Assignment 1: Mixnets

Santiago Aragón

s.e.aragonramirez@student.utwente.nl

Owais Ahmed

o.ahmed@student.utwente.nl

University of Twente

The following scenario is being analyzed: a program has been found vulnerable since it uses the insecure *strcpy* insted of the *strncpy* function without performing the proper sanity checks. The programs copy the content of file, under control of the attacker that is supposed to be 517 bytes long, into a buffer of 24 bytes long.

When the vulnerable function is called the stack looks as follows:

[buffer(24)][prelude][sfp(4)][ret(4)][badfile][str(517)][prelude]

Our final goal is to summon a root shell by overflowing the buffer.