OverTheWire: Krypton

Categoria: Cripto

Krypton0

Precisamos decodificar a mensagem `S1JZUFRPTklTR1JFQVQ=` para o próximo nível.

É dito que ela está em **base64**. Para resolver isso, é só usar o comando `base64`.

```
echo "S1JZUFRPTklTR1JFQVQ=" | base64 -d
```

Assim, obtemos a senha de Krypton1.

Resposta: `KRYPTONISGREAT`.

Krypton1

É preciso decodificar a mensagem `YRIRY GJB CNFFJBEQ EBGGRA`, encriptada por **rotação simples**.

Rotação simples pode significar alguma versão da Cifra de César, provavelmente ROT13. Para isso, podemos usar sites como dcode ou criar um programa em python que automatize isso: k1.py.

A resposta está na cifra decodificada por ROT13: `LEVEL TWO PASSWORD ROTTEN`.

Resposta: `ROTTEN`.

Krypton2

Temos no arquivo `krypton3` a mensagem `OMQEMDUEQMEK` que está criptografada em **Cifra de César**.

Há duas formas de resolver esse nível.

Podemos criar uma pasta em `/tmp/` e linkar a keyfile nele para usarmos o executável `encrypt`. Dessa forma, podemos encriptar um arquivo com `a` para descobrir a rotação usada.

Com isso, o arquivo encriptado terá a letra `m`, indicando que foi usado ROT12 para encriptação e deverá ser usado ROT14 para decriptação, obtendo a *flag*.

Outro modo, muito mais rápido, é usar o mesmo método do nível anterior, fazendo um *brute-force* das 26 rotações possíveis de uma Cifra de César. A que tiver a frase mais legível é a *flag*.

Resposta: `CAESARISEASY`.

Krypton3

Para esse nível, temos no arquivo `krypton4` a mensagem `KSVVW BGSJD SVSIS VXBMN YQUUK BNWCU ANMJS`, cifrada por alguma **cifra de substituição simples**. Nesse momento, usar *brute-force* não é mais uma opção.

Para resolver isso, podemos pegar o texto em `found1` e aplicar uma análise de frequência em suas letras.

Uma ferramenta online extremamente eficiente está localizada em guabala.de. Utilizando sua análise de frequência, obtemos o mapeamento:

```
abcdefghijklmnopqrstuvwxyz     This clear text ...
qazwsxedcrfvtgbyhnujmikolp     ... maps to this cipher text
```

Podemos, assim, decriptar a mensagem com o site dcode utilizando o alfabeto de susbtituição acima. O resultado é o texto `WELLD ONETH ELEVE LFOUR PASSW ORDIS BRUTE`.

Resposta: `BRUTE`.

Krypton4

Nesse nível, há a mensagem `HCIKV RJOX` em `krypton5`, codificada pela **Cifra de Vigenère**.

Primeiro, precisamos descobrir a *key* da cifra. Para isso usaremos o texto em `found1` e a ferramenta em dcode. Assim, encontramos a *key* `FREKEY`.

Dessa forma, utilizando novamente o dcode com a *key*, obtemos a *flag*.

Resposta: `CLEARTEXT`.

Krypton5

Para esse nível, também temos uma mensagem codificada pela **Cifra de Vigenère**, porém sem termos o conhecimento do tamanho da chave.

Para descobrir a *key* podemos usar o texto em `found1` e a ferramenta em dcode. Usando a análise estatística, obtemos uma resposta parcial: `KEYLEBGTH`.

Essa resposta é próxima de um termo legível: `KEYLENGTH`. Testando essa *key* em `found1` usando o dcode, vemos que ela decifra o texto perfeitamente.

Assim, decriptando o texto `BELOS Z` usando a *key* `KEYLENGTH` obtemos a flag.

Resposta: `RANDOM`.

- Nada ainda