

CyberSec Recruitment Tasks – Week 2 Release

- G.YESHWANTHI REDDY(CYS)

3. CryptoHack – General Category

- ENCODING :-

A.

☆ ASCII 5 pts · 63359 Solves

ASCII is a 7-bit encoding standard which allows the representation of text using the integers 0-127.

Using the below integer array, convert the numbers to their corresponding ASCII characters to obtain a flag.

```
[99, 114, 121, 112, 116, 111, 123, 65, 83, 67, 73, 73, 95, 112, 114, 49, 110, 116, 52, 98, 108, 51, 125]
```

💡 In Python, the `chr()` function can be used to convert an ASCII ordinal number to a character (the `ord()` function does the opposite).

Solution :-

```
ascii_codes = [99, 114, 121, 112, 116, 111, 123, 65, 83, 67, 73, 73, 95, 112, 114, 49, 110, 116, 52, 98, 108, 51, 125]

flag = ""
for num in ascii_codes:
    flag += chr(num)
print(flag)
```

Here I created a empty string flag . Then converted ascii to letters in FOR loop using `chr()` function. The FLAG is **crypto{ASCII_pr1nt4bl3}**

B.

★ Hex 5 pts · 59444 Solves

When we encrypt something the resulting ciphertext commonly has bytes which are not printable ASCII characters. If we want to share our encrypted data, it's common to encode it into something more user-friendly and portable across different systems.

Hexadecimal can be used in such a way to represent ASCII strings. First each letter is converted to an ordinal number according to the ASCII table (as in the previous challenge). Then the decimal numbers are converted to base-16 numbers, otherwise known as hexadecimal. The numbers can be combined together, into one long hex string.

Included below is a flag encoded as a hex string. Decode this back into bytes to get the flag.

```
63727970746f7b596f755f77696c6c5f62655f776f726b696e675f776974685f6865785f737  
472696e67735f615f6c6f747d
```

💡 In Python, the `bytes.fromhex()` function can be used to convert hex to bytes. The `.hex()` instance method can be called on byte strings to get the hex representation.

Solution :-

```
hex = "63727970746f7b596f755f77696c6c5f62655f776f726b696e675f776974685f6865785f737472696e67735f615f6c6f747d"
flag = bytes.fromhex(hex)
print(flag)
```

Here the function bytes.fromhex() is used to convert hex bytes to readable format. The Flag obtained is **crypto{You_will_be_working_with_hex_strings_a_lot}**

C.

Another common encoding scheme is Base64, which allows us to represent binary data as an ASCII string using an alphabet of 64 characters. One character of a Base64 string encodes 6 binary digits (bits), and so 4 characters of Base64 encode three 8-bit bytes.

Base64 is most commonly used online, so binary data such as images can be easily included into HTML or CSS files.

Take the below hex string, *decode* it into bytes and then *encode* it into Base64.

```
72bca9b68fc16ac7beeb8f849dca1d8a783e8acf9679bf9269f7bf
```

💡 In Python, after importing the `base64` module with `import base64`, you can use the `base64.b64encode()` function. Remember to decode the hex first as the challenge description states.

Solution :-

```
hex = "72bca9b68fc16ac7beeb8f849dca1d8a783e8acf9679bf9269f7bf"

byte_string = bytes.fromhex(hex)
print(byte_string)

byte = r"\xbc\x a9\x b6\x 8f\x c1j\x c7\x be\x eb\x 8f\x 84\x 9d\x ca\x 1d\x 8ax>\x 8a\x cf\x 96y\x bf\x 92i\x f7\x bf"

flag = base64.b64encode(byte)
print(flag)
```

Here first I converted hex to bytes using bytes.fromhex() function, i obtained
“r\xbc\x a9\x b6\x 8f\x c1j\x c7\x be\x eb\x 8f\x 84\x 9d\x ca\x 1d\x 8ax>\x 8a\x cf\x 96y\x bf\x 92i\x f7\x bf”

Then converted this bytes to base64 using base64.b64encode() function.Flag obtained is **crypto/Base+64+Encoding+is+Web+Safe/**

D.

Bytes and Big Integers

10 pts · 44377 Solves

Cryptosystems like RSA works on numbers, but messages are made up of characters. How should we convert our messages into numbers so that mathematical operations can be applied?

The most common way is to take the ordinal bytes of the message, convert them into hexadecimal, and concatenate. This can be interpreted as a base-16/hexadecimal number, and also represented in base-10/decimal.

To illustrate:

```
message: HELLO
ascii bytes: [72, 69, 76, 76, 79]
hex bytes: [0x48, 0x45, 0x4c, 0x4c, 0x4f]
base-16: 0x48454c4c4f
base-10: 310400273487
```

Solution :-

```
from Crypto.Util.number import long_to_bytes
a = 11515195063862318899931685488813747395775516287289682636499965282714637259206269
flag = long_to_bytes(a)
print(flag)
```

The flag obtained is **crypto{3nc0d1n6_4ll_7h3_w4y_d0wn}**

E.

Encoding Challenge

40 pts · 13291 Solves

Now you've got the hang of the various encodings you'll be encountering, let's have a look at automating it.

Can you pass all 100 levels to get the flag?

The [13377.py](#) file attached below is the source code for what's running on the server. The [pwntools_example.py](#) file provides the start of a solution.

For more information about connecting to interactive challenges, see the [FAQ](#). Feel free to skip ahead to the cryptography if you aren't in the mood for a coding challenge!

If you want to run and test the challenge locally, then check the FAQ to download the [utils.listener](#) module.

Connect at [socket.cryptochallenge.org 13377](http://socket.cryptochallenge.org:13377)

Challenge files:

- [13377.py](#)
- [pwntools_example.py](#)

Solution:-

```
from pwn import * # pip install pwntools
import json
import base64
import codecs
from Crypto.Util.number import long_to_bytes
# Connect to the Cryptohack challenge server
r = remote('socket.cryptohack.org', 13377, level='debug')
# Receive JSON from server
def json_recv():
    line = r.readline()
    return json.loads(line.decode())
# Send JSON to server
def json_send(hsh):
    request = json.dumps(hsh).encode()
    r.sendline(request)
# Decode based on encoding type
def decode(enc_type, value):
    if enc_type == "base64":
        return base64.b64decode(value).decode()
    elif enc_type == "hex":
        return bytes.fromhex(value).decode()
    elif enc_type == "rot13":
        return codecs.decode(value, 'rot_13')
    elif enc_type == "bigint":
        return long_to_bytes(int(value, 16)).decode()
    elif enc_type == "utf-8":
        return ''.join([chr(c) for c in value])
    else:
        return "unknown"
# Main loop: solve 100 levels
for _ in range(101):
    received = json_recv()

    # If flag is received
    if "#flag" in received:
        print("\n FLAG:", received["flag"])
        break
    print("\n Received:")
    print("Type:", received["type"])
    print("Encoded:", received["encoded"])
    decoded = decode(received["type"], received["encoded"])
    print("Decoded:", decoded)
    to_send = {
        "decoded": decoded
    }
    json_send(to_send)
```

I saved the above code in a file named encode.py then runned the command
python encode.py then obtained the flag **crypto{3nc0d3_d3c0d3_3nc0d3}**.

OVER THE WIRE -BANDIT

LEVEL -0

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit0@bandit.labs.overthewire.org
              _/\_ /\_ /\_ /\_ /\_ /\_ /\_ /\_ /\_ /\_ /\_
              | \_ / \_ | / \_ | / \_ | / \_ | / \_ | / \_ |
              | \_ / \_ | / \_ | / \_ | / \_ | / \_ | / \_ |
              | \_ / \_ | / \_ | / \_ | / \_ | / \_ | / \_ |
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit0@bandit.labs.overthewire.org's password:
              / \_ / \_ \_ \_ / \_ / \_ / \_ / \_ \_ \_ / \_ / \_ / \_ \_ \_ 
              / \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ;
              ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ;
              ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ;
              ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ;
              ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ;
              ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ;
              ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ;
              ; \_ ; \_ ; \_ ; \_ ; \_ ; \_ ;
www.---; ver.---; he---;" ire.org

Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on
discord or IRC.
```

LEVEL 0 – 1

```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
Congratulations on your first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules/
If you are following a course, workshop, walkthrough or other educational activity,
please inform the instructor about the rules as well and encourage them to
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNW0ZOTa6ip5If
```

```
bandit0@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit1@bandit.labs.overthewire.org
```



```
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
```

```
bandit1@bandit.labs.overthewire.org's password:
```

```
/' /' \    , , /' /' \    / . /'
/ . ;.. \ ;. ;. ;. \ /' /_ / \ : /
; | ; \ ; | | ; | /' /_ / \ |
| : | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
www. --- ver --- he --- ire.org
```

```
Welcome to OverTheWire!
```

LEVEL 1-2

```
bandit1@bandit:~$ cat <-
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
-----
```

```
bandit1@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit2@bandit.labs.overthewire.org
```



```
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
```

```
bandit2@bandit.labs.overthewire.org's password:
```

```
/' /' \    , , /' /' \    / . /'
/ . ;.. \ ;. ;. ;. \ /' /_ / \ : /
; | ; \ ; | | ; | /' /_ / \ |
| : | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
| ; | ; | ; | ; | ; | ; | ; | ;
www. --- ver --- he --- ire.org
```

```
Welcome to OverTheWire!
```

LEVEL 2 -3

```
bandit2@bandit:~$ cat "spaces in this filename"
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
[REDACTED]

bandit2@bandit: $ exit
logout
Connection to bandit.labs.overthewire.org closed.
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit3@bandit.labs.overthewire.org
[REDACTED]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit3@bandit.labs.overthewire.org's password:

[REDACTED]
www. ver he ire.org

Welcome to OverTheWire!
```

LEVEL 3 -4

```
bandit3@bandit:~/inhere$ ls -a
.  ..  ...Hiding-From-You
bandit3@bandit:~/inhere$ cat ...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGap0pFhF3NJ
[REDACTED]

bandit3@bandit:~/inhere$ exit
logout
Connection to bandit.labs.overthewire.org closed.
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit4@bandit.labs.overthewire.org
[REDACTED]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit4@bandit.labs.overthewire.org's password:

[REDACTED]
www. ver he ire.org

Welcome to OverTheWire!
```

LEVEL 4 -5

```
bandit4@bandit:~$ ls
inhere
bandit4@bandit:~$ cd inhere
bandit4@bandit:~/inhere$ ls -R
.:
-file00  -file01  -file02  -file03  -file04  -file05  -file06  -file07  -file08  -file09
bandit4@bandit:~/inhere$ cat <-file00
♦hOT♦♦S ♦plS]-EH♦t♦:-♦Z♦
bandit4@bandit:~/inhere$ cat <-file01
N$♦♦'♦♦Se♦♦
\♦- V♦P♦jls♦♦♦♦♦bandit4@bandit:~/inhere$ cat <-file02

o5e♦Mz9♦#P♦ws♦♦♦♦♦0h||xt♦♦bandit4@bandit:~/inhere$ cat <-file03
6|,♦♦V♦q ♦♦*rMX^';b\♦bandit4@bandit:~/inhere$ cat <-file04

x♦♦♦♦]C♦
♦H`♦/♦X♦♦♦OGLVbandit4@bandit:~/inhere$ cat <-file05
♦♦*♦♦-♦♦w9♦P♦RAz♦b♦♦[♦♦F♦bandit4@bandit:~/inhere$ cat <-file06
♦♦_♦♦+J♦♦2X1♦M♦0g♦♦Y♦♦♦d♦Tjbandit4@bandit:~/inhere$ cat <-file07
4oQYVPkxZ00E005pTW81FB8j8lxXGUQw
```

Found the password in file07

```
bandit4@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit5@bandit.labs.overthewire.org
[=] [=] [=] [=] [=]
[=] [G] [G] [G] [G] [G]
[=] [=] [=] [=] [=] [=]

      This is an OverTheWire game server.
      More information on http://www.overthewire.org/wargames

bandit5@bandit.labs.overthewire.org's password:
[=] [=] [=] [=] [=]
[=] [G] [G] [G] [G] [G]
[=] [=] [=] [=] [=] [=]

www. ver he ire.org

Welcome to OverTheWire!
```

LEVEL 5 – 6

```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere03  maybehere06  maybehere09  maybehere12  maybehere15  maybehere18
maybehere01  maybehere04  maybehere07  maybehere10  maybehere13  maybehere16  maybehere19
maybehere02  maybehere05  maybehere08  maybehere11  maybehere14  maybehere17
```

```
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ find -type f -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

```

bandit6@bandit:~$ exit
logout
Connection to bandit.labs.overthewire.org closed.
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit6@bandit.labs.overthewire.org
   _\_\_/\_\_/\_\_/\_\_/\_\_/\_\_
   | | | | | | | | | | | |
   \_\_/\_\_/\_\_/\_\_/\_\_/\_\_/\_\_

  This is an OverTheWire game server.
  More information on http://www.overthewire.org/wargames

bandit6@bandit.labs.overthewire.org's password:

   / \_ \_ / \_ \_ / \_ \_ / \_ \_ / \_ \_ / \_ \_ / \_ \_ / \_ \_ / \_ \_ / \_ \_ / \_ \_ / \_ \_ / \_ \_
  : ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | | | | | | | | | | | | | | | | | |
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : |
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : |
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : |
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : |
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : |
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : |
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : |
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : |
 | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : | : |
|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|:|
 www. '---' ver     '---' he     '---' ire.org

Welcome to OverTheWire!

```

LEVEL 6 -7

```

bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c
find: '/root': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/1143609/task/1143609/fdinfo/6': No such file or directory
find: '/proc/1143609/fdinfo/5': No such file or directory
find: '/boot/lost+found': Permission denied
find: '/boot/efi': Permission denied
find: '/etc/polkit-1/rules.d': Permission denied
find: '/etc/sudoers.d': Permission denied
find: '/etc/xinetd.d': Permission denied
find: '/etc/credstore': Permission denied
find: '/etc/multipath': Permission denied
find: '/etc/ssl/private': Permission denied
find: '/etc/credstore.encrypted': Permission denied
find: '/etc/stunnel': Permission denied
find: '/home/bandit29-git': Permission denied
find: '/home/ubuntu': Permission denied
find: '/home/bandit27-git': Permission denied
find: '/home/drifter6/data': Permission denied
find: '/home/bandit30-git': Permission denied
find: '/home/bandit5/inhere': Permission denied
find: '/home/bandit31-git': Permission denied
find: '/home/bandit28-git': Permission denied
find: '/home/drifter8/chroot': Permission denied
find: '/run/lock/lvm': Permission denied
find: '/run/systemd/inaccessible/dir': Permission denied
find: '/run/systemd/propagate/systemd-udevd.service': Permission denied
find: '/run/systemd/propagate/systemd-resolved.service': Permission denied

```

```

find: '/var/cache/ldconfig': Permission denied
find: '/var/cache/pollinate': Permission denied
find: '/var/cache/apparmor/2693c843.0': Permission denied
find: '/var/cache/apparmor/ac99afeb.0': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/private': Permission denied
find: '/var/crash': Permission denied
find: '/var/spool/rsyslog': Permission denied
find: '/var/spool/cron/crontabs': Permission denied
find: '/var/spool/bandit24': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/log/amazon': Permission denied
find: '/var/log/unattended-upgrades': Permission denied
find: '/var/log/private': Permission denied
find: '/var/tmp': Permission denied
find: '/var/lib/udisks2': Permission denied
find: '/var/lib/update-notifier/package-data-downloads/partial': Permission denied
find: '/var/lib/polkit-1': Permission denied
/var/lib/dpkg/info/bandit7.password
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/chrony': Permission denied
find: '/var/lib/amazon': Permission denied
find: '/var/lib/ubuntu-advantage/apt-esm/var/lib/apt/lists/partial': Permission denied
find: '/var/lib/snappy/cookie': Permission denied
find: '/var/lib/snappy/void': Permission denied
find: '/var/lib/private': Permission denied
find: '/drifter/drifter14_src/axTLS': Permission denied
find: '/tmp': Permission denied
bandit6@bandit:~$ cat </var/lib/dpkg/info/bandit7.password
mrbNTDkSW6jILUc0ymOdMaLn0lFAaj

```

Found the password in /var/lib/dpkg/info/bandit7.password.

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit7@bandit.labs.overthewire.org
[ _--_ / _--_ \ _--_ / _--_ ]
| | | | | | | | | | | | | |
| | | | | | | | | | | |
|_|_|_|_|_|_|_|_|_|_|_|_|_|

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit7@bandit.labs.overthewire.org's password:

[ _--_ / _--_ \ _--_ / _--_ ]
| | | | | | | | | | | | | |
| | | | | | | | | | | |
|_|_|_|_|_|_|_|_|_|_|_|_|_|

www. `---' ver      '---' he      '---" ire.org

Welcome to OverTheWire!
```

LEVEL 7 – 8

```
bandit7@bandit:~$ ls
data.txt
bandit7@bandit:~$ cat data.txt | grep millionth
millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit8@bandit.labs.overthewire.org
[ _--_ / _--_ \ _--_ / _--_ ]
| | | | | | | | | | | | | |
| | | | | | | | | | | |
|_|_|_|_|_|_|_|_|_|_|_|_|_|

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit8@bandit.labs.overthewire.org's password:

[ _--_ / _--_ \ _--_ / _--_ ]
| | | | | | | | | | | | | |
| | | | | | | | | | | |
|_|_|_|_|_|_|_|_|_|_|_|_|_|

www. `---' ver      '---' he      '---" ire.org

Welcome to OverTheWire!
```

LEVEL 8 – 9

```
bandit8@bandit:~$ sort data.txt | uniq -u  
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
```

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit9@bandit.labs.overthewire.org  
  
  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit9@bandit.labs.overthewire.org's password:  
  
  
www.---ver ---he ---"ire.org  
  
Welcome to OverTheWire!
```

LEVEL 9 – 10

```
bandit9@bandit:~$ strings data.txt  
l0@P(  
,k=?  
tIsrQ  
k'Dl5  
X7;9  
wR73I  
@k*=  
"1" f  
yCP  
qxQ>+0  
]t|C  
Kam9  
~V./  
ORFZ  
Tvw1
```

```
'>+_F  
j`VcX  
2#U?  
V/3(o  
=3?0t  
bD/@  
2wNXK|  
===== FGUW5illVJrxX9kMYMmlN4MgbpfMiqey  
v3A|  
"y~  
#kT\  
=D!f  
gD6YbTJ  
2a18  
fKes  
8xXZX  
frw\|  
2*Fx  
`9ZD  
S*7w  
h04W]  
hKQ\|
```

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit10@bandit.labs.overthewire.org
[ _ _ / _ _ \ _ _ \ _ _ / _ _ \ _ _ ]
[ | | | | | | | | | | | | | | | |
[ . . / \ _ _ \ _ _ \ _ _ \ _ _ \ _ _ ]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit10@bandit.labs.overthewire.org's password:
Permission denied, please try again.
bandit10@bandit.labs.overthewire.org's password:

[ _ _ / _ _ \ _ _ \ _ _ / _ _ \ _ _ ]
[ | | | | | | | | | | | | | | | |
[ . . / \ _ _ \ _ _ \ _ _ \ _ _ \ _ _ ]

www. `---` ver     ---' he     '---" ire.org

Welcome to OverTheWire!
```

LEVEL 10 -11

```
bandit10@bandit:~$ cat data.txt | base64 -d  
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr  
bandit10@bandit:~$
```

LEVEL 11 – 12

```
bandit11@bandit:~$ ls  
data.txt  
bandit11@bandit:~$ cat data.txt  
Gur cnffjbeq vf 7k16JArUVv5LxVuJfsSVdbbtahGlw9D4  
bandit11@bandit:~$ cat data.txt | tr 'a-zA-Z' 'n-zA-mN-ZA-M'  
The password is 7x16WNeHII5YkIhWsffIqoognUTyj9Q4
```

Here tr is used to rotate 13 encode/decode

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit12@bandit.labs.overthewire.org
[...]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit12@bandit.labs.overthewire.org's password:
[...]
www.---ver---he---ire.org

Welcome to OverTheWire!
```

LEVEL 12 -13

```
bandit12@bandit:~$ cd /tmp
bandit12@bandit:/tmp$ cd data.txt
-bash: cd: data.txt: Not a directory
bandit12@bandit:/tmp$ cd ~/data.txt
-bash: cd: /home/bandit12/data.txt: Not a directory
bandit12@bandit:/tmp$ cd ~
bandit12@bandit:~$ base 64 -d data.txt. > file.gz
-bash: file.gz: Permission denied
bandit12@bandit:~$ mkdir /tmp/chinki
bandit12@bandit:~$ cp data.txt /tmp/chinki
bandit12@bandit:~$ cd /tmp/chinki
bandit12@bandit:/tmp/chinki$ ls
data.txt
bandit12@bandit:/tmp/chinki$ xxd -r data.txt > data
bandit12@bandit:/tmp/chinki$ ls
data data.txt
bandit12@bandit:/tmp/chinki$ file data
data: gzip compressed data, was "data2.bin", last modified: Thu Apr 10 14:22:57 2025, m
al size modulo 2^32 585
bandit12@bandit:/tmp/chinki$ man gzip
bandit12@bandit:/tmp/chinki$ mv data file.gz
bandit12@bandit:/tmp/chinki$ gzip -d file.gz
bandit12@bandit:/tmp/chinki$ ls
data.txt file.....
```

Then after compressing continuously at end

```
bandit12@bandit:/tmp/chinki$ mv data8.bin data.gz
bandit12@bandit:/tmp/chinki$ gzip -d data.gz
bandit12@bandit:/tmp/chinki$ ls
data data.tar
bandit12@bandit:/tmp/chinki$ file data
data: ASCII text
bandit12@bandit:/tmp/chinki$ cat data
The password is F05dwFsc0cbaIiH0h8J2eUks2vdTDwAn
```

```
yeshwanthi@yeshwanthi-VirtualBox: $ ssh -p 2220 bandit13@bandit.labs.overthewire.org
[|_| \ /_ _/_ \ /_ \ /_ |]
[| |) |(| | | |(| | | |]
[_._. / \_ | | | \_ | \_ |]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit13@bandit.labs.overthewire.org's password:

[|_| \ /_ _/_ \ /_ \ /_ |]
[| |) |(| | | |(| | | |]
[_._. / \_ | | | \_ | \_ |]

www. --- ver     --- he     ---" ire.org

Welcome to OverTheWire!
```

LEVEL 13 -14

```
bandit13@bandit: $ ssh -p 2220 bandit14@localhost -i sshkey.private
The authenticity of host '[localhost]:2220 ([127.0.0.1]:2220)' can't be established.
ED25519 key fingerprint is SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfxC5XlhmAAM/urerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/home/bandit13/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/bandit13/.ssh/known_hosts).

[|_| \ /_ _/_ \ /_ \ /_ |]
[| |) |(| | | |(| | | |]
[_._. / \_ | | | \_ | \_ |]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

!!! You are trying to log into this SSH server with a password on port 2220 from localhost.
!!! Connecting from localhost is blocked to conserve resources.
!!! Please log out and log in again.
```

```
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit14@bandit: $ cat </etc/bandit_pass/bandit14
MU4VWeTyJk8R0of1qqmcBPaLh7lDCPvS
```

LEVEL 14 -15

```
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8R0of1qqmcBPaLh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo

^C
```

Connected to localhost server using nc command to get password for next level

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit15@bandit.labs.overthewire.org
[...]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit15@bandit.labs.overthewire.org's password:
[...]
www. ver he ire.org

Welcome to OverTheWire!
```

LEVEL 15 -16

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
---
Certificate chain
0 s:CN = SnakeOil
i:CN = SnakeOil
a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
v:NotBefore: Jun 10 03:59:50 2024 GMT; NotAfter: Jun  8 03:59:50
```

```
Start Time: 1753678373
Timeout      : 7200 (sec)
Verify return code: 18 (self-signed certificate)
Extended master secret: no
Max Early Data: 0

---
read R BLOCK
8xCjnmgoKbGLhHFAZlGESTmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed
bandit15@bandit:~$
```

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit16@bandit.labs.overthewire.org
[=] [=] [=] [=]
[=] [D] [C] [I] [ ] [C] [I] [ ]
[=] / [ ] [ ] [ ] [ ] [ ] [ ] [ ] [=]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit16@bandit.labs.overthewire.org's password:
[=] [ ] [ ] [ ] [ ] [ ] [ ] [=]
[=] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
[=] ; [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
[=] ; [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
[=] ; [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
[=] ; [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
[=] ; [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
[=] ; [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
[=] ; [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
[=] ; [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
[=] ; [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [ ; ] [=]
www.---ver---he---ire.org

Welcome to OverTheWire!
```

LEVEL 16 -17

```
bandit16@bandit:~$ nmap -sV localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-28 06:22 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port:1790-TCP:V=7.94SVN%T=SSL%I=%D=7/28%Time=68871753%P=x86_64-pc-linu
SF:x-gnu%GenericLines,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x2
SF:0current\x20password.\n")%r(GetRequest,32,"Wrong!\x20Please\x20enter\x
SF:20the\x20correct\x20current\x20password.\n")%r(HTTPOptions,32,"Wrong!\x
SF:20Please\x20enter\x20the\x20correct\x20current\x20password.\n")%r(RTS
SF:PRequest,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20current\x20
SF:password.\n")%r(Helper,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x
SF:20current\x20password.\n")%r(FourOhFourRequest,32,"Wrong!\x20Please\x20
SF:0enter\x20the\x20correct\x20current\x20password.\n")%r(LPDString,32,"W
SF:rong!\x20Please\x20enter\x20the\x20correct\x20current\x20password.\n")
SF:%r(SIPOptions,32,"Wrong!\x20Please\x20enter\x20the\x20correct\x20curren
SF:t\x20password.\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 162.81 seconds
```

```

bandit16@bandit: $ nc -ssl localhost 31790
kSkvUpMQ7lBYyCM4GPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkufmG6HL2YPI0jon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnx9Y7YT2bRPQ
Ja6Lzb558Y3Fz1870Ri+rW4LCDCNd2luvLE/GL2GwykN0kSiCd5TbtjzEkQTu
DSt2mcNn4rhAl+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbW
JGTi65CxhCnzc/w4+mQYvnzpkwtMAzJTzAzQxnkR2MBGySxDLrjg0LN6sK7wNX
x0YYVztz/zbIkPjfkU1jHS+9EbVNj+D1XF0JuqIDAQABAOIBAgpxpMiaoLwfVD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFth0ar69jp5RlwD1NhPx3iBl
J9nOM80J9toum43US8YxF8WhXriYGnc1sskbwpX0UDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wgbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52y0Q9q0kwFTEqpjF4uNtJom+asvlpms8A
vLY9r60wY5vmZhnqBUrj7LyCtXMIu1kkd4w7f77k-DjHoAYxcUp1GL5ls0ama
+T0WwgECgYEAEJtPxP0GRJ+IQkX262jM3dEIka8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBB2G82so8vUHk/fur850Efct9TncCY2crpoqsgifKLxrLgtT+qDpfZnx
SatLdt8Gf085yA7hnWJ2MxF3naeSDm75Lsm+tBbAyc9P2jGRNtMSkCgYEApHd
HCctNi/FwjuhltFx/rHYKhLidZDFYeIE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyyusavPzpaJmjdJ6tcFhVAbAjm7enCIVCCSx+X3lSSiw0A
R57hJgleziJvJy3aGwhwvLzvtzK6zV6oXAu0EcgyAbjo46t4hyPstJi93V5Hdi
TtieK7xRVxUl+iU7rWkgAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcVSPi/WEKlwgXinB3OhyimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULG0QKBgApLTfc1HOwMG0U3KpwYWe006CdTxkm0mL8Ni
blh9elyZ9FgCxsgtRBXRsqXuz7wtsQAgLhxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWku
Y0djHds0okvDQNWu6ucyLRAWFuISExw9a/9p7ftpxm0TSgyvnmLF2MIAEwyzRqaM
77pBAoGAmjmIJdj+ez8duyn3ieo36yrtF5NSsJLAbxFpdlc1gvgtGCWw+9Cq0b
dxviW8+TFVEBl04f7HVm6EpTscdDxu+bCXWkfjuRb7Dy9G0tt9JPsX8MBTakzh3
vBgsyi/sN3rqRbcGU40f0oZyfAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

```

```

-n namespace -s signature_file [-r krl_file] [-O option
bandit16@bandit:~$ mkdir -p /tmp/mybandit17
bandit16@bandit:~$ nano /tmp/mybandit17/privatekey
Unable to create directory /home-bandit16/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

bandit16@bandit:~$ chmod 600 /tmp/mybandit17/privatekey
bandit16@bandit:~$ ssh-keygen -1 -f /tmp/mybandit17/privatekey
unknown option -1

```

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit17@bandit.labs.overthewire.org
```



```

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

```

```
bandit17@bandit.labs.overthewire.org's password:
```



```
Welcome to OverTheWire!
```

LEVEL 17 -18

```
bandit17@bandit:~$ ls
passwords.new  passwords.old
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< C6XNBdY0kgt5ARXESMKwWOUwBeaIQZ0Y
---
> x2gLTTjFwM0hQ8oWNbMN362QKxfRqGlo

connection to bandit18@overthewire.org closed.
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit18@bandit.labs.overthewire.org

  _\ _ \ / _ \ / _ \ / _ \ / _ \ / _ \
 | | ) | ( | | | | | ( | | | | |
 |_._/ \_,_ | | | \_,_ | | | \_,_ |

      This is an OverTheWire game server.
      More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:

  _\ _ \ / _ \ / _ \ / _ \ / _ \ / _ \
 | | ) | ( | | | | | ( | | | | |
 |_._/ \_,_ | | | \_,_ | | | \_,_ |

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord
  Enjoy your stay!

  Byebye !
Connection to bandit.labs.overthewire.org closed.
```

LEVEL 18 -19

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit18@bandit.labs.overthewire.org "cat readme"

  _\ _ \ / _ \ / _ \ / _ \ / _ \ / _ \
 | | ) | ( | | | | | ( | | | | |
 |_._/ \_,_ | | | \_,_ | | | \_,_ |

      This is an OverTheWire game server.
      More information on http://www.overthewire.org/wargames

bandit18@bandit.labs.overthewire.org's password:
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
```

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit19@bandit.labs.overthewire.org
[ _/_\ /_--_ \_/\_ \_/_ ]
| | | | | | | | | | |
|_|_|_|_|_|_|_|_|_|_|_|

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit19@bandit.labs.overthewire.org's password:

      ,----,      ,----,      ,----,
     /    \ \       /    \ \       /    \ \
   . ;   ; \ ;   ; /   ; \ ;   ; /   ; \ ;
   ; |   ; \ ; |   ; /   ; \ ; |   ; /   ; \ ;
   | :   | ; | :   | /   | ; | :   | /   | ; |
   ; ;   ; \ ; ;   ; /   ; \ ; ;   ; /   ; \ ;
   \ \ \ \ \ ; /   ; |   ; \ \ \ \ \ ; /   ; \ \ \ \ \
   ; :   ; /   ; |   ; \ \ \ \ \ ; /   ; \ \ \ \ \
   \ \ \ \ \ ; ;   ; |   ; \ \ \ \ \ ; ;   ; \ \ \ \ \
www. `---` ver   ;---; he   '---" ire.org

Welcome to OverTheWire!
```

LEVEL 19 -20

```
bandit20
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ whoami
bandit19
bandit19@bandit:~$ ./bandit20-do whoami
bandit20
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8Zj0VMN9Ghs7i0WsCfZyXOUbY0
```

```
yeshwanthi@yeshwanthi-VirtualBox:~$ ssh -p 2220 bandit20@bandit.labs.overthewire.org
[ _/_\ /_--_ \_/\_ \_/_ ]
| | | | | | | | | | |
|_|_|_|_|_|_|_|_|_|_|_|

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit20@bandit.labs.overthewire.org's password:

      ,----,      ,----,      ,----,
     /    \ \       /    \ \       /    \ \
   . ;   ; \ ;   ; /   ; \ ;   ; /   ; \ ;
   ; |   ; \ ; |   ; /   ; \ ; |   ; /   ; \ ;
   | :   | ; | :   | /   | ; | :   | /   | ; |
   ; ;   ; \ ; ;   ; /   ; \ ; ;   ; /   ; \ ;
   \ \ \ \ \ ; /   ; |   ; \ \ \ \ \ ; /   ; \ \ \ \ \
   ; :   ; /   ; |   ; \ \ \ \ \ ; /   ; \ \ \ \ \
   \ \ \ \ \ ; ;   ; |   ; \ \ \ \ \ ; ;   ; \ \ \ \ \
www. `---` ver   ;---; he   '---" ire.org

Welcome to OverTheWire!
```

LEVEL 20-21

Terminal 1:-

```
bandit20@bandit:~$ ls
suconnect
bandit20@bandit:~$ echo "0qXahG8Zj0VMN9Ghs7i0WsCfZyX0UbY0" | nc -l -p 12345
EeoULMCra2q0dSkYj561DX7s1CpBu0Bt
```

Terminal 2:-

```
bandit20@bandit:~$ ./suconnect 12345
Read: 0qXahG8Zj0VMN9Ghs7i0WsCfZyX0UbY0
Password matches, sending next password
bandit20@bandit:~$
```

Echo – nc -l -p 12345(port 12345 is random)

./suconnect – connects to fake server(terminal1) and asks for password

If password is correct(ie in terminal1) then sends out the bandit21 password as output in terminal2

LEVEL 21 -22

```
bandit21@bandit:/etc/cron.d$ ls
clean_tmp cronjob_bandit22 cronjob_bandit23 cronjob_bandit24 e2scrub_all otw-tmp-dir sysstat
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q
```

Now logged in into bandit 22

```
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!

bandit22@bandit:~$
```

LEVEL 22- 23

```
bandit22@bandit:/etc/cron.d$ ls
clean_tmp cronjob_bandit22 cronjob_bandit23 cronjob_bandit24 e2scrub_all otw-tmp-dir sysstat
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh &> /dev/null
bandit22@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit23.sh
#!/bin/bash

myname=$(whoami)
mytarget=$(echo I am user $myname | md5sum | cut -d ' ' -f 1)

echo "Copying passwordfile /etc/bandit_pass/$myname to /tmp/$mytarget"

cat /etc/bandit_pass/$myname > /tmp/$mytarget
bandit22@bandit:/etc/cron.d$ echo I am user bandit23 | md5sum | cut -d ' ' -f 1
8ca319486bfBBC3663ea0fbe81326349
bandit22@bandit:/etc/cron.d$ cat /tmp/8ca319486bfBBC3663ea0fbe81326349
0Zf11ioIjMVN551jX3CmStKLYqjk54Ga
```

```
firewall.

--[ Tools ]--

For your convenience we have installed a few useful tools which you can find
in the following locations:

* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)

--[ More information ]--

For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!
```

1) XOR STARTER

```
given = "label"
print("crypto{", end="")
for x in given:
    print(chr(ord(x)^13), end="")
print("}")|
```

Ord() gives the ascii number for a character while chr() does the opposite(ie ascii no – character).

The flag obtained is :-

```
crypto{aloha}
```

2)XOR PROPERTIES

Here Flag = ciphertext ^ flag where ciphertext = flag ^key1^key2^key3

Key2 = (key2^key1) ^key1

Key 3 = (key2^key3)^key2

```
main.py + 
1 from pwn import xor
2 from binascii import unhexlify
3 # Convert all hex strings to bytes|
4 key1 = bytes.fromhex("a6c8b6733c9b22de7bc0253266a3867df55acde8635e19c73313")
5 key2_xor_key1 = bytes.fromhex("37dcb292030faa90d07eec17e3b1c6d8daf94c35d4c9191a5e1e")
6 key2_xor_key3 = bytes.fromhex("c1545756687e7573db23aa1c3452a098b71a7fbf0fddddde5fc1")
7 flag_xor_all = bytes.fromhex("04ee9855208a2cd59091d04767ae47963170d1660df7f56f5faf")
8
9 key2 = xor(key2_xor_key1, key1)
10 key3 = xor(key2_xor_key3, key2)
11 key_total = xor(xor(key1, key2), key3)
12 flag = xor(flag_xor_all, key_total)
13 print("Flag:", flag.decode())
```

The Flag obtained is **crypto{xOr_i5_ass0c1at1v3}**

3)FAVOURITE BYTE

```

def singlebyte_XOR(input_bytes, key):
    flag = b''
    for a in input_bytes:
        flag += bytes([a ^ key])
    return flag.decode('utf-8')
data = "73626960647f6b206821204f21254f7d694f7624662065622127234f726927756d"
decoded = bytes.fromhex(data)
for k in range(256):
    outcome = singlebyte_XOR(decoded, k)
    if 'crypto' in outcome:
        print(outcome)
        break

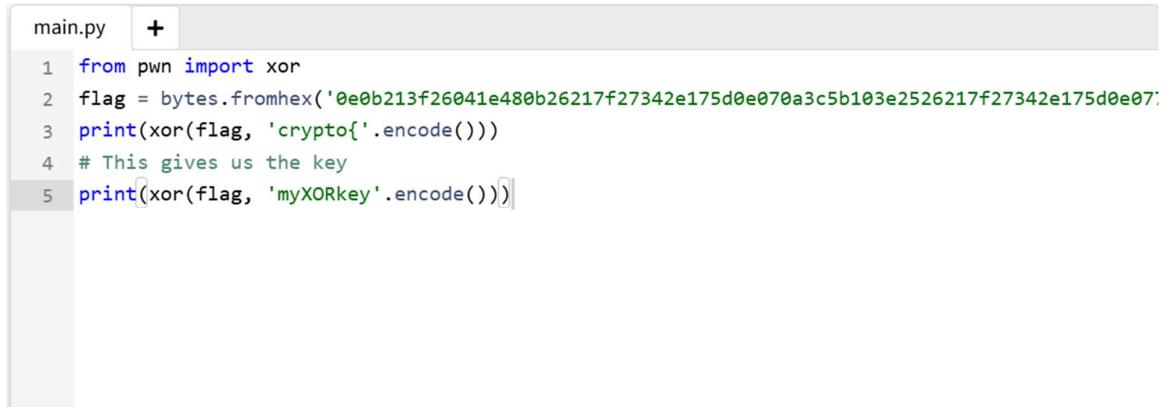
```

FLAG obtained is **crypto{0x10_15_my_f4v0ur173_by7e}**

4)YOU EITHER KNOW,XOR YOU DON'T

It contains one hexed string, and they also mentioned a “secret key” that's been XORed with the “Flag” the end result being the bytes that we can get after decoding the hex.

So We will have to get the “Secret Key” and XORing that with the encrypted string will give us the flag.



```

main.py + 
1 from pwn import xor
2 flag = bytes.fromhex('0e0b213f26041e480b26217f27342e175d0e070a3c5b103e2526217f27342e175d0e07'
3 print(xor(flag, 'crypto{'.encode()))
4 # This gives us the key
5 print(xor(flag, 'myXORkey'.encode()))

```

Firstly decoding the hex to bytes then xor with flag to retrive flag Finally using the actual key with ‘y’ added, to get the flag.

The flag obtained is **crypto{1f_y0u_Kn0w_En0uGH_y0u_Kn0w_1t_4ll}**

5) lemur xor

I couldn't solve this challenge ...

I couldn't paste the screenshot as its not working(some error)

LEVEL 0 -1

```
echo S1JZUFRPTkITR1JFQVQ= | base64 -d
```

OUTPUT : - **KRYPTONISGREAT**

LEVEL 1 – 2

Login to next level by command:-

```
sshpass -p KRYPTONISGREAT ssh krypton.labs.overthewire.org -p 2231 -l krypton1
```

Finding thepassword :-

```
krypton1@bandit:~$ cd /krypton/  
krypton1@bandit:/krypton$ ls  
krypton1 krypton2 krypton3 krypton4 krypton5 krypton6  
krypton1@bandit:/krypton$ cd krypton1  
krypton1@bandit:/krypton/krypton1$ ls  
krypton2 README  
krypton1@bandit:/krypton/krypton1$ cat README
```

.....

```
krypton1@bandit:/krypton/krypton1$ cat krypton2
```

YRIRY GJB CNFFJBEQ EBGGRA

```
krypton1@bandit:/krypton/krypton1$ echo "YRIRY GJB CNFFJBEQ EBGGRA" | tr [A-Z] [N-ZAM]
```

LEVEL TWO PASSWORD **ROTTEN**

LEVEL 2 – 3

Next level login acess:-

```
sshpass -p rotten ssh krypton.labs.overthewire.org -p 2231 -l krypton2
```

Finding the password :-

```
cd /tmp/tmp.WrDJiHZeW9
```

```
ln -s /krypton/krypton2/keyfile.dat
```

```
chmod 777
```

```
echo AAA > test
```

```
/krypton/krypton2/encrypt test
```

```
cat ciphertext
```

```
cat krypton3 | tr "[[:alpha:]]" "O-ZA-No-za-n"
```

CAESARISEASY

LEVEL 3 – 4

Initial access:-

```
sshpass -p caesariseeasy ssh krypton.labs.overthewire.org -p 2231 -l krypton3
```

Finding the password :-

```
cd /krypton
```

```
ls -l
```

```
cat krypton4
```

```
cat krypton4 | tr [A-Z] [BOIHGNQVTWYURXZAJEMSLDFPC]
```

WELLD ONETH ELEVE LFOUR PASSW ORDIS BRUTE

LEVEL 4 -5

```
sshpass -p brute ssh krypton.labs.overthewire.org -p 2231 -l krypton4
```

by using cyberchef the password obtained is **CLEAR TEXT**

OVERTHEWIRE - NATAS

LEVEL 0

Opened the link and go through page source(CTRL +U)

The password for natas1 is **OnzCigAq7t2iALyvU9xcHIYN4Mlkwlq**

LEVEL 0 -1

Opened the link and go through page source(CTRL +U)

The password for natas2 is **TguMNxKo1DSa1tujBLuZJnDUICcUAPII**

LEVEL 1 - 2

Viewed page source (CTRL + U), found an HTML comment leading to a hidden image or file.
opened the hidden resource and found the password.

The password for natas3 is **3gqisGdR0pjM6tpkDKdIW02hSvhLeYH**

LEVEL 2 - 3

The HTML source mentions a directory listing.

Navigated to the directory and found a users.txt file.

Opened it to retrieve the password.

The password for natas4 is **QryZXc2e0zahULdHrtHxzyYkj59kUxLQ**

LEVEL 3 - 4

Found a comment in the HTML pointing to a hidden URL.

Opened the hidden page and got the password.

The password for natas5 is **On35PkggAPm2zbEpOU802c0*0Msn1ToK**

LEVEL 4 - 5

Used browser Developer Tools (F12) to inspect network traffic and cookies.

Modified the cookie value to simulate "logged in" state (loggedin=1).

Page granted access and showed password.

The password for natas6 is **ORoJwHdSKWFTYR5WuiAewauSuNaBXned**

Or can be done with wireshark ...

LEVEL 5 - 6

Page mentions there is something hidden in an image directory.

Checked directory listing of images, found a specific file containing the password.

The password for natas7 is **bmg8SvU1LizuWjx3y7xkNERkHxGre0GS**

LEVEL 6 - 7

HTML mentions use of include() function in PHP.

Modified the ?page= parameter to traverse directories (e.g.,
?page=../../etc/natas_webpass/natas8).

Successfully retrieved password file.

The password for natas8 is **xcoXLmzMkoIP9D7hl9Plh9XD7OgLAe5Q**

LEVEL 7 - 8

Input to ?page= parameter was vulnerable.

Changed value to point to internal system files.

Read the password file directly.

The password for natas9 is **ZE1ck82lmdGloErIhQgWND6j2Wzz6b6t**

LEVEL 8 - 9

Input sanitization attempted to remove spaces and certain characters.

Used encoded characters like \$IFS (Internal Field Separator) or URL encoding to bypass it.

Injected a command to read the password file.

The password for natas10 is **t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu**

LEVEL 9 - 10

Discovered a form input vulnerable to command injection.

Appended ; cat /etc/natas_webpass/natas11 to the input.

Server executed the command and returned password.

The password for natas11 is **UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3IEk**

LEVEL 10 - 11

Input was filtered

Payload like \$(cat /etc/natas_webpass/natas12) executed.

Returned password from the file.

The password for natas12 is **yZdkjAYZRd3R7tq7T5kXMjMjlOlkzDeB**

LEVEL 11 - 12

Vulnerability in file upload functionality.

Uploaded a PHP file disguised as an image (e.g., .php.jpg).

Executed the uploaded shell to read password file.

The password for natas13 is **trbs5pCjCrkuSknBBKHaBxq6Wm1j3LC**

LEVEL 12 - 13

Logged browser requests using a custom User-Agent.

PHP code in logs was injected and later interpreted when the log file was included as a page.

Gained code execution and read password.

The password for natas14 is **z3UYcr4v4uBpeX8f7EZbMHlzK4UR2XtQ**

LEVEL 13 - 14

Login form vulnerable to SQL Injection.

Used payload ' OR 1=1 -- to bypass authentication.

Got access and password was revealed.

The password for natas15 is **SdqIqBsFcz3yotINYErZSzwbIkmoIrvx**

LEVEL 14 - 15

SQL Injection without visible response (blind SQLi).

Used payloads that confirmed character-by-character correctness.

Automated with a Python script.

The password for natas16 is **hPkJKYviLQctEW33QmuXL6eDfMW4sGo**

LEVEL 15 - 16

Blind SQL injection using time delay (SLEEP function).

Identified each character by measuring server response time.

Extracted password completely.

The password for natas17 is **EqjHJbo7LFNb8vwhHb9s75hoKh5TF00C**

LEVEL 16 - 17

Found that a custom XOR cipher was used in source code.

Wrote script to reverse XOR encryption.

Got original password by decoding.

The password for natas18 is **60G1PbKdVjyBlpxgD4DDbRG6ZLICGgCJ**

LEVEL 17 - 18

Used brute-force attack to find a valid session ID.

Each session ID represented a user.

Logged in as admin by finding correct session.

The password for natas19 is **tnwER7PdfWkxsG4FNWUtoAZ9VyZTJqJr**

LEVEL 18 - 19

Similar to previous level but sessions were encoded.

Used base64 decoding or similar method to decode and brute-force session.

Successfully authenticated and got password.

The password for natas20 is **p5mCvP7GS2K6Bmt3gqhM2Fc1A5T8MVyw**