NOVA CTF {2023} - mis1996crack

[REVERSE ENGINEERING CHALLENGE]

Given Description:

Ethan Hunt : talking in a safe house in Prague, referring to his previous mission he was in charge of Ahh, we missed you, Jim.

Jim Phelps : Missed you too, Ethan.

Jack Harmen : Were you on one of your cushy recruiting assignments again?

Ethan Hunt : Yeah, where did they put you up this time? The Plaza?

Jim Phelps : Drake Hotel, Chicago.

everybody "ooohs"*

Jack Harmen : Punishing. 24 hour room service?

Ethan Hunt : Chauffeured limos? Man's getting soft in his old age.

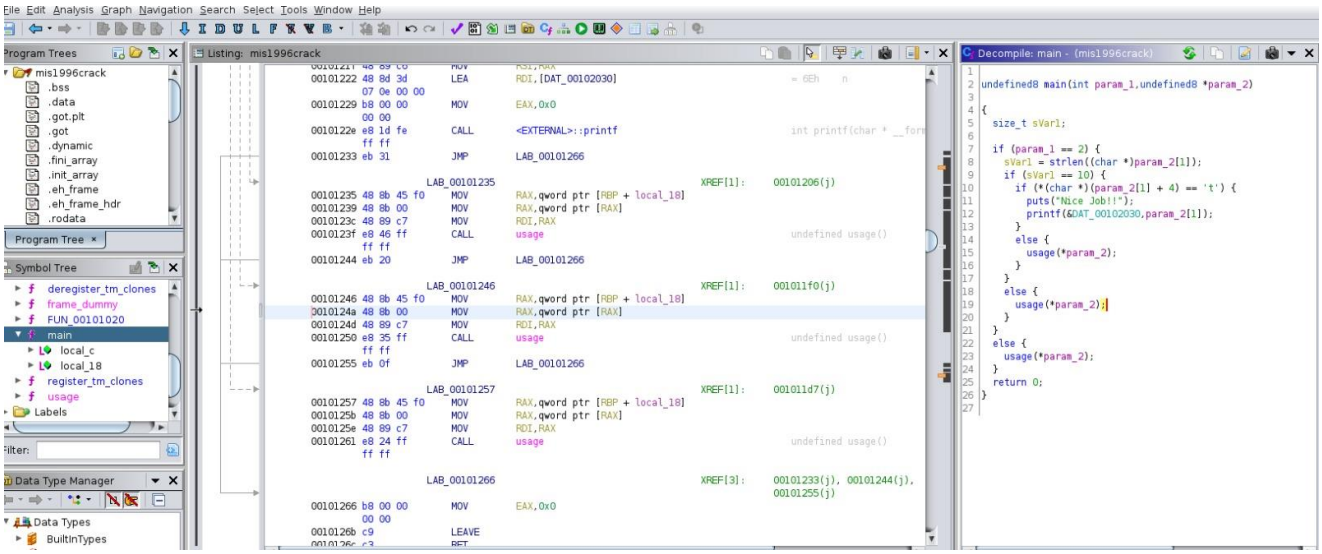
Analysing the File:

The Given File is: mis1996crack

FILE:

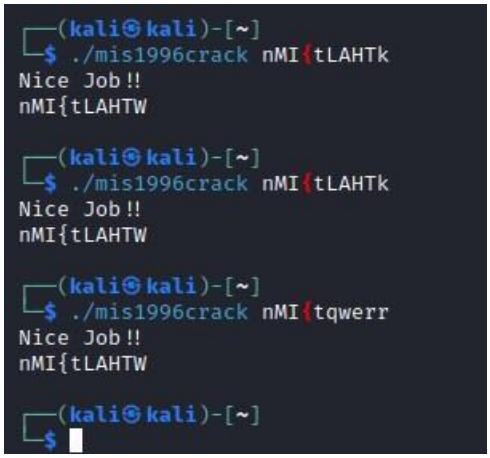
```
└─ $file mis1996crack
mis1996crack: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter
/lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=6db637ef1b479f1b821f45dfe2960e37880df4f
e, not stripped
```

I opened this in Ghidra You can use any disassembler or debugger you are comfortable will work.



- After analysing the Main function, we can infer this is small conditional checking program if the condition is met the data will be printed at the output simply satisfying the condition we can get the flag and that is not enough we can infer that every crack or malware uses certain type of encryption. XOR is commonly used by malware because it's easy to implement.
- After looking into the data

We can find the find the flag is NMI{tLSHTW



- We can infer here the condition is simple the parameter should be the length of 10 if it is satisfied then another condition is checked: if the 5th character is t and if it is

satisfied it should print the data we can give any random data that satisfies the condition or the data itself it also satisfies the condition.

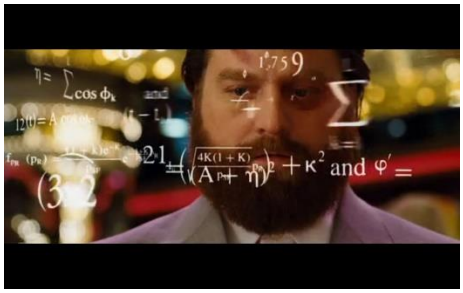
- **Ghidra's Decompile Window**

```
undefined8 main(int param_1,undefined8 *param_2)

{
  size_t sVar1;

  if (param_1 == 2) {
    sVar1 = strlen((char *)param_2[1]);
    if (sVar1 == 10) {
      if (*(char *)(param_2[1] + 4) == 't') {
        puts("Nice Job!!");
        printf(&DAT_00102030,param_2[1]);
      }
      else {
        usage(*param_2);
      }
    }
    else {
      usage(*param_2);
    }
  }
  else {
    usage(*param_2);
  }
  return 0;
}
```

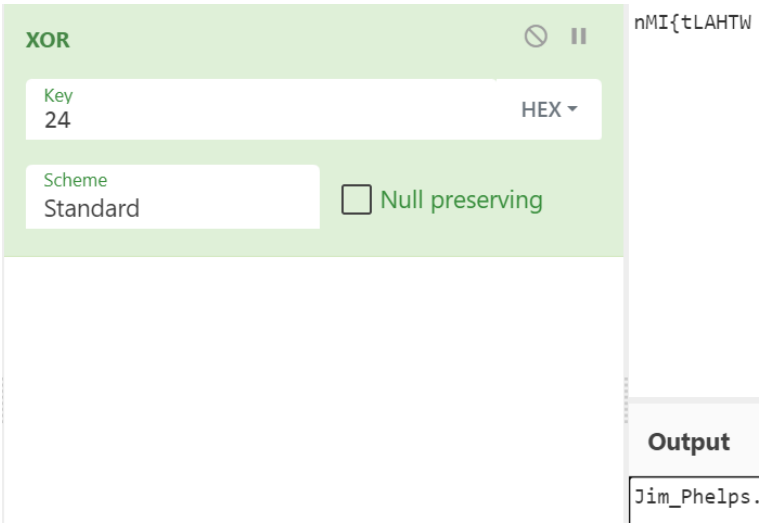
After we found out the Data we need to somehow find the encryption ?

We can xor the given data with key.

Now where is the Key?



After Reading the Description we can find the key is 24.



Now Enclose in Format.

we Got our Flag NOVA{Jim_phelps}

I hope you learnt something and enjoyed the challenge. Connect me via LinkedIn, https://www.linkedin.com/in/kishoreram-k/

Best of luck in capturing flags ahead!!!