Maze - Tower

Solution

I used the script I explained in the Maze - Emoji writeup:

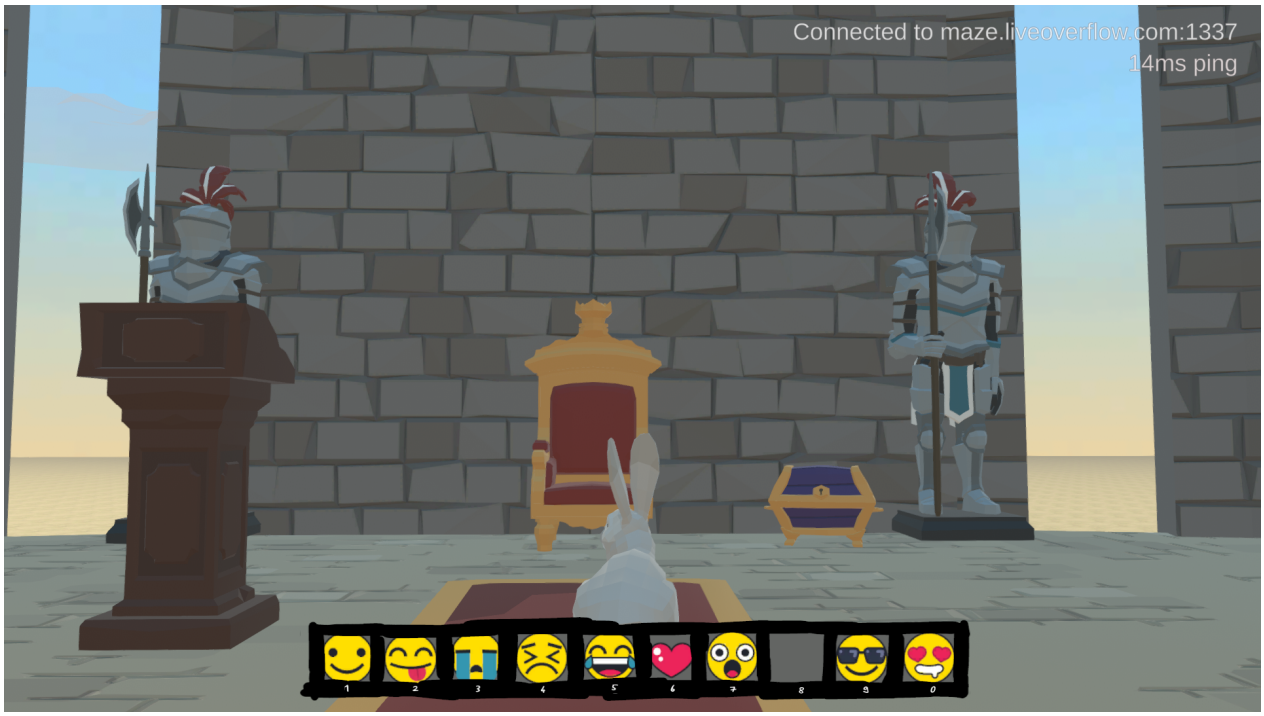
```
#!/usr/bin/env python3

from scapy.all import sniff
import subprocess
import socket
import sys


p = subprocess.run("netstat -u | grep 'hax' | awk -F' ' '{ print $4 }' | awk -F':' '{ print $2 }'", shell=Tru
LOCAL_PORT  = int(p.stdout.decode("utf-8").split("\n")[0])
REMOTE_IP   = "maze.liveoverflow.com"
SECRET      = [91, 249, 248, 237, 116, 183, 144, 7]
FILTER      = "udp and ( " + " or ".join(["dst port " + str(1337 +i) for i in range(21)]) + " )"


def getT():

    t = False

    while not t:

        pkt = sniff(filter=FILTER, count=1)

        r = bytes(pkt[0]["Raw"][0]).hex()

        if len(r) == 96:
            r = decode(r)
            t = int.from_bytes(r[9:17], byteorder="little")

    return int(t)


def decode(data):

    r = bytearray.fromhex(data)

    first_random    = r[0]
    second_random   = r[1]
    decoded = []

    for i in range(0, len(r) - 2):

        decoded.append(first_random ^ r[i+2])

        v21 = first_random + second_random
        first_random = (v21 + ((2155905153 * v21) >> 39)) & 0xff

    return decoded


def send(data, s):

    for remote_port in range(1337, 1358):
        for _ in range(0,3):
            s.sendto(data, (REMOTE_IP, remote_port))

    return


def encode(packet):

    encoded_packet = []
```

```
    random_0 = 24
    random_1 = 123

    encoded_packet.append(random_0)
    encoded_packet.append(random_1)

    for v in packet:

        encoded_packet.append(v ^ random_0)

        v21 = random_0 + random_1
        random_0 = (v21 + ((2155905153 * v21) >> 39)) & 0xff

    return bytes(encoded_packet)


def position(x, y, z):

    t = getT() + 10000

    packet = [80] + SECRET + [ b for b in int.to_bytes(t, length=8, byteorder="little") ]

    pos_x = int.to_bytes(x * 10000, length=4, byteorder="little")
    for i in range(0, 4):
        packet.append(pos_x[i])

    pos_y = struct.pack("<i", y * 10000)
    for i in range(0, 4):
        packet.append(pos_y[i])

    pos_z = int.to_bytes(z * 10000, length=4, byteorder="little")
    for i in range(0, 4):
        packet.append(pos_z[i])

    packet += [0, 0, 0, 0, 0, 161, 86, 53, 0, 0, 0, 0, 0, 1, 0, 1, 1]    # we don't care about euler values

    return packet


def emoji(n):

    packet = [69] + SECRET + [n]

    return packet


def main():

    sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    sock.bind(("", LOCAL_PORT))

    if sys.argv[1] == "P":

        x = int(sys.argv[2])
        y = int(sys.argv[3])
        z = int(sys.argv[4])
        pkt = encode(position(x,y,z))
        for _ in range(3):
            send(pkt, sock)

    elif sys.argv[1] == "E":

        n = int(sys.argv[2])
        send(encode(emoji(n)), sock)

if __name__ == "__main__":
    main()
```

I checked my coordinates with `sniff.py` and teleported myself into the sky:

```
$ sudo python send.py P 38 400 493
```

I then walked into the tower with the chest on the roof until I was here:



From there I once again telported myself into the sky and landed on the chest:

```
$ sudo python send.py P 28 400 459
```

Flag: `CSCG{SOLVED_THE_MAZE...LONG_WAY_BACK!}`

Mitigation

The same as in the Maze - Emoji writeup.