České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

B2M32IBEA – Informační bezpečnost

1. cvičení – Úvod, BOZP, podmínky pro udělení zápočtu

Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz

Osnova

- Představení předmětu a personální zabezpečení
- Osnova cvičení
- Podmínky pro udělení zápočtu
- Bodové hodnocení na cvičeních
- BOZP, kontrola platnosti vyhl. 50/1978 Sb.
- Zkouška

Kdy a kde se vyučuje

Přednášky

- Kdy – Čt od 16:15
- Kde – T2:B3-812a

Cvičení

- Kdy – Út od 7:30 a 9:15
- Kde – T2:B3-714
- **Studenti chodí na cvičení, které mají zapsáno v KOSu**

Studijní materiály (přednášky, cvičení, testy…)

- https://moodle.fel.cvut.cz
- přihlášení pomocí SSO (jméno/heslo stejné jako do KOSu)

Lidé

Přednášky

- Ing. Tomáš Vaněk, Ph.D. - garant předmětu, přednášející
  - tomas.vanek@fel.cvut.cz
  - T2:B3-602
  - tel.: 224 352 095

Cvičení

- Ing. Petr Hampl, Ph.D. – petr.hampl@fel.cvut.cz
- Ing. Jaromír Hrad, Ph.D. – hrad@fel.cvut.cz
- Ing. Jakub Klemsa – klemsjak@fel.cvut.cz

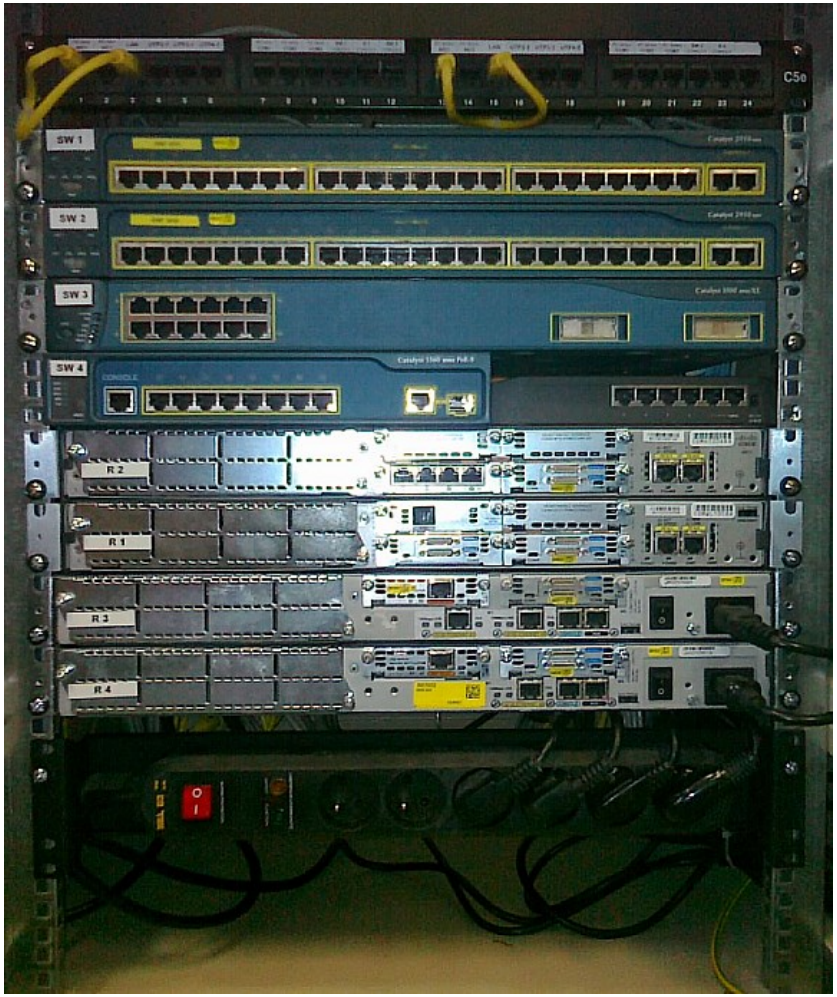
Osnova cvičení (LS 2018/2019)

Týden	Datum	Náplň cvičení
1.	19.02.	Úvodní cvičení, podmínky pro udělení zápočtu, BOZP
2.	26.02.	Kryptoanalýza monoalfabetických substitučních šifer
3.	05.03.	Kryptoanalýza polyalfabetických substitučních šifer
4.	12.03.	Kryptoanalýza transpozičních šifer
5.	19.03.	Úvod do laboratorních úloh
6.	26.03.	Lab. 1 – Útoky v lokálních sítích (skupina A)
7.	02.04.	Lab. 1 – Útoky v lokálních sítích (skupina B)
8.	09.04.	Lab. 2 – Virtuální privátní sítě zabezpečené pomocí IPsec (skupina A)
9.	16.04.	Lab. 2 – Virtuální privátní sítě zabezpečené pomocí IPsec (skupina B)
10.	23.04.	Lab. 3 – Virtuální privátní sítě zabezpečené pomocí SSL/TLS (skupina A)
11.	30.04.	Lab. 3 – Virtuální privátní sítě zabezpečené pomocí SSL/TLS (skupina B)
12.	07.05.	Lab. 4 – Zabezpečení VoIP komunikace (skupina A)
13.	14.05.	*Rozvrh jako ve středu*
14.	21.05.	Lab. 4 – Zabezpečení VoIP komunikace (skupina B)

Cvičení

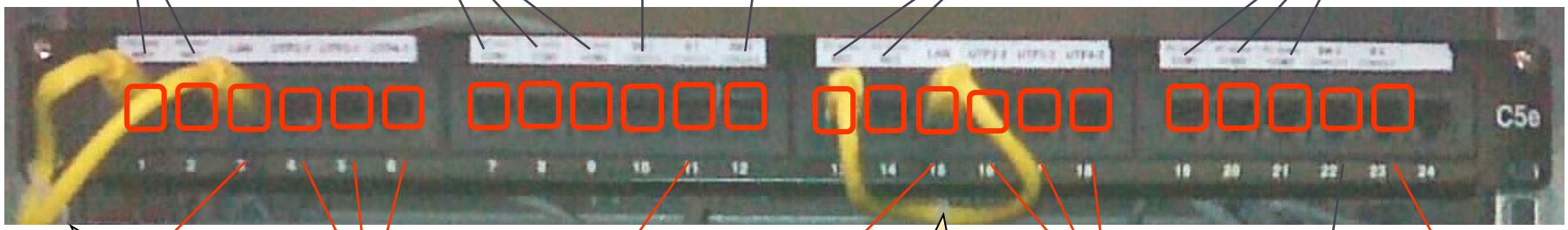
- Seminární (počítačová) cvičení:
  - 2.–5. týden
- Laboratorní cvičení (6.–14. týden):
  - studenti jsou rozděleni na dvě skupiny (A a B)
  - 10 studentů (skupina A) má cvičení
  - 10 studentů (skupina B) pracuje na individuálním projektu (případně provádí konzultace k projektu)
  - další týden si skupiny A a B prohodí role
  - vlastní měření probíhají ve dvojicích (1 řada = 2 studenti)
  - návody k laboratorním úlohám budou k dispozici na Moodle

Vybavení laboratoře 714



- v datovém rozvaděči je
  - L2 přepínač Cisco 2950 – 2x
  - L3 přepínač Cisco 3560
  - L2 přepínač Cisco 3500 XL
  - směrovač Cisco 2811 – 2x
  - směrovač Cisco 26xx – 2x
  - směrovač Cisco 2901 – 1x
- na stole dle potřeby
  - 2x PC
    - přihlašování: stejně jako do IS
  - HW firewall Cisco ASA 5505
    - pouze pro úlohu č. 3
  - IP telefon Cisco SPA504G – 2x
    - pouze pro úlohu č.4
  - rozbočovač Planet

Datový rozvaděč – zapojení technologie



Kabelová spojka pro propojení PC do LAN (a dále do Internetu)

Podmínky pro udělení zápočtu

- **Odevzdání individuálních semestrálních projektů v požadovaných termínech a kvalitě**
- **100% účast na laboratorních cvičeních**
- **Úspěšné absolvování laboratorních úloh**
  - v případě **předem** omluvené absence student absolvuje náhradní cvičení v dohodnutém termínu
  - v případě neomluvené absence na laboratorní úloze je náhrada možná pouze ze zdravotních (doklad od lékaře) či jiných závažných důvodů (posoudí vedoucí cvičení)

Body za práci během semestru

- Student může během semestru získat až 50 bodů, které se započítají k celkovému hodnocení předmětu.
- Body je možno získat za:
  - semestrální práci č. 1 – maximálně 25 bodů
    - kryptoanalýza jednoduchých šifer
  - semestrální práci č. 2 – maximálně 25 bodů
    - práce s elektronickým podpisem

- Kromě bodů za individuální práce lze získat i další tzv. bonusové body za aktivitu na cvičeních.

Individuální semestrální projekt č. 1

- Zadání ve 3. týdnu semestru
- Odevzdání **nejpozději do 12. 5. 2019 3:55 CET**
  - odevzdání úloh prostřednictvím LMS Moodle
  - úlohy odevzdané po tomto termínu nebudou hodnoceny
- Kryptoanalýza jednoduchých šifrovacích technik
  - metody budou probírány na cvičeních 2, 3 a 4
- Několik neznámých textů zašifrovaných různými způsoby
- Za vyluštění každé úlohy obdržíte body dle obtížnosti
- Za projekt č. 1 je celkem možno získat maximálně 25 bodů
  - 20 bodů za řešení jednotlivých úloh
  - 5 bodů za formální zpracování závěrečné zprávy

Individuální semestrální projekt č. 2

- Zadání ve 3. týdnu semestru
- Odevzdání **nejpozději do 12. 5. 2019 3:55 CET**
  - úlohy odevzdané po tomto termínu nebudou hodnoceny
- Práce s elektronickým podpisem
  - podepisování dokumentů PDF
    - technicky bude spojeno s projektem č. 1
    - 5 bodů za elektronický podpis závěrečné zprávy
  - práce s knihovnou OpenSSL
    - 10 bodů za vyřešení úlohy s elektronickým podpisem
  - podepisování e-mailu – S/MIME a PGP
    - 10 bodů za práci s elektronickým podpisem v e-mailu
- Za projekt č. 2 je možno získat maximálně 25 bodů

Zdají se vám standardní práce příliš jednoduché, nudné a neoriginální?

- Po dohodě s přednášejícím lze náplň libovolné semestrální práce změnit.
- Zájemci, kontaktujte přednášejícího před/po přednášce.

- Příklady témat, pro která hledám šikovné studenty:
  - Návrh a realizace víceúrovňové CA pomocí OpenSource technologií (např. OpenSSL nebo EJCBA)
  - CrypTool – možnosti využití ve výuce (analýza RSA, DH, AES, proudových šifer…)
  - Realizace OpenSource TSA (Time Stamp Authority), např. EJCBA
  - Návrh (a realizace) Exit Modulu pro MS ADCS
  - Monitoring funkčnosti ADCS

Bonusové body

- Každý cvičící má k dispozici $[1{,}5 \cdot n]$ bonusových bodů, kde n je počet studentů zapsaných na dané cvičení
- Slouží k hodnocení aktivity studentů především na laboratorních cvičeních
- Body nejsou nárokovatelné
- Cvičící může (ale nemusí) dle svého uvážení tyto body rozdělit
- Počet bodů přidělovaných jednotlivým studentům není omezen
- V případě rozdání všech bodů se již žádné další nerozdělují

Získané body + docházka

FAKULTA ELEKTROTECHNICKÁ
Spojujeme elektrotechniku a informatiku

zy ▶ Letní semestr 2015/16 ▶ A7B32KBE - Kódy a bezpečnost

ÁNÉ ODSTÁVCE

loodle FEL,
19.2.2016 v době od
plánovaná odstávka
lné údržby.

A7B32KBE - Kódy a bezpečnost

Předmět představuje vyčerpávající zdroj informací pro přehled v oblasti ochraně informačních systémů a informačních technologií. Studenti se seznámí s moderními šifrovacími algoritmy, hashovacími funkcemi a kryptografickými protokoly. Součástí předmětu jsou i laboratorní úlohy demonstrující praktické využití kryptografických technik.
Výsledek studentské ankety předmětu je zde: A7B32KBE

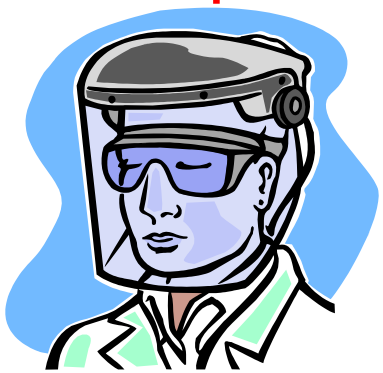
Novinky

Docházka a hodnocení práce během semestru

	Skupina na Laborky	Jméno	Docházka													Semestr. práce 1	Semestr. práce 2	Semest práce 3 (bonus			
			I.	II.	III.	IV.	V.	VI.	VII.	VIII.	IX.	X.	XI.	XII.	XIII.	XIV.	Luštění (max.20 bodů)	Programování (max. 15 bodů)	S/MIME PGP, PDF s podpis	Bonus body ze cvičení	Body ze cvičení celkem	Nárok na zápočet
1	A1	Babický Tomáš							-		-		-		-							
2	A1	Baroch Patrik							-		-		-		-							
3	A2	Baručić Denis							-		-		-		-							
4	A2	Bílek Petr							-		-		-		-							
5	A3	Brachaczek Petr							-		-		-		-							
6	A3	Dubravická Romana							-		-		-		-							
7	A4	Gintner Vojtěch							-		-		-		-							
8	A4	Kostyuk Petro							-		-		-		-							
9	A5	Moravenov Jordan							-		-		-		-							

Bezpečnost a ochrana zdraví při práci v laboratoři

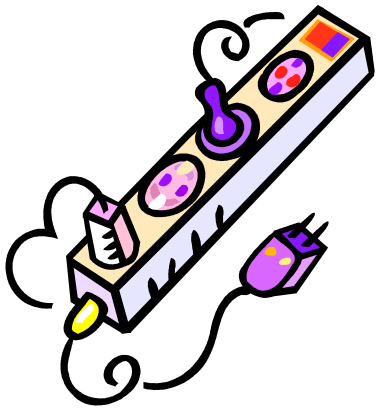
- Bundy, kabáty a rozměrná zavazadla patří do šatny
- Nejíst, nepít, nekouřit
- Zařízení a vybavení
- Červené tlačítko
- Důležitá čísla
- První pomoc



Bezpečnost a ochrana zdraví při práci v laboratoři

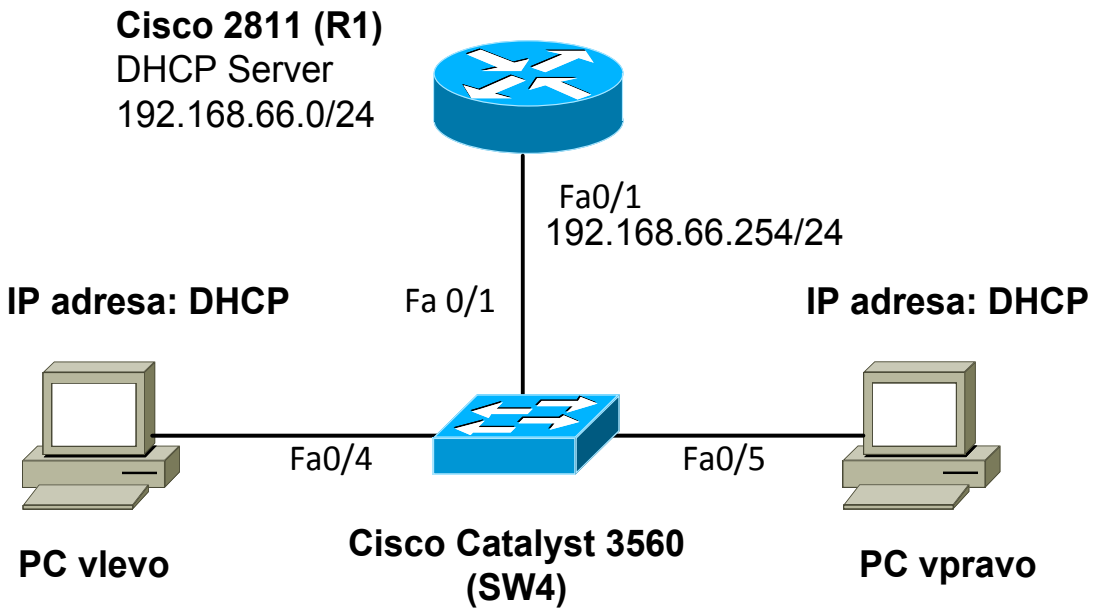
- Vyhláška 50/1978 Sb. o odborné způsobilosti v elektrotechnice
- Stačí §4 – pracovník poučený
- Platnost osvědčení – 3 roky
- Poslední datum absolvování kontrolního testu
- Zápočet v KOSu z předmětu BP1/BP2/BP3 musí být ze září 2017 nebo novější.

- Nutno splnit **nejpozději** do 19. 3. 2019

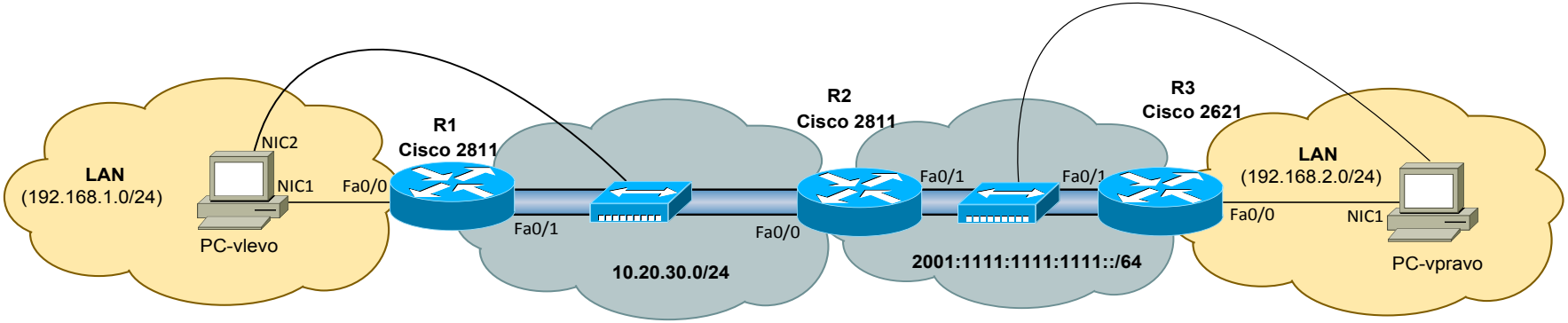


Dotazy

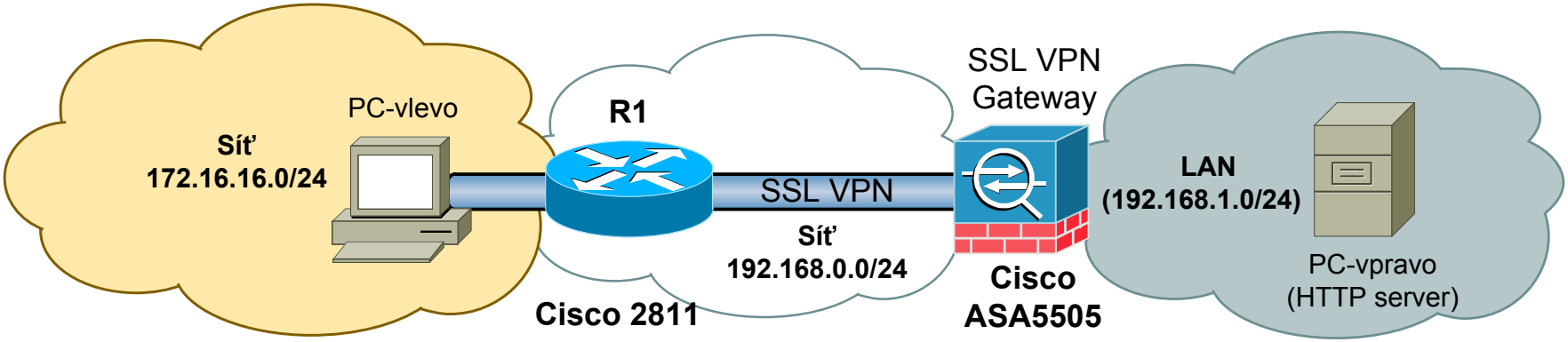
Laboratorní úloha č. 1 – Port Security



Laboratorní úloha č. 2 – IPsec VPN



Laboratorní úloha č. 3 – SSL VPN



Laboratorní úloha č. 4 – Zabezpečení VoIP