
מתקפות תשתיות



CYBER SCHOOL

בשיעור זה נלמד על התקפות תשתית באמצעות כלי Linux מובנים, וניתן
דגש מיוחד על כלי תקיפה המיועד להתקפות תשתית. MetaSploit.

MetaSploit ➤



CYBER SCHOOL



CYBER SCHOOL

MetaSploit

סקירה של Metasploit



נקודת תורפה - חולשה שניתן לנצל במערכת



מטען מיועד - קטע קוד הפועל על מערכת פגיעה
לאחר שעברה ניצול.



ניצול - העברת המטען המיועד אל המערכת
הפגיעה.





פרטי CVE - נקודות תורפה וחיפוש נפוצות.



Exploit-db.com - ארכיון שמלקט ניצולים, קודי מעטפת ועוד.



CVE.mi – קטלוג הכולל מספר גדול של CVE.





- עובד עם Exploit-db.
- מותקן מראש ב-Kali Linux.
- מכיל ניצולים חדשים.
- פקודה: `searchsploit [name]`





הפקודה **searchsploit** מפעילה את היישום.

כדי להוריד את הסקריפט, יש להריץ את הפקודה: **Searchsploit -m [full path]**

יש לשנות את ההרשאות של הסקריפט ולהריץ את היישום.

```
root@kali:~# searchsploit OpenSSH

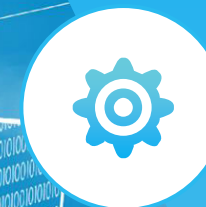
-----
Exploit Title                                                                 | Path
-----|-----
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation        | exploits/linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service          | exploits/multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution                            | exploits/freebsd/remote/17462.txt
Novell Netware 6.5 - OpenSSH Remote Stack Overflow                           | exploits/novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite                                    | exploits/linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration                                    | exploits/linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                               | exploits/linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One                           | exploits/unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow                    | exploits/linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (1)                          | exploits/unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (2)                          | exploits/unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service                  | exploits/multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation                         | exploits/linux/local/41173.c
OpenSSH 7.2 - Denial of Service                                              | exploits/linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection                     | exploits/multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration                                         | exploits/linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution                                 | exploits/linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution                                       | exploits/linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation | exploits/linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                     | exploits/linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                         | exploits/linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files                                   | exploits/multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident                          | exploits/linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery Tool                           | exploits/linux/remote/25.c
OpenSSHd 7.2p2 - Username Enumeration                                        | exploits/linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing Attack                         | exploits/multiple/remote/3303.sh
glibc-2.2 / openssl-2.3.0p1 / glibc 2.1.9x - File Read                       | exploits/linux/local/258.sh
-----

Shellcodes: No Result
root@kali:~#
```



מעבדה

SearchSploit



15-30 דק'

המשימה

יש לתרגל עבודה עם SearchSploit והורדת סקריפט.

השלבים

יש לערוך חיפושים בעזרת SearchSploit. ➤

כלים

VirtualBox
Kali Linux
SearchSploit

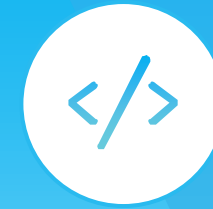
קבצים קשורים

מסמך מעבדה ➤



CYBER SCHOOL

MetaSploit



מסגרת לבדיקת חדירות.

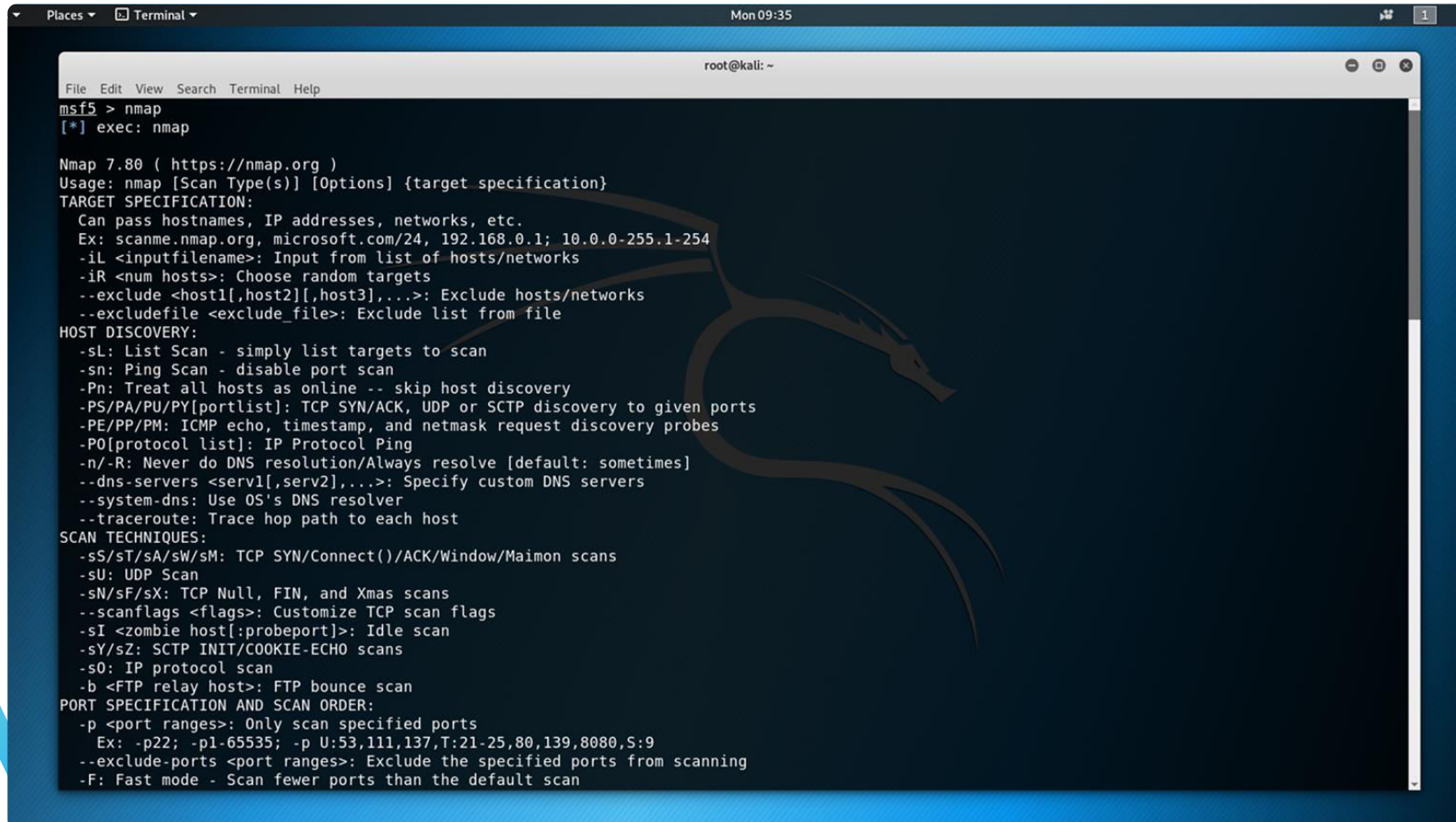
Msfconsole הוא ממשק משולב עבור Metasploit.

כולל מודולים נוספים להרחבת היכולות שלו.

```
root@kali:~# msfconsole
[-] **rting the Metasploit Framework console..\  
[-] * WARNING: No database support: No database YAML file  
[-] ***  
  
.:ok000kdc'      'cdk000ko:.  
.x000000000000c      c000000000000x.  
;00000000000000k,      ,k00000000000000;  
'00000000kkk00000: :000000000000000'  
o0000000 MMMM o000o0000l.MMMM 0000000o  
d00000000 MMMMMM c00000c MMMMMM 0000000x  
l0000000 MMMMMMMMM .d.MMMMMMMMM 0000000l  
.0000000 MMM ;MMMMMMMMMMMM MMMM 0000000o  
c0000000 MMM 00c.MMMMMM o00 MMM 0000000c  
o000000 MMM 0000 MMM 0000 MMM 000000o  
l00000 MMM 0000 MMM 0000 MMM 00000l  
;0000 MMM 0000 MMM 0000 MMM 0000;  
.d00o WM 0000o0000000 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 > |
```

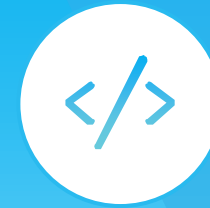


סריקה ברובה בהרצת nmap מ-Msfconsole.
ל-Msfconsole יש מגוון רחב של סורקים.
כל הסריקות נשמרות כדי לבנות מסד הנתונים.

A terminal window titled 'Terminal' with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar (root@kali: ~). The terminal shows the command 'msf5 > nmap' and its output, which is the help text for Nmap 7.80. The text includes sections for TARGET SPECIFICATION, HOST DISCOVERY, SCAN TECHNIQUES, and PORT SPECIFICATION AND SCAN ORDER. A faint Kali Linux dragon logo is visible in the background of the terminal.

```
msf5 > nmap
[*] exec: nmap

Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -s0: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
```





- ? - מציגה את כל הפקודות של MetaSploit
- Show options - מציגה הגדרות מודול.
- Show Info - מציגה מסמכים
- Show Targets - מציגה מטרות פגיעות.



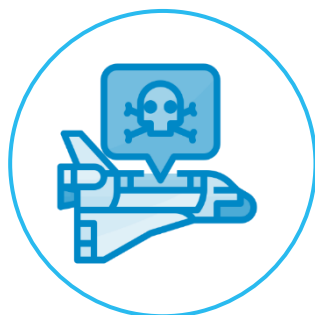
הגדרת מודול MetaSploit



שיטה	הסבר
[Use [name	מגדירה את המודול שיש להשתמש בו.
[RHOST [IP	מגדירה את מארח ה-IP המרוחק.
[RPORT [port	מגדירה את המטרה בפורט המרוחק.
[LHOST [IP	מגדירה את מארח ה-IP המקומי.
[LPORT [port	מגדירה את מספר הפורט המקומי.
ניצול	מריצה את הניצול.



סוגי מודולים של Metasploit



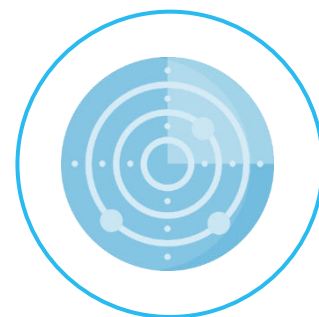
מטענים
מיועדים



מקודדים



ניצול



כלי עזר



Nops



המשימה

יש לתרגל עבודה עם תכונות MetaSploit שונות

השלבים

- יש לקבוע את התצורה של Metasploit. ➤
- יש להוציא לפועל מתקפת PsExec. ➤

קבצים קשורים

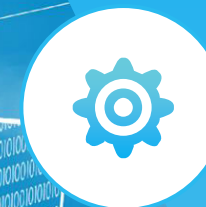
- מסמך מעבדה ➤

כלים

- VirtualBox
- Kali Linux
- 7 Windows
- Msfconsole

מעבדה

MetaSploit



30-45 דקות



CYBER SCHOOL



שאלות?

