

**Team Name: HackHunters**

**Team Members: Haria Dhruti Jagdish**

**Gala Dharmik Vimal**

**Commands:**

***Krypton***

**Level 0 → Level 1:**

---

1. Decode the Base64 password:
  2. `echo "S1JZUFRPTklTR1JFQVQ=" | base64 --decode`
  3. Log in via SSH:
  4. `ssh krypton1@krypton.labs.overthewire.org -p 2231`
  5. List files in the `/krypton/` directory:
  6. `ls /krypton/`
- 

**Level 1 → Level 2 :**

`ssh krypton1@krypton.labs.overthewire.org -p 2231`

`ls`

`cat krypton2`

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

---

**Level 2 → Level 3:**

`ssh krypton2@krypton.labs.overthewire.org -p 2231`

`ls`

`cat krypton3`

`mktemp -d`

```
cd /tmp/<tempdir>
ln -s /krypton/krypton2/keyfile.dat
chmod 777 .
/krypton/krypton2/encrypt /etc/issue
strings ciphertext
echo "CIPHERTEXT" | tr 'A-Z' 'U-ZA-T'
```

---

#### **Level 3 → Level 4 :**

```
ssh krypton3@krypton.labs.overthewire.org -p 2231
ls
cat krypton4
cat found1
cat found2
cat found3
cat krypton4 found1 found2 found3 > all_found
cat all_found
```

---

#### **Level 4 → Level 5:**

```
ssh krypton4@krypton.labs.overthewire.org -p 2231
ls
cat krypton5
cat found1
cat found2
# manual analysis and decrypt using Vigenère cipher
```

---

#### **Level 5 → Level 6:**

```
ssh krypton5@krypton.labs.overthewire.org -p 2231
ls
```

```
cat krypton6  
# manual kasiski examination  
# frequency analysis  
# manual decryption
```

---

**Level 6 → Level 7:**

```
ssh krypton6@krypton.labs.overthewire.org -p 2231  
ls  
hexdump -C krypton7  
echo -n "A" > inputfile  
./encrypt6 inputfile  
hexdump -C ciphertext  
xxd -p krypton7 > cipher_hex.txt  
# (then manual XOR analysis)
```

---