**nslookup nima?**

nslookup (Name Server Lookup) bu DNS (Domain Name System) ma’lumotlarini tekshirish uchun ishlatiladigan buyruq. Bu buyruq yordamida siz **IP manzilni domen nomiga**, yoki **domen nomini IP manzilga** o‘girishingiz mumkin.

**nslookup 93.170.6.43 nima qiladi?**

Bu buyruq **93.170.6.43** IP manzilining domen nomini aniqlashga harakat qiladi. Agar IP manzilga bog‘langan domen bo‘lsa, natijada shu domen nomi chiqadi. Agar bog‘langan domen bo‘lmasa, xatolik yoki faqat IP manzil ko‘rsatiladi.

**Natija qanday bo‘lishi mumkin?**

**Agar domen mavjud bo‘lsa:**

Name: example.com

Address: 93.170.6.43

Bu shuni anglatadi: **93.170.6.43** IP manzili **example.com** domeniga tegishli.

**Agar domen topilmasa:**

\*\* server can't find 93.170.6.43: NXDOMAIN

Bu shuni anglatadi: bu IP manzilga hech qanday domen bog‘lanmagan.

**nslookup qachon ishlatiladi?**

**IP manzildan domenni aniqlash**  
 **Domen nomining IP manzilini tekshirish**  
 **DNS muammolarini aniqlash va tahlil qilish**  
 **DNS serverlarni tekshirish**

Bu buyruq tarmoq administratori va IT xavfsizlik mutaxassislari tomonidan DNS muammolarini tekshirish va domenlar haqida ma’lumot olish uchun ishlatiladi.

### traceroute 93.170.6.43 ****nima qiladi?****

traceroute bu buyruq internet yoki tarmoq orqali ma’lum IP manzilga yetib borish uchun **qaysi marshrut (yo‘l) bo‘ylab harakat qilishini** tekshiradi.

Agar siz **traceroute 93.170.6.43** buyruqini ishlatsangiz, u **tarmoq tugunlari (routers)** orqali **93.170.6.43** manziliga boradigan yo‘lni ko‘rsatadi.

### ****Qanday natija chiqadi?****

**Namuna natija**

traceroute to 93.170.6.43 (93.170.6.43), 30 hops max, 60 byte packets

1 192.168.1.1 (192.168.1.1) 1.123 ms 1.456 ms 1.789 ms

2 10.10.10.1 (10.10.10.1) 3.456 ms 3.789 ms 4.123 ms

3 203.0.113.1 (203.0.113.1) 10.456 ms 11.789 ms 12.123 ms

4 93.170.6.43 (93.170.6.43) 50.123 ms 51.456 ms 52.789 ms

### ****Tahlil:****

1. **Birinchi qator**: traceroute to 93.170.6.43 – Buyruq qayerga yo‘naltirilganini ko‘rsatadi.
2. **1-qator**: 192.168.1.1 – Sizning **mahalliy routeringiz** (Wi-Fi yoki modem).
3. **2-qator**: 10.10.10.1 – Internet provayderingizning birinchi tuguni.
4. **3-qator**: 203.0.113.1 – Internetdagi oraliq marshrutizator.
5. **4-qator**: 93.170.6.43 – Manzilga yetib bordi.

Har bir tugun uchun **ms (millisekund)** vaqt ko‘rsatilgan, bu **ping kechikishini** bildiradi.

### traceroute ****nima uchun ishlatiladi?****

**Tarmoqda qayerda sekinlik borligini aniqlash**  
 **Tarmoqdagi muammolarni topish (bloklangan yo‘llar, kechikishlar)**  
 **IP manzilga boradigan yo‘lni tushunish**  
 **Internet provayderingiz qanday marshrutdan foydalanayotganini tekshirish**

Bu buyruq **tarmoq administratorlari va IT xavfsizlik mutaxassislari** tomonidan internetdagi marshrutlarni kuzatish va muammolarni aniqlash uchun ishlatiladi.

Agar **traceroute 93.170.6.43** ning ishlashini chuqur tushunmoqchi bo‘lsangiz, Linuxda quyidagi buyruqlarni bajaring. Bu buyruqlar **traceroute** ning ishlashini tekshirish, marshrutlar tahlili va tarmoq diagnostikasiga yordam beradi.

### **1. Traceroute asosiy buyruqlari**

#### **Traceroute orqali marshrutni tekshirish**

traceroute 93.170.6.43

**Natija:** IP-manzilga boradigan yo‘llar (hops) va har bir tugunga yetib borish vaqtlari (ping kechikishlari).

#### **Traceroute UDP o‘rniga ICMP orqali ishlatish (ba’zi tarmoqlarda kerak bo‘ladi)**

traceroute -I 93.170.6.43

**ICMP (ping protokoli) orqali marshrutni tekshiradi.** Agar **standart traceroute ishlamasa**, ushbu parametrni sinab ko‘ring.

#### **Traceroute maxsus port orqali (masalan, TCP 80 porti)**

traceroute -T -p 80 93.170.6.43

**Agar standart traceroute bloklangan bo‘lsa**, TCP 80 porti orqali harakat qilib ko‘rish mumkin.

### **2. Marshrutni to‘liq diagnostika qilish**

#### **Tarmoqdagi marshrutlarni real vaqtda kuzatish**

mtr 93.170.6.43

**MTR** (traceroute va ping ni birlashtirgan qudratli vosita) har bir marshrutdagi ping kechikishini real vaqtda kuzatib boradi. **Ctrl+C** bilan to‘xtatish mumkin.

#### **Faqat IP-manzillarni ko‘rsatish**

traceroute -n 93.170.6.43

IP-manzillarni bevosita ko‘rsatadi (DNS nomlarisiz). Bu **tezroq natija olish** uchun foydali.

### **3. Ping va Tarmoq aloqasini tekshirish**

#### **Serverga ping yuborish va tarmoq ulanishini tekshirish**

ping 93.170.6.43

Agar **ping javob bermasa**, demak u server **yopiq yoki firewall tomonidan bloklangan** bo‘lishi mumkin.

#### **Ping’ni cheksiz davom ettirish (-t parametrisiz)**

ping -i 0.5 93.170.6.43

**0.5 soniya oraliqda ping jo‘natadi** va kechikishni kuzatadi. **Ctrl+C** bilan to‘xtatish mumkin.

### **4. DNS va IP-manzil ma’lumotlarini tekshirish**

#### **93.170.6.43 ning domen nomini aniqlash**

nslookup 93.170.6.43

Bu **IP-manzilning DNS nomini (agar mavjud bo‘lsa) topadi.**

#### **Tarmoq haqida batafsil ma’lumot olish**

whois 93.170.6.43

**IP-manzil kimga tegishli ekanini** aniqlaydi (ISP, mamlakat, domen egasi va h.k.).

### **5. Tarmoqdagi blokirovkalarni tekshirish**

#### **Traceroute natijalarini filtrdan o‘tkazish va faqat kerakli qismni ko‘rish**

traceroute 93.170.6.43 | grep -E "ms|^$"

**Faqat kechikish (ms) bilan bog‘liq natijalarni chiqaradi.** Keraksiz ma’lumotlar ko‘rinmaydi.

#### **Agar marshrutizatorlar javob bermasa, maxsus TTL qo‘yish**

traceroute -m 50 93.170.6.43

**50 ta marshrutdan o‘tguncha davom etadi.** Standart qiymat **30**, agar uzoq yo‘nalish bo‘lsa, ushbu buyruqni ishlatish mumkin.

### **6. Tarmoqdagi muammolarni aniqlash**

#### **Traceroute bilan paket yo‘qotilishini ko‘rish**

mtr --report 93.170.6.43

**Har bir marshrut tugunidagi yo‘qotishlarni** va kechikishlarni ko‘rsatadi.

#### **Firewall yoki NAT blokirovka qilib turganini tekshirish**

telnet 93.170.6.43 80

**Agar telnet ishlamasa**, bu port ochiq emas yoki firewall tomonidan bloklangan bo‘lishi mumkin.

### ****Xulosa: Qaysi buyruq qachon kerak?****

| **Maqsad** | **Buyruq** |
| --- | --- |
| Oddiy traceroute | traceroute 93.170.6.43 |
| ICMP orqali (ping usuli) | traceroute -I 93.170.6.43 |
| TCP port 80 orqali | traceroute -T -p 80 93.170.6.43 |
| Ping orqali tekshirish | ping 93.170.6.43 |
| MTR bilan real vaqtda kuzatish | mtr 93.170.6.43 |
| DNS nomini aniqlash | nslookup 93.170.6.43 |
| IP manzil egasini bilish | whois 93.170.6.43 |
| Firewall blokirovkasini tekshirish | telnet 93.170.6.43 80 |

### ****Tajriba uchun tavsiyalar:****

1️. **traceroute ni turli IP-lar uchun ishlating:**

traceroute google.com

**Google serverlariga qanday yo‘l bilan bog‘lanayotganini tekshiring.**

2️.**Agar tarmoq juda sekin bo‘lsa, mtr bilan real vaqt tahlil qiling:**

mtr 93.170.6.43

**Qayerda muammo borligini aniqlang.**

3️. **whois bilan IP egasini toping:**

whois 93.170.6.43

**Bu IP qaysi mamlakatda va kimga tegishli ekanini bilib oling.**

Bu buyruqlarni bajarsangiz, **tarmoq qanday ishlashini va qayerda muammo borligini** yaxshi tushunib olasiz.

Hydradan tashqari **hujum (attacking)** yoki **penetratsion test** qilish uchun ishlatiladigan turli xil vositalar mavjud. Ular quyidagi kategoriyalarga bo‘linadi:

## **1️.Brute-Force va Parol Kreking Vositalari**

Hydra kabi vositalar login va parollarni taxmin qilish yoki sinab ko‘rish uchun ishlatiladi.

* **Medusa** – SSH, FTP, SMTP, va boshqa xizmatlarga brute-force hujum qilish uchun.
* medusa -h <IP> -U userlist.txt -P passlist.txt -M ssh
* **Ncrack** – SSH, RDP, VNC, FTP va boshqa protokollarni bruteforce qilish uchun.
* ncrack -p 22 -U userlist.txt -P passlist.txt <IP>
* **John the Ripper** – Hashlangan parollarni ochish uchun kuchli vosita.
* john --wordlist=rockyou.txt hashes.txt
* **Hashcat** – GPU yordamida hashlarni kreklash uchun.
* hashcat -m 0 -a 0 hash.txt rockyou.txt

## **2️.Tarmoq va Portlarni Tekshirish (Scanning) Vositalari**

Bu vositalar tarmoqdagi zaifliklarni aniqlash uchun ishlatiladi.

* **Nmap** – Ochiq portlar va xizmatlarni tekshirish uchun.
* nmap -sV -p- 192.168.1.1
* **Masscan** – Juda tezkor port skaner.
* masscan -p1-65535 --rate=100000 192.168.1.1
* **Zmap** – Internet masshtabida skanerlash uchun.

## **3️. Ekspluatatsiya (Exploit) Vositalari**

Bu vositalar zaifliklarni ekspluatatsiya qilish uchun ishlatiladi.

* **Metasploit Framework** – Mashhur ekspluatatsiya platformasi.
* msfconsole
* use exploit/multi/handler
* **ExploitDB** – Zaifliklar ro‘yxati va ekspluatatsiya kodlari to‘plami.
* **SQLmap** – SQL Injection zaifliklarini aniqlash va ekspluatatsiya qilish.
* sqlmap -u "http://target.com/page.php?id=1" --dbs

## **4️.Sniffing va Trafik Analizi Vositalari**

Bu vositalar tarmoq trafigini ko‘rish va tahlil qilish uchun ishlatiladi.

* **Wireshark** – Tarmoq trafigini real vaqtda analiz qilish uchun GUI vositasi.
* **Tcpdump** – Terminal orqali tarmoq trafigini kuzatish.
* tcpdump -i eth0 -nn port 80
* **Ettercap** – ARP Poisoning va Man-in-the-Middle (MITM) hujumlari uchun.

## **5️.Veb Zaifliklarni Tekshirish (Web Pentesting) Vositalari**

* **Burp Suite** – Veb zaifliklarni tahlil qilish va ekspluatatsiya qilish.
* **Wpscan** – WordPress saytlarini zaiflik uchun skanerlash.
* wpscan --url http://target.com --enumerate u
* **Nikto** – Veb-serverdagi xavfsizlik muammolarini aniqlash.
* nikto -h http://target.com

## **6️.DDoS Hujum Vositalari**

**E’tibor bering: bu vositalardan noqonuniy foydalanish jinoiy javobgarlikka olib kelishi mumkin.**

* **Hping3** – TCP/UDP ping hujumlari.
* hping3 -S -p 80 -c 10000 <IP>
* **Slowloris** – Apache va boshqa serverlarni DDoS qilish uchun.
* slowloris http://target.com

## **Xulosa**

Agar siz **penetratsion test qilish** yoki **zaifliklarni tekshirish** uchun vositalar izlayotgan bo‘lsangiz, yuqoridagi vositalardan foydalanishingiz mumkin.

Agar **hujum (attacking)** maqsadida noqonuniy foydalanish niyatida bo‘lsangiz, bu **jinoiy harakat** ekanligini unutmang. Har qanday vositani **faqat ruxsat berilgan test tizimlarida** ishlatish lozim. **Rahmat**!!!

**By Zuhra Shavkatova**