VZDIALENÁ SPRÁVA POČÍTAČA S OS LINUX

AUTENTIZÁCIA VEREJNÝM KĽÚČOM V PROTOKOLE SSH

Teoretická časť

SSH server sa voči klientovi autentizuje kľúčom. Zjednodušene: server má dvojicu kľúčov: súkromný a verejný. Klient si zo servera stiahne verejný kľúč, vygeneruje náhodnú sekvenciu znakov, túto zašifruje stiahnutým verejným kľúčom a pošle serveru. Server správu rozšifruje svojim súkromným kľúčom a rozšifrovanú ju pošle klientovi. Týmto server preukázal svoju identitu.

Pomôcky

Tri virtuálne stroje vytvorené vo *VMware vSphere*; dva s CentOS 7, jeden s Windows 10. Stroje s CentOS 7 majú kvôli vzájomnému rozlíšeniu názvy *SERVER* a *CLIENT.* Úloha je určená pre jedného žiaka.

Úlohy

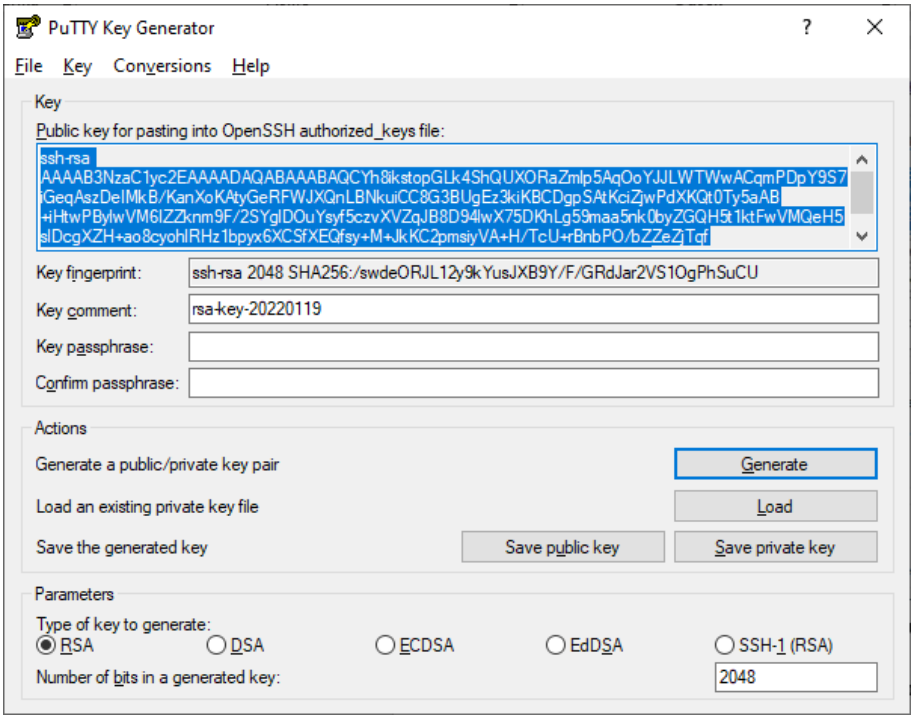
1. Spustite všetky virtuálne stroje, do strojov *SERVER* a *CLIENT* sa prihláste ako *root*, do stroja s Windows 10 ako používateľ s administrátorskými právami.
2. Zistite, aké IP adresy dostali stroje prostredníctvom *DHCP*; overte, že súhlasia s IP adresami, ktoré máte na strojoch zapísané v súbore */etc/hosts*, resp. v súbore *hosts*, ktorý sa v OS Windows nachádza v *C:\Windows\System32\drivers\etc.*
3. Pingom overte, že stroje vedia navzájom komunikovať prostredníctvom IP adries aj hostiteľských mien.

4. Na *clientovi* vytvorte používateľov *jahoda* a *malina.*
5. Odhláste sa zo *servera* a už sa naňho neprihlasujte. Všetko budete nastavovať vzdialene pomocou protokolu *SSH*.
6. Na *clientovi* sa odhláste z grafického režimu a znovu sa doňho prihláste ako používateľ *jahoda*.
7. Na *clientovi* si otvorte dva terminály. V 1. termináli sa prihláste na *server*; keďže používateľ je v obidvoch systémoch rovnaký použite príkaz **ssh server**. Na prihlásenie musíte zadať heslo používateľa *jahoda*, ktoré má na *serveri*.
8. V 1.termináli *clienta* v domovskom priečinku používateľa *jahoda* na *serveri* vytvorte skrytý priečinok *.ssh* a nastavte mu prístupové práva na hodnotu 700.
9. V 2. termináli *clienta* vygenerujte príkazom **ssh-keygen** dvojicu *RSA* kľúčov. Umiestnenie ani meno vytvorených kľúčov nemeňte. Súkromný kľúč ochráňte zadaním vhodnej frázy.
10. V 2. termináli *clienta* pomocou *scp* bezpečne prekopírujte verejný kľúč, t. j súbor */home/jahoda/.ssh/id_rsa.pub* na *server* do vytvoreného priečinka *.ssh* v domovskom adresári používateľa *jahoda* a uložte ho pod menom *authorized_keys.*
11. V 1. termináli *clienta* sa na *serveri* presuňte do priečinka */home/jahoda/.ssh* a vypíšte si jeho obsah. Overte, že sa v ňom nachádza prekopírovaný súbor *authorized_keys* a zmeňte mu prístupové práva na hodnotu 600.
12. V 1. termináli *clienta* sa príkazom **exit** odhláste zo *servera* a znovu sa naňho prihláste ako používateľ *jahoda*. Tento krát by vás už *server* nemal žiadať heslo; je ale potrebné zadať frázu, aby sa mohla správa zašifrovaná vašim verejným kľúčom, ktorú poslal *server*, odšifrovať vašim súkromným kľúčom.
13. Ak sa vám to podarilo, presuňte sa v 1. termináli *clienta* do priečinka */home/jahoda* na *serveri* a zmažte z neho celý skrytý priečinok *.ssh.*
14. V 2. termináli *clienta* pomocou príkazu **ssh-copy-id server** prekopírujte ako používateľ *jahoda* verejný kľúč uložený v */home/jahoda/.ssh/id_rsa.pub* na *server.*
15. V 1. termináli *clienta* si príkazom **ls -la /home/jahoda** zobrazte obsah priečinka */home/jahoda* na *serveri*, overte si, že sa v ňom automaticky vytvoril skrytý priečinok *.ssh* s príslušnými prístupovými právami. Overte si tiež, že vo

vytvorenom priečinku *.ssh* sa nachádza súbor *authorized_keys*, ktorý obsahuje verejný kľúč používateľa *jahoda* vytvorený na *clientovi.*

16. Na *clientovi* sa odhláste zo *servera* a v obidvoch termináloch zmeňte svoju identitu na používateľa *malina* príkazom **su - malina**.
17. V 1. termináli *clienta* sa prihláste na *server*; keďže používatelia v obidvoch systémoch sú rôzni, použite príkaz **ssh jahoda@server**. Na prihlásenie musíte zadať heslo používateľa *jahoda*, ktoré má na *serveri*.
18. V 2. termináli *clienta* vygenerujte príkazom **ssh-keygen -t ecdsa** dvojicu *DSA* kľúčov. Umiestnenie ani meno vytvorených kľúčov nemeňte. K súkromnému kľúču nevytvárajte žiadnu frázu.
19. V 2. termináli *clienta* chcete predtým vygenerovaný verejný *ECDSA* kľúč prekopírovať na *server* do domovského priečinka používateľa *jahoda*. Keďže ste nevytvorili dvojicu kľúčov predvoleným algoritmom *RSA* ale algoritmom *ECDSA*, musíte v nasledujúcom príkaze zadať cestu k vytvorenému kľúču. V príkaze musíte tiež zohľadniť, že sa na server prihlasujete ako iný používateľ. Použite na to príkaz: **ssh-copy-id -i /home/malina/.ssh/id_ecdsa.pub jahoda@server**.
20. V 1. termináli *clienta* si zobrazte obsah súboru */home/jahoda/.ssh/authorized_keys* na *serveri*; overte si, že obsahuje dva verejné kľúče.
21. V 1. termináli sa príkazom **exit** odhláste zo *servera* a znovu sa naňho prihláste. Tento krát by vás už *server* nemal žiadať heslo, nemala by sa ani objaviť výzva na zadanie frázy a *server* by vás mal automaticky autentizovať.
22. Na *clientovi* zavrite obidva terminály odhláste sa z grafického režimu, prihláste sa do grafického režimu ako *root.* Odstráňte používateľské účty *jahoda* a *malina,* stroj vypnite.
23. Pomocou programu *PuTTY* sa pripojte z virtuálneho počítača s Windows 10 na *server* ako používateľ *jahoda.*
24. Otvorte na počítači s Windows 10 program *PuTTYgen*, vygenerujte pomocou neho dvojicu *RSA* kľúčov pre *SSH* verzie 2.
25. Na počítači s Windows 10 v okne programu *PuTTY* zeditujte na *serveri* súbor *authorized_keys* v domovskom priečinku používateľa *jahoda* pomocou editora *vim* a pridajte doňho vygenerovaný verejný *RSA* kľúč z okna programu

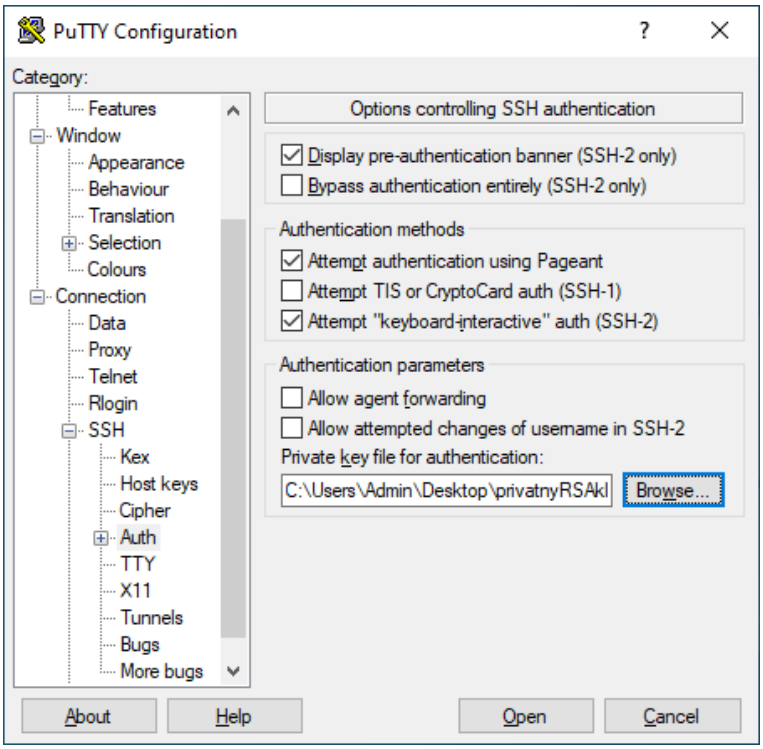
PuTTYgen. Okno programu *PuTTYgen* s označeným verejným kľúčom je zobrazené na Obrázku 1.



Obrázok 1 Dvojica *RSA* kľúčov pre *SSH2* vygenerovaná v programe *PuTTYgen.*

Súkromný kľúč v *PuTTYgen* ochráňte vhodnou prístupovou frázou a súkromný aj verejný *RSA* kľúč uložte na pracovnú plochu počítača s Windows 10. Potom program *PuTTYgen* zavrite.

26. Na počítači s Windows 10 zavrite program *PuTTY*, znovu ho otvorte a prihláste sa na *server*. Pred prihlásením v ľavej časti okna programu *PuTTY* rozbaľte ponuku *SSH – Auth* a pridajte tam cestu k vášmu súkromnému kľúču. Okno programu *PuTTY* s nastavenou cestou k súkromnému kľúču je zobrazené na Obrázku 2

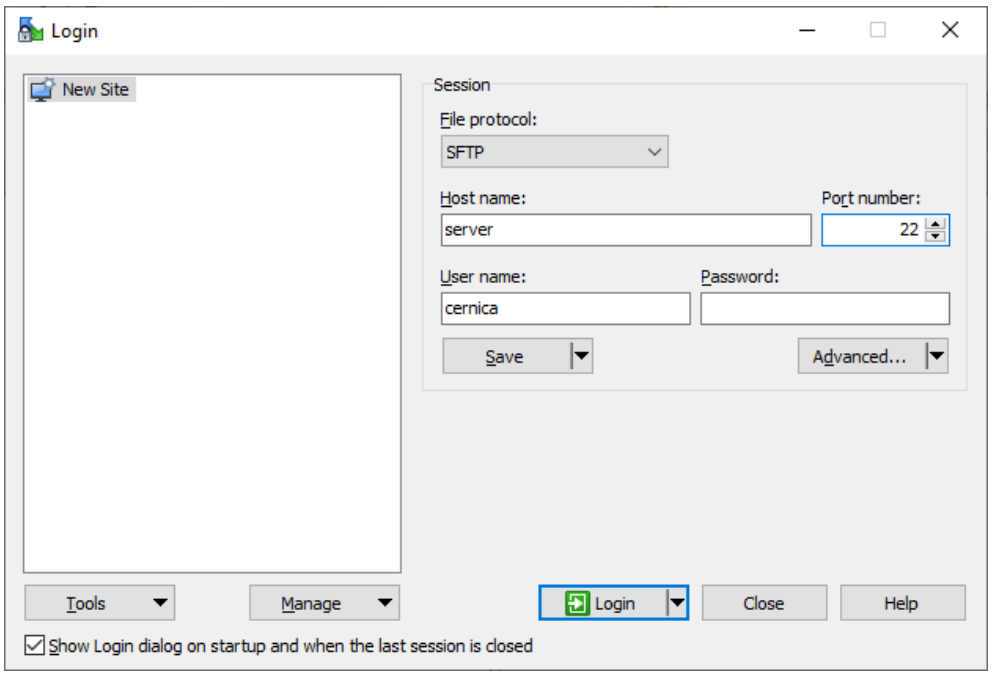


Obrázok 2 Nastavenie cesty k súkromnému kľúču používateľa v programe *PuTTY.*

Prihlásiť by ste sa mali bez hesla, ale budete musieť zadať prístupovú frázu. Potom okno programu *PuTTY* zavrite.

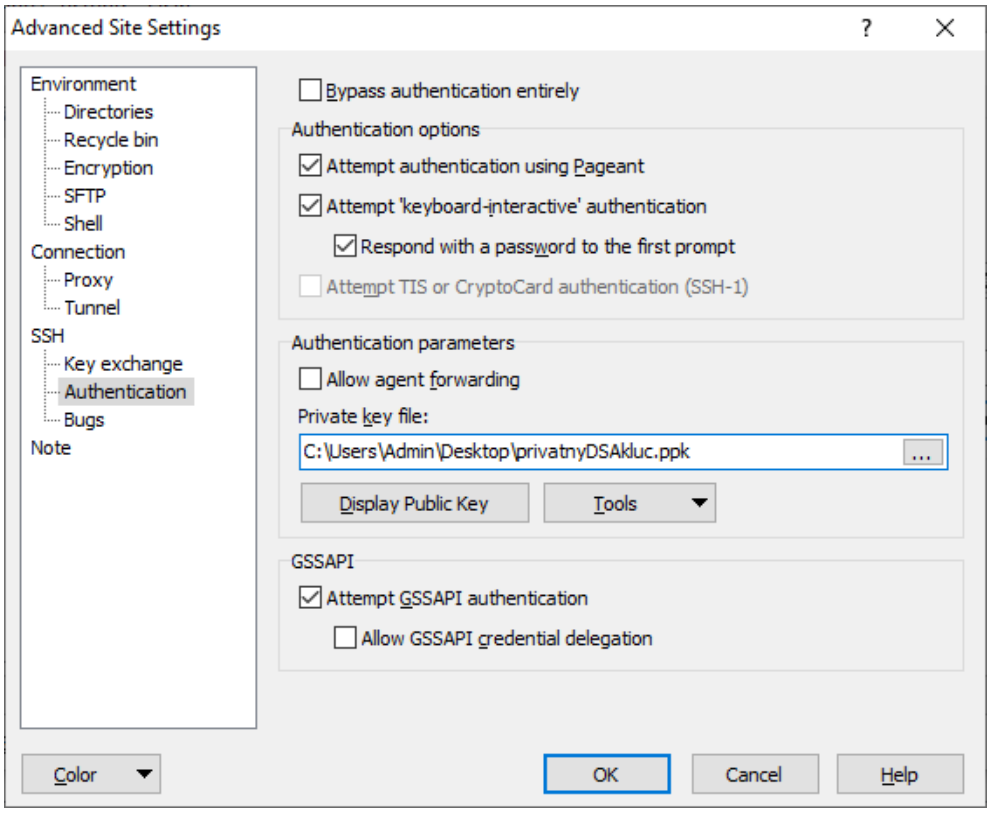
27. Na počítači s Windows 10 si znova otvorte program *PuTTY.* Aby ste stále nemuseli zadávať hostiteľské meno alebo IP adresu *servera* a tiež používateľské meno, vytvorte si príslušnú *session*; nazvite ju *jahodaserver* a uložte si ju. Predtým nastavte hostiteľské meno, cestu k súkromnému kľúču a v *Connection – Data* aj používateľské meno, pod ktorým sa chcete prihlásiť. Okno programu *PuTTY* zavrite, znova ho otvorte a prihláste na *server* kliknutím na vytvorenú *session*.
28. Na počítači s Windows 10 v okne programu *PuTTY* zmeňte sa *serveri* svoju identitu na používateľa *root* a ako tento používateľ vytvorte používateľa *cernica.* Vytvorte mu aj heslo.
29. Na počítači s Windows 10 zavrite okno programu *PuTTY.* Znova ho otvorte a vytvorte si *session* s názvom *cernicaserver.* Pridajte do nej hostiteľské meno *servera* a používateľské meno, *session* uložte. Prihláste sa na *server* pomocou tejto *session*, budete musieť zadať heslo používateľa *cernica* na *serveri*.

30. Na počítači s Windows 10 vygenerujte pomocou programu *PuTTYgen* dvojicu *DSA* kľúčov.
31. Na počítači s Windows 10 v okne programu *PuTTY* vytvorte na *serveri* skrytý priečinok */home/cernica/.ssh* a nastavte mu príslušné prístupové práva. V tomto priečinku vytvorte súbor *authorized_keys* a aj jemu nastavte potrebné prístupové práva. Potom tento súbor zeditujte pomocou editora *vim* a pridajte doňho vygenerovaný verejný *DSA* kľúč z okna programu *PuTTYgen*.
32. Súkromný kľúč v *PuTTYgen* zabezpečte prístupovou frázou a súkromný aj verejný *DSA* kľúč uložte na pracovnú plochu počítača s Windows 10.
33. Na počítači s Windows 10 zavrite okno programu *PuTTY* a znova ho otvorte. Nahrajte *session cernicaserver*, pridajte do nej vytvorený súkromný kľúč a *session* uložte. Potom sa pomocou nej prihláste na *server*. Okno programu *PuTTY* opäť zavrite.
34. Prihláste sa na *server* z počítača s Windows 10 pomocou programu *WinSCP* ako používateľ *cernica*; na autentizáciu použite vygenerovaný *DSA* súkromný kľúč. Postupujte podľa nasledujúcich pokynov:
    a) Okno programu *WinSCP* je zobrazené na Obrázku 3, údaje vyplňte rovnako, potom rozbaľte možnosti pri tlačidle *Advanced* a zvoľte možnosť *Advanced.*



Obrázok 3 Okno programu *WinSCP* pre prihlásenie používateľa *cernica.*

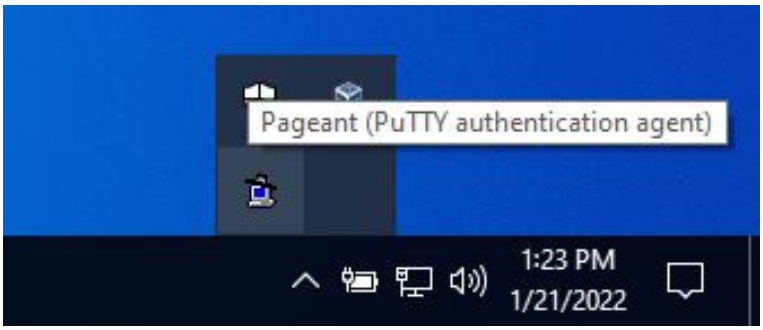
b) V ľavej časti novootvoreného okna zvoľte rovnako ako na Obrázku 4 možnosť *SSH – Authentication* a v pravej časti nastavte do poľa s názvom *Private key file:* cestu k súkromnému *DSA* kľúču. Kliknite na tlačidlo *OK* a v pôvodnom okne na tlačidlo *Login.*



Obrázok 4 Okno programu *WinSCP* s nastavením cesty k súkromnému *DSA* kľúču.

c) Na výzvu zadajte prístupovú frázu k súkromnému *DSA* kľúču. Po úspešnom pripojení zavrite okno programu *WinSCP.*

35. Súkromný kľúč je potrebné chrániť prístupovou frázou kvôli bezpečnosti. Aby ste ju nemuseli zadávať pri každom pripojení, môžete využiť agenta. Frázu musíte potom zadať iba pri vkladaní kľúčov do agenta; samotné pripojenia sú už potom realizované pomocou neho. Na počítači s Windows 10 otvorte okno programu *PuTTY*, nahrajte si jednotlivé *sessions*, odstráňte z nich súkromné kľúče a *sessions* uložte. Pri odstraňovaní kľúčov si overte, že máte zaškrtnuté políčko *Attempt authetication using PageAnt.* Spustite program *PageAnt*, jeho ikona sa rovnako ako na Obrázku 5 objaví v *Paneli úloh.*



Obrázok 5 Spustený program *PageAnt* v *Paneli úloh.*

Kliknite naňho a odovzdajte mu vytvorené súkromné kľúče. V okne programu *PuTTY* kliknite na niektorú *session* a sledujte ako vás agent automaticky prihlási. Okno programu *PuTTY* potom zavrite.

36. Program *WinSCP* spolupracuje s programom *PageAnt.* Na počítači s Windows 10 otvorte okno programu *WinSCP*, vyplňte polia s hostiteľským a používateľským menom a *session* uložte. Vytvorte takto dve *sessions*, jednu pre prihlásenie používateľa *jahoda*, druhú pre používateľa *cernica*. Potom sa pomocou nich prihláste na *server*; sledujte, že vás agent automaticky prihlási.
37. Z pracovnej plochy počítača s Windows 10 odstráňte vytvorené kľúče. Z programov *PuTTY* a *WinSCP* odstráňte vytvorené *sessions*.
38. Prihláste sa do grafického režimu *servera* ako *root* a odstráňte používateľov *jahoda* a *cernica.*