PV210 Bezpečnostní analýza síťového provozu

Organizace předmětu a úvod

~~RNDr. Jan Vykopal, Ph.D.~~
doc. Ing. Pavel Čeleda, Ph.D.

17. 9. 2014

Aktuální informace o předmětu

- Předmět stále ve vývoji, letos rozšíření přednášek.
- Loni nově zavedená cvičení se osvědčila,
  i letos **nepovinná cvičení** 1x za 14 dnů (pá 12–14).
- Přednášky s ukázkami a diskuzí, cvičení, (domácí)
  analytické úkoly, závěrečný test s pohovorem.
- Slídy nejsou skripta, účast na přednáškách nepovinná, ale silně doporučená.
- **Interakce velmi vítána!**

Ukončení předmětu

- Tři domácí úkoly v průběhu semestru (15, 25 a 10 % celkového hodnocení).
- Povinný písemný test s ústním pohovorem na konci semestru (50 %).
- Zisk kolokvia = alespoň 60 %.
- Domácí úkoly bez možnosti opravy, test s pohovorem možno opakovat **jednou**.
- Možnost získání bonusových bodů (10 %) ve cvičení na forenzní analýzu.

Domácí úkoly

- Nedílná součást předmětu.
- **Samostatná** analytická činnost, protiváha přednášek.
- Odevzdávají se formou Odpovědníků v IS MU
  do určené středy 16.00 (přesně).
- Hodnocení se objeví v Poznámkovém bloku
  (nejpozději týden po odevzdání).
- Pro konzultaci každého úkolu úkolu je vyhrazeno cvičení.

Rozvrh přednášek I

- 17. 9. Úvod. Opakování TCP/IP. ~~Vykopal~~ Čeleda
- 24. 9. Útoky podle vrstev sítě I. Vykopal
- 1. 10. Útoky podle vrstev sítě II. Vykopal
- 8. 10. Základní prvky zabezpečení sítě. Vykopal
  Zadání 1. domácího úkolu.
- 15. 10. Úvod do bezpečnostního monitorování sítě. Jirsík
- 22. 10. Jednoduché metody zpracovávající síťové toky.
  Odevzdání 1. úkolu. Vykopal
- 29. 10. Automatické systémy detekce a vizualizace toků.
  Čeleda

Rozvrh přednášek II

- 5. 11. Odhalování botnetů pomocí statistik síťového provozu (botnet Chuck Norris), útoky na HTTPS. Čeleda
  Zadání 2. domácího úkolu
- 12. 11. Pokročilé metody zpracovávající síťové toky. Jirsík
- 19. 11. Incident handling, základní služba CSIRT. Vykopal
  Odevzdání 2. úkolu. Zadání 3. úkolu
- 26. 11. Služby CSIRT. Vykopal
- 3. 12. Úvod do forenzní analýzy Procházka M./Kouřil
  Odevzdání 3. úkolu. Zadání bonusového úkolu.
- 10. 12. Analýza probíhajícího incidentu, ex-post analýza
  Procházka M./Kouřil

Rozvrh přednášek III

- 17. 12. Dva řádné termíny **kolokvia** = test + pohovor.
  První termín v době přednášky, další bude upřesněn podle volné místnosti.
  Odevzdání bonusového úkolu.
- Případný opravný termín kolokvia v lednu 2015.

Rozvrh cvičení I

První skupina (PV210/01):

- 26. 9. Wireshark a hloubková analýza paketů. Vykopal
  19. 9. je děkanské volno
- 10. 10. První úkol – hledání útoku v PCAPu (Wireshark). Vykopal
- 24. 10. Nástroje nfdump a ipfixcol a síťové toky. Velan
- 7. 11. Druhý úkol – hledání útoku v síťových tocích (nfdump/ipfixcol) Velan
- 21. 11. Incident handling. Třetí úkol. Vykopal
- 5. 12. Analýza simulovaného incidentu, práce s daty různého typu a z více zdrojů. Procházka M., Kouřil

Rozvrh cvičení II

Druhá skupina (PV210/02):

- 3. 10. Wireshark a hloubková analýza paketů. Vykopal
- 17. 10. První úkol – hledání útoku v PCAPu (Wireshark). Vykopal
- 31. 10. Nástroje nfdump a ipfixcol a síťové toky. Velan
- 14. 11. Druhý úkol – hledání útoku v síťových tocích (nfdump/ipfixcol) Velan
- 28. 11. Incident handling. Třetí úkol. Vykopal
- 12. 12. Analýza simulovaného incidentu, práce s daty různého typu a z více zdrojů. Procházka M., Kouřil

Motivace I

Co očekáváte od předmětu?

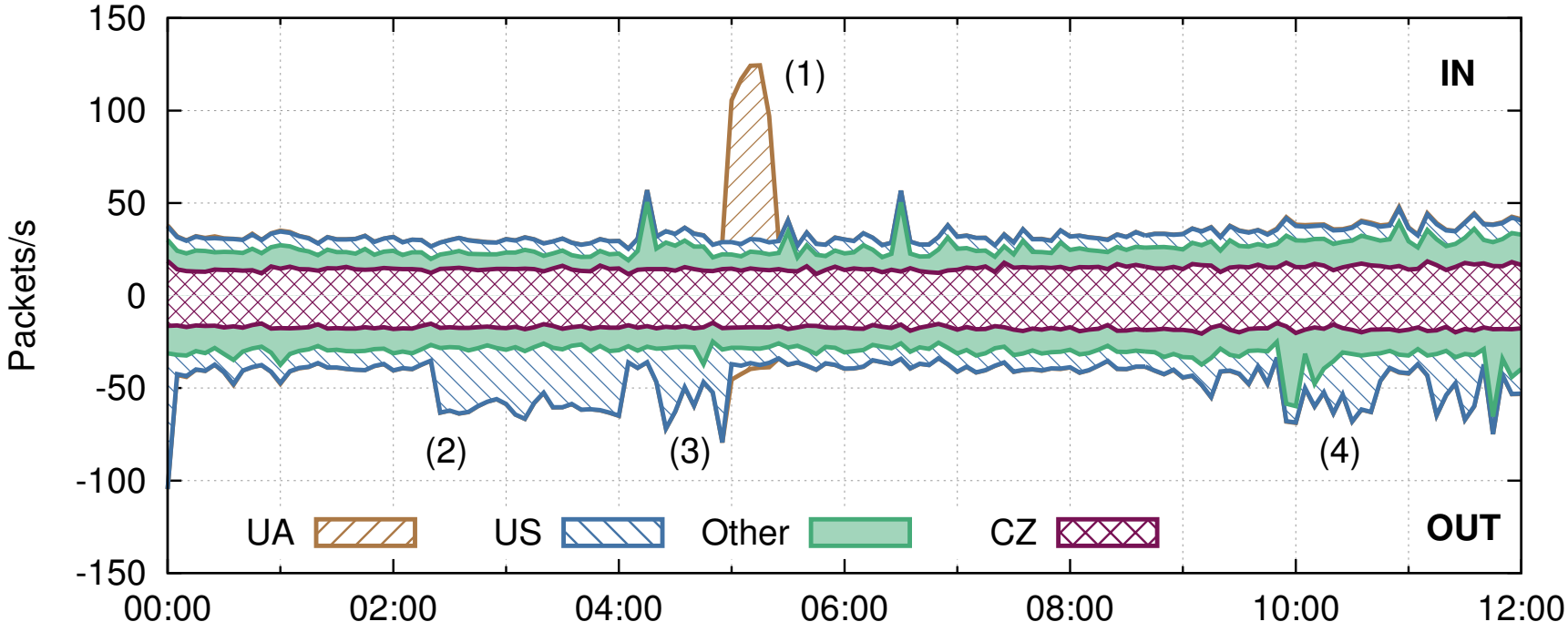
Jaké máte zkušenosti?

Motivace II

Proč se zabývat analýzou síťového provozu?

- Je to zajímavé.
- Je to užitečné.
- Je to obtížné.

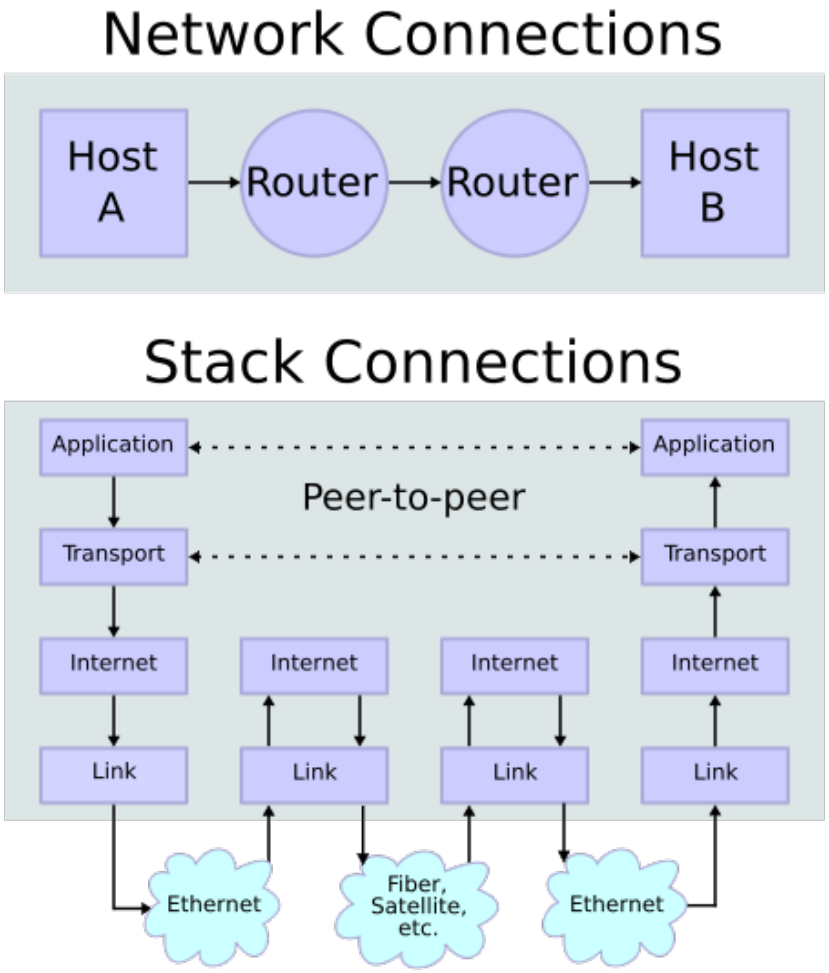
Motivace III



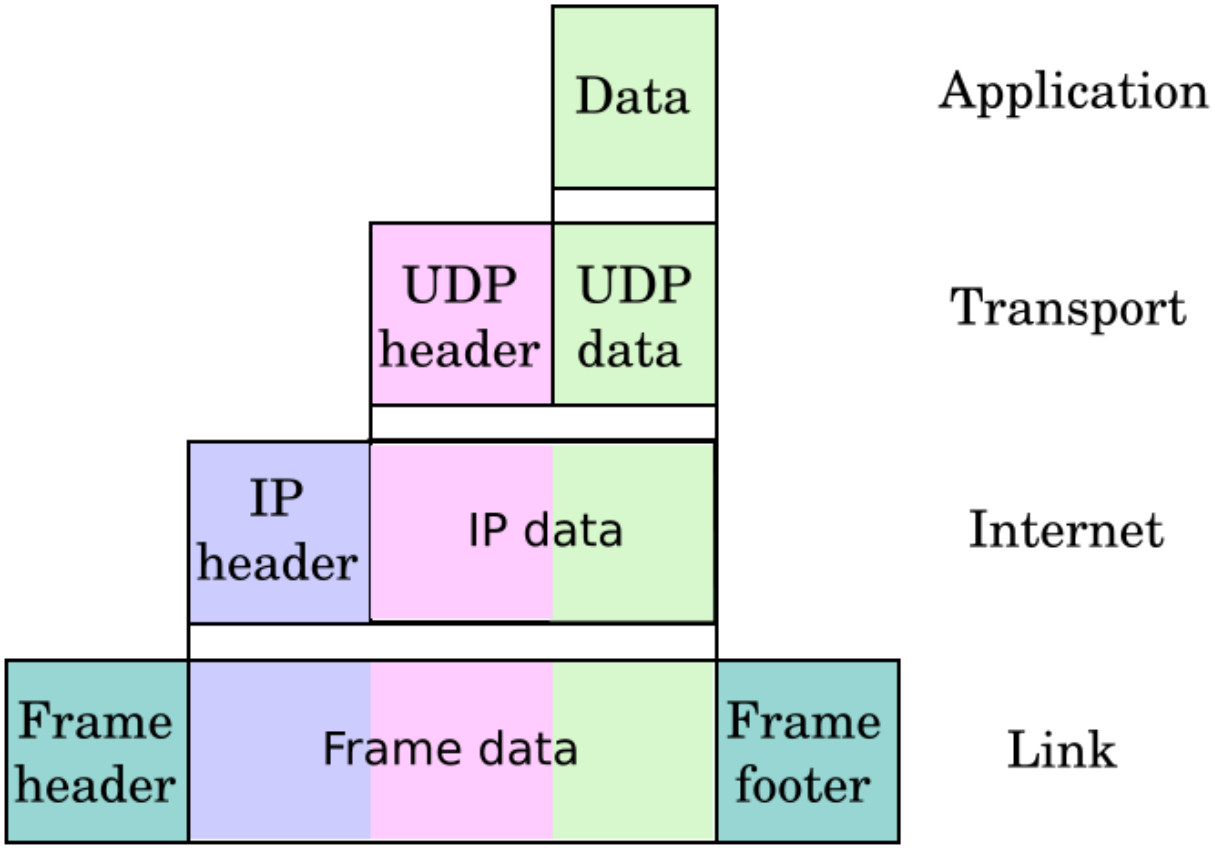
Motivace IV

```
Sep 14 17:52:31 nfsen sshd[21349]: Accepted
publickey for flowmon from 88.83.176.254 port 48930
ssh2

2013-09-14 17:52:42.837 6.943 TCP
88.83.176.254:48930 -> 147.251.14.40:22 68 7845 1

254.176.83.88.in-addr.arpa domain name pointer
dsl-d03pool-254.cust.termsnet.cz.
```

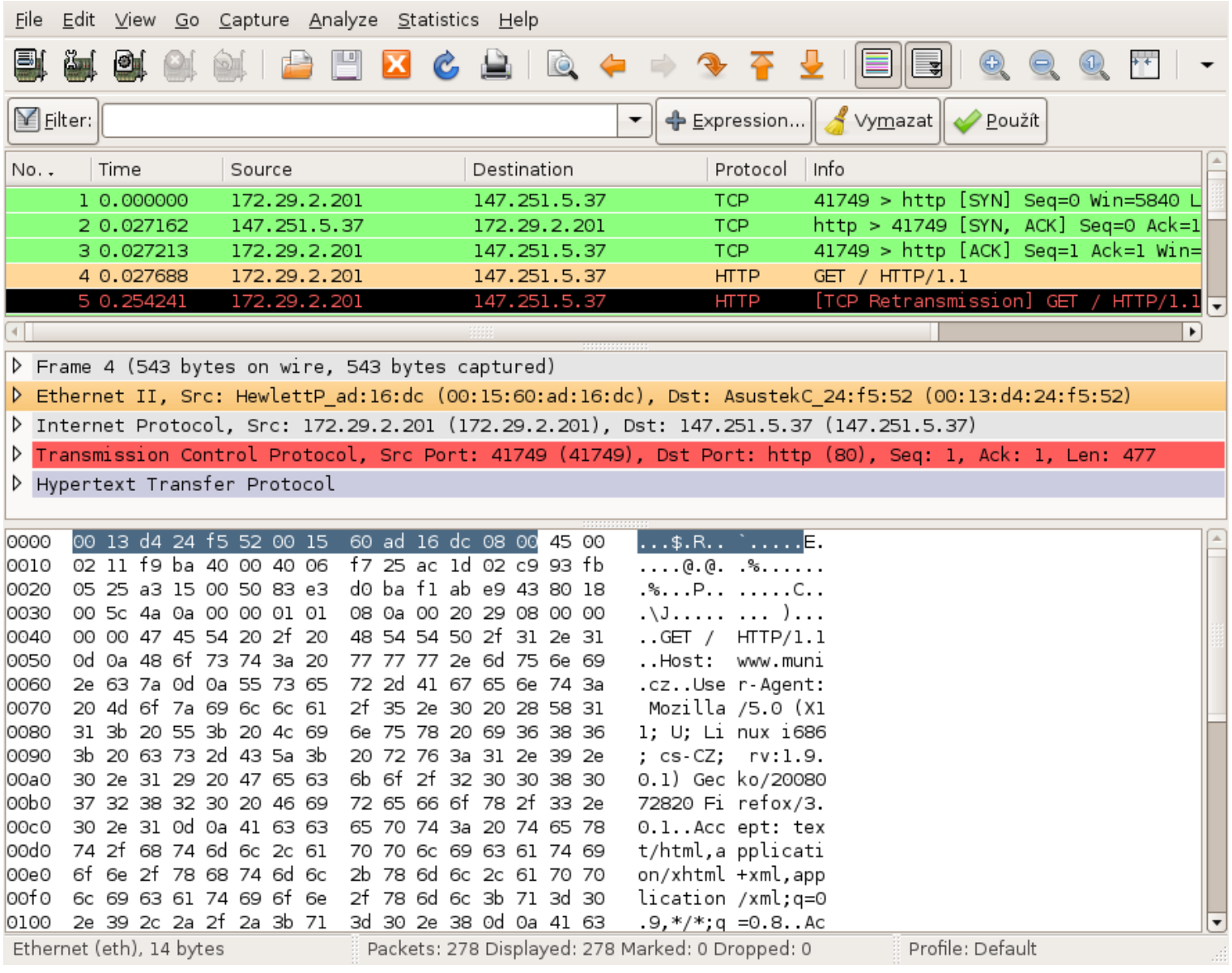
ISO/OSI a TCP/IP I



ISO/OSI a TCP/IP II



Praktický příklad



Pozorování

Protokoly sady TCP/IP používané dodnes vznikly v době, kdy bezpečnost nebyla „na pořadu dne”.