Binary Exploitation

PART 2

@sleepunderflow

HOPR CTF

18th March 5pm – 25th March 4pm 2020

Online Wargames, Jeopardy Style

Team based, Course-Wide, 2 persons per team

Interesting Challenges

Website announced 1 week before the start

Registration will open on starting date @5pm

5:00pm 18.03 - 4:00pm 25.03

https://hopr.computer

Return To Reg

- Can be used when string operation is done before returning or when the return value is a pointer to the string (input)
- Doesn’t work if NX bit is enabled
- Overwrite a return pointer with one pointing to call *rax
- Input = shellcode

ROP chain

- ROP – Return Oriented Programming
- Technique that chains a set of short pieces of code (gadgets) to get to a required result
- Each gadget finishes with RET instruction
- Doesn’t require executable stack
- No shellcode (usually)
- Uses only pieces of code already in the binary
- Usually combined with Return to Libc

ROP chain differences 32 and 64-bit

- 32-bit
  - Function arguments passed on the stack

  - `Function(x) – address of a function you want to call`
  - `ARGx – argument for that function`

  - CHAIN:
  - `FUNCTION(1) + ARG1 + FUNCTION(0) + FUNCTION(2) + ARG1 + ARG2`

64-bit

- Arguments passed using registers: RDI, RSI, RDX, RCX, R8, and R9
  - Function(z) – address of a function you want to call accepting z arguments
  - ARGx – argument for that function
  - POP y – address of POP y, RET gadget
  - CHAIN:
  - POP RDI + ARG1 + POP RSI + ARG2 + FUNCTION(2) + POP RDI + ARG1 + FUNCTION(1) + FUNCTION(0)

PLT & GOT

- PLT – Procedure Linkage Table
  - call [got]
- GOT – Global Offset Table
  - Pointer to one of two routines
    - Resolver
    - Libc

Return To Libc

- Leak the address of a function in libc from GOT
- Calculate the base of libc using GOT and symbol table
- Calculate the address of target function (system/execve) using base and symbol table
- Create the `/bin/bash\x00` string in a known location or use one from libc itself
- Create a chain that will call system("/bin/bash")

PWNTOOLS

- Python2 module
- Do not use on skills test
- Use everywhere else
- http://docs.pwntools.com/en/stable/
- Pip2 install pwn
- From pwn import *

Challenge for today

```
curl http://bit.ly/2HXtACL | sh
```