מעבדה 6

CSRP

DFIR

מבוא ל-DFIR

תרחישי שלישיית CIA

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

נושאי המעבדה

השיגו הבנה מקיפה של שלישיית ה- CIA , על ידי תרגול מצבים מסוימים.

זמן מוערך

10-15 דקות.

סביבת המעבדה

כתבן

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

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).
   פתרון:
   שלמות (Integrity) – המחירים השתנו, כך שאי אפשר יותר לסמוך על שלמות 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.
   פתרון:
   שלמות (Integrity) - התוקף שלח מועמדים *מזויפים* לצוות משאבי אנוש, כך שהם לא יכולים עוד לדעת מי אמיתי ומי לא. בסיס הנתונים כרגע מלא בנתונים כוזבים.
   זמינות (Availability) – שרת המיילים הפסק לעבוד, אז לקוחות לא יכלו לשלוח מיילים וכל החברה לא יכולה יותר לקבל מיילים.

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.
   פתרון:
   סודיות (Confidentiality) – אסור לאדם בלי הרשאות מתאימות ולא בגבולות ה-"צריך לדעת" לגנוב נתונים או אישורים של אדם אחר. נמרוד פרץ לנתונים הפרטיים של חברתו (כנראה לשעבר) נוי.
   אי דחייה (Non-Repudiation) – נמרוד השתמש באישורים של יובל בלי רשות. אם היו עוקבים אחרי הפעילות, נמרוד לא יהיה האדם שיואשם בפריצת לנתונים של נוי, אלא יובל.

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 להפגיז שרת ספציפי עם תעבורה עד שהוא קרס.
   פתרון:
   זמינות (Availability) – אתרים רבים לא היו זמינים בשל ההתקפה על ה-DNS.

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

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.

פתרון:

סודיות (Confidentiality) – ההאקר יכול לצפות במידע רגיש של לקוחות.

זמינות (Availability) – השרת לא עובד יותר כיוון שהשירות נפל.

אחריות (Accountability) – ההאקר מחק את היומנים במערכת כך שלא ניתן יהיה להשתמש בהם כדי למצוא את שורש הבעיה.

6 האקרית מנסה לפרוץ למערכת הציונים של בית ספר. היא מצליחה להשיג רק הרשאות קריאה לציוני התלמידים.

פתרון:

סודיות (Confidentiality) – ההאקרית יכולה לצפות במידע רגיש לגבי התלמידים.

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