**Commands used for KRYPTON Level 0 🡪 Level 1: -**

1. **echo S1JZUFRPTklTR1JFQVQ= | base64 -d**

**This decodes a Base64-encoded string**

1. **ssh -p 2231** [**krypton1@krypton.labs.overthewire.org**](mailto:krypton1@krypton.labs.overthewire.org)

**This command is for logging into Krypton Level 1 on OverTheWire.**

**Commands used for KRYPTON Level 1 🡪 Level 2: -**

1. **cd /krypton/**

**To go to the krypton directory**

1. **ls**

**To see the list of files present in that directory**

1. **cd krypton1**

**To go to the krypton1 directory**

1. **cat krypton2, cat README**

**To see the content of the files**

**Commands used for KRYPTON level 2 🡪 level 3: -**

1. **ssh -p 2231** [**krypton2@krypton.labs.overthewire.org**](mailto:krypton2@krypton.labs.overthewire.org)

**This command is for logging into Krypton Level 2 on OverTheWire.**

1. **cd /krypton/, cd krypton2**

**To go to the desired directory.**

1. **ls**

**To see the list of files present in that directory**

1. **cat krypton3**

**To see the content of the file**

**Commands used for KRYPTON level 3 🡪 level 4: -**

1. **ssh -p 2231** [**krypton3@krypton.labs.overthewire.org**](mailto:krypton3@krypton.labs.overthewire.org)

**This command is for logging into Krypton Level 3 on OverTheWire.**

1. **cd /krypton/, cd krypton3**

**To go to the desired directory.**

1. **ls**

**To see the list of files present in that directory**

1. **cat krypton4, cat HINT1, cat HINT2, cat found1, cat found2, cat found3**

**To see the content of the file**

**Commands used for KRYPTON level 4 🡪 level 5: -**

1. **ssh -p 2231** [**krypton4@krypton.labs.overthewire.org**](mailto:krypton4@krypton.labs.overthewire.org)

**This command is for logging into Krypton Level 4 on OverTheWire.**

1. **cd /krypton/, cd krypton4**

**To go to the desired directory.**

1. **ls**

**To see the list of files present in that directory**

1. **cat krypton5, cat HINT, cat found1, cat found2**

**To see the content of the file**

**Commands used for KRYPTON level 5 🡪 level 6: -**

1. **ssh -p 2231** [**krypton5@krypton.labs.overthewire.org**](mailto:krypton5@krypton.labs.overthewire.org)

**This command is for logging into Krypton Level 5 on OverTheWire.**

1. **cd /krypton/, cd krypton5**

**To go to the desired directory.**

1. **ls**

**To see the list of files present in that directory**

1. **cat krypton6, cat found1, cat found2, cat found 3**

**To see the content of the file**

**Commands used for KRYPTON level 6 🡪 level 7: -**

1. **ssh -p 2231** [**krypton6@krypton.labs.overthewire.org**](mailto:krypton6@krypton.labs.overthewire.org)

**This command is for logging into Krypton Level 6 on OverTheWire.**

1. **cd /krypton/, cd krypton6**

**To go to the desired directory.**

1. **ls**

**To see the list of files present in that directory**

1. **mktemp -d**

**To make a temporary directory**

1. **cd /tmp/tmp.4cLpyvLutA**

**To go to the temporary directory**

1. **ln -s /krypton/krypton6/keyfile.dat**

**To link the keyfile.dat to the temporary directory**

1. **chmod 777 .**

**To give all permissions to the directory**

1. **nano tale.txt**

**created a file to pass some plain text**

1. **/krypton/krypton6/encrypt6 tale.txt ciphertale**

**To make a O/P file of encrypted message of tale.txt**

1. **xxd -b tale.txt**

**To display the binary representation of tale.txt**

1. **xxd -b ciphertale.txt**

**To display the binary representation of ciphertale.txt**

1. **nano a.txt**

**To create a text file that contains A’s**

1. **cat ciphera.txt**

**To make a O/P file of encrypted message of tale.txt**

1. **python3 v\_d.py /krypton/krypton6/krypton7 EICTDGYIYZKTHNSIRFXYCPFUEOCKRN**

**Used python script to decode the Encrypted Message.**

**Commands used for Leviathan 0 🡪 Leviathan 1: -**

1. **ssh -p 2223 leviathan0@leviathan.labs.overthewire.org**

**This connects yo u to the Leviathan 0 level via SSH on port 2223.**

1. **ls -a**

**Lists all files, including hidden ones (starting with .), in the current directory. This helps in discovering any hidden folders like .backup.**

1. **cd .backup**

**Navigates into the .backup directory which is hidden.**

1. **cat bookmarks.html**

**Displays the contents of the bookmarks.html file found in the .backup directory. This file contains clues or possibly the password for Leviathan 1.**

1. **cat bookmarks.html | grep leviathan**

**Filters the contents of bookmarks.html to display only lines containing the keyword "leviathan". This is likely to reveal the password for leviathan1.**

**Commands used for Leviathan 1 🡪 Leviathan 2: -**

1. **ssh -p 2223 leviathan1@leviathan.labs.overthewire.org**

**SSH into the Leviathan 1 level using the password found from the previous level.**

1. **ls**

**Lists files in the current directory. You probably saw the binary file named check.**

1. **ltrace ./check**

**Runs the program check with ltrace, which shows calls to C library functions.**

**This revealed that the program compares the input with the string "sex" (or similar), showing it uses strcmp("sex", input).**

1. **password:sex**

**This just notes the password found via ltrace, which is sex.**

1. **. /check**

**Run the program normally.**

**Then we prompted:**

**password:sex**

**$ bash**

**Typing sex at the prompt and then bash gives you a shell with leviathan2 privileges.**

1. **cat /etc/leviathan\_pass/leviathan2**

**Read the password for leviathan2 from the password file using your escalated privileges.**

**Commands used for Leviathan 2 🡪 Leviathan 3: -**

1. **ssh -p 2223 leviathan2@leviathan.labs.overthewire.org**

**SSH into Leviathan 2 using the password obtained from the previous level.**

1. **mktemp -d**

**Create a temporary directory (e.g., /tmp/tmp.BXOhhk8cvd). This is a safe, writable location for your exploitation setup.**

1. **cd /tmp/tmp.BXOhhk8cvd**

**Change to the newly created temp directory.**

1. **chmod 777 /tmp/tmp.BXOhhk8cvd**

**Grant full permissions to the directory so any user/program can access it.**

1. **ln -s /etc/leviathan\_pass/leviathan3 shortcut**

**Create a symbolic link named shortcut pointing to the password file for leviathan3.**

1. **ls -l**

**Verify that the symlink shortcut has been created properly.**

1. **touch 'shortcut file'**

**Create a file literally named "shortcut file" to trick the program into resolving this to the symlink, depending on how printfile handles names and paths.**

1. **ls -l**

**Confirm that 'shortcut file' exists and check all file details.**

1. **~/printfile "shortcut file"**

**Run the vulnerable binary. If printfile naively prepends ./ or ignores paths, it may follow the symlink and print the leviathan3 password.**