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, SNTP, 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
```

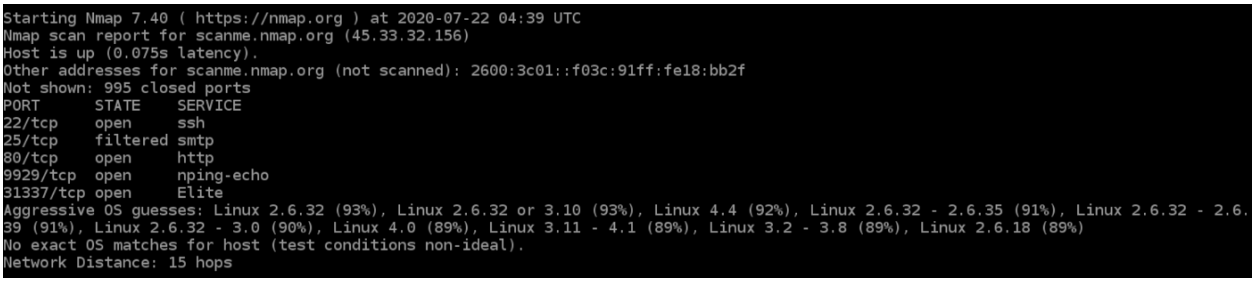
- Versiyani skanerlash uchun "-sV" buyrug'idan foydalaning. Nmap o'z versiyalari bilan xizmatlar ro'yxatini taqdim etadi. Shuni yodda tutingki, versiyani skanerlash har doim ham 100% aniq emas, lekin bu sizni tizimga muvaffaqiyatli kirishga bir qadam yaqinlashtiradi.

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.

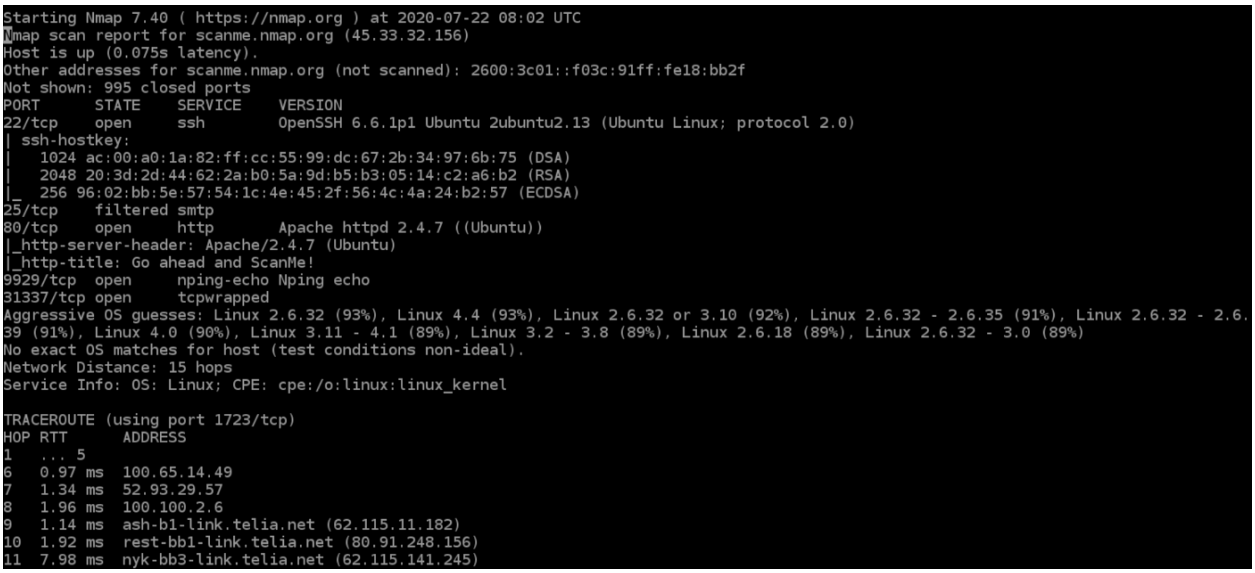


Agressiv skanerlash

💡 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.`



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.

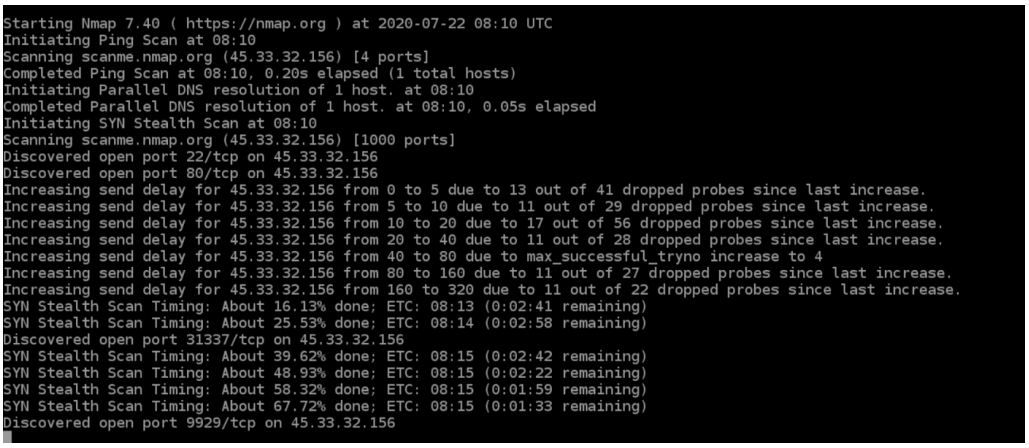
Aniqlik va skanerlash natijalarini eksport qilish

💡 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
```

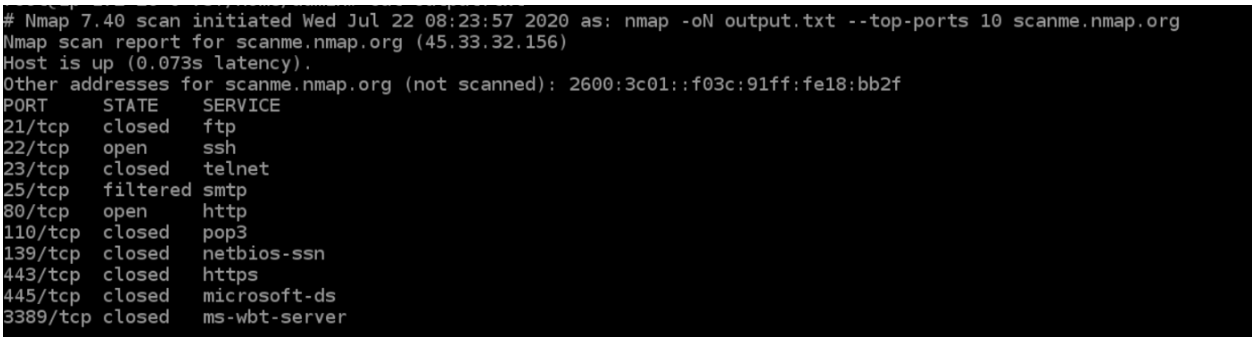
`Batafsil chiqish amalga oshirilayotgan skanerlash haqida qo'shimcha ma'lumot beradi. Nmap tarmog'ida amalga oshiradigan harakatlarni bosqichma-bosqich kuzatish foydalidir, ayniqsa siz mijoz tarmog'ini skanerlayotgan begona bo'lsangiz.`



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
```



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
```

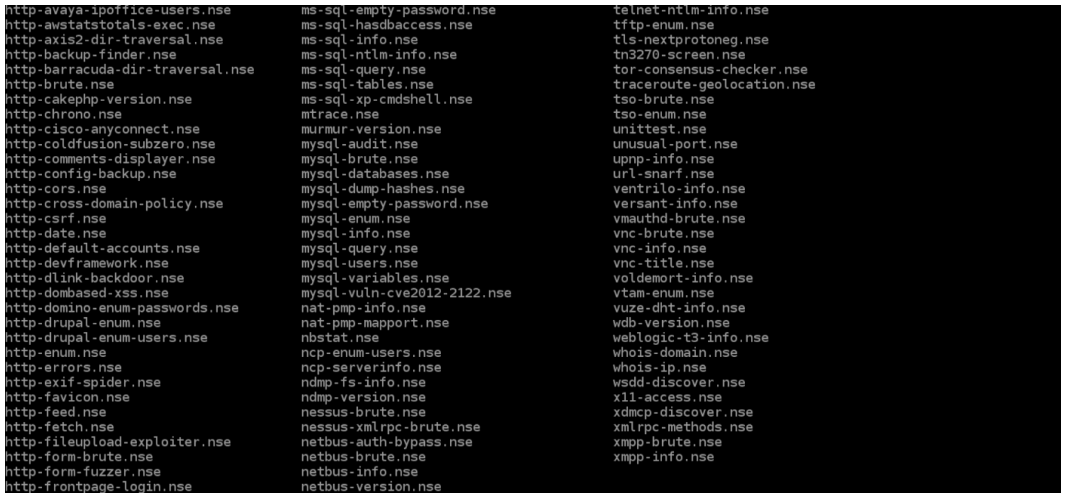
Nmap skript mexanizmi

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

Mr Ton