקן אף שילמו על מנת לפענח (לשחרר) את הנתונים השבויים.

סוס טרויאני

סוס טרויאני הוא תוכנה זדונית המגיעה לעתים קרובות דרך דואר אלקטרוני או נדחפת אל המשתמשים כאשר הם מבקרים באתר נגוע.

הסוס הטרויאני חייב להיות מופעל על ידי הקורבן, ובדרך כלל מספק לתוקף גישה מרחוק.

סוסים טרויאנים יכולים להיות מוסתרים בקבצים לגיטימיים ותוקפים יכולים לדחוף את הקבצים באמצעות הנדסה חברתית, ומאפשרים לקורבנות להפעיל את התוכנית בעצמם.

ניתן לזהות חלק מהסוסים הטרויאנים בעזרת יישומי אנטי וירוס וחומות אש, אך אחרים עשויים לעבור ללא זיהוי.

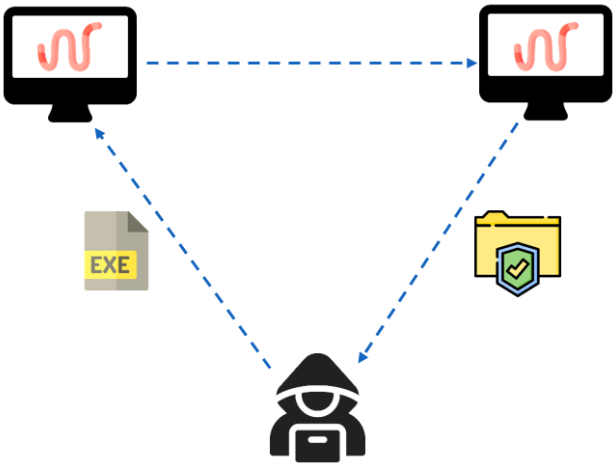
כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

תולעת

תולעת היא סוג של תוכנה זדונית המפיצה עותקים של עצמה ממחשב אחד למשנהו. תולעים אינן צריכות לצרף את עצמן לתוכנות או תוכניות כדי לגרום נזק.

תוכנות זדוניות מסוג תולעת יכולות לבחור כל אובייקט ולשכפל את עצמו עד שימצא את המטרה המיועדת.

תולעים עלולות לגרום לנזקים הדומים לווירוסים על ידי ניצול תקלות אבטחה בתוכנה וגניבת מידע רגיש.



תולעת בפעולה

Botnet

המילה Botnet היא שילוב של המילים robot (רובוט) ו-network (רשת) ומשמשת בדרך כלל לציון פעילות זדונית.

Botnet מתייחס למחשבים ברשת פרטית שהסתננו אליהן תוכנות זדוניות שהתוקף משתמש בהן למטרות מזיקות.

על ידי יצירת רשת של Botnet, תוקף יכול להפעיל התקפות DDoS עוצמתיות שנועדו לשלוח ספאם, לגנוב נתונים או לגשת מרחוק למכשירים.

הבעלים יכול לשלוט בפעולות התקפיות באמצעות שרת C&C (שליטה ובקרה).

טוב לדעת

Botnet יכול לשמש כמנגנון כריית קריפטו.

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383