



מעבדה 4



CSRP

DFIR

מבוא ל-DFIR

בוחר מתודולוגיית DFIR

- עמוד 1 -

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

נושאי המעבדה

נתחו מספר תרחישי התקפה על ארגון, ובחרו במתודולוגיית ה-DFIR הטובה ביותר לכל תרחיש.

זמן מוערך

20-30 דקות.

סביבת המעבדה

- סביבה וכלים
- כתבן

משימת מעבדה:

ענו על השאלות הבאות והסבירו איזה סוג אירוע קרה ואיך לטפל בו. שימו לב שאין תשובות מוחלטות לתרגיל זה, התכלית של מעבדה זו היא לעודד חשיבה לוגית.

הסבירו וקטלגו כל אחד מהתרחישים הבאים. בכל תרחיש, חשוב על מה צריך לעשות כדי לאסוף כמה שיותר מידע וכדי להתמודד עם האירוע. השאלות דורשות ממך לחשוב "מחוץ לקופסה".

תרחיש א'

אדם קורא לצוות האבטחה בחברה גדולה, אומר שהוא ממחלקת ה-IT, ואומר שהוא צריך להתחבר למחשב ספציפי כדי לעדכן משהו. קצין האבטחה בודק עם מחלקת ה-IT אם מי שהתקשר הוא עובד החברה, ומגלה כי הוא לא חלק מהחברה.

הקצין מדווח את האירוע לצוות ה-IR כשהאדם שהתקשר עדיין על הקו.

1 לאיזו קטגוריה ניתן לשייך את אירוע זה?

פתרון: ניתן לתייג אירוע זה כהתקפת הנדסה חברתית.

2 אילו צעדים ניתן לנקוט כדי להשיג מידע נוסף אודות ההתקפה?

פתרון:

- השג את מספר הטלפון של המתקשר אם אפשר, ובדוק באינטרנט אם למספר זה יש קשרים חשובים.
- נסה לגלות עוד מידע על זהות המתקשר.
- בדוק אם התוקף התקשר לעוד אנשים בחרה.

3 אילו צעדים ניתן לנקוט כדי לטפל באירוע?

פתרון:

- תן למתקשר להתחבר למכונה שלא מחוברת לרשת, ובדוק מה הוא עושה על המחשב (מכונה וירטואלית).
- שלח את הפרטים לגורמי אכיפת חוק מוסמכים.
- העלה את רמת המודעות של עובדים.

תרחיש ב'

צוות ה-NOC של חברה מקבל התרעה שאתר החברה שונה לפוסטר תעמולת בחירות, כנראה עבודה של כמה האקרים אקטיביסטיים (hacktivists). צוות ה-NOC מדווח על האירוע לצוות ה-IR.

1 לאיזו קטגוריה ניתן לשייך את אירוע זה?

פתרון:

ניתן לתייג אירוע זה כהתקפת השחתה.

2 אילו צעדים ניתן לנקוט כדי להשיג מידע נוסף אודות ההתקפה?

פתרון:

- שמור יומנים מהשרת ומשירות הרשת.
- שמור את המצב הנוכחי של התהליכים ע"י לכידת זיכרון (RAM) לחקירה עתידית.
- אסוף מידע בנוגע לכתובת ה-IP ששימשה למתקפה.

3 אילו צעדים ניתן לנקוט כדי לטפל באירוע?

פתרון:

- כבה מיידית את השרת (חלק מהחברות לא ירצו לעשות את זה, אבל זו עדיין אפשרות).
- שחזר את האתר מהגיבוי.
- הבן איך ההתקפה קרתה וחסום (אם אפשר) את השירות האחראי לכך עד שהשירות יתוקן.
- תקן את הפגיעות שגרמה להתקפה לקרות.
- אם נראה שההתקפה באה מכתובת IP פרטית, חסום אותה מהאתר לחצי שנה (או תקופת זמן לבחירתך).
- עדכן את ה-IDS, IPS ו-WAF.

תרחיש ג'

רועי מקבל אימייל מחברתו לעבודה יערה, עם קישור שנראה חשוד. כאשר הוא שואל את יערה לגבי האימייל, היא אומרת שהיא לא שלחה אותו, ואינה יודעת איך השתמשו במייל שלה. רועי ויערה יוצרים קשר עם צוות ה-IR ומודיעים להם לגבי האירוע.

1 לאיזו קטגוריה ניתן לשייך את אירוע זה?

פתרון:

ניתן לתייג את האירוע (ככל הנראה) בהתקפת סוס טרויאני.

2 אילו צעדים ניתן לנקוט כדי להשיג מידע נוסף אודות ההתקפה?

פתרון:

- בדוק אם עובדים אחרים קיבלו את אותו המייל. אם כן, בדוק כיצד המייל נשלח בכל מכונה.
- שמור את היומנים מהמחשב של יערה ובצע snapshot ל-RAM.
- בצע סריקה מלאה על המחשב של יערה באמצעות יישום אנטי וירוס.

3 אילו צעדים ניתן לנקוט כדי לטפל באירוע?

פתרון:

- חקור את המחשב של יערה (חפש תוכנות זדוניות).
- בדוק את התוכנות הזדוניות (אם נמצאו) ומחק אותן. חסום את ה-IOCs (indications of compromise) שלהן.
- חקור את מקור ההתקפה (איך יערה מעורבת בו), וחסום את שורש הבעיה (אם אפשרי) ותקן את הפגיעות.
- יישם צעדי אבטחה הקשורים לעובדים והגבר את מודעות העובדים.
- התקן או עדכן מוצרי אנטי וירוס (אם הם לא מותקנים או מעודכנים כעת).