

# PV210 Bezpečnostní analýza síťového provozu

Organizace předmětu a úvod

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

17. 9. 2014

Organizace předmětu

Motivace

Opakování protokolů sady TCP/IP

## 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 doporučena.
- **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?

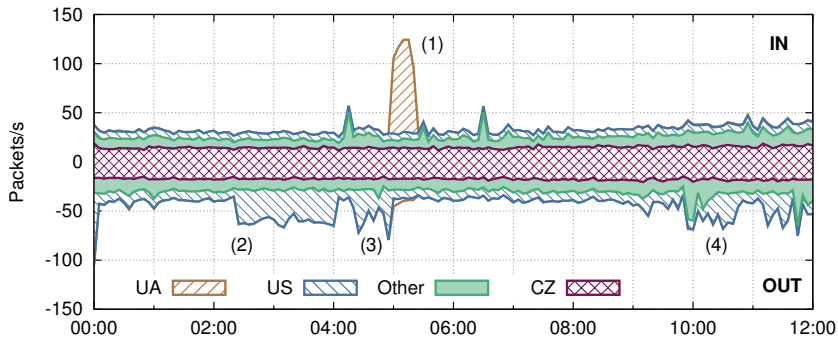
Jaké máte zkušenosti?

## Motivace II

Proč se zabývat analýzou síťového provozu?

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

# Motivace III



## Motivace IV

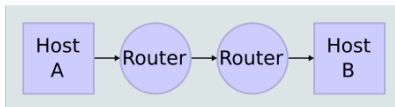
```
Sep 14 17:52:31 nfsen sshd[21349]: Accepted  
publickey for flowmon from 88.83.176.254 port 48930  
ssh2
```

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

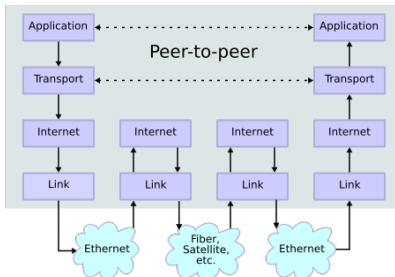
```
254.176.83.88.in-addr.arpa domain name pointer  
dsl-d03pool-254.cust.termsnet.cz.
```

# ISO/OSI a TCP/IP I

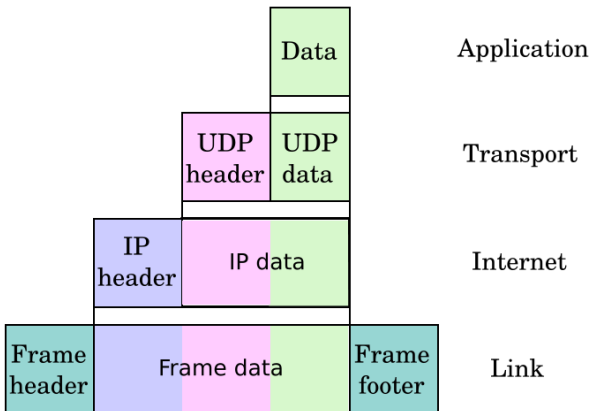
## Network Connections



## Stack Connections



# ISO/OSI a TCP/IP II





# Praktický příklad

The screenshot shows the Wireshark interface with a packet list and packet details pane. The packet list shows a sequence of five packets:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.29.2.201	147.251.5.37	TCP	41749 > http [SYN Seq=0 Win=5840 L...
2	0.027162	147.251.5.37	172.29.2.201	TCP	http > 41749 [SYN, ACK] Seq=0 Ack=1
3	0.027213	172.29.2.201	147.251.5.37	TCP	41749 > http [ACK] Seq=1 Ack=1 Win=
4	0.027688	172.29.2.201	147.251.5.37	HTTP	GET / HTTP/1.1
5	0.254241	172.29.2.201	147.251.5.37	HTTP	[TCP Retransmission] GET / HTTP/1.1

The packet details pane for Frame 4 (543 bytes on wire, 543 bytes captured) shows the following layers:

- Ethernet II, Src: HewlettP\_ad:16:dc (00:15:60:ad:16:dc), Dst: AsustekC\_24:f5:52 (00:13:d4:24:f5:52)
- Internet Protocol, Src: 172.29.2.201 (172.29.2.201), Dst: 147.251.5.37 (147.251.5.37)
- Transmission Control Protocol, Src Port: 41749 (41749), Dst Port: http (80), Seq: 1, Ack: 1, Len: 477**
- Hypertext Transfer Protocol

The raw data pane shows the hex and ASCII representation of the captured data:

```

0000 00 13 d4 24 f5 52 00 15 60 ad 16 dc 08 00 45 00  ..$.R.. ....E.
0010 02 11 f9 ba 40 00 40 06 f7 25 ac 1d 02 c9 93 fb  ....@.@. %. ....
0020 05 25 a3 15 00 50 83 e3 d0 ba f1 ab e9 43 80 18  .%...P. ....C.
0030 00 5c 4a 0a 00 00 01 01 08 0a 00 20 29 08 00 00  .\J..... )...
0040 00 00 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  ..GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 75 6e 69  ..Host: www.muni
0060 2e 63 7a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a  .cz..Use r-Agent:
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31  Mozilla /5.0 (X1
0080 31 3b 20 55 3b 20 4c 69 6e 75 78 20 69 36 38 36  l; U; Li nux i686
0090 3b 20 63 73 2d 43 5a 3b 20 72 76 3a 31 2e 39 2e  ; cs-CZ; rv:1.9.
00a0 30 2e 31 29 20 47 65 63 6b 6f 2f 32 30 30 38 30  0.1) Gec ko/20080
00b0 37 32 38 32 30 20 46 69 72 65 66 6f 78 2f 33 2e  72820 Fi refox/3.
00c0 30 2e 31 0d 0a 41 63 63 65 70 74 3a 20 74 65 78  0.1..Acc ept: tex
00d0 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69  t/html,a pplicati
00e0 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70  on/xhtml +xml,app
00f0 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30  lication /xml;q=0
0100 2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63  .9,*/*;q =0.8..Ac
  
```

At the bottom of the interface, it shows: Ethernet (eth), 14 bytes | Packets: 278 Displayed: 278 Marked: 0 Dropped: 0 | Profile: Default

# Pozorování

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