



# פתרון מעבדה 1



## SearchSploit

- עמוד 1 -

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

## נושאי המעבדה

דרך ההצגה של כל הניצולים הזמינים וכיצד להוריד אותם באמצעות SearchSploit דרך .CLI

## זמן מוערך

15-30 דקות

## סביבת מעבדה

- סביבה וכלים
  - VirtualBox
    - Kali Linux
      - SearchSploit

## משימת מעבדה: עבודה עם SearchSploit

יש להשתמש ב-SearchSploit כדי למצוא ולהוריד ניצולים עבור שירותי OpenSSH ו-Apache.

- 1 יש לוודא שהמכונות הווירטואליות Kali ו-pfSense פועלות.
- 2 במחשב Kali, יש להשתמש ב-SearchSploit כדי לחפש נקודות תורפה ב-OpenSSH 7.7.

פתרון:

יש להתחיל הפעלת מסוף על ידי לחיצה על הסמל המודגש בצילום המסך למטה.



כדי לחפש נקודות תורפה באמצעות SearchSploit, יש להריץ את הפקודה:  
**searchsploit OpenSSH 7.7**

```
root@kali:~# searchsploit OpenSSH 7.7
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
OpenSSH 2.3 < 7.7 - Username Enumerati | exploits/linux/remote/45210.py
OpenSSH 2.3 < 7.7 - Username Enumerati | exploits/linux/remote/45233.py
OpenSSH < 7.7 - User Enumeration (2) | exploits/linux/remote/45939.py
-----
Shellcodes: No Result
root@kali:~#
```

יש שלוש נקודות תורפה פוטנציאליות שאפשר לנצל.

יש לשים לב כמה נקודות תורפה פוטנציאליות אפשר לנצל.  
3 יש להשתמש ב-SearchSploit כדי לחפש נקודות תורפה ב-שירות Apache 2.4 ולשים לב כמה נקודות תורפה פוטנציאליות יש ב-Apache 2.4.

פתרון :

כדי לחפש נקודות תורפה באמצעות SearchSploit, יש להריץ את הפקודה:

### searchsploit Apache 2.4

```
root@kali:~# searchsploit Apache 2.4
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Apache 2.2.4 - 413 Error HTTP Request | exploits/unix/remote/30835.sh
Apache 2.4.17 - Denial of Service | exploits/windows/dos/39037.php
Apache 2.4.17 < 2.4.38 - 'apache2ctl g | exploits/linux/local/46676.php
Apache 2.4.23 mod_http2 - Denial of Se | exploits/linux/dos/40909.py
Apache 2.4.7 + PHP 7.0.2 - 'openssl_se | exploits/php/remote/40142.php
Apache 2.4.7 mod_status - Scoreboard H | exploits/linux/dos/34133.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS M | exploits/linux/webapps/42745.py
Apache Tomcat 3.2.3/3.2.4 - 'RealPath. | exploits/multiple/remote/21492.txt
Apache Tomcat 3.2.3/3.2.4 - 'Source.js | exploits/multiple/remote/21490.txt
Apache Tomcat 3.2.3/3.2.4 - Example Fi | exploits/multiple/remote/21491.txt
-----
Shellcodes: No Result
root@kali:~#
```

ניתן לנצל שש נקודות תורפה אפשריות. יש שלוש נקודות תורפה פוטנציאליות שאפשר לנצל.

4 יש להשתמש ב-SearchSploit כדי העתיק את הסקריפט של Apache ולאמת שהקובץ קיים לאחר ההורדה.

## פתרון :

כדי להוריד את הסקריפט, יש להריץ את הפקודה את `searchsploit -m Apache2`

```
root@kali:~# searchsploit -m Apache2
Exploit: Microsoft IIS 5.0 - WebDAV Remote
URL: https://www.exploit-db.com/exploits/2
Path: /usr/share/exploitdb/exploits/windows/remote/2.c
File Type: UTF-8 Unicode text, with CRLF line terminators
Copied to: /root/2.c
root@kali:~#
```

כדי לוודא שהקובץ הורד, יש להריץ את הפקודה `ls` בספרייה שאליה הוא הועתק, או פשוט `ls /root/Desktop` בספרייה הנוכחית:

```
root@kali:~# ls
2.c      Documents  Music      payload.exe  Public     Videos
Desktop  Downloads  paused.conf Pictures      Templates
root@kali:~#
```

## רמזים

### משימת מעבדה

- מריצים את SearchSploit דרך המסוף.
- יש לשקול להשתמש במדריך העזרה של SearchSploit כדי ללמוד איך להעתיק את הניצול.