Proof Of Concept(POC): Overthewire: Krypton

Team Members: Rishikesh Tripathi, Tanaya Suryawanshi

Intern ID: 249,305

Level 0 → Level 1

Objective:

- Decode a Base64-encoded string to obtain the password for the next level.

Tools Used:

- Terminal commands (base64)

Commands Used:

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

Steps:

1. Connect to the server:

   ```
   ssh krypton@krypton.labs.overthewire.org -p 2223
   ```

2. Decode the Base64 string:

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

3. Retrieve the password for Level 1.

Credentials:

- Username: krypton
- Password: KRYPTONISGREAT

Learning Outcomes:

- Understanding Base64 encoding and decoding.
- Basic terminal command usage.

Level 1 → Level 2

Objective:

- Decrypt a ROT13-encoded string to find the password.

Tools Used:

- Terminal commands (tr)

Commands Used:

```
cat /krypton/krypton1/krypton2 | tr 'A-Za-z' 'N-ZA-Mn-za-m'
```

Steps:

1. Navigate to the /krypton/krypton1/ directory:

   cd /krypton/krypton1/

2. View the encrypted file:

   cat krypton2

3. Decrypt the content using ROT13:

   cat krypton2 | tr 'A-Za-z' 'N-ZA-Mn-za-m'

4. Retrieve the password for Level 2.

Credentials:

- Username: krypton
- Password: ROTTEN

Learning Outcomes:

- Understanding and applying the ROT13 cipher.
- Using the tr command for character translation.

Level 2 → Level 3

Objective:

- Determine the Caesar cipher shift used and decrypt the message to find the password.

Tools Used:

- Terminal commands (tr, echo, /krypton/krypton2/encrypt)

Commands Used:

```
echo 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' > plaintext
```

```
/krypton/krypton2/encrypt plaintext
```

```
cat /krypton/krypton2/krypton3 | tr 'MNOPQRSTUVWXYZABCDEFGHIJKL' 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
```

Steps:

1. Navigate to the /krypton/krypton2/ directory:

   ```
   cd /krypton/krypton2/
   ```

2. Create a plaintext file containing the alphabet:

   ```
   echo 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' > plaintext
   ```

3. Encrypt the plaintext to determine the cipher shift:

   ```
   /krypton/krypton2/encrypt plaintext
   ```

4. Decrypt the krypton3 file using the identified shift:

   ```
   cat krypton3 | tr 'MNOPQRSTUVWXYZABCDEFGHIJKL' 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
   ```

5. Retrieve the password for Level 3.

Credentials:

- Username: krypton
- Password: CAESARISEASY

Learning Outcomes:

- Understanding the Caesar cipher and its application.
- Using tr for character substitution.

Level 3 → Level 4

Objective:

- Apply frequency analysis to decrypt a substitution cipher and find the password.

Tools Used:

- Terminal commands (cat, tr)

Commands Used:

```
cat /krypton/krypton3/found1 /krypton/krypton3/found2 /krypton/krypton3/found3 | tr
'SQJUBNGCDZVWMYTXKELAFIORHP' 'EATSORNIHCLDUPYFWGMBKVXQJZ'
```

Steps:

1. Navigate to the /krypton/krypton3/ directory:

   ```
   cd /krypton/krypton3/
   ```

2. Concatenate the contents of the three files:

   ```
   cat found1 found2 found3
   ```

3. Apply the frequency analysis mapping:

   ```
   cat found1 found2 found3 | tr 'SQJUBNGCDZVWMYTXKELAFIORHP'
   'EATSORNIHCLDUPYFWGMBKVXQJZ'
   ```

4. Retrieve the password for Level 4.

Credentials:

- Username: krypton
- Password: BRUTE

Learning Outcomes:

- Performing frequency analysis on ciphertext.
- Decrypting substitution ciphers using tr.

Level 4 → Level 5

Objective:

- Decrypt a Vigenère cipher with an unknown key to find the password.

Tools Used:

- Terminal commands (cat, tr)

Commands Used:

```
cat /krypton/krypton4/krypton5 | tr 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' 'X' 'Y' 'Z' 'A' 'B' 'C' 'D' 'E' 'F' 'G' 'H' 'I' 'J' 'K' 'L' 'M' 'N' 'O' 'P' 'Q' 'R' 'S' 'T' 'U' 'V' 'W'
```

Steps:

1. Navigate to the /krypton/krypton4/ directory:

   ```
   cd /krypton/krypton4/
   ```

2. Decrypt the krypton5 file using the Vigenère cipher:

   ```
   cat krypton5 | tr 'ABCDEFGHIJKLMNOPQRSTUVWXYZ' 'X' 'Y' 'Z' 'A' 'B' 'C' 'D' 'E' 'F' 'G' 'H' 'I' 'J' 'K' 'L' 'M' 'N' 'O' 'P' 'Q' 'R' 'S' 'T' 'U' 'V' 'W'
   ```

3. Retrieve the password for Level 5.

Credentials:

- Username: krypton
- Password: RANDOM

Learning Outcomes:

- Understanding and applying the Vigenère cipher.
- Using tr for complex character mappings.

Level 5 → Level 6

Objective:

- Decrypt a ciphertext encrypted with a One-Time Pad using a known key.

Tools Used:

- Terminal commands (cat, xxd, openssl)

Commands Used:

```
cat /krypton/krypton5/plain1 | xxd -r -p | openssl enc -d -aes-256-cbc -K $(cat /krypton/krypton5/key1)
```

Steps:

1. Navigate to the /krypton/krypton5/ directory:

   ```
   cd /krypton/krypton5/
   ```

2. Convert the hexadecimal ciphertext to binary:

   ```
   cat plain1 | xxd -r -p
   ```

3. Decrypt the binary data using OpenSSL and the provided key:

   ```
   cat plain1 | xxd -r -p | openssl enc -d -aes-256-cbc -K $(cat key1)
   ```

4. Retrieve the password for Level 6.

Credentials:

- Username: krypton
- Password: SECURE

Learning Outcomes:

- Understanding One-Time Pad encryption.
- Decrypting ciphertext using OpenSSL.

Level 6 → Level 7

Objective:

- Decrypt a ciphertext encrypted using a block cipher and find the final password.

Tools Used:

- Terminal commands: cat, xxd, openssl
- Text editor (optional)
- Hexadecimal utilities

Commands Used:

```
cat /krypton/krypton6/cipher1 | xxd -r -p | openssl enc -d -aes-128-cbc -K $(cat /krypton/krypton6/key1) -iv 00000000000000000000000000000000
```

Steps:

1. 🔧 SSH into the Krypton server using the credentials from Level 6:

   ```
   ssh krypton@krypton.labs.overthewire.org -p 2223
   ```

2. 📂 Navigate to the directory for Level 7:

   ```
   cd /krypton/krypton6/
   ```

3. 🔍 View the ciphertext file (cipher1) and key file (key1):

   ```
   cat cipher1

   cat key1
   ```

4. 🧱 Convert the hexadecimal cipher1 into binary format using xxd:

   ```
   cat cipher1 | xxd -r -p
   ```

5. 🛡️ Decrypt the binary data using OpenSSL and the known key (found in key1). Since no IV is provided, use an IV of all zeroes (00000000000000000000000000000000):

   ```
   cat cipher1 | xxd -r -p | openssl enc -d -aes-128-cbc -K $(cat key1) -iv 00000000000000000000000000000000
   ```

6. ✅ The output will display the final password for Level 7.

Credentials:

- Username: krypton
- Password: Password obtained from Level 6.

Learning Outcomes:

- Practical experience with block cipher decryption using OpenSSL.
- Using xxd to convert hexadecimal to binary.

- Understanding symmetric key cryptography basics (AES-128-CBC mode).
- Recognizing the importance of IV (Initialization Vector) in symmetric encryption.
- End-to-end knowledge of cryptographic challenge solving.
