# Bez(a)Dis Security Weekend 2013

# (Digital security around us)

# Popis akcie

Seminár **Bez(a)Dis** je určený pre záujemcov o informatiku - najmä však o aktuálne a s praxou prepojené oblasti informatiky. Seminár je **otvorený všetkým**, ktorí sa chcú niečo nové dozvedieť, bez ohľadu na študijný odbor alebo školu. Jedným z cieľov je aj spoznať ľudí, ktorí sa venujú jednotlivým oblastiam v rámci informatiky, a naštartovať možnú spoluprácu na spoločných projektoch. Vítaní sú najmä študenti, ktorí pracujú na záverečných prácach, resp. projektoch, a potrebujú pomôcť, usmerniť, či sú ochotní poradiť ostatným alebo majú skúsenosti z praxe, s ktorými sú ochotní podeliť sa.

Cieľom víkendového workshopu seminára Bez(a)Dis s názvom **„Bez(a)Dis Security Weekend“** bude vytvorenie priestoru na stretnutie IT profesionálov z oblasti počítačovej bezpečnosti (Slovensko, Maďarsko, ČR) a študentov stredných a vysokých škôl, programátorov a širokú verejnosť zaujímajúcu sa o digitálnu bezpečnosť.

# Miesto a čas akcie

Akcia by sa konala v **zimnom semestri akademického roka 2013-2014** (prelom **október-november**).

Miestom uskutočnenia projektu by boli priestory **Prírodovedeckej Fakulty UPJŠ – Jesenná 5 a Park Angelinum 9, Košice.**

Akcia by trvala **2 dni** s tým, že by sa začalo v piatok v popoludňajších hodinách. Piatkový program by končil o 20.00. Sobotňajší program by sa začínal od 9.00 a končil o 19.00.

# Obsah workshopu

Workshop by sa dotýkal rôznych oblastí informačnej bezpečnosti. Sú privítané prednášky najmä z oblastí:

* penetračného testovania
* digitálnej forénznej analýzy
* právnych aspektov informačnej bezpečnosti
* nových trendov v informačnej bezpečnosti
* atď.

# Cieľová skupina

Akciou chceme osloviť niekoľko skupín, ktorých oblasť informačnej bezpečnosti zaujíma:

* **študenti vysokých škôl** – táto cieľová skupina by sa mohla dozvedieť zaujímavé informácie z oblasti informačnej bezpečnosti, ktoré sa na prednáškach na vysokých školách neučia, alebo sa im nevenuje dostatočná pozornosť. Tiež by mohli nadviazať kontakty z odborníkmi z praxe, čo by im mohlo pomôcť pri výbere, resp. pri písaní svojich záverečných prác alebo projektov.
* **odborníci z oblasti informačnej bezpečnosti** – odborníci z praxe by si takto mohli vymeniť svoje poznatky a skúsenosti.
* **programátori užívateľských a serverových aplikácii** - táto cieľová skupina by týmto workshopom mohla získať cenné informácie o zvýšení bezpečnosti svojich kódov, o možnostiach penetračného testovania a iné.
* **študenti stredných škôl a iná široká verejnosť, ktorú oblasť digitálnej bezpečnosti zaujíma** – pre túto cieľovú skupinu sú určenie praktické prednášky a workshopy, ktorých obsahom budú „ľahšie“ bezpečnostné témy.

# Formy workshopu

**„Bez(a)Dis Security Weekend“** by po formálnej stránke tvorilo niekoľko častí (ide o predbežný návrh formálnej stránky, ktorý sa v priebehu príprav môžu upraviť). Rozsah a uskutočnenie jednotlivých častí bude záležať od účasti jednotlivých ľudí a zabezpečenia hardvéru.

1. **Prednášky pre širokú verejnosť** – tie by sa konali v piatok poobede. (predpokladaný rozsah 50 min + 10 min diskusia). V tomto prípade by išlo o praktické prednášky, resp. semináre na zaujímavé oblasti, napr. elektronický podpis, šifrovaná komunikácia (https) a pod.
2. **Odborné prednášky** – sobota. Odborná prednáška by bola v rozsahu 45 až 90 minút + 15 min na diskusiu.
3. **Capture the flag súťaž** - počas soboty – účastníci by si mohli vyskúšať niektoré prvky práce penetračného testera.
4. **Panelová diskusia** – sobota (koniec akcie) – diskusia na zaujímavú tému z oblasti informačnej bezpečnosti. Príkladom zaujímavej diskusie by bola diskusia medzi odborníkmi z oblasti IT a odborníkmi z oblasti práva napr. na tému „Právna úprava digitálnej bezpečnosti v podmienkach Slovenskej republiky“.

# Predpokladané prínosy

* worshop z praktickej bezpečnosti na akademickej pôde (zvyčajne sú takéto workshopy organizované komunitami venujúcimi sa etickému hackovaniu alebo IT firmami pre svojich partnerov) – **študenti** sa tak môžu **zúčastniť akcie**, ktorej by sa za normálnych okolností počas štúdia nedostali,
* účastníci môžu **nadviazať kontakty s bezpečnostnými expertmi z praxe** (zo Slovenska, Čiech a Maďarska) aj na neformálnej úrovní, neformálne diskusie o stave počítačovej bezpečnosti.
* **Poukázať na úskalia zabezpečenie bezpečnosti**, resp. etického hackovania, na zodpovednosť, ktorá prichádza v prípade správy prvkov počítačovej siete, ktoré je potrebné zabezpečiť, resp. v prípade penetračných testov, skúšania rôznych metód útokov a pod. Tiež poukázať na bezpečnostné aspekty vytvorených aplikácii a bezpečnostné chyby, ku ktorým pri programovaní dochádza.