Hacking de Binários em Hexadecimal

Mateus Gabi Moreira e Yan Uehara

8 de abril de 2018

1 Introdução

O trabalho consiste no desenvolvimento de três ferramentas para a injeção de conteúdo textual em arquivos binários. As três ferramentas são denominadas: Finder, Extractor e Injector. O Finder é responsável por encontrar as strings de busca dentro do binário. O Extractor é responsável por remover a string de dentro do binário sem corromper o binário. O Injector é responsável por substituir um trecho do arquivo por outro.

2 Métodos

O trabalho foi desenvolvido utilizando Python na versão 2.7.14 e Github[1] para o desenvolvimento distribuído.

3 Resultados

As três ferramentas foram desenvolvidas. O Finder foi implementado usando a busca relativa. Infelizmente, a busca relativa funciona apenas para caracteres minúsculas. Isto é, na hora de realizar a busca tem que informar apenas caracteres minúsculos, exemplo, busque por **elcome** ao invés de **Welcome**. Além disso, a tabela é gerada de forma automatizada para letras minúsculas, maiúsculas e caracteres especiais e exportada para um arquivo binário com extensão **.btbl** no mesmo local do binário.

O Extractor retira todas as strings a partir de um **offset** que é encontrado pelo Finder. Esse offset nada mais é que a posição no binário da primeira ocorrência da palavra buscada. O Extractor gera um arquivo de saída no mesmo diretório do arquivo binário e com o mesmo nome, acrescido da extensão **.extracted.txt**

Já o Injector injeta em uma caixa de diálogo do binário um texto. Esse texto necessita estar na mesma pasta do binário em um arquivo de mesmo nome com a extensão **.inj.txt**. As quebras de linha da caixa são automaticamente colocadas e o texto é truncado automaticamente para não ultrapassar os limites da caixa e corromper o binário.

Um exemplo de execução pode ser visto abaixo:

```
1 python Finder\finder.py ..\smario.sfc elcome
2 python Extractor\extractor.py ..\smario.sfc ..\smario.btbl
3 python Injector\injector.py ..\smario.sfc ..\smario.btbl ..\smario.inj.txt
```

E uma imagem com o texto alterado pode ser visto na Figura 1

[1] Disponível em: https://github.com/MateusGabi/Binary-Hacking-String-Replacer

Figura 1: Exemplo de funcionamento