



## מעבדה 2



# MetaSploit

- עמוד 1 -

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

## נושאי המעבדה

הבנת הדרך להשתמש ב-HSTS וב-SMB\_login כדי להשיג מעטפת מרוחקת.

## זמן מוערך

35-45 דקות

## סביבת מעבדה

- סביבה וכלים
  - VirtualBox
  - Kali Linux
  - MetaSploit
  - Windows 7
- קישורי מעבדה נוספים
  - מידע HSTS:

<https://www.globalsign.com/en/blog/what-is-hsts-and-how-do-i-use-it/>

# משימת מעבדה 1: קונפיגורציית Metasploit

המטרה של משימה זו היא לחפש מודולי MSF מעוצבים מראש. בזמן המשימה, ניתן לסרוק את האתר [www.hack-yourself-first.com](http://www.hack-yourself-first.com) ולראות אם ה-HSTS פועל.

- 1 יש לוודא שהמחשבים Kali ו-pfSense פועלים.
- 2 במחשב Kali Linux, יש לחפש את מודול העזר שסורק את מצב התפעול של HSTS ב-MSFconsole.

## פתרונות:

התחילו הפעלת מסוף על ידי לחיצה על הסמל המודגש בצילום המסך הבא.



כדי להפעיל את קונסולת Metasploit, יש להריץ את הפקודה `msfconsole` ב-CLI.

```

root@kali:~# msfconsole
[-] **rtng the Metasploit Framework console...\
[-] * WARNING: No database support: No database YAML file
[-] ***

      .:ok000kdc'          'cdk000ko:
      .x0000000000000c    c00000000000x,
      :00000000000000k,    ,k0000000000000;
      '00000000kkk00000;  ;000000000000000'
      o0000000 MMMM .o000o0000l MMMM, 00000000o
      d0000000 MMMMMM c00000c MMMMMM, 00000000x
      l00000000 MMMMMMMMMM;d MMMMMMMMMM, 00000000l
      .00000000 MMM , MMMMMMMMMMMM MMMM, 00000000.
      c0000000 MMM 00c MMMMM  o00.MMM, 0000000c
      o0000000.MMM 0000.MMM 0000.MMM, 000000o
      l0000000.MMM 0000.MMM 0000.MMM, 000000l
      ;0000.MMM 0000.MMM 0000.MMM;0000;
      .d00o WM 0000ccc0000.MX x00d.
      ,k0l M 000000000000.M d0k,
      :kk;.000000000000;.0k:
      ;k00000000000000k:
      ,x00000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v5.0.41-dev ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 4 evasion ]

msf5 >

```

HSTS מודיע לדפדפנים איך לטפל בחיבורים שלהם דרך כותרות. הוא בעצם מכריח חיבור דרך HTTPS. ניתן למצוא מידע נוסף על HSTS בקישור המופיע בקטע משאבים (Resources) בתחילת מסמך זה.

כדי לחפש HSTS, יש להריץ את הפקודה **Search hsts**

```

msf5 > search hsts

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - - -                               - - - - -      - - -  - - -  - - - - -
0  auxiliary/scanner/http/http_hsts         2017-01-01      normal Yes    HTTP Strict Transport Security (HSTS) Detection
1  post/multi/manage/hsts_eraser           2017-01-01      normal No     Web browsers HSTS entries eraser

msf5 >

```

3 יש להשתמש בסורק העזר HSTS, למלא את הנתונים הדרושים ולהריץ אותו. יש לבצע את הסריקה על <https://hack-yourself-first.com>

## משימת מעבדה 2: מתקפת התחברות SMB

המטרה של משימה זו היא הטמעה של מתקפת SMB בסיסית בעזרת המודול המעוצב מראש smb\_login ב-Msfconsole.

- 1 יש להפעיל את המחשב Windows 7.
- 2 יש לחפש ניצולים קשורים ל-smb\_login.
- 3 יש להגדיר את Metasploit להשתמש בניצול smb\_login ולמלא את הנתונים הנדרשים כדי לתקוף את מכונת Windows 7.

## רמזים

### משימת מעבדה 1

- ניתן להשתמש ב-msfconsole באמצעות המסוף על ידי הרצת הפקודה **msfconsole**.
- פקודת החיפוש משמשת לצורך חיפוש.
- יש להשתמש ב-show options כדי להציג את השדות הדרושים.

### משימת מעבדה 2

- יש להגדיר RHOST, SMBPass ו-SMBUser.
- פרטי ההתחברות אמורים להשתייך למשתמש Windows 7.