BOB'S ENCRYPTED MAIL

[Publish Date]

European Cyber Security Challenge 2018

London, United Kingdom

1. Initial Write-Up

Description:

The main idea of the challenge is the weakness of the software private keys protected using the password-based encryption. In the real world, there are still many production configurations using such a weak type of security.

2. Challenge specifications

- Category: Crypto
- Difficulty : Easy

3. Questions and answers

1) The flag: *This content is your critical flag, please make a copy of it!*

2) The PIN used to encrypt the private key is: ***4531***

4. Tools needed

Description:

Tools needed for the solution of the challenge:

- General Linux tools

5. Artifacts provided

List of artifacts provided with checksums.

File name	Cheksums
Bob.prv	c48c3d4e0a70b31c8679615cb2bf650d
email.encrypted	c40ad798dc87b828a93736645876f8e4

6. Walkthrough (writeup)

- The idea is to brute-force the PIN that encrypts the Bob's private key.
- It is quite simple to see that the encrypted form of the key has an older style format. You can use a tool like openssl trying to check the decryption of the key in a bash script.

Use the bash script **solution_crack_bob_key.sh** to brute force the PIN used to protect the Bob.prv (Bob's private key). The script finds the PIN and then decrypts the file *email.encrypted* printing out the flag's content. The script outputs also the flag to file *flag.plaintext*.