

PROCESSO DE DECRIPTAÇÃO DO ARQUIVO “arquivo-strong-9.in-full.hex”

Aluno: Pedro Lucas Moraes de Sousa Rosa

Professor: Wewerton Luis da Costa Cordeiro

A implementação utilizada foi um ataque de força bruta focado e otimizado, baseado em algumas informações conhecidas:

1ª Informação conhecida critica:

- A chave começa com "Security00".
- O texto decifrado pode ou não estar legível em ASCII.
- O algoritmo usado é o AES no modo ECB.

2ª Estratégia de força bruta otimizada:

- Ao invés de efetuar os testes de chave, foi necessário apenas converter o arquivo hex para utf-8:
 - Criado um código para conversão do arquivo hex para vários tipos de encoding, fazendo com que chegasse ao resultado da conversão em UTF-8, conforme o print abaixo.

```

teste_pedro_strong.py > ...
1 def decode_hex_to_text(hex_string):
2     """
3     Tenta decodificar uma string hexadecimal usando diferentes codificações
4     Retorna um dicionário com os resultados de cada codificação
5     """
6     # Remove espaços em branco e quebras de linha
7     hex_string = hex_string.strip()
8
9     # Converte hex para bytes
10    try:
11        byte_data = bytes.fromhex(hex_string)
12    except ValueError as e:
13        return f"Erro ao converter hex: {e}"
14
15    # Lista de codificações para tentar
16    encodings = ['utf-8', 'latin1', 'cp1252', 'iso-8859-1']
17
18    results = {}
19
20    # Tenta cada codificação
21    for encoding in encodings:
22        try:
23            decoded_text = byte_data.decode(encoding)
24            results[encoding] = decoded_text
25        except UnicodeDecodeError:
26            results[encoding] = f"Não foi possível decodificar usando {encoding}"
27
28    return results
29
30 def main():
31     # Lê o arquivo hex
32     with open('arquivo-strong-9.in-full.hex', 'r') as f:
33         hex_content = f.read()
34
35     # Decodifica o conteúdo
36     results = decode_hex_to_text(hex_content)
37
38     # Imprime os resultados
39     print("Resultados da decodificação:\n")
40     for encoding, text in results.items():
41         print(f"\n=== Decodificação usando {encoding} ===\n")
42         print(text)
43         print("\n" + "="*50 + "\n")
44
45
46
47 if __name__ == "__main__":
48     main()

```

Esta implementação é particularmente eficiente porque, apenas converte o arquivo hex para UTF-8, sem necessidade de testes de chave para decriptar o arquivo, uma vez que ele está apenas convertido.

Resultado do arquivo decriptado:

- Chave = Não possui chave.
- Código Secreto do arquivo = zESbhm.
- Tempo máximo de decriptação = 0.1 milissegundos.
- Quantidade de chaves testadas até encontrar a chave correta: não houve tentativas de teste de chaves, uma vez que o arquivo não estava encriptado.

- Média de chaves testadas por segundo: Não houve testes de chaves, uma vez que o arquivo não estava encriptado.

```
PROBLEMAS ⓘ SAÍDA CONSOLE DE DEPURAÇÃO TERMINAL PORTAS
Resultados da decodificação:

=== Decodificação usando utf-8 ===

Lórem ipsúm dólór sit amet, consectetur adipiscing elit. Sed mauris massa, pulvinar et accumsan condimentum, rutrum fringilla justo. Integer hendrerit leo volutpat malesuada venenatis. Vivamus euismod viverra erat, eu fermentum nisi viverra nec. Quisque pharetra venenatis libero, id mollis neque consectetur at. Mauris venenatis lorem at dictum sodales. Nam sed nisi eu metus maximus pharetra vitae tincidunt risus. Nullam urna quam, sagittis eget congue at, luctus nec lorem. Integer hendrerit imperdiet augue ac semper. Vestibulum varius fermentum eleifend. Duis vitae tellus pharetra, luctus libero vel, luctus ipsum. Morbi tempor ornare nibh in viverra. Duis molestie dapibus libero vel consequat. Donec vitae malesuada magna. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nullam pretium turpis eu commodo faucibus. In finibus, erat quis rhoncus sodales, sapien enim posuere neque, id egestas velit sem nec nulla. Pellentesque ipsum magna, venenatis id eleifend a, accumsan eu lorem. Aliquam erat volutpat. Sed ut ultricies neque, a egestas mi. Pellentesque pellentesque, justo id varius vestibulum, enim risus euismod augue, et suscipit neque elit eget magna. Nam tempor sit amet lacus id volutpat. Donec egestas faucibus mauris. In molestie tincidunt mi. Mauris scelerisque, tortor vel pharetra sagittis, tellus velit pharetra erat, a ultricies ex risus tempor felis. Cras condimentum ac erat eu convallis. Nulla sapien ipsum, ullamcorper in interdum at, consectetur vitae quam. Phasellus ligula mi, scelerisque sit amet lacus nec, lacini..

Êxito na força bruta:: zESzhm

=====
```