[pwnable.kr WriteUp]

이태규(ltg2030)

[Toddler's Bottle] lotto 2PT

문제 설명
Mommy! I made a lotto program for my homework. do you want to play? ssh lotto@pwnable.kr -p2222 (pw:guest)

문제 풀이(이론)

1. 우선 Xshell을 통해 lotto@pwnable -p2222에 접속한 뒤 ls -l 명령어를 통해 어떤 파일들이 있는지 확인했다.

2.
-r--r----- 1 lotto2 root 55 Feb 18 06:26 flag
-r-sr-x--- 1 lotto2 lotto 13081 Feb 18 06:35 lotto
-rwxr----- 1 root lotto 1713 Feb 18 06:35 lotto.c
이런 3가지 파일이 있는 것을 알 수 있다. 우리는 지금 lotto라는 사용자를 사용하고 있고 이는 root 그룹이 아니기 때문에 flag를 직접 열어볼 수는 없고 SetUID가 적용된 lotto 프로그램을 이용하여 이를 열어야 하는 것을 추측할 수 있다.

3. lotto.c를 열어 lotto 프로그램이 어떻게 동작하는지 알아보자. cat lotto.c 명령어를 사용하여 lotto.c의 내용을 확인한 결과 shell에서 프로그램을 실행할 때 파라미터로 submit 배열에 6개의 로또 번호를 입력을 받고 그를 랜덤 한 lotto 배열 즉 로또 당첨 번호와 36번 비교하여 맞는 값이 6개일 경우 flag를 출력해준다.

4. 하지만 여기서 submit으로 제출한 값이 서로 다른지 확인하는 과정이 없다. 즉 로또 당첨 번호가 1 2 3 4 5 6 일 때 우리가 submit으로 1 1 1 1 1 1을 제출하면 모든 submit은 당첨 번호 1과 비교하여 맞기 때문에 match가 6이 되고 flag의 내용을 볼 수 있다.

5. 당첨 확률을 알아보자 내가 a라는 숫자 6개를 제출했을 때 당첨될 확률은 랜덤하게 생성된 로또 당첨 번호가 1개는 a이고 나머지는 a가 아니게 생성될 확률이다. 이 때 랜덤하게 생성하는 당첨번호도 서로 다른지 확인하는 과정이 없고 a가 6개의 숫자중 하나가 되야하기 때문에 (6*44^5)/(45^6)의 확률을 갖고 이는 약 0.12 정도이다. 즉 a를 6번 제출했을 때 flag를 얻을 확률이 0.12 이고 못 얻을 확률이 0.88인데 이를 10번 반복하면 한 번도 flag를 얻지 못할 확률은 0.27밖에 되지 않는다. 따라서 하나의 숫자를 6번 submit 하면 높은 확률로 flag를 얻을 수 있다.

문제 풀이(실습)

[pwnable.kr WriteUp]

이태규(ltg2030)

```
lotto@ubuntu:~$ (python -c 'print "1"';python -c 'print "\x01\x01\x01\x01\x01\x01"';python -c 'print "3"';) | ./lot
- Select Menu -
1. Play Lotto
2. Help
3. Exit
Submit your 6 lotto bytes : Lotto Start!
sorry mom... I FORGOT to check duplicate numbers... :(
- Select Menu -
1. Play Lotto
2. Help
3. Exit
bye
```

몇 번의 시도를 하고 flag를 얻어냈지만 나머지 부분은 삭제하고 flag를 얻은 부분만 캡쳐하면 sorry mom... I FORGOT to check duplicate numbers... :(가 flag임을 알 수 있따.

실행화면