

CYBER INVASION

#nc3ctf2021 - Cyber Invasion 2021

En nemmere reversing opgave, som måske kunne lokke nye til reversing området.

Brugeren får et Windows spil, der er inspireret af Space Invaders. Der kommunikeres med en server, der kører på TryHackMe. Opgaven er ikke at hacke denne server, men derimod at hacke netværkskommunikationen mellem spillet og serveren. Målet er at slå highscoren, der er på 1 million. Når serveren ser en ny highscore kommer flaget tilbage.

Spillet er lavet i C# og kan derfor nemt decompiles med "dnspy".

Heri kan man finde frem til netværksdelen. Denne kan analyseres, og reimplementeres i f.eks. Python, hvor man så emulerer spillet ved at sende de samme netværkspakker som spillet ville sende hver gang spilleren får et point. Man kan da sætte antal point op til maks, således at man hurtigere opnår highscoren. Et sådant script er vedlagt.

Et alternativt, der blev brugt internt, er at ændre C# koden direkte i dnspy således at scoren er maks, og at score funktionen ("IncreaseScoreOnNetwork") køres konstant.

Flaget:

nc3{wooooow_du_er_jo_en_cybercop_4real}

