Uubantu18堆栈平衡问题+ret2text---rip

ret2text---warmup\_csaw\_2016

在ida里查看浮点数的十六进制+浮点数的标识+栈溢出---ciscn\_2019\_n\_1

ret2text+c++字符替换函数---pwn1\_sctf\_2016

jarvisoj\_level0--ret2text

ret2libc+puts函数泄露libc地址+libcsearcher使用---ciscn\_2019\_c\_1

格式化字符串+任意地址写入---第五空间2019 决赛]PWN5

简单的逻辑---ciscn\_2019\_n\_8

strlen截断返回正确结果+ret2libc---[OGeek2019]babyrop

ret2text---jarvisoj\_level2

1. -无leave指令不需要覆盖rbp+ret2text栈溢出参数+ mprotect修改内存权限ret2shellcode---get\_started\_3dsctf

ret2text---bjdctf\_2020\_babystack

和ciscn\_2019\_c\_1一模一样的题目---ciscn\_2019\_en\_2

无leave指令不需要覆盖rbp+ret2text双重返回+ mprotect修改内存权限ret2shellcode---not\_the\_same\_3dsctf\_2016

简单rop---[HarekazeCTF2019]baby\_rop

简单rop---jarvisoj\_level2\_x64

ret2shellcode---ciscn\_2019\_n\_5

直接nc即可+syscall---others\_shellcode

flush中的sh字符+ret2text---ciscn\_2019\_ne\_5

ret2libc---铁人三项(第五赛区)\_2018\_rop

ret2libc---bjdctf\_2020\_babyrop

ret2text+整数溢出---bjdctf\_2020\_babystack2

格式化字符串+fmtstr模块---jarvisoj\_fm

整数溢出+ret2libc+本地不通远程通---pwn2\_sctf\_2016

printf利用ret2libc---[HarekazeCTF2019]baby\_rop2

堆溢出+两种方法+malloc\_hook+---babyheap\_0ctf\_2017

ret2csu+srop---ciscn\_2019\_s\_3

利用leave\_ret实现栈偏移+stack pivoting计算偏移---ciscn\_2019\_es\_2

ret2text+注意函数对ebp是否操作---jarvisoj\_tell\_me\_something

ret2libc+利用32位write---jarvisoj\_level3

ret2shellcode+ida偏移显示错误动态计算偏移---ez\_pz\_hackover\_2016

32位多次ret2text---picoctf\_2018\_rop chain

栈偏移到bss段+ret2libc---[Black Watch 入群题]PWN

ret2libc+利用32位write+和level3基本一样+dynelf的使用+bss读入binsh---jarvisoj\_level4

ret2libc+利用64位write+不设置rbx\_环境自带\_不使用

csu---jarvisoj\_level3\_x64

64位格式化字符串泄露carry+ret2libc---bjdctf\_2020\_babyrop2

House\_Of\_Spirit+堆溢出+动调找特殊字节7f---[ZJCTF 2019]EasyHeap

seccomp沙盒详解+使用open+write+read---pwnable\_orw

linux下';'连接命令---bjdctf\_2020\_router

堆利用+uaf入门题+fastbin---hitcontraining\_uaf

一定要有返回地址+32位ret2text---jarvisoj\_test\_your\_memory

汇编代码分析+ret2shellcode---mrctf2020\_shellcode

汇编代码分析+alpha3转换shellcode+可见字符

ret2shellcode---mrctf2020\_shellcode\_revenge

堆利用+uaf修改fd指针+任意地址写入---wustctf2020\_easyfast

32位ret2syscall+无pie写入bss段bin\_sh---cmcc\_simplerop

32位ret2syscall+无pie写入bss段bin\_sh---inndy\_rop

堆利用+uaf利用add替换地址+fastbin---actf\_2019\_babyheap

32位ret2text+参数设置---picoctf\_2018\_buffer overflow 2

标准32位ret2libc---xdctf2015\_pwn200

ret2text+gdb动态调偏移---bbys\_tu\_2016

栈溢出覆盖下一个变量+难度和ret2text类似

---mrctf2020\_easyoverflow

堆利用+uaf或double\_free+malloc\_hook利用onegadget

---gyctf\_2020\_some\_thing\_interesting

call调用和plt调用的区别+ret2call---wustctf2020\_getshell\_2

堆溢出+长度检查相邻chunk漏洞+非fastbin

---babyfengshui\_33c3\_2016

c++pwn题+汇编溯源call\_rax+字符串截断---[ZJCTF 2019]Login

ret2shellcode远程无回显转ret2libc---jarvisoj\_level1

堆利用+uaf覆盖函数（入门题）+system\_plt---ciscn\_2019\_n\_3

32位栈偏移到stack+泄露ebp+动调ebp和buffer偏移

---ciscn\_2019\_s\_4

fmt\_str格式化字符串实现泄露libc+任意地址写---axb\_2019\_fmt32

堆溢出+unsorted\_bin\_attack入门题---hitcontraining\_magicheap

64位栈偏移ret提高字节防止覆盖got表+one\_gadget什么时候使用---gyctf\_2020\_borrowstack

内联汇编+int80+write二次调用泄露栈地址+21字节手动shellcode---pwnable\_start

64位put泄露ret2libc+泄露carry---others\_babystack

close函数+exec重定向标准输入输出---wustctf2020\_closed

两种那道题(做过)+unsorted\_bin泄露libc+覆盖malloc\_hook

---0ctf\_2017\_babyheap

堆溢出+off\_by\_one+堆重叠+free\_got覆盖

---hitcontraining\_heapcreator

堆溢出+exit\_hook+FILE\_FSOP---ciscn\_2019\_n\_7

堆溢出+exit\_hook+FILE\_FSOP+FSOP未完全理解（两种方法）

---hctf2018\_the\_end

堆溢出+off\_by\_one堆重叠+unsorted\_bin泄露libc+realloc\_hook

---roarctf\_2019\_easy\_pwn

堆溢出+unlink全解析+覆写got表---hitcon2014\_stkof

21字节手动shellcode+汇编调整栈指针shellcode+ret2shellcode

---ciscn\_2019\_s\_9

堆利用+uaf经典利用+system截断执行字符串---pwnable\_hacknote

SROP+类似ciscn\_2019\_s\_3---ciscn\_2019\_es\_7

读汇编找参数+直接写shellcode---picoctf\_2018\_shellcode

ret2csu+覆写got表+不利用system和exec系统调用---jarvisoj\_level5

堆溢出+house\_of\_force+unlink使用show---hitcontraining\_bamboobox

简单rop---cmcc\_pwnme2

覆盖got表+16进制输入数据---picoctf\_2018\_got\_shell

堆溢出+off\_by\_one覆盖free\_got---npuctf\_2020\_easyheap

Uubantu18堆栈平衡问题+去掉push\_rbp+ret2text---suctf\_2018\_stack

堆利用+house\_of\_force+realloc\_hook---gyctf\_2020\_force

2.27堆利用+tache\_dup+unsorted\_leak+tache玩坏警告

---ciscn\_2019\_final\_3

64位栈偏移到栈上+ret2libc+Ubantu18对齐---actf\_2019\_babystack

标准格式化字符串泄露libc+覆盖got表地址---wdb\_2018\_2nd\_easyfmt

栈相邻字符串puts溢出打印---picoctf\_2018\_leak\_me

格式化字符串修改bss+z3计算---mrctf2020\_easy\_equation

jmp\_esp+sub\_sep栈偏移+栈溢出程序pwntools调试---x\_ctf\_b0verfl0w

堆溢出+house\_of\_force+unlink使用show---hitcontraining\_unlink

ret2text---suctf\_2018\_basic pwn

fmt\_str格式化字符串64位+手动payload修改低三字节

---axb\_2019\_fmt64

32位格式化字符串---inndy\_echo

ret2libc或ret2text---cmcc\_pwnme1

2.27堆利用+tache\_dup+unsorted\_leak---ciscn\_2019\_es\_1

mmap函数和jmp\_rsp+沙盒溢出(orw)---[极客大挑战 2019]Not Bad

brop无附件盲打+ret2libc---axb\_2019\_brop64

开启pie情况下的fmt格式化字符串+off\_by\_one+unlink

---axb\_2019\_heap

carry崩溃利用任意地址读+environ泄露栈地址+argv[0]改写---wdb2018\_guess

堆利用+uaf简单利用---gyctf\_2020\_some\_thing\_exceting

简化版ret2libc---oneshot\_tjctf\_2016

栈溢出---护网杯\_2018\_gettingstart

sizie0溢出+unlink---zctf2016\_note2

int类型负数取补码仍然为负数+数字游戏

---wustctf2020\_number\_game

pop\_gadget拼凑shellcode+00字节绕过

shellcode---starctf\_2019\_babyshell

劫持fileno文件标识符+tcache\_double\_free+libc2.27

---ciscn\_2019\_final\_2

少见的数组溢出+栈溢出覆盖ret---wustctf2020\_name\_your\_cat

少见的数组溢出+bss溢出覆盖got表---wustctf2020\_name\_your\_dog

tcache\_dup+ret2libc\_leak---ciscn\_2019\_en\_3

signal函数+ssh连接---picoctf\_2018\_buffer overflow 0

tcache逻辑漏洞+strdup函数---picoctf\_2018\_are you root

堆格式化字符串+rbp格式化字符串低位覆写返回地址

---xman\_2019\_format

格式化字符串栈上数据读---judgement\_mna\_2016

简单uaf复用chunk+堆利用---bjdctf\_2020\_YDSneedGrirlfriend

libc2.27+calloc不使用tcache+tcache特性知识点---gyctf\_2020\_signin

ret2shellcode---wdb\_2018\_3rd\_soEasy

fmt覆写fini\_arry+手动payload---ciscn\_2019\_sw\_1

tcache\_dup+off\_by\_null伪造堆合并---hitcon\_2018\_children\_tcach

堆利用+house\_of\_spirit经典例题---lctf2016\_pwn200

mmap函数+ret2shellcode---[BSidesCF 2019]Runit

ASLR+特殊栈帧找偏移+数组溢出+好题---qctf2018\_stack2

ROPgadget+ropchain+静态编译无法利用plt和got表

---PicoCTF\_2018\_can-you-gets-me

ROPgadget+ropchain+静态编译无法利用plt和got表---强网杯2019 拟态 STKOF

堆利用+特殊整数溢出+size0无限制读入+unlink---zctf\_2016\_note3

堆利用+uaf堆重叠+unsortd\_leak+free\_hook---gyctf\_2020\_document

整数溢出---hgame2018\_flag\_server

strcpy字符溢出+house\_of\_force任意地址写+free\_got

---bcloud\_bctf\_2016

ptr数组低四位遍历index+index0x10按位或导致ptr增加+tcache\_dup

---ciscn\_2019\_final\_5

house\_of\_orange+frop+unsorted\_bin\_attack---houseoforange\_hitcon\_2016

srop\_双frame+特殊gadget\_leave使用rbp---rootersctf\_2019\_srop

vm\_pwn+虚拟栈泄露真实栈+opcode分析---wdb\_2020\_1st\_boom2

无show函数爆破IO\_stdout泄露+add利用realloc

---roarctf\_2019\_realloc\_magic

tcache\_perthread污染+tcache\_dup绕过+unorted\_bin\_leek+free\_hook模板---ciscn\_2021\_lonelywolf【ciscn\_2021】

scanf函数分配堆空间+数组溢出+read分配失败+environ动调获得栈地址---ciscn\_2021\_pwny【ciscn\_2021】

lonelywolf升级版+setcontext沙盒溢出堆题（2.27+2.29+2.31）---ciscn\_2021\_silverwolf【ciscn\_2021】

游戏命令输入逆向+迷宫数组溢出+setcontext沙盒溢出+tcache\_perthread污染---ciscn\_2021\_game【ciscn\_2021】