Googliš si klingonštinu, lebo assembler už poznáš?

- Chceš spoznať tajomnú oblasť reverzného inžinierstva?
- Chceš skills aké majú uber l33t hackeri?
- Chceš výhodu pri získavaní dream jobu v ESETe, či inej IT firme?

Áno? Tak si zapíš **Aplikácie reverzného inžinierstva (ARI_B)**. Vyučujú odborníci z praxe.

Aplikácie reverzného inžinierstva

„Ako programátor som zrazu dostal úplne nový pohľad na to, ako fungujú aplikácie. Odvtedy píšem oveľa efektívnejší kód a za každým zanedbaným if-om vidím dieru v systéme."
– Dano

ARI_B | 6 kreditov

Absolvovaním získaš základné znalosti o technikách reverzného inžinierstva a ich aplikácii v praxi pri analýze funkcionality softvéru, pri analýze škodlivého kódu a pri ladení programu hľadaním a odstraňovaním chýb v programe. Tieto techniky sa skúmajú v prostredí jazyka assembler na platforme x86 a prípadne v prostredí jazyku C. Okrem toho sa oboznámiš s princípmi vyšších programovacích jazykov (Java, .NET) a technikami reverzného inžinierstva na platformách Linux a Android.

O čom to bude?

- CrackMe challenge.
- Disassembling, debugging, dekompilácia, virtualizácia.
- Reverzné inžinierstvo na platforme Windows – PE formát, Windows API.
- Anti-debugovacie triky: run-time kompresia, obfuskácie.
- Reverzné inžinierstvo vyšších programovacích jazykov (Java, .NET).
- Reverzné inžinierstvo na platforme Android.
- Reverzné inžinierstvo na platforme Linux.
- Základy bezpečného programovania.
- Bezpečnostné zraniteľnosti, exploity.

Čo by si už mal ovládať?

Očakávame znalosť jazyka assembler na platforme x86 a programovania v jazyku C, kedže ich výučba nie je súčasťou tohoto predmetu. Pre účasť na cvičeniach a zápis predmetu je potrebné úspešne absolvovať vstupný test.