Nmap

מה הוא Nmap?

NMAP הינה תוכנת open source שיודעת לסרוק את הרשת כדי למצוא פרטים רבים על ההתקנים שמחוברים לרשת. NMAP שולחת להתקנים פקטות ומצפה לקבל מהם תגובה.

ניתוח תגובת ההתקנים מאפשר ל NMAP להסיק מסקנות.

פעולות שימושיות בכלי:

בדיקת הגרסא:

```
└# nmap | head -1
Nmap 7.92 ( https://nmap.org )
```

פקודות סריקת מטרות:

nmap {ip/name} # סריקת מטרה אחת
nmap {target1 target2} # סריקת מספר מטרות

nmap {192.168.1.0/24} # סריקת כתובת רשת

nmap {192.168.1.10-20,22,25} # סריקת טווח/רשימת כתובות

nmap {10.1.1.0/24} -exclude {10.1.1.70} # הוצאת מטרות מטווח הסריקה

לדוגמא, בתמונה שלהלן אני סורק את הכתובות רשת ברשת שלי. ניתן לראות שפורט 80 פתוח בכתובת 192.186.1.1:

```
root@elior-virtual-machine:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-22 09:12 IDT
Nmap scan report for _gateway (192.168.1.1)
Host is up (0.019s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 7C:B7:33:C1:A2:69 (Askey Computer)

Nmap scan report for 192.168.1.2
Host is up (0.0084s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
21/tcp   closed ftp
139/tcp  closed netbios-ssn
445/tcp  closed microsoft-ds
9000/tcp closed cslistener
MAC Address: 18:1E:78:7F:A6:53 (Sagemcom Broadband SAS)

Nmap scan report for 192.168.1.3
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.3 are filtered
MAC Address: 00:03:81:B3:6F:56 (Ingenico International)

Nmap scan report for 192.168.1.4
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.1.4 are closed
MAC Address: 00:03:81:B3:6F:61 (Ingenico International)

Nmap scan report for 192.168.1.10
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.1.10 are closed
MAC Address: F0:81:75:40:B4:C2 (Sagemcom Broadband SAS)
```

מסקנות שאנו יכולים להסיק בסריקת פורטים:

במידה והיעד שולח SYN\ACK אז הפורט **פתוח.**

כמן כן לאחר הסריקה הוא ישלח RST (RESET) כדי שלא תפתח תקשורת שלא יהיה תיעוד לסריקה.

Source	Destination	Protocc	Info
192.168.1.121	192.168.1.1	TCP	64793 → 80 [SYN] Seq=0
192.168.1.1	192.168.1.121	TCP	80 → 64793 [SYN, ACK]
192.168.1.121	192.168.1.1	TCP	64793 → 80 [RST] Seq=1

==========

במידה **והיעד** שולח RST Packet אז הפורט **סגור.**

Source	Destination	Protocc	Info
192.168.1.121	192.168.1.1	TCP	61661 → 22 [SYN] Seq=
192.168.1.1	192.168.1.121	TCP	22 → 61661 [RST, ACK]

==========

במידה **והיעד לא מגיב,** הפורט מוגדר כחסום בחומת האש (Filtered).

פקודות לזיהוי מערכת ההפעלה של היעד:

nmap {target} **-O** # גילוי סוג המערכת הפעלה

nmap {target} **-O** --osscan-guess # סריקה יותר אגרסיבית

```
root@elior-virtual-machine:~# nmap 192.168.1.34 -O --osscan-guess
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-22 09:30 IDT
Nmap scan report for 192.168.1.34
Host is up (0.00094s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: CC:F9:E4:6B:10:B6 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 (93%), Microsoft Windows Server 2008 SP1 (90%), Microsoft Windows 10 1703 (89%), Microsoft Windows 10 1607 (87%), Microsoft Windows 10 1511 (87%), Microsoft Wi
ndows Server 2016 (87%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (87%), Microsoft Windows 10 1511 - 1607 (87%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windo
ws Vista SP2, Windows 7 SP1, or Windows Server 2008 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.35 seconds
root@elior-virtual-machine:~#
```

פקודה לגילוי התקנים פעילים ברשת (Ping Sweep)

FLAG **SN**- מבצע סריקה מהירה ושקטה שמטרה לגלות איזה התקנים פעילים ברשת ללא **סריקת פורטים**.

הפקודה מתבצעת באופן הבא:

nmap -n -sn {target}

FLAG n- תפקידו **אי** תרגום כתובות לשמות.

```
root@elior-virtual-machine:~# nmap -n -sn 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-22 09:36 IDT
Nmap scan report for 192.168.1.1
Host is up (0.098s latency).
MAC Address: 7C:B7:33:C1:A2:69 (Askey Computer)
Nmap scan report for 192.168.1.2
Host is up (0.029s latency).
MAC Address: 18:1E:78:7F:A6:53 (Sagemcom Broadband SAS)
Nmap scan report for 192.168.1.3
Host is up (0.098s latency).
MAC Address: 00:03:81:B3:6F:56 (Ingenico International)
Nmap scan report for 192.168.1.4
Host is up (0.097s latency).
MAC Address: 00:03:81:B3:6F:61 (Ingenico International)
Nmap scan report for 192.168.1.10
Host is up (0.096s latency).
MAC Address: F0:81:75:40:B4:C2 (Sagemcom Broadband SAS)
Nmap scan report for 192.168.1.11
Host is up (0.087s latency).
MAC Address: F0:81:75:40:B4:C3 (Sagemcom Broadband SAS)
Nmap scan report for 192.168.1.12
Host is up (0.81s latency).
MAC Address: 5C:C5:63:59:D8:13 (Unknown)
Nmap scan report for 192.168.1.13
Host is up (0.11s latency).
MAC Address: 18:90:D8:0D:BE:F7 (Sagemcom Broadband SAS)
```

כדי לראות רק כתובות IP נשתמש בפקודה:

nmap -sn -n {target}| grep for | cut -d " " -f 5

```
root@elior-virtual-machine:~# nmap -sn 192.168.1.0/24 | grep for | cut -d " " -f 5
gateway
192.168.1.2
192.168.1.3
192.168.1.4
192.168.1.10
192.168.1.11
192.168.1.12
192.168.1.13
192.168.1.14
192.168.1.15
192.168.1.16
192.168.1.19
192.168.1.20
192.168.1.21
192.168.1.22
192.168.1.26
192.168.1.32
192.168.1.34
192.168.1.40
elior-virtual-machine
root@elior-virtual-machine:~#
```