13

# Detekce síťových útoků pomocí jejich deklarativního popisu

Jindřich Dudek

*xdudek04@stud.fit.vutbr.cz*

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Excel@FIT 2018

## MOTIVACE

Cílem práce je navrhnout a implementovat **nástroj pro detekci síťových útoků** ze zachycené síťové komunikace. Hlavní důraz je kladen na **snadnou rozšiřitelnost** tohoto nástroje **o detekci nových síťových útoků** bez nutnosti provádět výrazné změny v jeho implementaci. Součástí práce je tedy návrh obecného textového deklarativního popisu síťových útoků, které jsou předkládány jako jeden ze vstupů nástroje a na jejichž základě jsou útoky v zachycené komunikaci detekovány.

## PRINCIP

Vstupní soubor se zachycenou komunikací je převeden pomocí nástroje **tshark** do formátu **PDML**, který je možné zpracovat jako XML dokument a není tak nutné používat disektory pro interpretaci síťových protokolů. Nástroj pak funguje jako interpret **deklarativních zápisů** síťových útoků, na jejichž základě jsou v PDML souboru detekovány jednotlivé útoky. Při nutnosti rozšířit nástroj o nový síťový útok pak stačí vytvořit nový zápis, který nástroj automaticky intepretuje.

## PŘÍKLAD ZÁPISU

```yaml
name: LAND  # Název útoku
scope: atomic  # Typ útoku
properties:  # Filtrování paketů
  - field-name: tcp.flags  # Název pole
    value: '0x00000002' # SYN paket
    valid: true
detection-conditions:
  type: and
  conditions:  # Podmínky pro detekci
    - condition-type: expression
      expression: SrcIp == DstIp
      variables:  # Seznam proměnných
        - name: SrcIp
          type: field-value
          field-name: ip.src
          value-type: specific
        - name: DstIp
          type: field-value
          field-name: ip.dst
          value-type: specific
threshold-error: 1  # Práh detekce
```