

NMAP



NMAP - bu tarmoqni tekshirish va xavfsizlikni baholash uchun keng qo'llaniladigan vosita. Bu dastur tarmoqdagi kompyuterlar va boshqa qurilmalarni aniqlash, xizmatlarni tekshirish va turli portlarni skanerlash uchun ishlatiladi. NMAP yordamida tarmoqning holati va xavfsizlik darajasi haqida batafsil ma'lumot olish mumkin.

Asosiy skanerlar



Tarmoqdagi faol qurilmalar ro'yxatini skanerlash tarmoq xaritasini yaratishda birinchi qadamdir. Buning uchun ikkita skanerdan foydalanishingiz mumkin:

- **Ping skanerlash** – ma'lum bir quyi tarmoqda ishlayotgan va ishlayotgan qurilmalar ro'yxatini skanerlaydi.

```
nmap -sp 192.168.1.1/24
```

- **Yagona xostni skanerlash** – 1000 ta taniqli port uchun bitta xostni skanerlaydi. Bu portlar SQL, SMTP, apache va boshqalar kabi mashhur xizmatlar tomonidan ishlatiladigan portlardir.

```
nmap scanme.nmap.org
```

Yashirin skanerlash



Yashirin skanerlash SYN paketini yuborish va javobni tahlil qilish orqali amalga oshiriladi. Agar SYN/ACK qabul qilinsa, bu port ochiqligini bildiradi va siz TCP ulanishini ochishingiz mumkin.

- Biroq, yashirin skanerlash hech qachon 3 tomonlama qo'l siqishni tugatmaydi, bu esa nishonga skanerlash tizimini aniqlashni qiyinlashtiradi.

```
nmap -sS scanme.nmap.org
```

- Yashirin skanerlash uchun **"-sS"** buyrug'idan foydalanishingiz mumkin. Esda tutingki, yashirin skanerlash boshqa skanerlash turlari kabi sekinroq va tajovuzkor emas, shuning uchun javob olish uchun biroz kutishingiz mumkin.

Versiyani skanerlash



Ilova versiyalarini topish penetratsion testning muhim qismidir.

- Bu sizning hayotingizni osonlashtiradi, chunki siz xizmatning ma'lum bir versiyasi uchun **Common Vulnerabilities and Exploits (CVE) ma'lumotlar bazasidan mavjud zaiflikni topishingiz mumkin. Keyin uni Metasploit** kabi ekspluatatsiya vositasi yordamida mashinaga hujum qilish uchun ishlatishingiz mumkin .

```
nmap -sV scanme.nmap.org
```

- Versiyani skanerlash uchun "-sV" buyrug'idan foydalaning. Nmap o'z versiyalari bilan xizmatlar ro'yxatini taqdim etadi. Shuni yodda tutingki, versiyani skanerlash har doim ham 100% aniq emas, lekin bu sizni tizimga muvaffaqiyatli kirishga bir qadam yaqinlashtiradi.

```
admin@ip-172-26-0-73:~$ nmap -sV scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 03:00 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered  smtp
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open      nping-echo   Nping echo
31337/tcp open      tcpwrapped

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
admin@ip-172-26-0-73:~$
```

OS skanerlash



Xizmatlar va ularning versiyalariga qo'shimcha ravishda, Nmap TCP/IP barmoq izlari yordamida asosiy operatsion tizim haqida ma'lumot berishi mumkin. Nmap shuningdek, OS skanerlash paytida tizimning ish vaqtini topishga harakat qiladi.

```
nmap -sV scanme.nmap.org
```

- Qidiruvni bir nechta kutilgan maqsadlar bilan cheklash uchun `osscan-limit` kabi qo'shimcha bayroqlardan foydalanishingiz mumkin. Nmap har bir OS taxmini uchun ishonch foizini ko'rsatadi.
- Shunga qaramay, operatsion tizimni aniqlash har doim ham aniq emas, lekin bu qalam testeriga o'z maqsadiga yaqinlashishiga yordam berish uchun uzoq yo'lni bosib o'tadi.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 04:39 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
25/tcp    filtered  smtp
80/tcp    open       http
9929/tcp  open       nping-echo
31337/tcp open       Elite
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.39 (91%), Linux 2.6.32 - 3.0 (90%), Linux 4.0 (89%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
```

Agressiv skanerlash



Nmap operatsion tizimini aniqlash, versiyani aniqlash, skriptni skanerlash va traceroute imkonini beruvchi agressiv rejimga ega. Agressiv tekshiruvni amalga oshirish uchun `-A` argumentidan foydalanishingiz mumkin.

```
nmap -A scanme.nmap.org
```

- Agressiv skanerlar oddiy skanerlarga qaraganda ancha yaxshi ma'lumot beradi. Biroq, tajovuzkor skanerlash ko'proq tekshiruvlarni yuboradi va xavfsizlik tekshiruvlari paytida aniqlanishi ehtimoli ko'proq.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 08:02 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.075s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp    filtered smtp
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 4.4 (93%), Linux 2.6.32 or 3.10 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.39 (91%), Linux 4.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%), Linux 2.6.32 - 3.0 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT ADDRESS
1 ... 5
6 0.97 ms 100.65.14.49
7 1.34 ms 52.93.29.57
8 1.96 ms 100.100.2.6
9 1.14 ms ash-b1-link.teliana.net (62.115.11.182)
10 1.92 ms rest-bb1-link.teliana.net (80.91.248.156)
11 7.98 ms nyk-bb3-link.teliana.net (62.115.141.245)
```

Bir nechta xostlarni skanerlash



Nmap bir vaqtning o'zida bir nechta xostlarni skanerlash imkoniyatiga ega. Bu xususiyat keng tarmoq infratuzilmasini boshqarayotganingizda juda foydali bo'ladi.

- Ko'p yondashuvlar orqali bir nechta xostlarni skanerlashingiz mumkin:
- Bir vaqtning o'zida barcha xostlarni skanerlash uchun barcha IP manzillarni bir qatorga yozing.

```
nmap 192.164.1.1 192.164.0.2 192.164.0.2
```

- Bir vaqtning o'zida barcha pastki tarmoqlarni skanerlash uchun yulduzcha (*) dan foydalaning.

```
nmap 192.164.1.*
```

- Butun domenlarni yozish o'rniga manzillar oxirini ajratish uchun vergul qo'ying.

```
nmap 192.164.0.1,2,3,4
```

- IP-manzillar oralig'ini belgilash uchun chiziqchadan foydalaning

```
nmap 192.164.0.0-255
```

Port skanerlash



Portni skanerlash Nmap-ning eng asosiy xususiyatlaridan biridir. Siz portlarni bir necha usulda skanerlashingiz mumkin.

- Bitta portni skanerlash uchun -p parametridan foydalanish

```
nmap -p 973 192.164.0.1
```

- Agar siz port turini belgilasangiz, ma'lum bir ulanish turi, masalan, TCP ulanishi haqida ma'lumotni skanerlashingiz mumkin.

```
nmap -p T:7777, 973 192.164.0.1
```

- Bir qator portlarni defis bilan ajratish orqali skanerlash mumkin.

```
nmap -p 76-973 192.164.0.1
```

- Skanerlash uchun eng yuqori n portni belgilash uchun `top-ports` bayrog'idan ham foydalanishingiz mumkin .

```
nmap --top-ports 10 scanme.nmap.org
```

Fayldan skanerlash



Agar siz IP-manzillarning katta ro'yxatini skanerlashni xohlasangiz, uni IP-manzillar ro'yxati bilan faylni import qilish orqali qilishingiz mumkin.

```
nmap -iL /input_ips.txt
```

- Yuqoridagi buyruq "input_ips.txt" faylidagi barcha berilgan domenlarni skanerlash natijalarini chiqaradi. IP-manzillarni oddiy skanerlashdan tashqari, siz qo'shimcha parametrlar va bayroqlardan ham foydalanishingiz mumkin.

Aniqlik va skanerlash natijalarini eksport qilish



Penetratsion test kunlar yoki hatto haftalar davom etishi mumkin. Nmap natijalarini eksport qilish ortiqcha ishni oldini olish va yakuniy hisobotlarni yaratishda yordam berishi mumkin. Nmap skanerlash natijalarini eksport qilishning ba'zi usullarini ko'rib chiqaylik.

Batafsil chiqish

```
nmap -v scanme.nmap.org
```

Batafsil chiqish amalga oshirilayotgan skanerlash haqida qo'shimcha ma'lumot beradi. Nmap tarmog'ida amalga oshiradigan harakatlarni bosqichma-bosqich kuzatish foydalidir, ayniqsa siz mijoz tarmog'ini skanerlayotgan begona bo'lsangiz.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 08:10 UTC
Initiating Ping Scan at 08:10
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 08:10, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:10
Completed Parallel DNS resolution of 1 host. at 08:10, 0.05s elapsed
Initiating SYN Stealth Scan at 08:10
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 13 out of 41 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to 11 out of 29 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 10 to 20 due to 17 out of 56 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 20 to 40 due to 11 out of 28 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 40 to 80 due to max_successful_tryno increase to 4
Increasing send delay for 45.33.32.156 from 80 to 160 due to 11 out of 27 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 160 to 320 due to 11 out of 22 dropped probes since last increase.
SYN Stealth Scan Timing: About 16.13% done; ETC: 08:13 (0:02:41 remaining)
SYN Stealth Scan Timing: About 25.53% done; ETC: 08:14 (0:02:58 remaining)
Discovered open port 31337/tcp on 45.33.32.156
SYN Stealth Scan Timing: About 39.62% done; ETC: 08:15 (0:02:42 remaining)
SYN Stealth Scan Timing: About 48.93% done; ETC: 08:15 (0:02:22 remaining)
SYN Stealth Scan Timing: About 58.32% done; ETC: 08:15 (0:01:59 remaining)
SYN Stealth Scan Timing: About 67.72% done; ETC: 08:15 (0:01:33 remaining)
Discovered open port 9929/tcp on 45.33.32.156
```

Oddiy chiqish

Nmap skanerlarini matnli faylga ham eksport qilish mumkin. Bu buyruq satrining asl chiqishidan biroz farq qiladi, lekin u barcha muhim skanerlash natijalarini oladi.

```
nmap -oN output.txt scanme.nmap.org
```

```
# Nmap 7.40 scan initiated Wed Jul 22 08:23:57 2020 as: nmap -oN output.txt --top-ports 10 scanme.nmap.org
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.073s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
23/tcp    closed telnet
25/tcp    filtered smtp
80/tcp    open  http
110/tcp   closed pop3
139/tcp   closed netbios-ssn
443/tcp   closed https
445/tcp   closed microsoft-ds
3389/tcp  closed ms-wbt-server
```

XML chiqishi



Nmap skanerlarini XML-ga ham eksport qilish mumkin. Bu, shuningdek, ruchkalarni sinovdan o'tkazish vositalarining ko'pchiligining afzal ko'rgan fayl formati bo'lib, skanerlash natijalarini import qilishda uni osongina tahlil qilish imkonini beradi.

```
nmap -oX output.xml scanme.nmap.org
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.40 scan initiated Wed Jul 22 08:17:51 2020 as: nmap -oX scanme.nmap.org -#45;top-ports 10 -->
<nmaprun scanner="nmap" args="nmap -oX scanme.nmap.org -#45;top-ports 10" start="1595405871" startstr="Wed Jul 22 08:17:51 2020" version="7.40" xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="10" services="21-23,25,80,110,139,443,445,3389"/>
<verbose level="0"/>
<debugging level="0"/>
<runstats><finished time="1595405871" timestr="Wed Jul 22 08:17:51 2020" elapsed="0.03" summary="Nmap done at Wed Jul 22 08:17:51 2020; 0 IP addresses (0 hosts up) scanned in 0.03 seconds" exit="success"/><hosts up="0" down="0" total="0"/>
</runstats>
</nmaprun>
```

Nmap skript mexanizmi

Nmap Scripting Engine (NSE) - bu skriptlarni yozish va ko'plab tarmoq xususiyatlarini avtomatlashtirish uchun foydalanishingiz mumkin bo'lgan juda kuchli vosita.

Siz Nmap bo'ylab tarqatilgan ko'plab skriptlarni topishingiz yoki talablaringiz asosida o'z skriptingizni yozishingiz mumkin. Hatto [Lua dasturlash tilidan](#) foydalanib, mavjud skriptlarni o'zgartirishingiz mumkin .

NSE shuningdek, tarmoqqa va turli tarmoq protokollariga hujum qilishda foydalaniladigan hujum skriptlariga ega.

Skriptlash mexanizmini chuqur o'rganish ushbu maqola uchun ko'rsatilmagan bo'lar edi, shuning uchun [bu erda Nmap skript mexanizmi haqida ko'proq ma'lumot](#).

http-avaya-ipoffice-users.nse	ms-sql-empty-password.nse	telnet-ntlm-info.nse
http-awstatstotals-exec.nse	ms-sql-hasdbaccess.nse	tftp-enum.nse
http-axis2-dir-traversal.nse	ms-sql-info.nse	tls-nextprotoneg.nse
http-backup-finder.nse	ms-sql-ntlm-info.nse	tn3270-screen.nse
http-barracuda-dir-traversal.nse	ms-sql-query.nse	tor-consensus-checker.nse
http-brute.nse	ms-sql-tables.nse	traceroute-geolocation.nse
http-cakephp-version.nse	ms-sql-xp-cmdshell.nse	tso-brute.nse
http-chrono.nse	mtrace.nse	tso-enum.nse
http-cisco-anyconnect.nse	murmur-version.nse	unittest.nse
http-coldfusion-subzero.nse	mysql-audit.nse	unusual-port.nse
http-comments-displayer.nse	mysql-brute.nse	upnp-info.nse
http-config-backup.nse	mysql-databases.nse	url-snarf.nse
http-cors.nse	mysql-dump-hashes.nse	ventrilo-info.nse
http-cross-domain-policy.nse	mysql-empty-password.nse	versant-info.nse
http-csrf.nse	mysql-enum.nse	vmauthd-brute.nse
http-date.nse	mysql-info.nse	vnc-brute.nse
http-default-accounts.nse	mysql-query.nse	vnc-info.nse
http-devframework.nse	mysql-users.nse	vnc-title.nse
http-dlink-backdoor.nse	mysql-variables.nse	voldemort-info.nse
http-dombased-xss.nse	mysql-vuln-cve2012-2122.nse	vtam-enum.nse
http-domino-enum-passwords.nse	nat-pmp-info.nse	vuze-dht-info.nse
http-drupal-enum.nse	nat-pmp-mapport.nse	wdb-version.nse
http-drupal-enum-users.nse	nbstat.nse	weblogic-t3-info.nse
http-enum.nse	ncp-enum-users.nse	whois-domain.nse
http-errors.nse	ncp-serverinfo.nse	whois-ip.nse
http-exif-spider.nse	ndmp-fs-info.nse	wsdd-discover.nse
http-favicon.nse	ndmp-version.nse	x11-access.nse
http-feed.nse	nessus-brute.nse	xdmcp-discover.nse
http-fetch.nse	nessus-xmlrpc-brute.nse	xmlrpc-methods.nse
http-fileupload-exploiter.nse	netbus-auth-bypass.nse	xmpp-brute.nse
http-form-brute.nse	netbus-brute.nse	xmpp-info.nse
http-form-fuzzer.nse	netbus-info.nse	
http-frontpage-login.nse	netbus-version.nse	



Mr Ton