1 Description

Title: Cosmic generator

Category: Crypto

Value: 400

Дан файл spacesecrets.jpg, содержащий зашифрованную информацию. Также, дан файл encode.py, осуществляющий шифрование и spacenoize.pcap с дампом трафика.

2 Legend

Космос пронизывают бесчисленные множества радиоволн, некоторые из которых являются просто случайным шумом, а некоторые специально сгенерированным.

3 Flag

Flag regex:	simple text
Flag:	дажешумсодержитсмысл

4 Solution

В питоновском скрипте реализован стандартный алгоритм шифрования при помощи XOR с псевдослучайной последовательностью, сгенерированной линейным сдвиговым регистром с обратной связью. В дампе трафика можно найти ICMP пакеты и собрать из их содержимого последовательность (коды 30 и 31 - это ASCII коды нуля и единицы). Далее следует догадаться, что поксорив ее с зашифрованной картинкой - получается валидная сигнатура. Однако, последовательность только 120 байт, а нужно для картинки гораздо больше. Применяем алгоритм Берлекемпа-Месси и получаем результат. Подробнее в файле solver.py. Возможны и иные варианты ввиду того, что seed и polynom имеют небольшые значения.

5 Hints

1. Космический шум, всем известно, передается пингами по 10 значений в каждом.

2. Это довольно известный алгоритм генерации гаммы.

3. иссэМ — апмэкелреБ мтироглА.

4. Алгоритм Берлекэмпа — Мэсси.

5. Если совсем не идет - seed 3 бита, polynom 12 бит.

6 Discussion

Тут и проще и сложнее некуда. Разве что можно PCAP похитрее закодировать.

7 Setup

Выдать командам файлы censored.jpg, encoding_script.py, spacenoize.pcap.