Canary보호기법 우회

2018021147 임동윤

목차 INDEX

● Canary

-Canary란?

-우회하려면?

● 우회방식

-Brute Force

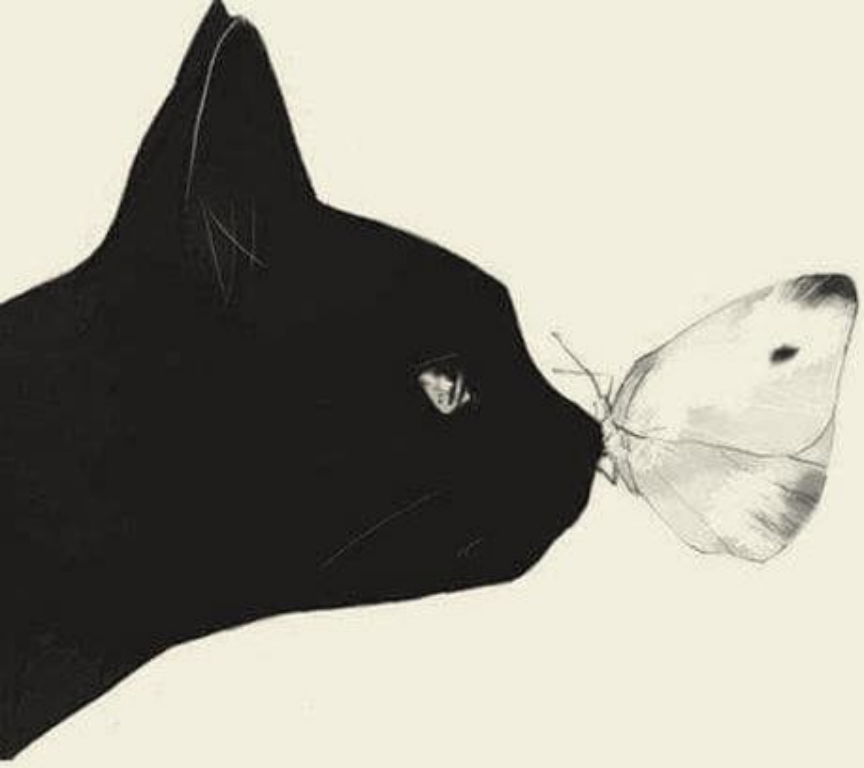
-recv, strncpy

-Canary루틴 노출

-fork이용

● 느낀 점

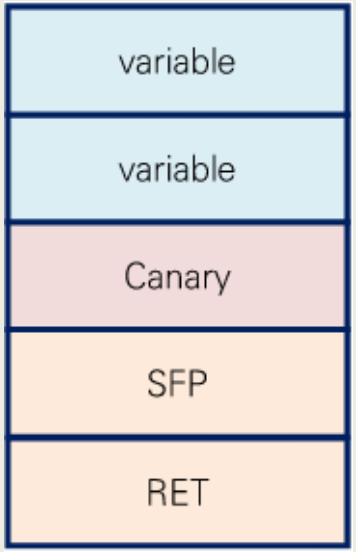
● Question?



Canary

Canary란?

- SFP와 지역변수 사이에 삽입하여 RET의 변조를 방지하는 역할을 한다.
- Canary 고유의 값(16진수)를 생성하여 그 값이 변조되면 프로그램이 터진다.



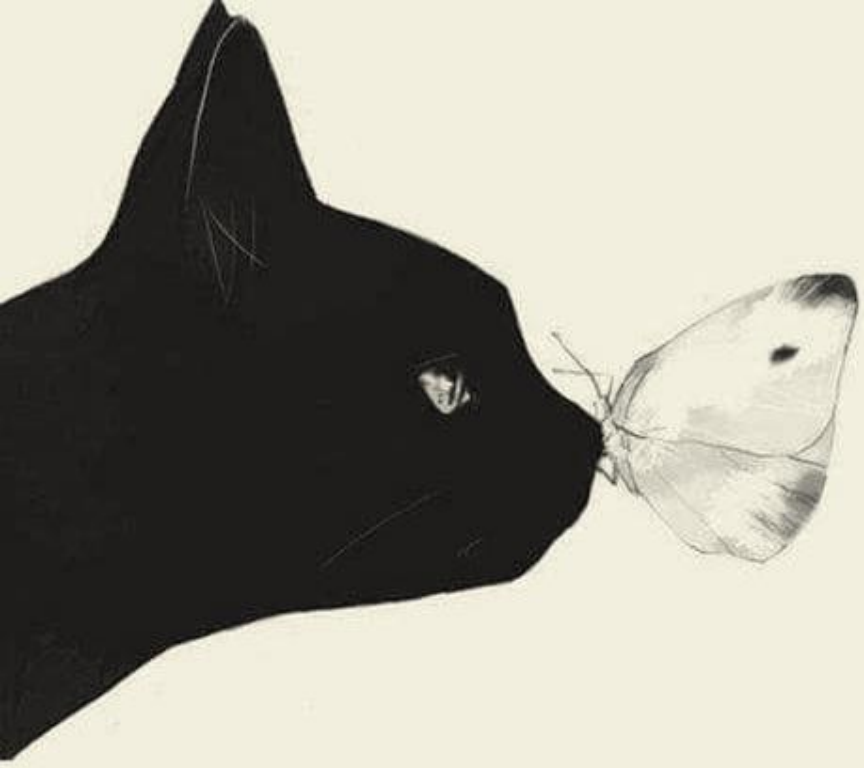
우회하려면?

Canary의 고유 값을 유지해준다!

Ex) Canary 값 : Oxaabbcdef

공격 시 Canary위치에 같은 값

Oxaabbcdef를 넣어준다.



우회방식

Brute Force

- Brute Force?
  - Brute Force는 무차별 대입 공격이라는 뜻!
  - 암호 조합을 무차별적으로 시도한다
- 방법
  - 우선 Canary값은 4byte이다.
  - 1byte씩 Canary값을 덮으면서 대입 시도
  - 0x00~0xFF까지 256가지를 4번반복한다.

recv, strncpy

- recv 함수
  - 연결된 소켓으로 부터 data를 수신한다.
- strncpy
  - 문자열을 복사하는 함수

recv, strncpy

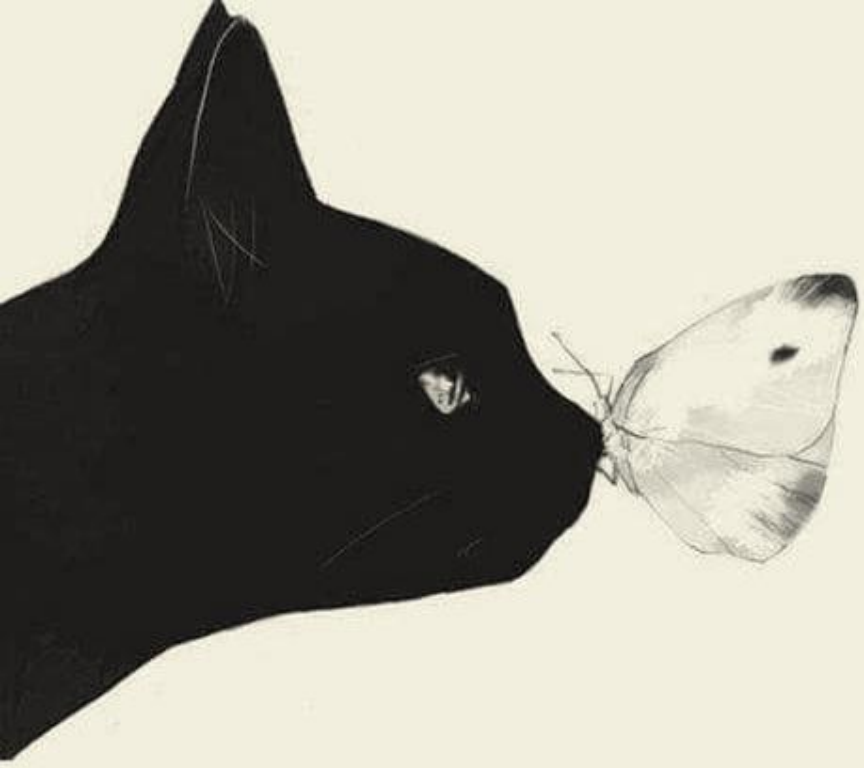
- recv와 strncpy 함수는 문자열을 입력 받을 시 NULL이 들어가지 않는다.
- Buffer가 printf() 된다면 buffer를 꽉 채워 null을 없애 canary까지 출력할 수 있게 한다.

Canary루틴 노출

- Canary를 만드는 만드는 루틴이 노출될 경우 역 연산을 통해 canary를 알아낼 수 있다.

fork 이용

- fork?
  - 프로세스를 생성하고자 할때 사용하는 함수
  - 호출하는 프로세스 → 부모 프로세스
  - 생성되는 프로세스 → 자식 프로세스
- 이 때 부모, 자식은 동일한 Canary 공유!
  - 따라서 몇 번의 시도로 Canary를 추측할 수 있으면 Canary값을 찾아 낼 수 있음.

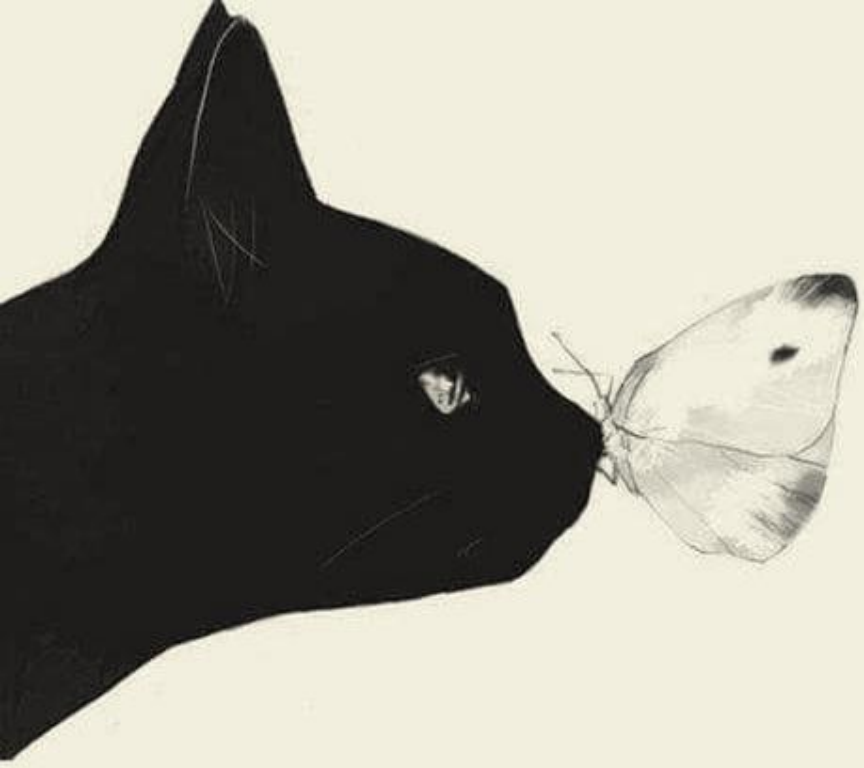


느낀점

느낀 점

- 생각보다 Canary 보호기법은 취약점이 많아 보인다.
- 효율적이지 못한 메모리 보호 방식이기 때문에 새로운 방법이 필요해 보인다.

- p.s. 앞으로 배우겠지...?



Question?