



# מעבדה 5



CSRP

DFIR

## מבוא ל-DFIR

נבסי רשת

- עמוד 1 -

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

## נושאי המעבדה

התקינו והגדירו תוכנת ניהול נכס רשת בסיסית.

## זמן מוערך

20-30 דקות.

## סביבת המעבדה

VirtualBox שכולל Bridged Adapter עם:

• Windows

○ כונן משני קטן

## משימת מעבדה:

התקינו והגדירו LanSweeper כדי לקבל מבט על הרשת.

- 1 על המכונה הוירטואלית Microsoft Windows שלכם, הוסיפו למכונה המקומית את המשתמש johnd עם הסיסמה Aa123456! באמצעות שורת הפקודה. הוסיפו את המשתמש לקבוצת administrators.  
**שימו לב:** אסור שבמכונה וירטואלית זו יהיו קבצים פרטיים או סיסמאות. כשמעבדה זו נגמרת, הסר את המשתמש johnd.
- 2 ב-VirtualBox, שנו את NIC ל-"Bridged Adapter".  
**שימו לב:** צעד זה נעשה כדי לשפר את התוצאות ע"י סריקת כל ה-Class (עם כל המכונות בעלי אותה התצורה). אם ה-bridged networking לא עובד עקב בעיות DHCP, ניתן לבצע מעבדה זו בתצורת NAT.
- 3 הורידו והתקינו LanSweeper עם הגדרות ברירת המחדל שלו, מהקישור הבא :  
<https://www.lansweeper.com/download/>
- 4 הפעילו את ההתקנה באמצעות ה-key שקיבלת באימייל.  
**שימו לב:** תקופת הניסיון היא לגרסת ה-unlimited. אחרי 30 ימים עדיין תוכלו להשתמש ב-LanSweeper עם יותר מ-100 מכשירים.  
a. במסך "Asset Types", בחרו "only Windows and network devices".  
b. הזינו את האישורים של johnd כשאתם מתבקשים לעשות זאת.
- 5 הגדירו את התצורה של LanSweeper וסרקו את הרשת באמצעות האישורים של johnd.  
**שימו לב:** שאם ה-ports משמשים את המחשב שלך, בחר אחרים, כמו 8181 או 8443.
- 6 בחרו עמדת עבודה וענו על השאלות הבאות:  
a. מי המשתמש שהתחבר לאחרונה?  
b. איזו תוכנה מותקנת על הלקוח?  
c. האם האנטי וירוס עובד בעמדת העבודה?  
7 ערכו את מידע הנכס כדי שיכלול את הפרטים הבאים:  
a. קשר הנכס לנכס אחר.  
b. יחס הנכס למשתמש.  
c. תגובות על הנכס (החשיבות שלו וכו').  
d. מיקום הנכס.

הערת מעבדה: LanSweeper הוא יישום של IT Asset Management (ITAM) – ניהול נכסים של IT) שלא כולל את כל הנכסים החומריים והמופשטים. בדרך כלל ניתן לעקוב אחרי מערך הנכסים השלם באמצעות מסמכי העובדים וגיליונות האלקטרוניים של הארגון.