Bezpieczeństwo
Laboratorium 3
Rozwal.to

Mateusz Mańka

1. Starter – Stegano : http://training.securitum.com/rozwal/starter/rozwal.jpg
   Zadanie za 100 pkt a było stosunkowo proste, polegało na przeklejeniu całego skryptu do konsoli I odpaleniu.
   Wynik został wyświewtlony w postaci flagi : ROZWAL_{PLATFORMAHACKMENADCHODZI}
2. Crypto – BOB : http://training.securitum.com/rozwal/abc/6.php
   Poniewaz w tym zadaniu bob kodował tylko jednym znakiem wystarczyło przeriterować się po wszystkich znakach ascii I sprawdzić czy w wyniku znajduje sie słowo ROZWAL_
   (Program w folderze /bob)
   Flaga : ROZWAL_{SingleXorByteCipher}
3. Crypto Cweyk fincbjqlsiluqe - http://training.securitum.com/rozwal/crypto/3.php
   Zadanie polegało na odszyfrowaniu tekstu angielskiego ,
   Jak na razie nie udało mi się go wykonać lecz mam już odszyfrowane kilka znaków :
   Na przykład „KUWQJG_{„ jest ewidentnie początkiem flagi czyli ROZWAL_{
   dodatkowo najczęściej występującą literą jest „s” wiec najprawdopodobniej będzie to „t” występujące najczęściej w alfabecie angielskim a „1950’c mówi nam że „c” będzie najprawdopodobniej „s” z braku czasu nie dokończyłem tego zadania
4. Crypto – Nie kłam -http://training.securitum.com/rozwal/abc/4.php

Ponieważ MCRYPT_RIJNDAEL_128 dokłąda byty zerowe należy przeprowadzić null patting Oracle attack i ustawić odpowiednie ciastko (Jeszcze mi się to nei dudało)