Descarcati aplicatia SecuritateSoftware-v3.5

\*Analizam comanda get a serverului prin prisma TOCTOU

\*Analizam codul sursa al fisierului executabil toctou.exe poate fi gasit in arhiva in folderul release

\*Lansam serverul, toctou.exe si client.exe

\*Ne logam cu user-ul pop/pop si incercam sa exploatam vulnerabilitatea din comanda get.

\*Ce obtinem dupa exploatarea vulnerabilitatii?

You are given this VirtualBox image (1 GB). You have to log in using the "attacker/attacker" credentials.

There is a /home/attacker/race-conditions/ directory with two sub-directories, each one for a different challenge.

Correspondingly, there are two executable files "/usr/bin/race-conditions-ctf\*".

You have to display the contents of the following flag files:

"/root/race-conditions/ctf1.txt", by exploiting the "/usr/bin/race-conditions-ctf1" program (look at its source code file in "/home/attacker/race-conditions/ctf1")

"/root/race-conditions/ctf2.txt", by exploiting the "/usr/bin/race-conditions-ctf2" program (look at its source code file in "/home/attacker/race-conditions/ctf2")