LEVEL 0

echo "S1JZUFRPTklTR1JFQVQ=" | base64 –decode

LEVEL 1

1. Display the encoded password

cat /krypton/krypton1/krypton2

2. Decode with ROT13

echo "YRIRY GJB CNFFJBEQ EBGGRA" | tr 'A-Za-z' 'N-ZA-Mn-za-m'

LEVEL 3

1. Login to Krypton3 (already done)

2. List files in home directory

ls -la

3. Move to the krypton3 challenge directory

cd /krypton/krypton3

4. List all files

ls

5. View the first hint

cat HINT1

6. View the second hint

cat HINT2

7. View the ciphered text for krypton4 password

cat krypton4

8. View the larger ciphertext (for frequency analysis practice)

cat found1

9. Copy the text from 'found1' and use an online frequency analysis tool (e.g., quipqiup.com) to decode it

10. Use the decoded text or password to log in to krypton4

ssh krypton4@krypton.labs.overthewire.org -p 2231

LEVEL 4

Step 1: Combine the Cipher Text

cat found1 found2 | tr -d ' ' > /tmp/combined.txt

Step 2: Split the Cipher Text into Columns Based on Key Length

cat /tmp/combined.txt | awk '{ for (i=0; i<length($0); i++) print i%6, substr($0,i+1,1) }' > /tmp/split.txt

Step 3: Extract Each Column and Count Frequencies

grep "^0 " /tmp/split.txt | cut -d" " -f2 > /tmp/col0.txt

grep "^1 " /tmp/split.txt | cut -d" " -f2 > /tmp/col1.txt

grep "^2 " /tmp/split.txt | cut -d" " -f2 > /tmp/col2.txt

grep "^3 " /tmp/split.txt | cut -d" " -f2 > /tmp/col3.txt

grep "^4 " /tmp/split.txt | cut -d" " -f2 > /tmp/col4.txt

grep "^5 " /tmp/split.txt | cut -d" " -f2 > /tmp/col5.txt

Step 4: Frequency Analysis

cat /tmp/col0.txt | sort | uniq -c | sort -nr

cat /tmp/col1.txt | sort | uniq -c | sort -nr

cat /tmp/col2.txt | sort | uniq -c | sort -nr

cat /tmp/col3.txt | sort | uniq -c | sort -nr

cat /tmp/col4.txt | sort | uniq -c | sort -nr

```
cat /tmp/col5.txt | sort | uniq -c | sort -nr

# Step 5: Python Decryption Code (after deriving the key 'FREKEY')
cipher = 'HCIKVRJOX'
key = 'FREKEY'
plain = ''
for i, c in enumerate(cipher):
    shift = ord(key[i % len(key)].upper()) - ord('A')  # The key should be uppercase
    plain += chr((ord(c) - shift - 65) % 26 + 65)
print(plain)
```

LEVEL 5

```
cd /krypton/krypton5
cat krypton6
cat found1
cat found2
```

LEVEL 6

1. Navigate to the krypton6 directory:

```
cd /krypton/krypton6
```

2. List the contents of the directory:

```
ls
```

3. Read the contents of HINT1:

```
cat HINT1
```

4. Read the contents of HINT2:

```
cat HINT2
```

5. Create a temporary directory:

```
mktemp -d
cd /tmp/tmp.tmP7qig8WF
```

6. Create a symbolic link to keyfile.dat:

ln -s /krypton/krypton6/keyfile.dat

7. Set the appropriate permissions to the directory (optional):

chmod 777 .

8. Create a file named life.txt and add content to it:

touch life.txt

nano life.txt

Content added to life.txt:
"ITWASTHEBESTOFTIMESITWASTHEWORSTOFTIMES"

9. Encrypt life.txt to cipherlife:

/krypton/krypton6/encrypt6 life.txt cipherlife

10. View the content of cipherlife:

cat cipherlife

11. View the binary representation of life.txt:

xxd -b life.txt

12. View the binary representation of cipherlife:

xxd -b cipherlife

13. Create a new file d.txt with 100 'A' characters:

python3 -c "print('A'*100)" > d.txt

14. Encrypt d.txt to cipher_d.txt:

/krypton/krypton6/encrypt6 d.txt cipher_d.txt

15. View the content of cipher_d.txt:

cat cipher_d.txt

16. View the content of krypton7 to check for any additional clues:

cat /krypton/krypton6/krypton7