# Bezpečnosť informačných systémov z pohľadu praxe

Peter Švec
peter_svec@stuba.sk

# Motivácia

- *Binary exploitation* (podmnožina **hackingu**)
- Reverzné inžinierstvo
- Hľadanie a exploitovanie zraniteľností
- **C**apture **T**he **F**lag (CTF)
  - DEFCON, GoogleCTF, Pwn2Win,...
  - https://ctftime.org/

# Predpoklady

- PROG 1, PROG 2, OS, UPB
- C, Python
- Linux príkazový riadok
- GDB
- Virtuálna pamäť, program/proces, zásobník,...

# Organizácia

1. Úvod + Assembler
2. **Shellcoding (10 b)**
3. Shellcoding
4. **Reverzné inžinierstvo (10 b)**
5. Reverzne inžinierstvo
6. **Pamäťové zraniteľnosti (10 b)**
7. Pamäťové zraniteľnosti
8. **Návratovo orientované programovanie (10 b)**
9. Návratovo orientované programovanie
10. **Exploitačné scenáre (10 b)**
11. Exploitačné scenáre
12. .*

- Riešenie úloh v menších tímoch
- Každý tematický okruh bude obsahovať **n** malých úloh so stupňujúcou náročnosťou (max. 7-10)
- Každá úloha za 10/**n** bodu
- Zápočet: 50%

# Riešenie úloh

- Každá úloha bude v samostatnom kontajneri (Ubuntu 20.04)
  - V každom kontajneri sú nainštalované všetky potrebné nástroje (gcc, gdb, python, rp++, checksec,...)
- Je potrebné si nainštalovať **Docker**
  - Návod na inštaláciu podľa platformy: https://docs.docker.com/engine/install/
- Server s úlohami:
  - https://feictf.gq/

Ukážka.