C2110 *Operační systém UNIX a základy programování*

2. lekce

Linux jako víceuživatelský systém

Petr Kulhánek

kulhanek@chemi.muni.cz

Národní centrum pro výzkum biomolekul, Přírodovědecká fakulta
Masarykova univerzita, Kamenice 5, CZ-62500 Brno

Linux vs UNIX

UNIX je v informatice ochranná známka operačního systému vytvořeného v Bellových laboratořích americké firmy AT&T v roce 1969. Ochranou známku v současné době vlastní konsorcium The Open Group a mohou ji používat pouze systémy, které jsou certifikovány podle Single UNIX Specification.

Existují různé systémy, které jsou **s UNIXem v různé míře kompatibilní**, ale nemohou nebo nechtějí platit licenční poplatky, a proto často používají varianty názvů, které na název UNIX odkazují (například XENIX, MINIX, **Linux**), ale mohou se jmenovat i jinak (například BSD varianty OpenBSD, NetBSD, ale též **Mac OS X** atd.). Souhrnně je označujeme jako unixové systémy (anglicky unix-like).

GNU/Linux nebo jen krátce **Linux** je v informatice označení pro operační systém založený na **Linuxovém jádru**. První verzi jádra naprogramoval Linus Torvalds v roce 1991, který se dále na jeho vývoji aktivně podílí.

Upraveno z:
https://cs.wikipedia.org/wiki/Unix
https://cs.wikipedia.org/wiki/Linux
https://cs.wikipedia.org/wiki/Linux_%28j%C3%A1dro%29

Obsah

- **Opakování**
  - terminály, příkazová řádka
- **Příkazy**
  - manuálové stránky
- **Vzdálené přihlašování**
  - ssh, zabezpečení přenosu (šifrování), vnořené přihlašování, vzdálené spouštění grafických aplikací, přihlašovaní bez hesla (Kerberos)
- **Virtualizace**
  - co je to virtualizace, typické použití, přehled hypervisorů, MS Windows ve VirtualBoxu, Putty, instalace Ubuntu OS

Opakování

- terminály
- příkazová řádka

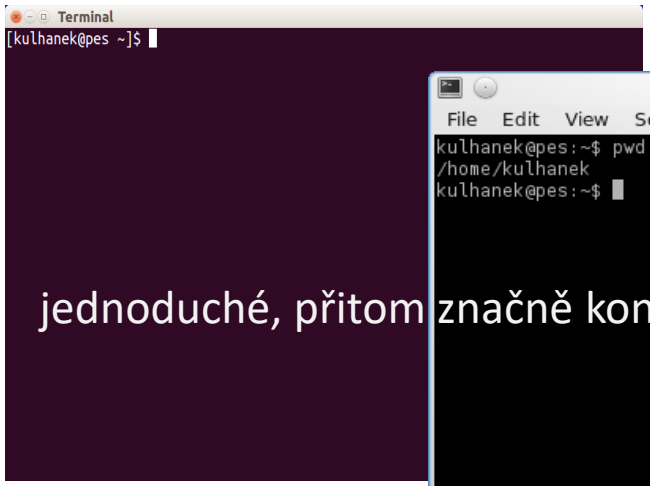
Terminály

Příkazová řádka je přístupná přímo z textových terminálů. V grafickém prostředí X11 je nutné spustit vhodnou aplikaci emulující textový terminál:

- **gnome-terminal (Terminal)**
- **konsole**
- **xterm**

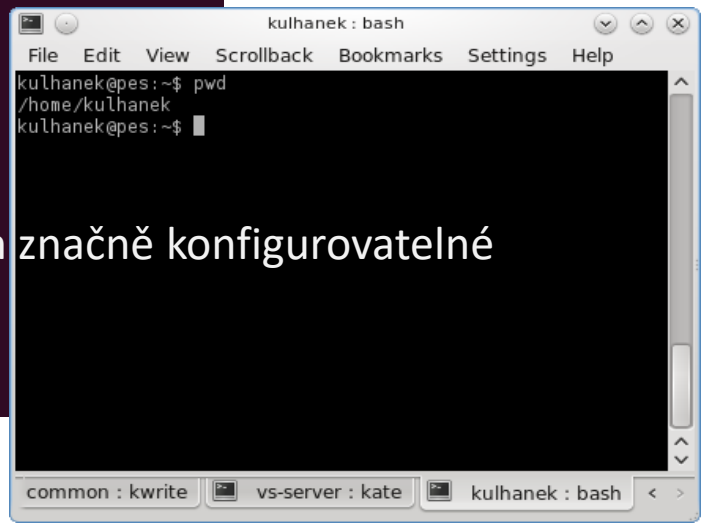
Výchozím adresářem je: **/home/username**

gnome-terminal

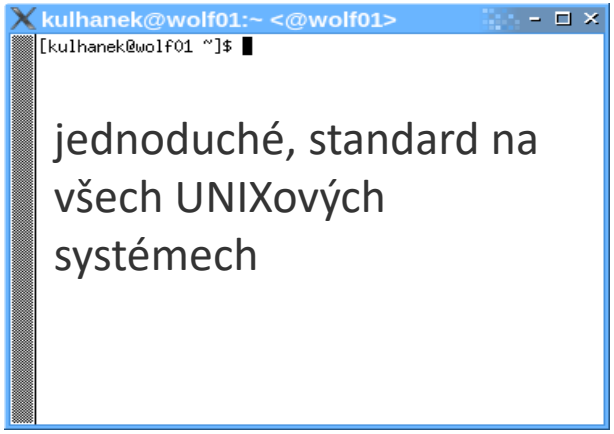


jednoduché, přitom značně konfigurovatelné

konsole

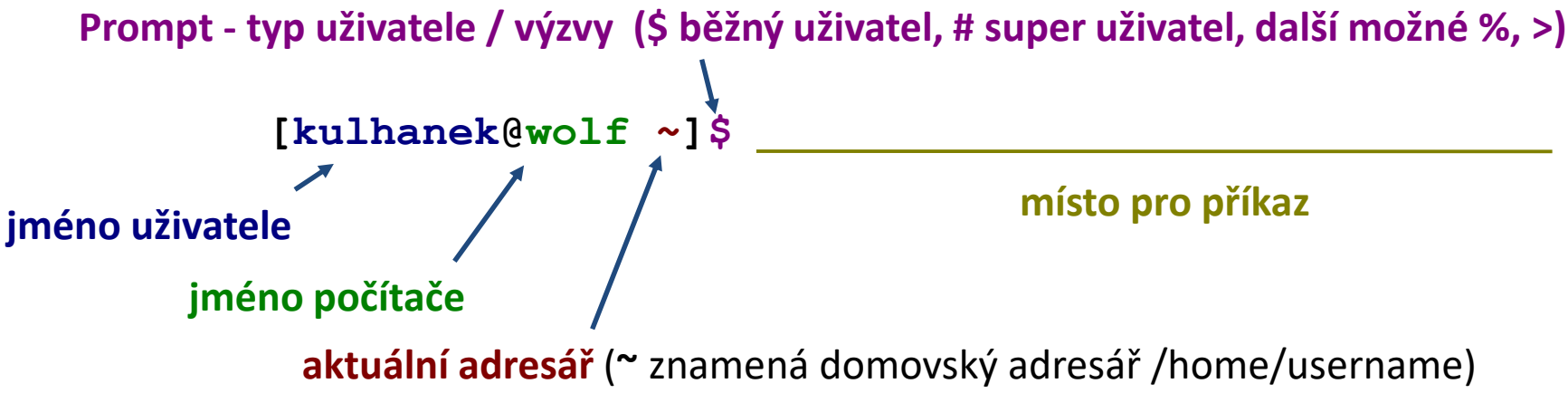


xterm



jednoduché, standard na všech UNIXových systémech

Příkazová řádka



Příkaz se vykoná zmáčknutím klávesy **Enter**.

Historie: pomocí kurzorových šipek nahoru a dolů lze procházet seznamem již zadaných příkazů. Příkaz z historie lze znovu použít nebo upravit a upravený použít. Historie je přístupná i příkazem **history**.

Zápisy:

```
$ ls -l
$ ssh wolf01.ncbr.muni.cz ls -l
# apt-get install firefox
```

Značí, že se jedná o zápis do příkazové řádky. Samotný znak $ a # se do ní nepíše.

Příkazy

- **manuálové stránky**

Nápověda k příkazům

Manuálové stránky (aneb co dělat, když si nevím rady):

man vypíše manuálovou stránku příkazu

```
$ man [section_number] topic
```

jméno příkazu, funkce, tématu, kapitoly apod.

Dostupné sekce:

- *Section 1* user commands
- *Section 2* system calls
- *Section 3* library functions
- *Section 4* special files
- *Section 5* *file formats*
- *Section 6* games
- *Section 7* conventions and miscellany
- *Section 8* administration and privileged commands
- *Section L* math library functions
- *Section N* tcl functions

Číslo sekce je nutné udávat u témat se stejným jménem zařazených do různých sekcí.

$ man 1 printf manuálová stránka příkazu printf

$ man 3 printf manuálová stránka funkce printf() jazyka C

Nápověda, hledání příkazů

Navigace v textu nápovědy:

- posun v textu po řádcích (kurzorové šipky nahoru a dolů nebo klávesy **j** a **k**)
- posun v textu po stránkách (**PgDn** a **PgUp** nebo klávesy **f** a **b**)
- vyhledávání (**/hledaný_text** , klávesa **n** pro další vyhledávání)
- zavření nápovědy (klávesa **q**)

On-line manuálové stránky ve formátu HTML:

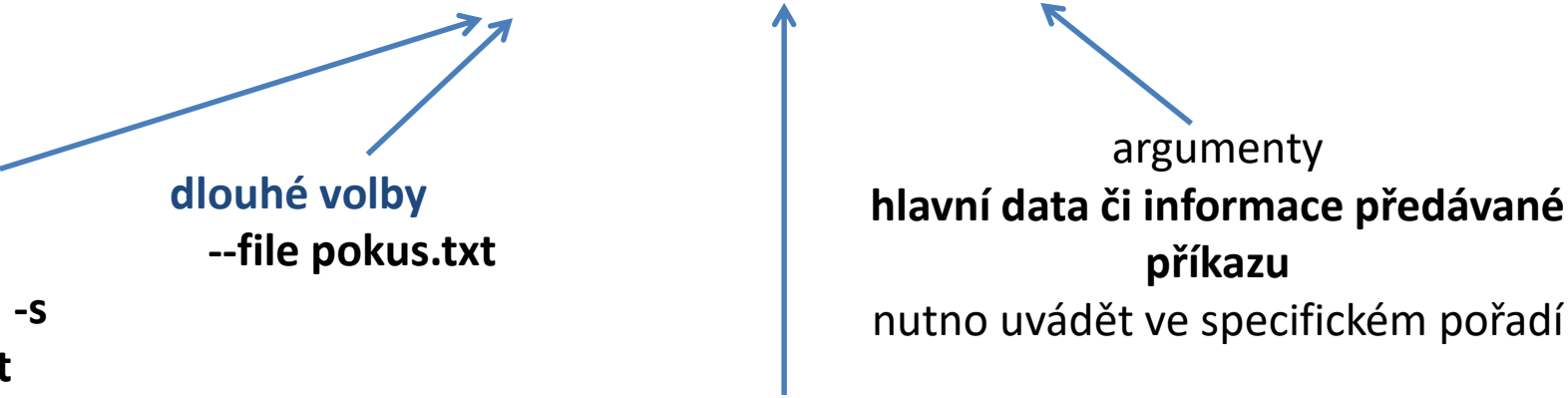
http://linux.die.net/man/

Užitečné příkazy:

whatis	vypíše krátký popisek příkazu (z manuálové stránky)
apropos	hledá příkazy obsahující v popisku v manuálu zadané klíčové slovo
info	zobrazení info stránek příkazů (obdoba manuálových stránek)

Popis/zadávání příkazu

```
$ command [options] [--] [arguments]
```



krátké volby
- **-a**
- **-as** nebo **-a -s**
- **-f pokus.txt**

dlouhé volby
- **--file pokus.txt**

argumenty
hlavní data či informace předávané příkazu
nutno uvádět ve specifickém pořadí

rozšiřují/mění chování příkazu
lze většinou uvádět v libovolném pořadí

ukončení zadávání voleb, je nutné použít jen ve velmi speciálních případech, běžně se nepoužívá

[] značí **volitelné** volby nebo argumenty
<> značí **povinné** volby nebo argumenty, popř. je uvedeno bez závorek

Příkazy

man	manuálové stránky příkazů
whatis	vypíše krátký popisek příkazu (z manuálové stránky)
apropos	hledá příkazy obsahující v popisku v manuálu zadané klíčové slovo
info	zobrazení info stránek příkazů (obdoba manuálových stránek)
whoami	vypíše jméno přihlášeného uživatele
hostname	vypíše jméno stroje, na kterém jste přihlášeni
id	vypíše identifikační údaje přihlášeného uživatele a jeho zařazení do skupin
w	vypíše, kdo je na stroj přihlášen a co dělá
who	vypíše, kdo je na stroj přihlášen
ps	vypíše běžící procesy
top	monitoruje běžící procesy
ssh	příkaz pro zabezpečené přihlášení na vzdálený stroj

Cvičení I

1. Jaké je celé jméno vašeho počítače (příkaz **hostname** a volba dle manuálových stránek).
2. Vypište vaše přihlašovací jméno příkazem **whoami**.
3. Jaké je vaše identifikační číslo (**uid**)?
4. Zjistěte, kdo je přihlášen k vaší pracovní stanici příkazem **w** a **who**.
5. Jaký je rozdíl mezi příkazy **w** a **who** podle manuálových stránek nebo příkazu **whatis**?
6. Najděte manuálové stránky ze sekce 1, které obsahují klíčové slovo **directory** nebo **directories**. Který příkaz slouží k vytváření adresářů?
7. Nechte si vypisovat přehled o běžících procesech příkazem **top** (běh příkazu se ukončuje klávesou q).

Vzdálené přihlášení

- ssh
- šifrování
- vnořené přihlašování
- vzdálené spouštění grafických aplikací
- autorizované veřejné klíče (přihlašovaní bez hesla)

Vzdálené přihlášení

Existuje několik možností vzdáleného přihlášení (rsh, XDMCP, apod.) avšak nejpoužívanějším a **nejbezpečnějším** je použití příkazu **ssh** (secure shell).

[] - možno vynechat

Syntaxe:

```
$ ssh [user@]hostname [command]
```

jméno uživatele;
pokud není uvedeno, použije se jméno přihlášeného uživatele

jméno počítače

příkaz, který se má vykonat; pokud není uveden, zpřístupní se příkazová řádka v interaktivním režimu

Příklady použití:

```
$ ssh wolf.ncbr.muni.cz
$ ssh wolf01 who
```

Odhlášení:

Vzdálené interaktivní přihlášení (sezení) se ukončuje příkazem **exit**.

Prvotní vzdálené přihlášení

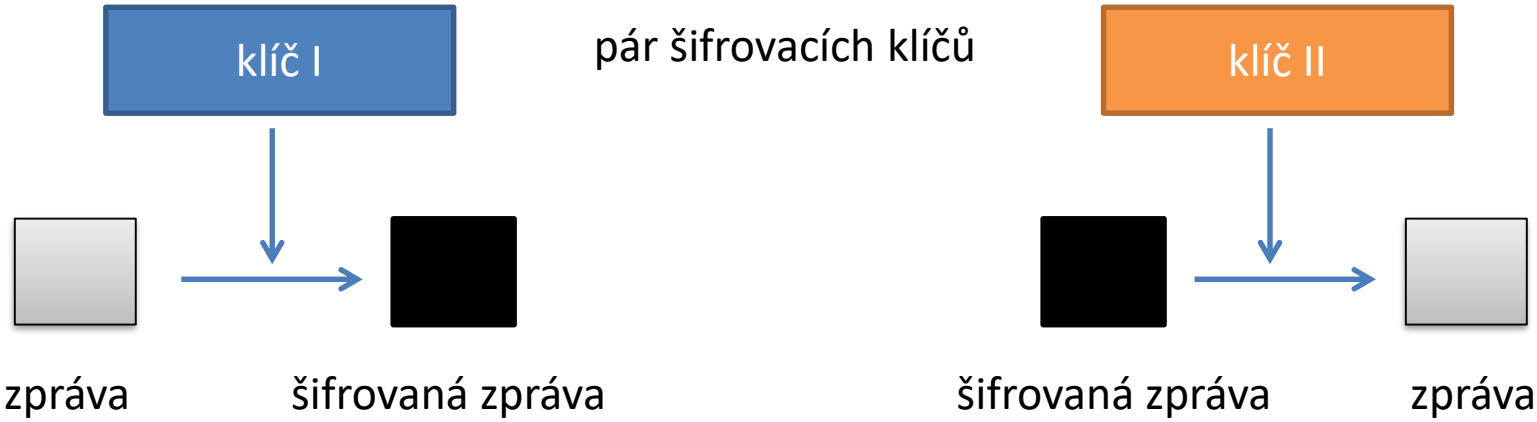
```
[kulhanek@pes ~]$ ssh skirit.ics.muni.cz
The authenticity of host 'skirit.ics.muni.cz
(2001:718:ff01:1:216:3eff:fe20:382)' can't be established.
ECDSA key fingerprint is SHA256:Splg9bGTNCeVSLE0E4tB30pcLS80sWuv0ezHrH1p0xE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'skirit.ics.muni.cz' (ECDSA) to the list of known
hosts.

[kulhanek@skirit ~]$
```

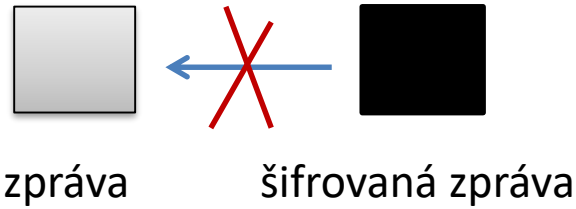
Při prvním přihlášení je nutné potvrdit autenticitu stroje, na který se hlásíme. Ve věrohodné síti můžeme otisk palce přijmout bez ověření. V nezabezpečeném prostředí je však vhodné otisk palce stroje ověřit nezávislou cestou (např. zasláním otisku palce poštou od správce vzdáleného stroje).

Poznámka:
Na klastru WOLF jsou všechny počítače vůči sobě důvěryhodné a toto potvrzení tak není vyžadováno.

Asymetrické šifrování



Dešifrování zprávy klíčem použitým pro šifrování **není prakticky proveditelné**.

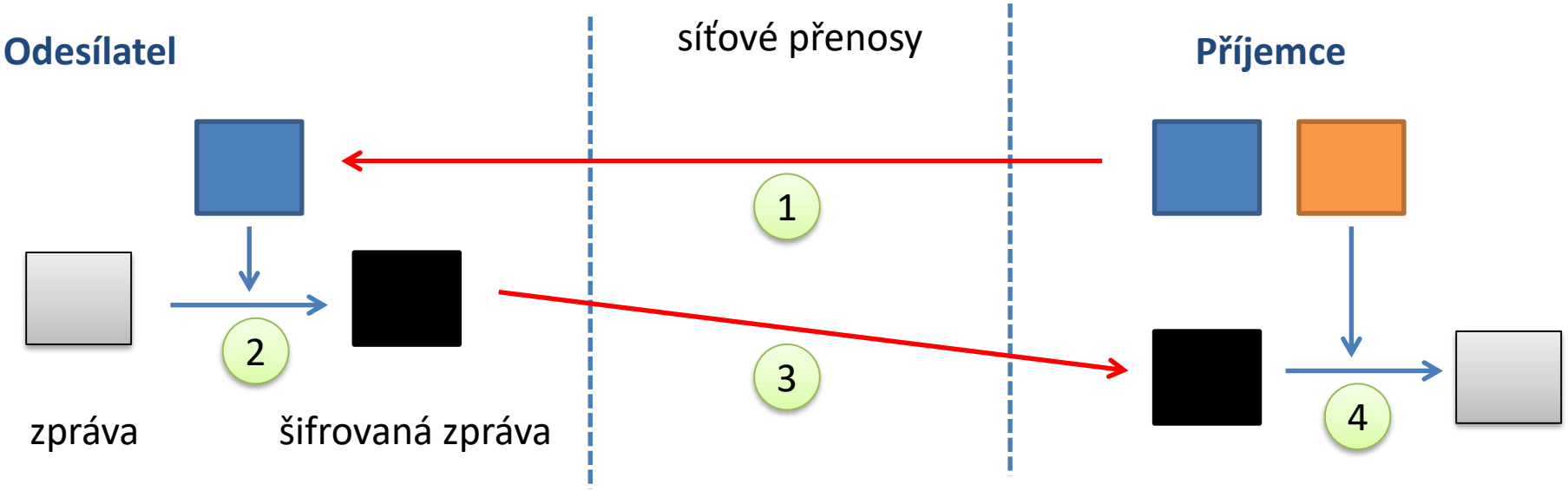


Asymetrické šifrování, použití I

veřejný klíč | soukromý klíč — pár šifrovacích klíčů

Utajený přenos zprávy:

1. získání veřejného klíče příjemce
2. šifrování zprávy odesílatele veřejným klíčem příjemce
3. odeslání šifrované zprávy přes nezabezpečenou síť
4. příjemce dešifruje zprávu svým soukromým klíčem



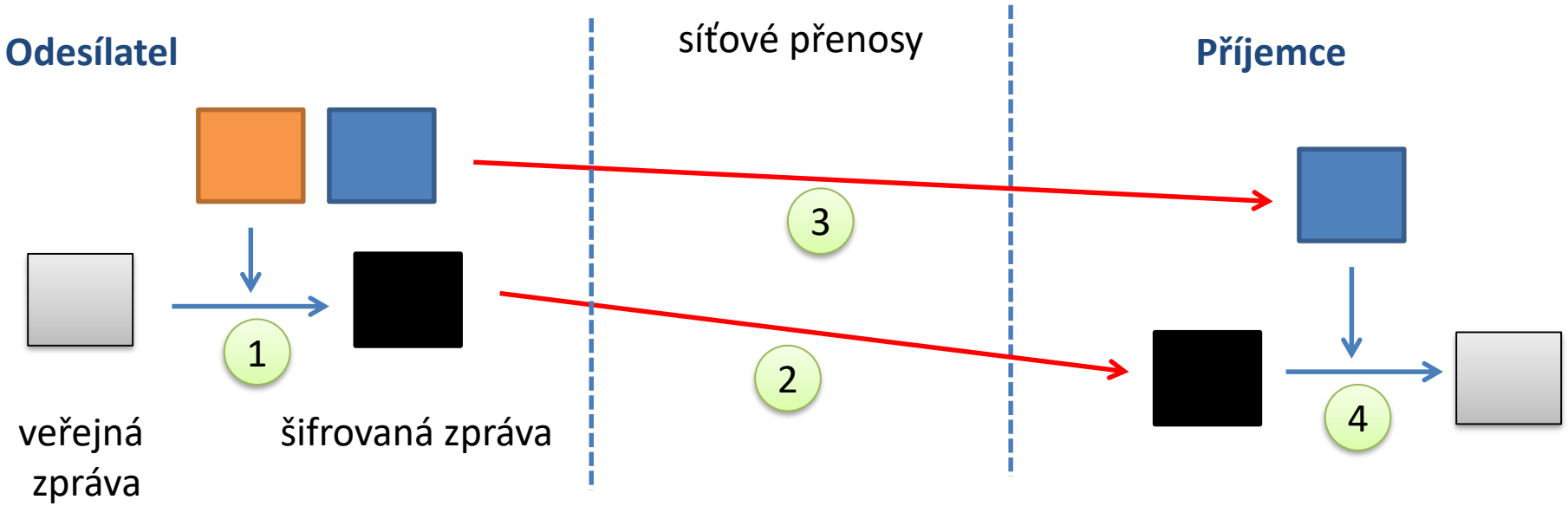
Kdokoliv, kdo zcizí soukromý klíč příjemce, muže dešifrovat přenášené zprávy!

Asymetrické šifrování, použití II

veřejný klíč | soukromý klíč — pár šifrovacích klíčů

Ověření odesílatele veřejné zprávy:

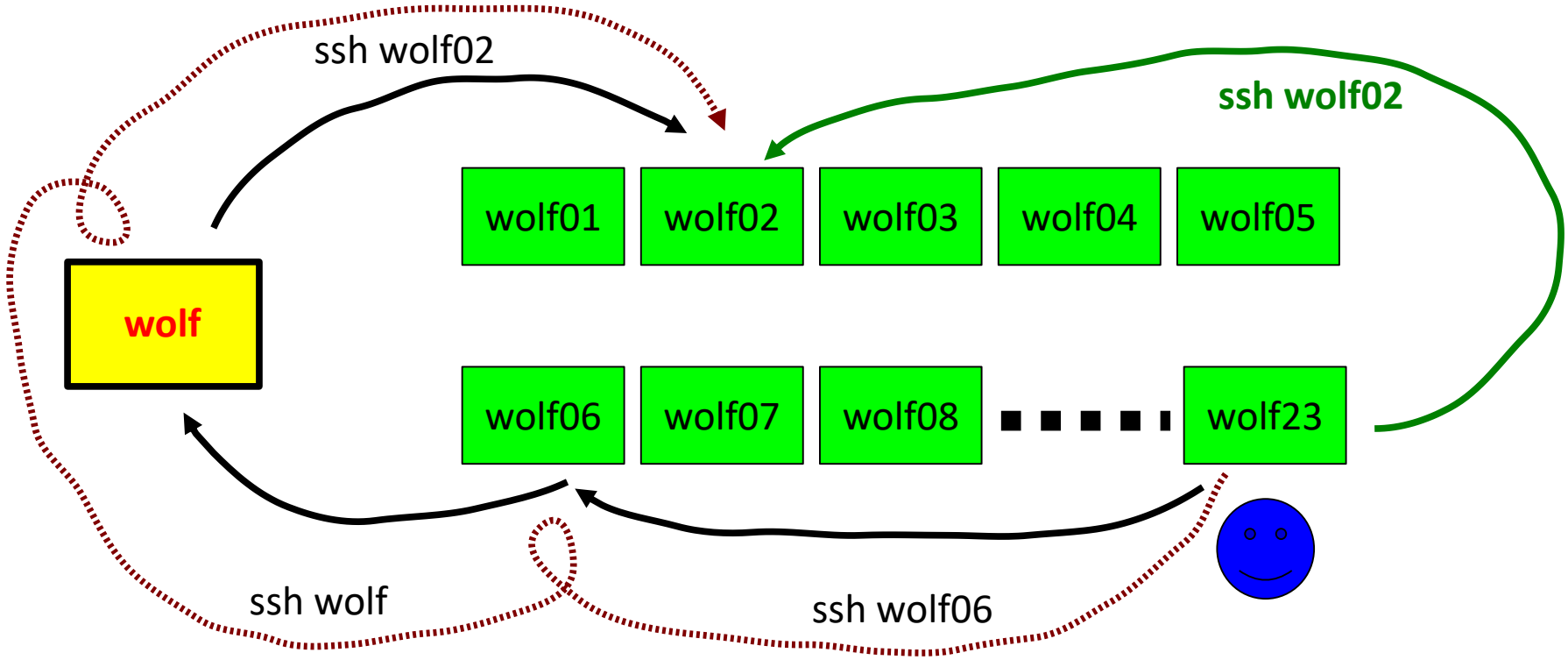
1. zašifrování zprávy soukromým klíčem odesílatele
2. příjemce získá zašifrovanou zprávu a veřejný klíč odesílatele
3. příjemce dešifruje zprávu veřejným klíčem odesílatele



Kdokoliv, kdo zcizí soukromý klíč odesílatele, se za něj může vydávat!

Vzdálené přihlášení

Pomocí příkazu ssh je možné provést **vnořené vzdálené přihlášení**.



S každou novou úrovní vzdáleného přihlášení **roste režie**, proto, pokud je to možné, použijeme **nejpřímější vzdálené přihlášení**.

Vnořené vzdálené přihlašovaní je nutné použít pro přístup na počítače v neveřejných sítích. (detaily superpočítaní C2115).

Cvičení II

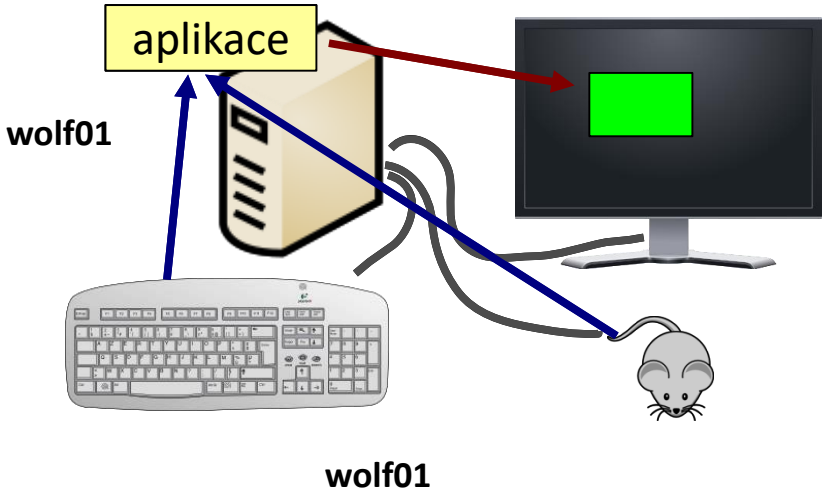
1. Přihlaste se na vzdálený uzel **wolf01.ncbr.muni.cz**
2. Ověřte, že se skutečně jedná o uzel wolf01 (příkaz **hostname**). Příkazy **w** a **who** pak zjistěte, kdo je na uzlu přihlášen.
3. Odhlaste se z uzlu **wolf01.ncbr.muni.cz**
4. Zjistěte, kdo je přihlášen na uzlu **wolf01.ncbr.muni.cz**, aniž byste se na něj interaktivně přihlásili.

používejte více terminálů

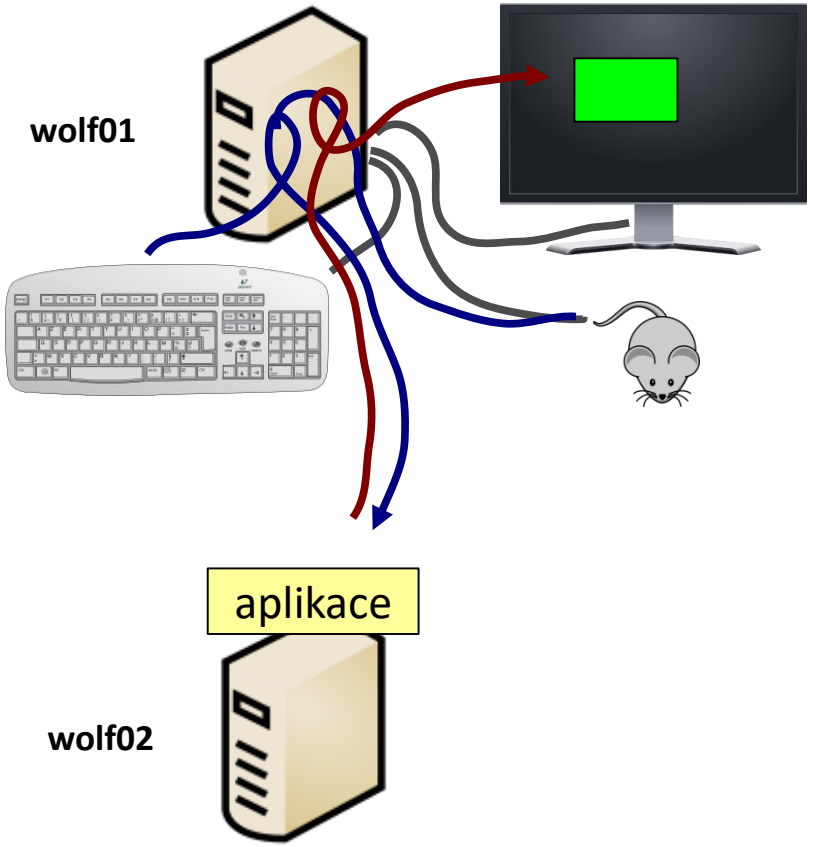
Vzdálené spouštění GUI aplikací

Grafické aplikace je možné spouštět přímo v prostředí X11 (grafickém terminálu) nebo s exportem displeje na vzdálenou plochu prostředí X11.

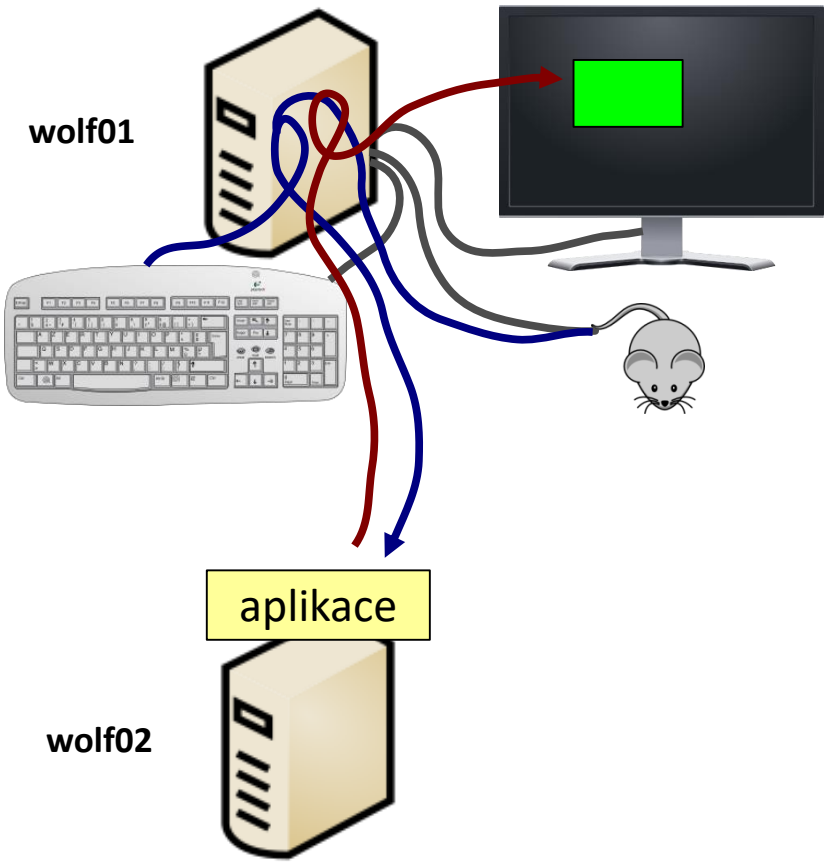
Přímé spouštění



Export displeje



Export displeje



Příkaz **ssh** nastaví všechny potřebné náležitosti pro export displeje automaticky při použití volby -X (velké X).

```
[wolf01] $ ssh -X wolf02
[wolf02] $ ./my_application
```

Volba -x (malé x) export naopak zakáže.

Na klastru WOLF je volba –X implicitně zapnutá.

Export displeje, lze provest i manuálně, nicméně je nutné nastavit proměnnou DISPLAY a správně volat příkazy xhost a xauth.

Export displeje - doporučení

- Export displeje vyžaduje kvalitní sítovou konektivitu s nízkou latencí a vysokou přenosovou rychlostí.
- V případě exportu aplikací zobrazujících 3D grafiku (OpenGL) značně narůstají nároky na přenosovou rychlost a kompatibilitu grafických rozhraní lokálního a vzdáleného počítače.
- Doporučením je vyhnout se používaní exportu displeje (např. přenosem dat na lokální počítač a jejích zobrazení pomocí lokálně spuštěné aplikace). V nezbytných případech je pak vhodnější použít např. **VNC (Virtual Network Computing).**

Poznámky k VNC:

- Na klastru WOLF jsou zakázané (firewall) porty 5900 a výše, které využívá protokol VNC. Pro připojení VNC klienta je tedy nutné po spuštění VNC serveru příslušný port protáhnout na klienta pomocí ssh tunelu.
- Na strojích, kde je dostupné prostředí Infinity, tyto náležitosti automatický nastavují programy z modulu tigervnc.

$ module help tigervnc

Podrobnější informace v kurzu C2115.

Cvičení III

1. Přihlaste se na pracovní stanici vašeho kolegy.
2. Spusťte na ní program **nemesis** (modul nemesis).
3. Ověřte ve výpisu běžících programů (**ps -e**), že aplikace na vzdáleném stroji skutečně běží.
4. Ověřte, že na vaší stanici běží program nemesis spuštěný vašim kolegou (**ps -u username**).
5. Co znamenají volby **e** a **u** příkazu **ps**?

používejte více terminálů
pracujte ve dvojicích

Kerberos

https://cs.wikipedia.org/wiki/Kerberos_%28protokol%29

Aneb proč to po mne pak nechce heslo?

Podrobnější informace v kurzu C2115.

Kerberos

Na klastru WOLF je využíván **systém Kerberos** k ověřovaní identity uživatele. Po primárním ověření (přihlašovací jméno/heslo), uživatel získá lístek z realmu **META**, který jej opravňuje bez opětovného zadávání hesla využívat služby klastru či se přihlašovat na jiné klastry využívající k autentizaci stejný realm (např. MetaCentrum) a to po celou dobu platnosti lístku.

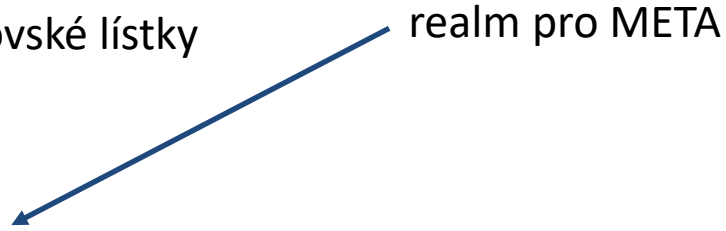
Kerberos je síťový autentizační protokol umožňující komukoli komunikujícímu v nezabezpečené síti prokázat bezpečně svoji identitu někomu dalšímu. Kerberos zabraňuje odposlechnutí nebo zopakování takovéto komunikace a zaručuje integritu dat. Byl vytvořen primárně pro model klient-server a poskytuje vzájemnou autentizaci – klient i server si ověří identitu své protistrany. Kerberos je postavený na symetrické kryptografii, a proto potřebuje důvěryhodnou třetí stranu. Volitelně může využívat asymetrického šifrování v určitých částech autentizačního procesu.

Kerberos má **přísné požadavky na synchronizaci času klientů a serverů**. Tikety mají danou životnost a pokud není čas klienta synchronizován s časem serveru, autentizace selže. Standardní nastavení podle MIT požaduje, aby se tyto časy **nerozcházely o více jak 5 minut**. V praxi se používá **NTP (Network Time Protocol)** démonů k synchronizaci hodin.

wikipedia.org

Příkazy

kinit	vytvoří nový kerberovský lístek
klist	vypíše existující kerberovské lístky
kdestroy	odstraní existující kerberovské lístky




```
[kulhanek@pes ~]$ kinit
Password for kulhanek@META:
[kulhanek@pes ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1001
Default principal: kulhanek@META

Valid starting       Expires              Service principal
01/30/2016 23:28:30  01/31/2016 23:28:24  krbtgt/META@META
[kulhanek@pes ~]$ kdestroy
[kulhanek@pes ~]$ klist
klist: No credentials cache found (ticket cache
FILE:/tmp/krb5cc_1001)
[kulhanek@pes ~]$
```

Vypršení lístků

Pokud vyprší lístek, tak bude odmítnut další přístup ke službám, které jej vyžadují. To může vést k viditelným chybám s odepřením přístupu. **Některé chyby se však viditelně neprojeví a hledání příčiny tak nemusí být "snadné"**. Typicky tato situace nastává u sezení, které jsou otevřené déle než je platnost kerberovského lístku a týká se převážně software aktivovaného pomocí příkazu module a fyzicky umístěného na AFS souborovém systému (téměř většina software v MetaCentru a na klastru WOLF).

Pokud se něco začne chovat divně (nefungující softwarové moduly), tak si nejdříve ověřte, že máte platné kerberovské lístky (klist) a případně je znovu vytvořte (kinit).

Cvičení IV

1. Ověřte stav kerberovských lístku. Kdy vyprší?
2. Přihlaste se na sousední počítat příkazem ssh. Je vyžadováno heslo?
3. Akci opakujte, ale lístky nejdříve odstraňte příkazem **kdestroy**.
4. Akci opakujte, ale nejdříve si lístky obnovte příkazem **kinit**.

Virtualizace

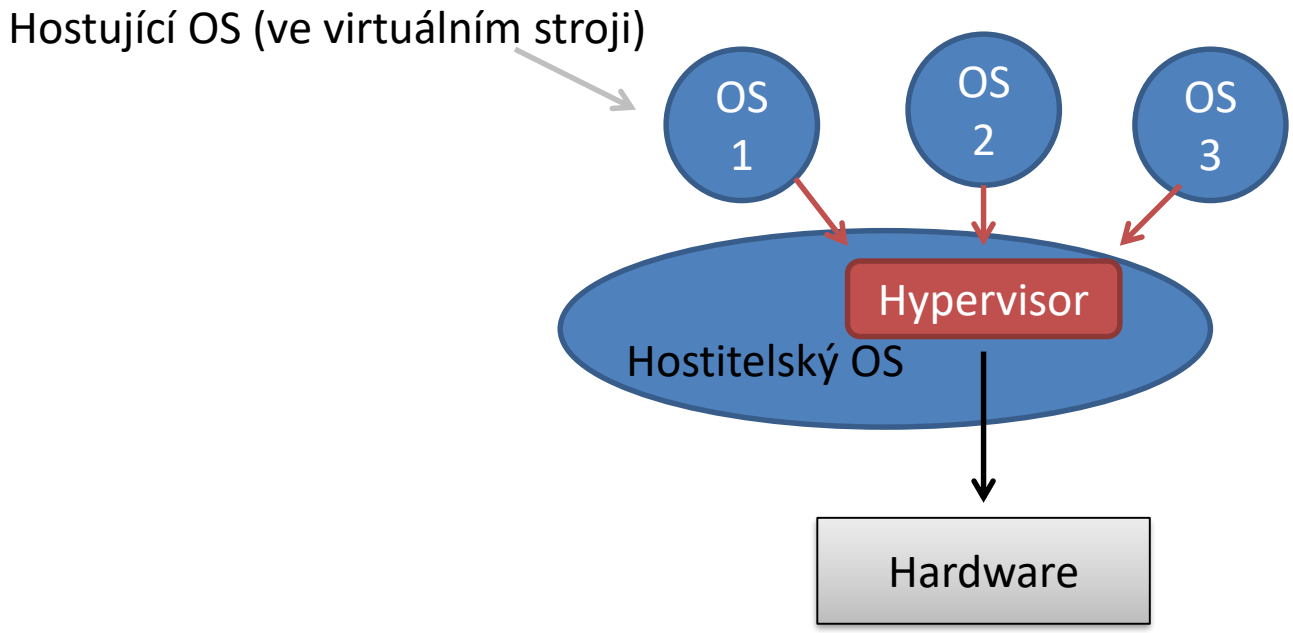
- co je to virtualizace
- typické použití
- přehled hypervisorů
- MS Windows ve VirtualBoxu
- instalace Ubuntu OS

Virtualizace - Hypervisor

Virtualizace jsou postupy a techniky, které umožňují k dostupným zdrojům přistupovat jiným způsobem, než jakým fyzicky existují. Virtualizovat lze **na různých úrovních**, od celého počítače (tzv. **virtuální stroj**), po jeho jednotlivé hardwarové komponenty (např. virtuální procesory, virtuální paměť atd.), případně pouze softwarové prostředí (virtualizace operačního systému).

zdroj: www.wikipedia.org

Hypervisor – správce virtuálních strojů



Výhody virtualizace

- Na jednom fyzickém stroji může běžet **více virtuálních strojů** (každý může mít instalován jiný OS).
- Výkon fyzického hardware je lépe využit (nižší provozní náklady).
- Snadnější zálohování. Stav virtuálních strojů je možné zaznamenávat do tzv. **snímků** (snapshosts), ze kterých je možné chod virtuálního stroje **obnovit**.
- **Teleportace**. Virtuální stroje lze přenést mezi dvěma fyzickými stroji s minimální dobou zastavení virtuálního stroje. Vhodné pří výměně vadného hardware nebo jeho upgrade.
- **Snadnější testování** OS.

Přehled nástrojů pro virtualizaci

VirtualBox **www.virtualbox.org**
Podporovaný hostitelský OS: MS Windows, Mac OS X, Linux
Licence: freeware + proprietární rozšíření pro nekomerční použití

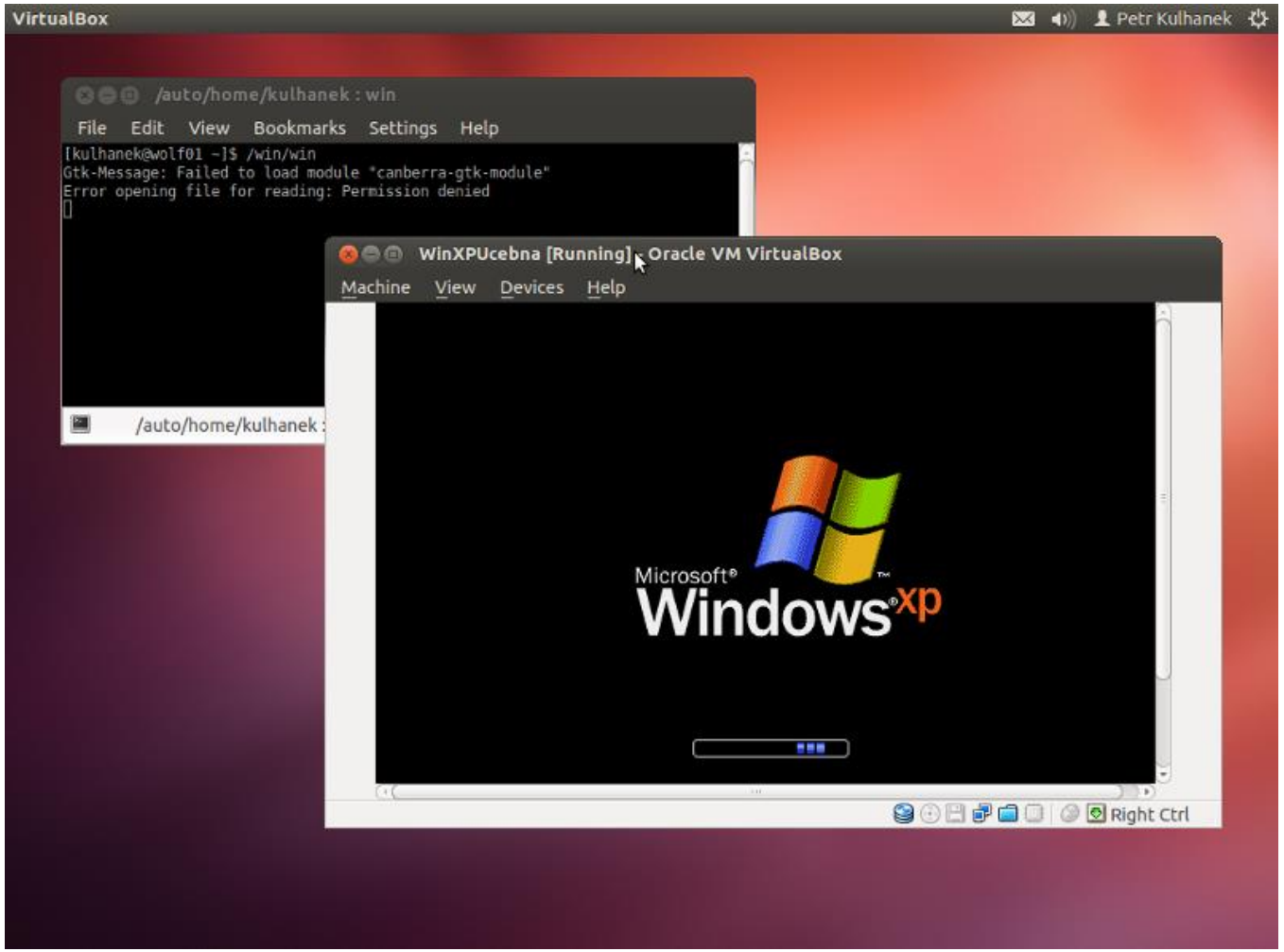
KVM součástí kernelu Linuxu
Podporovaný hostitelský OS: Linux
Podpůrné programy: virt-manager, qemu
Licence: freeware

VMWare **http://www.vmware.com/**
Podporovaný hostitelský OS: MS Windows, Linux
Licence: komerční

MS Windows na klastru WOLF

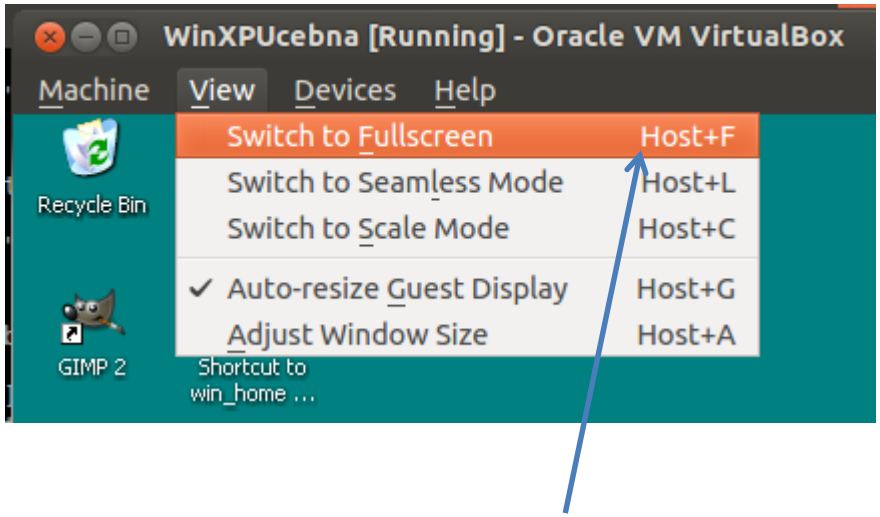
Spuštění MS Windows XP ve virtuálním stroji (hypervisor VirtualBox)

```
$ /win/win
```



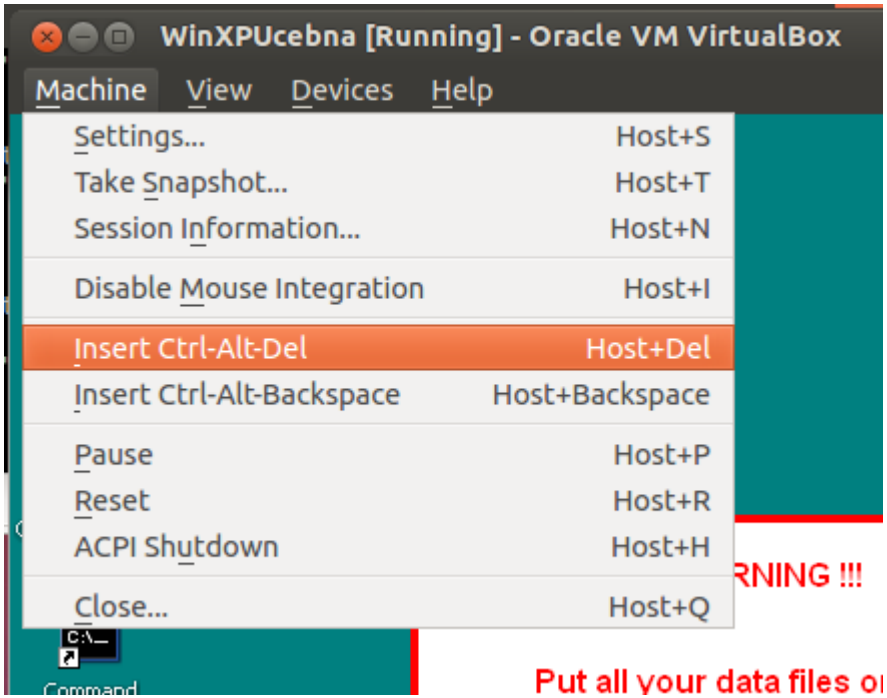
Ovládání virtuálního stroje

Přepnutí do/z Fullscreen



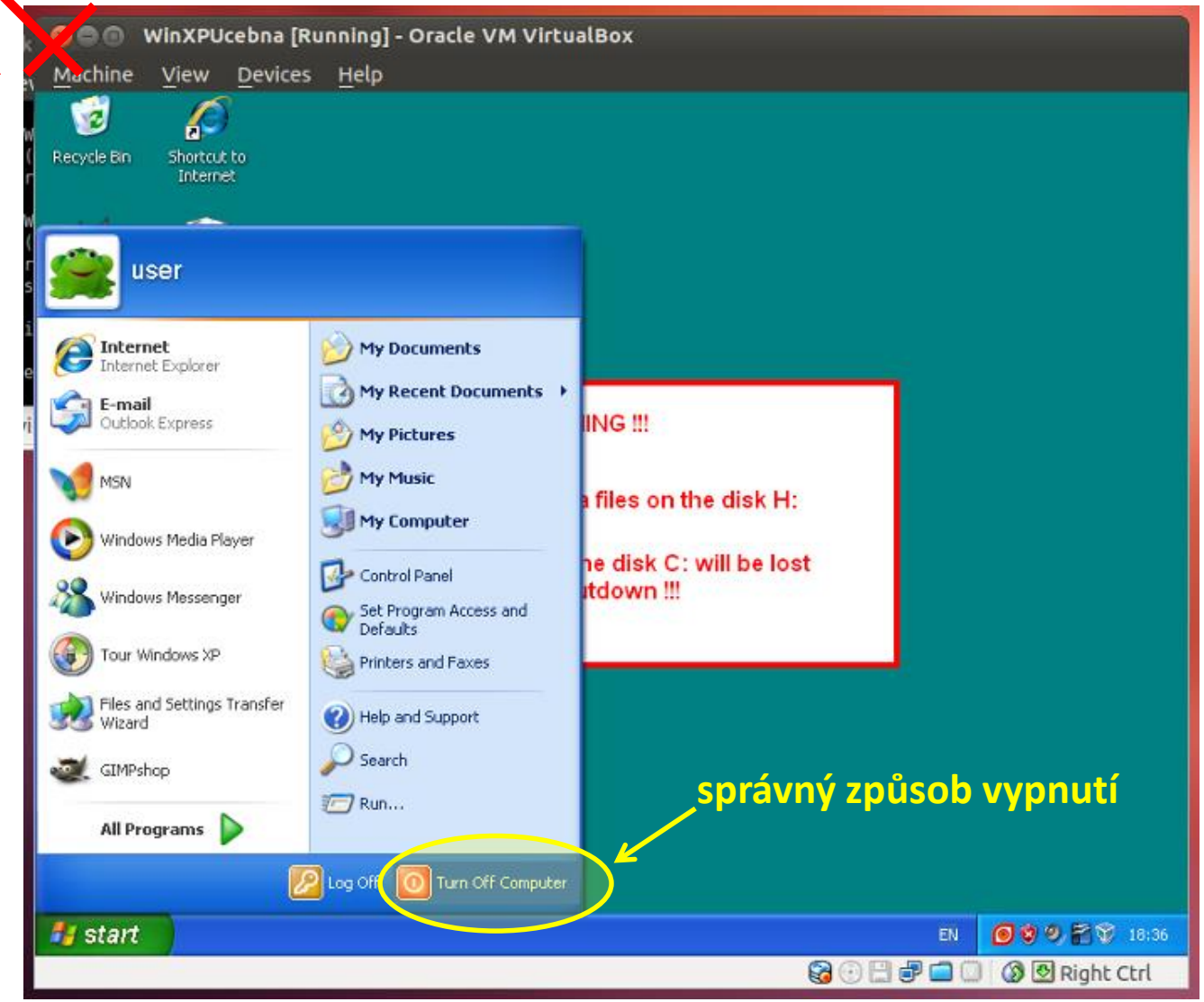
Host = (pravá klávesa Ctrl)
(pod MSWindows a Linuxem)

Zmáčknutí kláves Ctrl+Alt+Del



Vypnutí virtuálního stroje

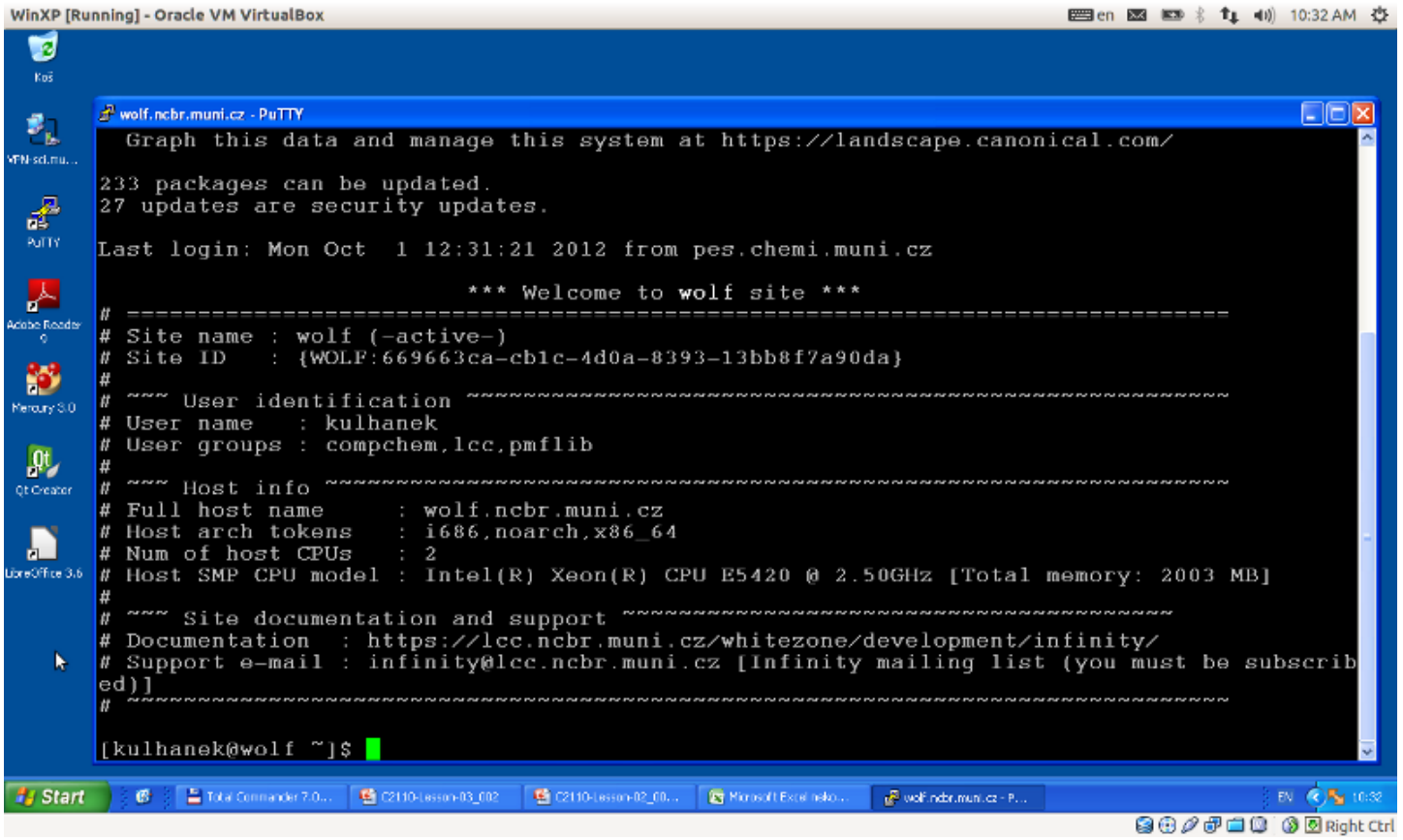
špatný způsob vypnutí



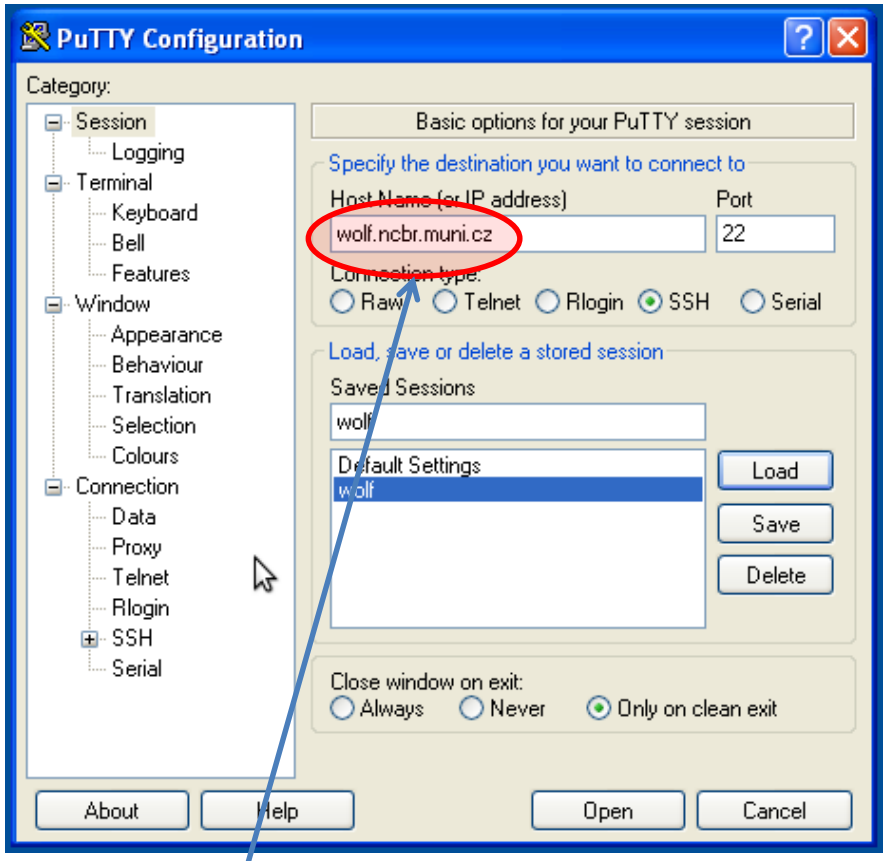
Putty

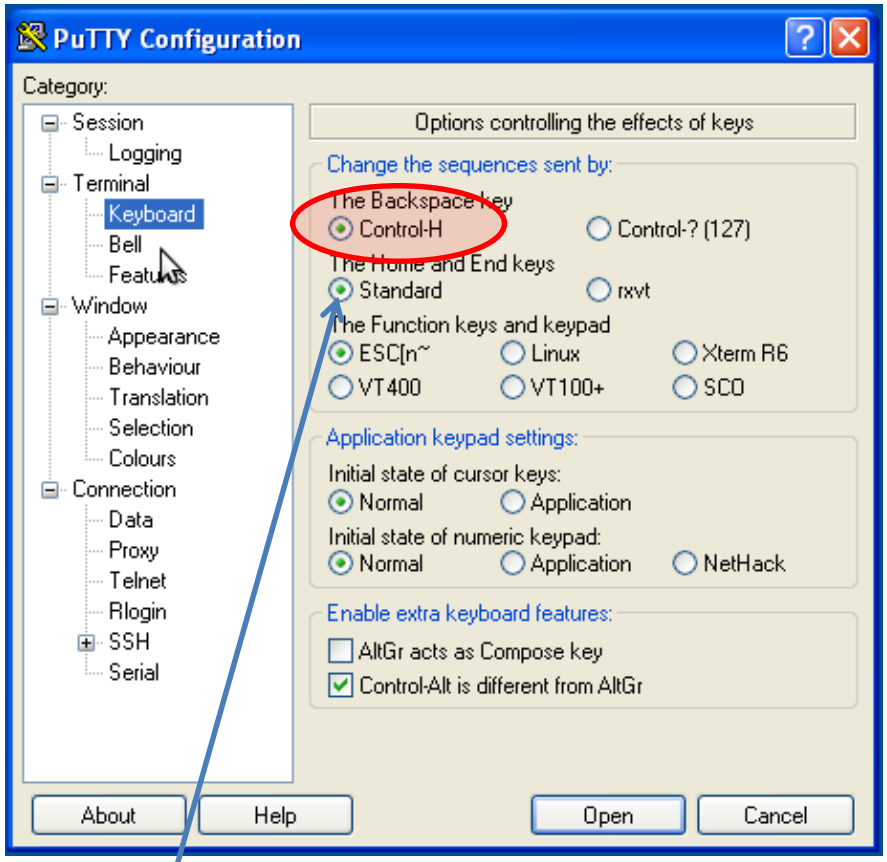
Putty http://www.chiark.greenend.org.uk/~sgtatham/putty/

Implementace SSH (Secure Shell) pro Windows, která umožňuje vzdálené připojení k počítačům podporující tento protokol (převážně unixového typu).



Putty – nastavení



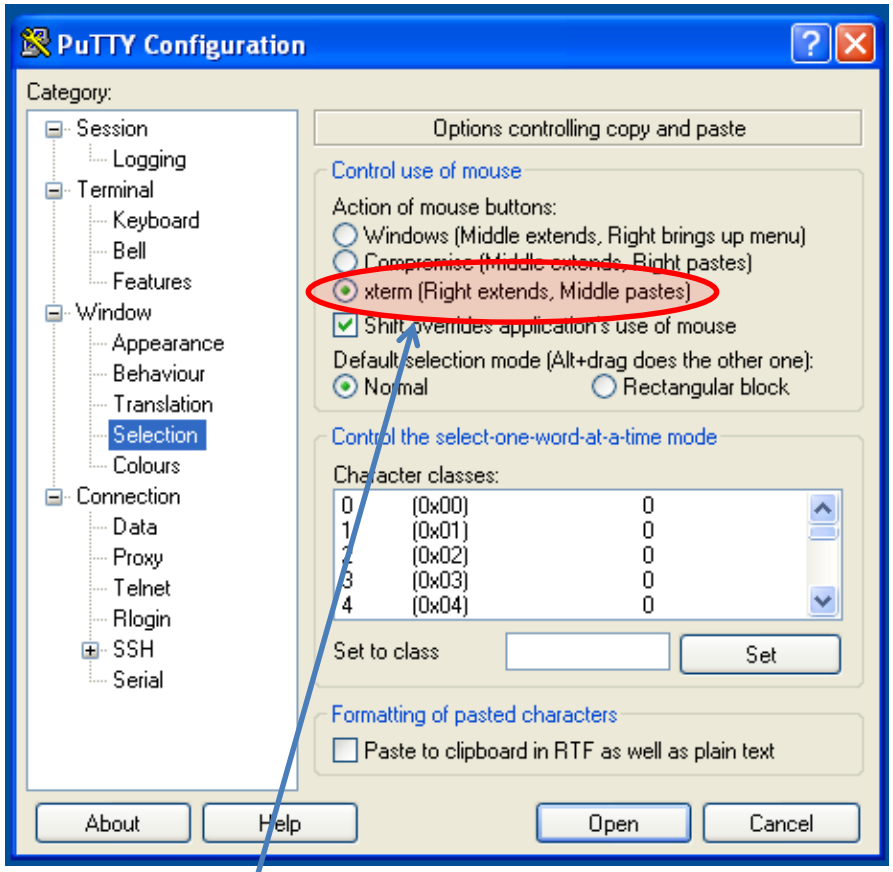


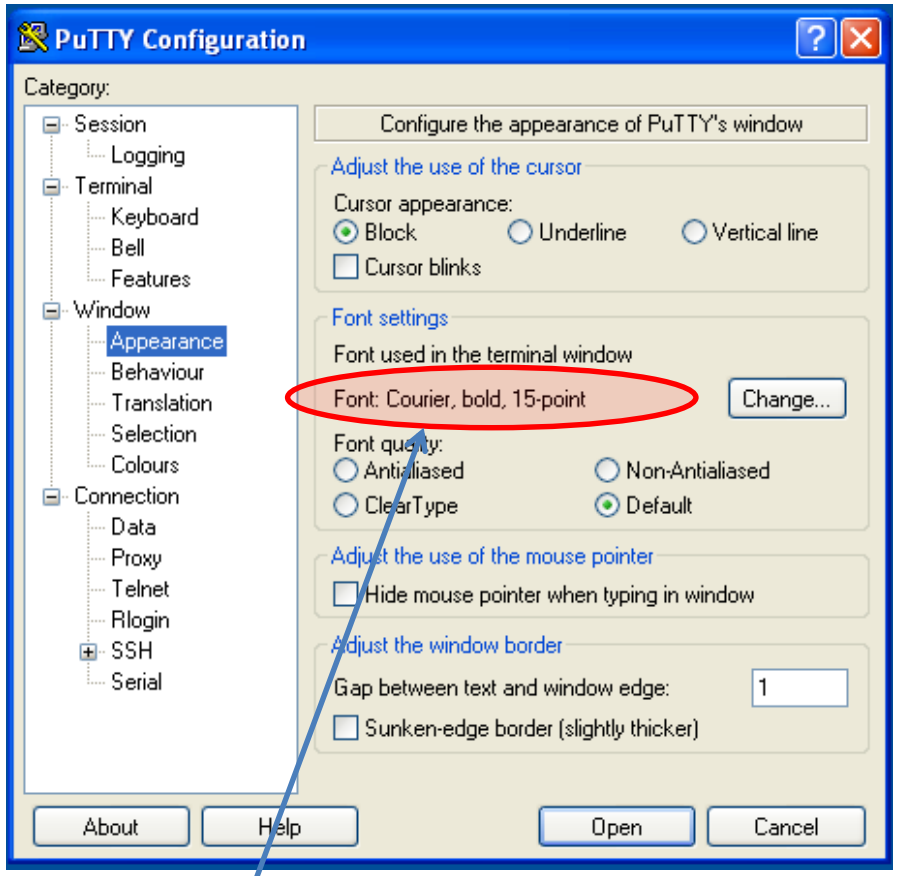
adresa vzdáleného stroje

wolf.ncbr.muni.cz

Správné fungování klávesy backspace.

Putty – nastavení II





selekce myší kompatibilní s Unixovými terminály

neproporcionální písmo
(všechny znaky mají stejnou šířku)

Cvičení V

1. Spusťte virtuální stroj s MS Windows XP (příkaz **/win/win**).
2. Ve virtuálním stroji otevřete **Internet Explorer** a ve Wikipedii (anglické) nalezněte klíčové slovo Hypervisor.
3. Na hostitelském OS monitorujte běh hypervisoru pomocí příkazu **top** (běh příkazu se ukončuje klávesou q).
4. Pozastavte a obnovte běh virtuálního stroje.
5. Otevřete program **Putty** v prostředí MS Windows.
6. Proveďte nastavení dle předchozích stránek a přihlaste se na čelní uzel klastru WOLF (**wolf.ncbr.muni.cz**).
7. Vypište přihlášené uživatele na čelním uzlu a to jak v terminálu **Putty**, tak i na vašem hostitelském stroji. Výpisy porovnejte.
8. V terminálu **Putty** spusťte aplikaci **nemesis** (modul nemesis). Chování vysvětlete?
9. Ukončete program Putty příkazem **exit**.
10. Ukončete běh virtuálního stroje.

Závěr

Závěr

- Linux je **víceuživatelským operačním systémem**, který umožňuje souběžnou práci několika uživatelů, kteří mohou být **přihlášeni místně nebo vzdáleně**
- Linux má nativní podporu pro **vzdálené spouštění aplikací** s grafických výstupem (GUI)
- Linuxu má **podporu pro spouštění virtuálních strojů**, lze v něm tedy spouštět instance operačního systému MS Windows
- **Systém je velmi dobře dokumentován** (příkazy, apod.)

Domácí úkoly

- **Instalace Ubuntu 16.04 LTS**

Instalace Ubuntu 16.04 LTS

- Nainstalujte si program VirtualBox (**http://www.virtualbox.org**).

- Stáhněte si instalační obraz pro OS Ubuntu ve formě iso obrazu.
  http://www.ubuntu.com/
  Ubuntu 16.04 LTS (Ubuntu Desktop)

- Vytvořte virtuální stroj ve správci VirtualBoxu
  zvolíme OS Linux a verzi Ubuntu
  zbytek nastavení je vhodné nechat na výchozích hodnotách

- První spuštění virtuálního stroje
  při prvním spuštění virtuálního stroje budeme vyzváni k vložení instalačního media, médium vložíme do virtuálního OS ve formě iso obrazu – souboru s koncovkou .iso - (ikona vpravo a zvolení staženého instalačního obrazu)

- Instalace systému
  po spuštění instalátoru z instalačního média pokračujte dle průvodce

Domácí úkol.