



מעבדה 6



CSRP

DFIR

מבוא ל-DFIR תרחישי שלישיית CIA

- עמוד 1 -

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

נושאי המעבדה

הבנה של שלישיית CIA דרך תרגול סיטואציות.

זמן מוערך

10-15 דקות.

סביבת המעבדה

כתבן

משימת מעבדה:

לכל אחד מהתרחישים הבאים, ציינו איזה סוג של הפרה קרתה לפי שלישיית CIA. הסבירו מדוע בחרתם בסוג זה של פריצה עבור התרחיש (אי דחייה ואחריות נחשבים גם כהפרות).

שימו לב: לכל תרחיש עשויות להיות נקודות מבט רבות.

- 1 תוקף משנה את המחירים של הנעליים האהובות עליו בחנות אינטרנטית, ואז רוכש אותם. (השינוי אינו קבוע בבסיס הנתונים).
- 2 תוקף מחליט להתעלל בצוות משאבי אנוש של החברה, ושולח להם יותר מעשרת אלפים מיילים עם פרטים כוזבים על מועמדי גיוס, עד ששרת הדואר כולו מתמוטט.
- 3 מבלי אישורה של נוי, נמרוד בודק את הרשומות הפיננסיות שלה כדי לבדוק איך היא קנתה את המכונית החדשה שלה. מבלי אישורו של יובל, נמרוד משתמש באישוריו של יובל כדי להשיג את המידע שהוא רוצה.
- 4 מתקפת סייבר שהפילה את רוב האינטרנט באמריקה בשנת 2006 בוצעה באמצעות נשק שנקרא "Mirai botnet". הסיבה להפלת האינטרנט הייתה התקפת DDoS נגד ספק DNS גדול. במהלך ההתקפה, רשת של מחשבים נדבקה בתוכנה הזדונית "botnet", והמחשבים תואמו יחדיו כדי להפיגז שרת ספציפי עם תעבורה עד שהוא קרס.
- 5 תוכנת כופר תוקפת את בסיס הנתונים של החברה שמאחסן PII, ומצפינה את כל הקבצים ובסיסי הנתונים. לפני ההצפנה, התוקף מעלה את כל בסיסי הנתונים לענן. אחרי ההצפנה, כל היומנים נמחקו.
- 6 האקרית מנסה לפרוץ למערכת הציונים של בית ספר. היא מצליחה להשיג רק הרשאות קריאה לציוני התלמידים.