🛠️ Step 1: TryHackMe VPN से कनेक्ट करना

(ताकि Target Machine तक पहुँच सकें)

TryHackMe पर Hack करने से पहले **VPN से कनेक्ट करना ज़रूरी है**, क्योंकि टार्गेट मशीन **VPN नेटवर्क में ही रहती है**।

✅ TryHackMe VPN से जुड़ने के लिए:

1️⃣ **TryHackMe में लॉगिन करो**

2️⃣ **Dashboard पर जाओ** और **Access > OpenVPN** सेक्शन खोलो

3️⃣ **VPN Configuration File (.ovpn) डाउनलोड करो**

4️⃣ Kali Linux में टर्मिनल खोलो और यह कमांड चलाओ:

bash

CopyEdit

sudo openvpn <your-vpn-file.ovpn>

(यहाँ <your-vpn-file.ovpn> को अपने डाउनलोड किए गए फाइल के नाम से बदलो।)

5️⃣ **अगर VPN कनेक्ट हो गया**, तो यह कमांड चलाकर चेक करो:

bash

CopyEdit

ifconfig tun0

अगर इसमें **"tun0" इंटरफेस दिखता है**, तो ✅ **VPN सही से कनेक्ट हो गया!** 🎉

🔍 Step 2: Target Machine (10.10.0.45) का स्कैनिंग करना

(पता करो कौन-कौन सी सर्विस चल रही है?)

अब हमें यह देखना है कि **Target Machine (10.10.0.45)** पर **क्या-क्या सर्विस (जैसे SSH, HTTP, etc.) चल रही हैं**।

✅ Target Machine के Open Ports चेक करने के लिए:

bash

CopyEdit

nmap -A -T4 10.10.0.45

यह कमांड हमें बताएगी:

✅ कौन-कौन से **Ports खुले हैं** (22, 80, 443, etc.)

✅ कौन-कौन से **सॉफ़्टवेयर चल रहे हैं** (Apache, SSH, etc.)

✅ कोई **वॉल्नरेबिलिटी (कमज़ोरी) है या नहीं**

📌 **Example Output:**

arduino

CopyEdit

22/tcp open ssh OpenSSH 7.2p2

80/tcp open http Apache 2.4.18

445/tcp open smb Samba 3.0.20

➡️ यहाँ दिख रहा है कि **SSH (22), Website (80), और SMB (445) खुला है।**

➡️ इसका मतलब हमें इन्हें **Hack करने के तरीके खोजने होंगे!**

💥 **Step 3: Target Machine को हैक करने की कोशिश**

अब हमें देखना होगा कि **हम टार्गेट में घुस सकते हैं या नहीं!**

✅ **अगर Port 80 (Website) खुला है तो:**

1️⃣ वेबसाइट खोलो:

- अपने ब्राउज़र में जाओ और URL डालो:

cpp

CopyEdit

http://10.10.0.45

2️⃣ Website के Hidden Files खोजो:

bash

CopyEdit

gobuster dir -u http://10.10.0.45 -w /usr/share/wordlists/dirb/common.txt

➡️ अगर /admin, /login, /hidden जैसी कोई **सीक्रेट डायरेक्टरी** मिलती है, तो उसे खोलो।

✅ **अगर Port 22 (SSH) खुला है तो:**

SSH एक ऐसी सर्विस है जिससे **सीधे सिस्टम के अंदर लॉगिन कर सकते हैं**।

1️⃣ अगर हमें कोई **Username और Password मिल गया**, तो लॉगिन करें:

bash

CopyEdit

ssh user@10.10.0.45

2️⃣ अगर पासवर्ड नहीं पता, तो **Brute Force Attack** ट्राई कर सकते हैं:

bash

CopyEdit

hydra -l user -P rockyou.txt ssh://10.10.0.45

➡️ यह कोशिश करेगा कि कोई **सही पासवर्ड मिल जाए** और हम अंदर घुस सकें।

🚀 **Step 4: User Flag (user.txt) और Root Flag (root.txt) ढूँढना**

अगर हम **सिस्टम में घुस गए**, तो अब हमें **फ्लैग्स** ढूंढने होंगे!

✅ **सबसे आसान तरीका – जल्दी से Flag निकालने की Trick:**

bash

CopyEdit

find / -type f \(-name "user.txt" -o -name "root.txt" \) 2>/dev/null -exec cat {} +

📌 **यह क्या करेगा?**

✔ **पूरे सिस्टम में "user.txt" और "root.txt" को ढूँढेगा**

✔ **अगर मिला तो उसका content (flag) दिखा देगा**

Example Output:

pgsql

CopyEdit

THM{user-flag-found}

THM{root-flag-found}

➡️ **बस इन Flags को Copy करो और TryHackMe में Submit कर दो!** 🎉

✅ **Quick Recap (सारांश)**

Step	Task
1	**TryHackMe VPN से कनेक्ट करो** (openvpn <file.ovpn>)
2	**Nmap से Target Machine (10.10.0.45) को स्कैन करो** (nmap -A -T4 10.10.0.45)
3	**अगर वेबसाइट (Port 80) खुला है तो Gobuster से Hidden Files खोजो**
4	**अगर SSH (Port 22) खुला है, तो SSH लॉगिन ट्राई करो**
5	**अगर सिस्टम में घुस गए, तो Flag (user.txt, root.txt) खोजो**
6	**Flag को TryHackMe में Submit करो और CTF जीत जाओ!** 🎯

🔴 **अब आपकी बारी!**

💡 **TryHackMe पर कोई CTF ट्राई करो और इन Steps को Follow करो।**