BINARY EXPLOITATION 101

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

OVERVIEW

- PREREQUISITES
- BINARY EXPLOITATION
- PROCESS MEMORY
- REGISTERS
- STACK IN DETAIL
- BASIC BUFFER OVERFLOW AND HOW IT WORKS
- TOOLS TO ANALYZE A BINARY
- MITIGATIONS/PROTECTIONS

OVERVIEW

- COMMON BUGS & HOW TO EXPLOIT IT
- PWNTOOLS
- RETURN ORIENTED PROGRAMMING (ROP)
- LEARNING PATH
- RESOURCES
- DOUBTS

PREREQUISITES

1. C PROGRAMMING LANGUAGE
2. ASSEMBLY LANGUAGE (BASICS)
3. SOME EXPERIENCE IN REVERSE ENGINEERING, USING DEBUGGERS, UNDERSTANDING LOW-LEVEL CONCEPTS
4. PYTHON SCRIPTING
5. A LOT OF PATIENCE

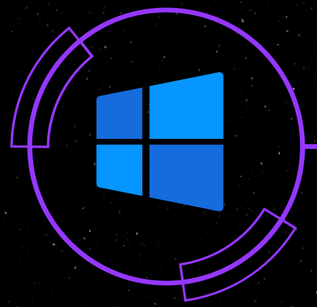
WHAT IS BINARY EXPLOITATION?

WHAT IS BINARY EXPLOITATION?

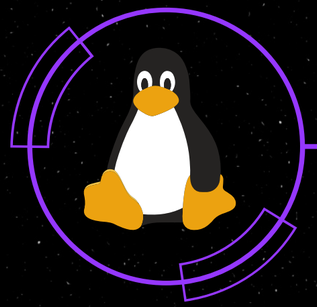
Finding vulnerablities in program and exploiting it

BINARY

EXECUTABLE FILE



exe



ELF

PROCESS MEMORY

LOCAL VARIABLES
ENVIRONMENT VARIABLES
PARAMETERS....

DYNAMICALLY
ALLOCATED DATA

CODE

REGISTERS?

Registers are small storage areas in the memory

IMPORTANT REGISTERS

RIP

RSP

RBP

STACK
IN DETAIL

STACK

- DATA STRUCTURE
- LIFO
- PUSH/POP
- RIP,RBP,RSP
- PROLOGUE & EPILOGUE

BUFFER OVERFLOW

IN DETAIL

TOOLS

- GDB
- RADARE 2
- GHIDRA
- BINARY NINJA
- IDA

MITIGATIONS

- NX
- PIE
- CANARY
- RELRO
- ASLR

EXPLOITATION

- RET2WIN
- RET2SHELLCODE
- FORMAT STRING BUG
- GOT OVERWRITE
- ROP

PWNTOOLS

RETURN ORIENTED PROGRAMMING (ROP)

LEARNING PATH

RESOURCES

DOUBTS

THANK YOU

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