STACK BASED BINARY EXPLOITATION

JOPRAVEEN

ABOUT ME

JOHANS PRAVEEN

A.K.A Jopraveen

CTF PLAYER AT TAMILCTF | PWN & REV

- Currently studying CSE II year
- I love to learn low level concepts

jopraveen18

Jopraveen#0476

IN THIS SESSION...

- OVERVIEW OF LAST SESSION
- PWNDBG
- RET2WIN
- FORMAT STRING BUG (LEAK)
- GOT OVERWRITE
- BYPASS CANARY
- RET2LIBC

PREREQUISITES

1. WATCH PREVIOUS SESSION

PWNDBG

A plugin for GDB.
Has many useful commands & features

RETURN TO

WIN

FORMAT STRING

BUG

GOT

OVERWRITE

GOT GLOBAL OFFSET TABLE

PLT PROCEDURE LINKAGE TABLE


PLT
GOT
LIBC ADDR
0X401030 <PUTS@PLT>
0X401040 <GETS@PLT>
[0X404018] PUTS@GLIBC_2.2.5
[0X404020] GETS@GLIBC_2.2.5
0X7F8F694C0DE0
0X7F8F694C0350

BYPASS

CANARY & PIE

RET2LIBC

> WE NEED A LEAK TO BYPASS ASLR
> BUT WE DONT HAVE A FORMAT STRING VULN

```
puts(const char *s);
```

WE HAVE PUTS

WE HAVE SOME GADGETS

WE CAN CONTROL RIP

THERE'S NO PIE
SO WE CAN CALL ANY FUNCTION

PUTS(GOT_ADDRESS_OF_PUTS)

DOUBTS

THANK YOU

I HOPE THIS SESSION WAS USEFUL TO YOU AND YOU LIKED IT