Bezpečnost síťových aplikací

2019/2020

Př 1

Základní informace

- Přednášející
  - Ing. Luboš Matějka, Ph.D.
    - Email : lmatejka @ kiv.zcu.cz
    - Konzultace : St 10:05-11:00 / email, UN 358
- Cvičící
  - Ing. Jindřich Skupa
    - Email : skupaj @ kiv.zcu.cz
    - Konzultace : St 13:00-13:30, Čt 15:00-15:30, UN 305

Organizace předmětu

- Přednášky:
  - Teoretický úvod do problematiky
- Cvičení:
  - Praktické odzkoušení témat z přednášek
  - Nastavení vybraných příkladů na Linuxu

Hodnocení předmětu

- Zápočet
  - 1. Strojové ověření nastavení virtuálu
    - (nutná podmínka pro praktický test)
  - 2. Praktické zvládnutí úkolů na PC
    - 0-10 bodů, 7 minimum,
    - Body nad 7b se započítávají ke zkoušce
- Zkouška:
  - Písemný test
  - 0-40b + až 3b ze zápočtu

Obsah předmětu

- Úvod do problematiky bezpečnosti počí-tačových sítí, OSI, X.800
- Ověření identity, úrovně oprávnění
- Zabezpečení síťových přenosů
- Zabezpečení uložených dat, datová in-tegrita, důvěryhodnost dat
- Zabezpečení serverů a stanic
- Zabezpečení WWW aplikací

Obsah předmětu

- Zabezpečení mailových služeb
- Centralizované řízení bezpečnosti a zabezpečení mobilních aplikací
- Detekce útoků, IDS, PDS, monitorování systémů, bezpečné logování
- Důvody a typy útoků, scénáře realizace
- Práva a povinosti v IT

Status předmět

- Bezpečnost není jeden všemocný příkaz či HW, ale velké množství malých nastavení či omezení....
- Celý předmět je náhled na danou prob-lematiku, ne dogma
- Odvětví se stále mění podle SW / HW
- Dotazy kdykoliv … ;)

Základní pojmy

Zabezpečení x Bezpečnost

Security X Safety

- Zabezpečení – hesla, ACL, firewall, ...
- Dostupnost – redundatní prvky, zálohování

Základní pojmy

Počítačová bezpečnost

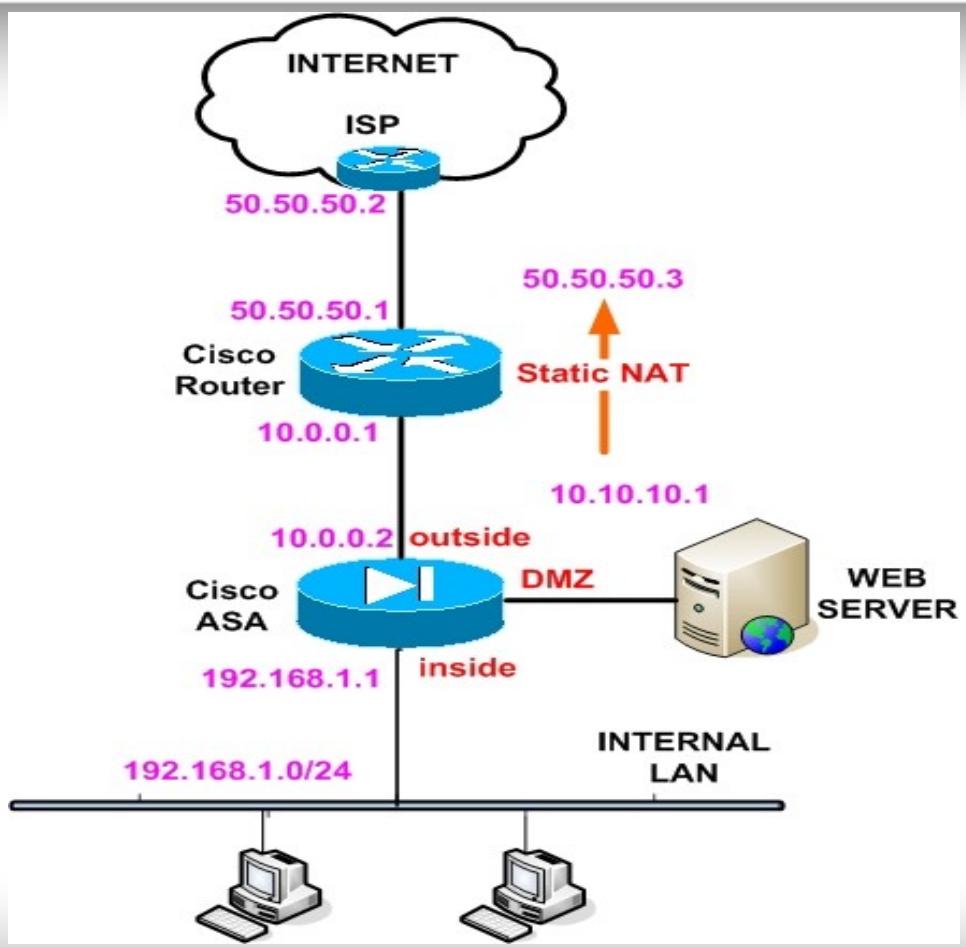
- Soubor prostředků k zabezpečení dat a systému

Síťová bezpečnost

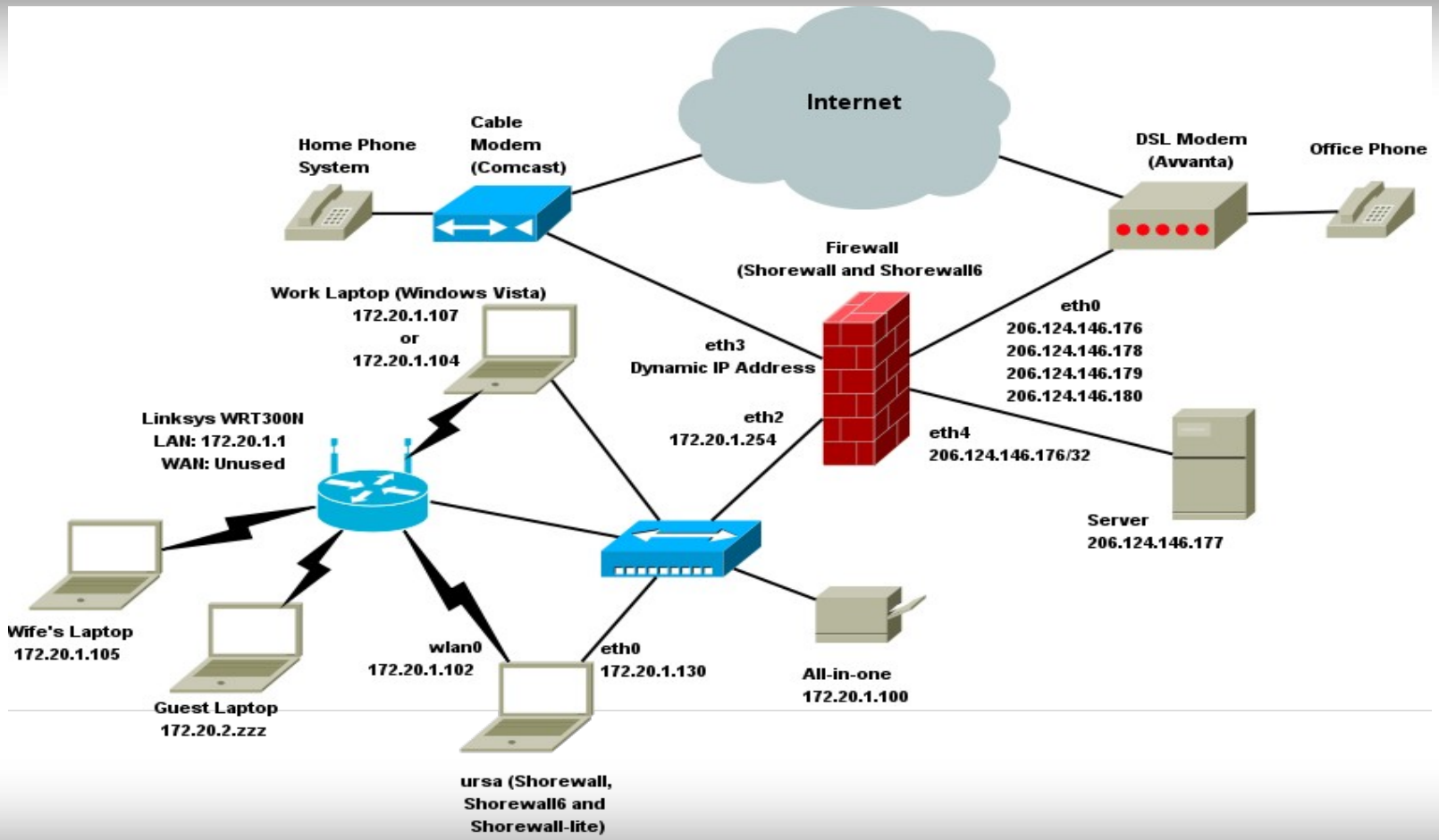
- Soubor opatření k ochraně dat během přenosu sítí

Neexistuje ostrá hranice ;(

Základní prostředí



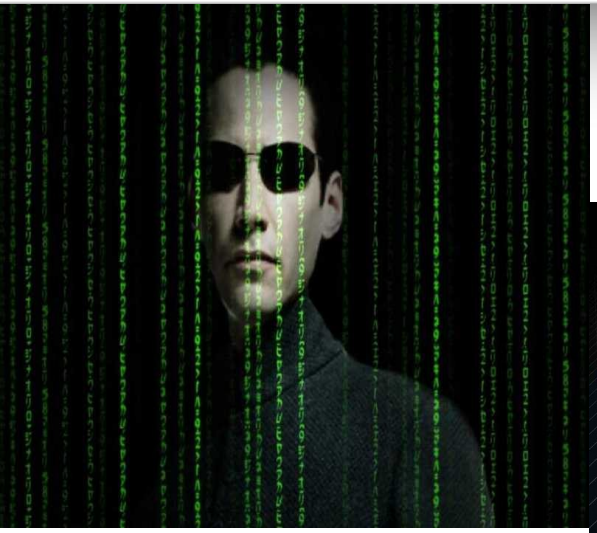
Základní prostředí

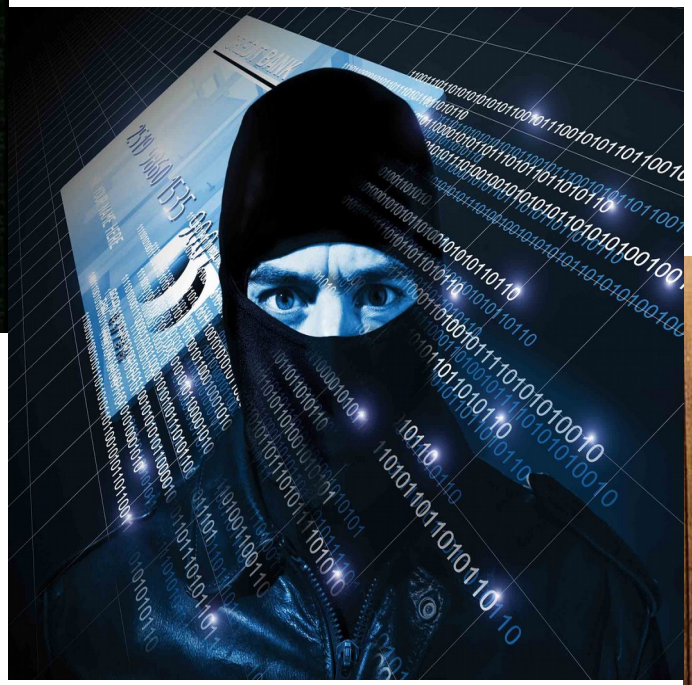


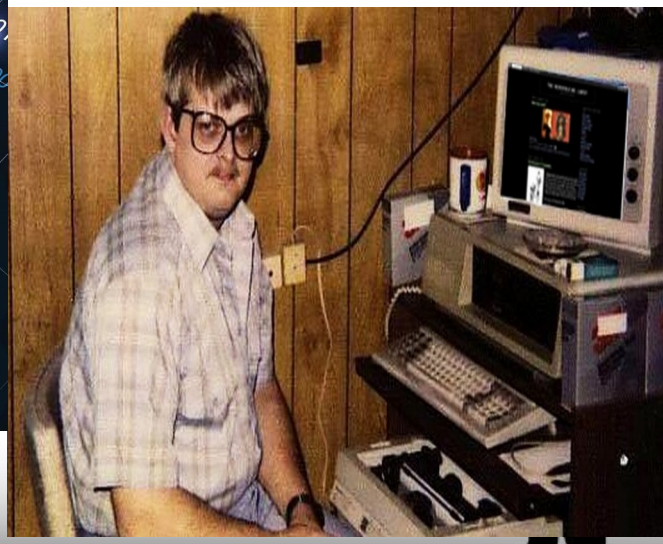
Základní otázky

- Co zabezpečuji ?
  - Síť, server, data, …
- Na jaké úrovni ?
  - ***vzdálený*** x fyzický přístup
  - lokální x ***externí*** přístup
  - aplikační x systémový
- Před kým ?
  - robot, vir, zaměstnanec, hacker/cracker => ?

Kdo je útočník ??? ;)







Popis bezpečnostních systémů

- Existuje více bezpečnostních modelů a norem
  - X.800
  - IT ISO/IEC 10181 Security Frameworks for Open Systems
  - ISO 7498-2 ISO/OSI Security Architecture
  - ISO/IEC 18028 – 5 částí
  - ISO/IEC 27033 – 7 částí

Architektura OSI

- Útoky na bezpečnost
  - Úmyslné incidenty nerušující bezpečnost
- Služby bezpečnosti
  - Postupy pro zvýšení bezpečnosti využívající bezpečnostní mechanizmy
- Mechanismy bezpečnosti
  - Postupy pro detekci, prevenci a odstranění škod po útocích

Typy útoku

- Pasivní
  - odposlechy, sběr, analýza toku dat
  - Neovlivňují chod systému, těžko detekovatelné
- Aktivní
  - aktivně “*cíleně*” provedená činnost
  - Možnost dohledání / monitorování
  - Na více úrovních ISO/OSI

Aktivní útoky

- ***Získání cizí identity či zdroje***
- **Zneužití zdrojů**
- *Odmítnutí služby*
- Předstírání identity na základě získaných údajů
- Opakování částí zpráv
- Modifikace zpráv

…

Služby bezpečnosti

- **Autentizace** – ověření identity
- **Autorizace** - řízení přístupu
- Zabezpečení **důvěrnosti** dat
- Zabezpečení **intergrity** dat
- Ochrana proti **odmítnutí** původu zprávy
- Služba **dostupnosti**
- **Prokazatelnost odpovědnosti**

SB - Autentizace

- Zajišťuje ověření, že prováděná komunikace je autentická
- Dva typy
  - Autentizace komunikujících uživatelů
  - Autentizace zdroje dat
- Jméno/heslo, certifikát, Kerberos, ...

SB – Řízení přístupu

- Schvaluje / omezuje přístup
- Neautorizovaný uživatel
  - Odmítnutí přístupu
- Autorizovaný uživatel
  - Přístup podle definovaných oprávnění
  - Různé role: Unix perm, ACL, Vlan Access

SB – Zabezpečení důvěryhodnosti dat

- Zajištění ochrany dat při přenosu
- Skrytí před neautorizovaným uživatelem
- Možnost identifikace podvržených dat
- Elektronické podpisy, certifikáty, šifrování

SB – Zabezpečení integrity dat

- Zajištění integrity dat při přenosu
- Znemožnění manipulace s daty během přenosu
- Možnost identifikace modifikovaných dat
- S a Bez možnosti obnovení integrity dat
- Kontrolní součty

SB – Ochrana odmítnutí původu dat

- Ověření původu zaslaných zpráv
- Zajišťuje popření odpovědnosti za
  - přijatá data
  - odeslaná data
- Příklad elektronické podpisy
  - Stále aktuálnější téma s ohledem na digitalizaci komunikace s úřady

SB – Služba dostupnosti

- Snaha zajistit dostupnost informací dle implementačního návrhu
- Snaha vždy dodat informace těm, kteří na ně mají právo
- Úzce souvisí se spolehlivostí
  - Vysoká dostupnost je zajištěna díky vysoké spolehlivosti systému
- Časté útoky na zamezení dostupnost
  - DoS, DDoS

SB – Prokazatelnost odpovědnosti

- Využívá předchozích služeb
- Pokud už dojde k potížím, musím mít možnost sjednat nápravu, prevenci a trest
- Nepopiratelné prokázání úmyslu
  - POZOR VSTUPUJETE KAM NEMÁTE
- Nepopiratelnost úmyslu
  - Školení / odsouhlasené normy / pravidla

Mechanismy bezpečnosti

- Kryptografie
  - šifrování, podepisování, ….
- Softwarová kontrola
  - Hesla, antiviry, oddělení uživatelů, ...
- Hardwarová kontrola
  - otisk prstu, token, firewall, ids, ...
- Fyzická kontrola
  - zámky, ochranka, zeď, ...
- Politiky a procesy – metodiky fungování

Cíle bezpečnosti

- Nadefinovat / popsat požadovaný systém
- Nadefinovat pravidla užívání systému
- Definovat a zabezpečit přístupové body
- Nadefinovat automatickou detekci zneužití
- Zajistit možnost zpětného zjištění průniku
- Zajistit možnost rychlé obnovy systému
- Nadefinovat následné právní kroky