F4270 UNIX, počítačové sítě (jaro 2016), Cvičení 10

Příkazy: `ssh, ssh-keygen, ssh-copy-id, ssh-agent, ssh-add`. Projděte si `man` stránky k těmto příkazům.

A1 Zkuste se přihlásit pomocí `ssh` na vzdálený server, po úspěšném nalogovaní se zase odhlašte (ctrl-D || exit || logout).
`[guy@nix ~]$ ssh ucet@hostname`

A2 Zkontrolujte záznam v `.ssh/known_hosts`.
`[guy@nix ~]$ ssh-keygen -F hostname`

A3 Vytvořte klíč s prázdnou `passphrase`.
`[guy@nix ~]$ cd ./ssh`
`[guy@nix ~]$ ssh-keygen -t rsa -f klic_rsa`

A4 Zaveďte příslušný veřejný klíč na vzdálený server bez použití `ssh-copy-id`. V manualové stránce hledejte popis v kontextu k ‘`authorized_keys`. Tip: na vzdáleném serveru musí být `chmod 700 .ssh`, `chmod 600 authorized_keys`.

A5 Zkuste se přihlásit na vzdálený server.
`[guy@nix ~]$ ssh ucet@hostname`
Chce po vás `passwd` nebo `passphrase`, proč?

A6 Zkuste se přihlásit na vzdálený server s novou identitou (`.ssh/klic_rsa`)
`[guy@nix ~]$ ssh -i .ssh/klic_rsa ucet@hostname`
A co teď?

A7 Zrušte klíče a vymaže záznam v `authorized_keys` na servru.

A8 Vygenerujte si klíč pro příslušný účet pomocí `ssh-keygen` určený pro `ucet@hostname`, zadejte silnou `passphrase`.
`[guy@nix ~]$ cd ./ssh`
`[guy@nix ~]$ ssh-keygen -t rsa -f klic_rsa -n ucet@hostname`

A9 Zkopírujte veřejný klíč na vzdálený server
`[guy@nix ~]$ ssh-copy-id -i .ssh/klic_rsa.pub ucet@hostname`

A10 Zkuste se přihlásit na vzdálený server.
`[guy@nix ~]$ ssh ucet@hostname`
Chce po vás `passwd` nebo `passphrase`, proč?

A11 Zkuste se přihlásit na vzdálený server s novou identitou (`.ssh/klic_rsa`)
`[guy@nix ~]$ ssh -i .ssh/klic_rsa ucet@hostname`
A co teď?

A12 Zkontrolujte jestli vám běží ssh-agent.
`[guy@nix ~]$ ps auxw |grep ssh_agent`

A13 Případně si nastartujte `ssh-agenta`:
`[guy@nix ~]$ ssh-agent -s`

A14 Nakrmte `ssh-agenta` identitou `.ssh/klic_rsa`
`[guy@nix ~]$ ssh-add .ssh/klic_rsa`

A15 Zkuste se přihlásit na vzdálený server
`[guy@nix ~]$ ssh ucet@hostname`
Povedlo se bez hesla a bez fráze?

A16 Smažte nahranou idenitu z ssh agenta
`[guy@nix ~]$ ssh-add -d .ssh/klic_rsa`

A17 Přihlaste se na vzdálený server s ‘trusted X11 forwarding’. Použijte také kompresi (předpokládejte pomalou síť). Spusťte si vzdálenou aplikaci s gui rozhraním (použijte parametr `-no-remote` v případě firefoxu).
`[guy@nix ~]$ ssh -CY ucet@hostname`

A18 Spusťte si terminál přímo ze vzdáleného počítače přes ssh.
`[guy@nix ~]$ ssh -CY ucet@hostname -f xfce4-terminal`

A19 Prostudujte si `man ssh_config`. Všimněte si parametrů `ServerAliveInterval, TCPKeepAlive`.