SIEŤOVÉ PROSTREDIE V LINUXE

NASTAVENIE STATICKÝCH CIEST DO VZDIALENÝCH SIETÍ, NÁSTROJE NA DIAGNOSTIKU SIETE

Teoretická časť

Počítače s OS Linux slúžiace ako servery majú väčšinou viac ako jednu sieťovú kartu a v smerovacej tabuľke majú často nastavené aj statické cesty do vzdialených sietí. Cesty sa dajú nastavovať len dočasne pomocou programu *ip route* alebo natrvalo úpravou príslušných konfiguračných súborov (v prípade, že systém beží v grafickom režime je najjednoduchšie na to použiť *NetworkManager* applet).

Na komunikáciu medzi počítačmi môžeme namiesto IP adries používať mená nastavené v súbore */etc/hosts.* Aj v prípade, že je v sieti nakonfigurovaná služba *DNS* sa hostiteľské mená najskôr vyhľadávajú v tomto súbore.

Jedným z dôležitých nástrojov na diagnostiku siete je program *netstat.* Použitím vhodných prepínačov zobrazuje smerovaciu tabuľku počítača, informácie o jeho sieťových adaptéroch, ale hlavne zobrazuje informácie o sieťových spojeniach.

Program *nmap* slúži na zisťovanie informácií o počítačoch v sieti, podporuje veľké množstvo skenov. Skenovať porty sa však môže považovať za prvú fázu útoku, a preto je potrebné narábať s ním opatrne.

Protokol *TELNET* nie je dostatočne bezpečný na to, aby sa používal na vzdialenú správu počítača v nedôveryhodnej sieti. Klientský program tohto protokolu sa ale často využíva na zisťovanie informácií o bežiacich službách na vzdialenom

počítači tak, že sa nepripojí na predvolený port serveru *TELNET*, ale na port inej služby, napr. port 25, ktorý patrí protokolu *SMTP.*

Sieťová prevádzka sa väčšinou analyzuje grafickým programom *Wireshark*, na Linuxovom serveri bez grafického režimu sa namiesto neho často používa *tcpdump.*

Pomôcky

Virtuálny stroj s CentOS 7 vytvorený vo *VMware vSphere*. Úloha je určená pre jedného žiaka.

Úlohy

1. V prostredí *VMware vSphere* vytvorte klon vášho virtuálneho stroja. Pôvodný stroj premenujte na *SERVER*, nový na *CLIENT*.
2. Zapnite obidva virtuálne stroje, prihláste sa do ich grafického režimu ako *root.*
3. Stroju *SERVER* zmeňte jeho hostiteľské meno na *server* príkazom **hostnamectl set-hostname server**. Aby sa zmena prejavila, zavrite a znovu otvorte terminál. Analogicky zmeňte hostiteľské meno aj stroju *CLIENT.*
4. Zistite, aké IP adresy majú stroje nastavené na rozhraní *ens192*.
5. Na *serveri* zeditujte súbor */etc/hosts.* Zakomentujte v ňom riadok týkajúci sa IPv6 a pridajte doňho nasledujúce riadky (IP adresy prispôsobte zisteným IP adresám):

   10.200.0.127 server

   10.200.0.144 client
6. Rovnako zmeňte súbor */etc/hosts* aj na stroji *CLIENT*.
7. Overte, že vám funguje sieťová komunikácia medzi virtuálnymi strojmi; zo *servera* pingnite počítač *client*. V príkaze najprv použite IP adresu stroja *CLIENT*, potom jeho hostiteľské meno.
8. Predstavte si situáciu, že *server* má ďalšiu sieťovú kartu s IP adresou zo siete z rozsahu 192.168.60.0/24 a že pre počítače z tejto siete je predvolenou bránou. Chcete, aby počítače zo siete 192.168.60.0/24 boli dostupné aj pre počítač *client*,

preto musíte na *clientovi* nastaviť statickú cestu do tejto siete. Postupujte podľa nasledujúcich pokynov:

a) Danú situáciu chcete len simulovať, preto na *serveri* netreba pridávať ďalšiu sieťovú kartu ani k nemu pripájať ďalšie počítače. Sieťovému rozhraniu v Linuxe môže byť priradených viac IP adries. Pridajte si na rozhranie *ens192* ďalšiu IP adresu príkazom **ip address add 192.168.60.10/24 broadcast + dev ens192**. Pomocou príkazu **ip address show dev ens192** si overte, že na tomto rozhraní máte nastavené dve rôzne IP adresy. Skúste použiť aj starý príkaz **ifconfig ens192**; tento príkaz vám vo výpise nezobrazí obidve IP adresy.

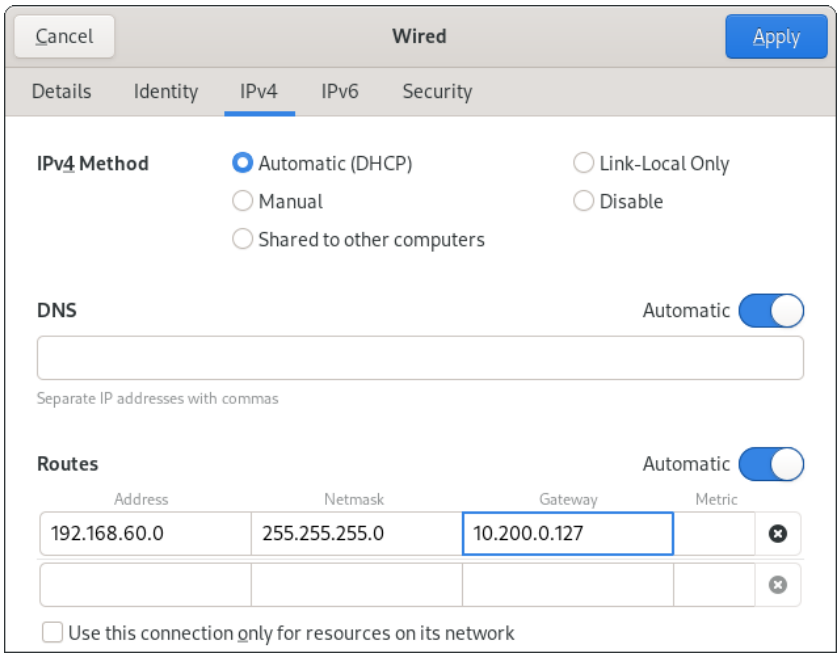
b) Z počítača *client* pingnite IP adresu 192.168.60.10. Ping nebude úspešný, lebo *client* nemá nastavenú cestu do siete 192.168.60.0/24 a keďže má nastavenú predvolenú bránu, posiela *ICMP* pakety týmto smerom.

c) Pridajte na *clientovi* statickú cestu do siete 192.168.60.0/24 príkazom **ip route add 192.168.60.0/24 via 10.200.0.127 dev ens192** (IP adresu 10.200.0.127 v príkaze nahraďte IP adresou vášho stroja *SERVER*).

d) Z *clienta* opäť pingnite IP adresu 192.168.60.10, ping bude tento krát úspešný.

e) Nastavená statická cesta na počítači *client* je len dočasná. Odstráňte ju príkazom **ip route del 192.168.60.0/24**.

f) Na *clientovi* nastavte statickú cestu do siete 192.168.60.0/24 pomocou *Network Manager* appletu; príslušné okno je zobrazené na Obrázku 1. Nezabudnite sieťovú kartu odpojiť a znovu pripojiť.



Obrázok 1 Pridanie statickej cesty do vzdialenej siete pomocou *NetworkManager* appletu.

g) Na *clientovi* si príkazom **ip route** overte, že v smerovacej tabuľke máte záznam pre sieť 192.168.60.0/24.

h) Funkčnosť overte pingom IP adresy 192.168.60.10 z počítača *client*.

i) Na *clientovi* pomocou *NetworkManager* appletu odstráňte cestu do siete 192.168.60.0/24, na *serveri* zmažte z rozhrania *ens192* IP adresu 192.168.60.10/24.

9. Na *serveri* vytvorte nového používateľa *slanina*, vytvorte mu aj heslo.
10. Na *serveri* si zobrazte jeho smerovaciu tabuľku príkazom **netstat -r**. Výstup porovnajte s výstupom príkazov **route** a **ip route**.
11. Na *serveri* si zobrazte sieťové štatistiky príkazom **netstat -s**.
12. Na *serveri* si zobrazte informácie o sieťových rozhraniach postupne príkazmi **netstat -i** a **netstat -ie**. Výstup druhého príkazu porovnajte s výstupom príkazu **ifconfig**.
13. Na serveri si príkazom **yum info net-tools** zobrazte informácie o balíčku *net-tools.* Program *netstat* s príslušnými prepínačmi poskytuje rovnaký výpis ako programy *route* a *ifconfig*, lebo sú súčasťami toho istého balíčka.
14. Na *serveri* spustite príkaz **netstat -a** a zobrazte si tak informácie o všetkých spojeniach. Ak je výpis dlhý použite príkaz **netstat -a | less**.

15. Na *serveri* spustite príkaz **netstat -at** a zobrazte si tak informácie o všetkých *TCP* spojeniach.
16. Na *serveri* spustite príkaz **netstat -atn** a porovnajte ho s predchádzajúcim výpisom. Pri *TCP* spojeniach, ktoré sú v stave *LISTEN* (čakajú na pripojenie) sú namiesto mien služieb čísla portov a namiesto hviezdičiek IP adresy. IP adresa 0.0.0.0 znamená, že služba načúva na všetkých rozhraniach, dvojbodky znamenajú to isté ale pre IP protokol verzie 6.
17. Na *serveri* spustite príkaz **netstat -atnp** a porovnajte ho s predchádzajúcim výpisom. Pribudol stĺpec obsahujúci meno načúvajúceho programu a jeho *PID*.
18. Na *serveri* spustite príkaz **netstat -ltnp** a porovnajte ho s predchádzajúcim výpisom. Výpis obsahuje iba *TCP* služby v stave *LISTEN.*
19. Na *serveri* spustite príkaz **netstat -tnp** a porovnajte ho s predchádzajúcimi dvomi výpismi. Výpis obsahuje iba *TCP* služby, ktoré nie sú v stave *LISTEN.*
20. Na *serveri* si príkazom **netstat -aunp** zobrazte informácie o všetkých *UDP* spojeniach.
21. Na *serveri* si príkazom **netstat -atunp** zobrazte informácie o všetkých *TCP* a *UDP* spojeniach.
22. Na *serveri* si príkazom **netstat -atnp | grep ssh** zobrazte informácie o spojeniach protokolu *SSH*. Z výpisu by malo byť jasné, že *SSH* server načúva na všetkých rozhraniach a akceptuje pripojenia protokolom IP verzie 4 aj 6.
23. Z *clienta* sa pripojte na *server* pomocou protokolu *SSH* s loginom *slanina.* Použite na to príkaz **ssh slanina@server**. Po úspešnom pripojení spustite na *serveri* opäť príkaz **netstat -atnp | grep ssh** a overte si, že okrem spojení v stave *LISTEN* obsahuje aj spojenie v stave *ESTABLISHED.* Z nadviazaného spojenia určte IP adresu *clienta* a zdrojový port, z ktorého sa k *SSH* serveru pripojil.
24. Príkaz **netstat -atnp** spustite aj na *clientovi* ale v termináli, v ktorom je pripojený na *server*. Prepínač *-n* môže používať iba *root*, a preto je v stĺpci *PID/Program name* iba pomlčka. Na *clientovi* ukončite *SSH* spojenie príkazom **exit**.
25. Príkazom **systemctl status firewalld.service** overte, či je na *serveri* zapnutý firewall, ak je, vypnite ho príkazom **systemctl stop firewalld.service**.

26. Na *clientovi* príkazom **yum install nmap telnet** nainštalujte port scanner *nmap* a klienta protokolu *TELNET.*
27. Na *clientovi* príkazom **nmap -sT server** zistite, ktoré *TCP* porty na *serveri* sú otvorené.
28. Na *clientovi* príkazom **nmap -sS server** zistite, ktoré *TCP* porty na *serveri* sú otvorené. Tento krát používate *stealth scan*, ktorý pošle iba *TCP* paket s príznakom *SYN*, čaká na *TCP* paket s príznakom *SYN/ACK* a spojenie už nedokončí.
29. Na *clientovi* príkazom **nmap -sX server** zistite, ktoré *TCP* porty na *serveri* sú otvorené. Tento krát používate *xmas scan*, ktorý posiela *TCP* paket s nastavenými príznakmi *FIN*, *URG* a *PUSH*. V niektorých prípadoch je tento druh skenu úspešnejší ako predchádzajúce.
30. Na *clientovi* príkazom **nmap -sU server** zistite, ktoré *UDP* porty na *serveri* sú otvorené. Je možné, že nedostanete žiadny výstup.
31. Na *clientovi* si zobrazte manuálovú stránku programu *nmap* a použite na skenovanie *servera* prvý spomínaný príklad, reprezentatívny sken **nmap -A -T4 server**.
32. Na *clientovi* ešte raz zistite otvorené porty ľubovoľným typom skenu. Pomocou klientskeho programu protokolu *TELNET* si zistite informácie o *SSH* serveri spustenom na počítači *server* príkazom **telnet server 22**, potom spojenie zrušte.
33. Na *serveri* nainštalujte príkazom **yum install httpd vsftpd** web sever *Apache* a *FTP* server *vsftpd.* Príkazmi **service httpd status** a **service vsftpd status** zistite, či sú tieto služby spustené. To že spustené nie sú si overte aj príkazom **netstat -ltpn**.
34. Na *serveri* zapnite obidve nainštalované služby príkazmi **service httpd start** a **service vsftpd start**. To, že služby naozaj bežia si overte príkazom **netstat -ltpn**.
35. Na *clientovi* spustite príkaz **nmap -sT server**, vo výpise by mali pribudnúť aj otvorené porty 80 a 21 patriace službám *http* a *ftp*.
36. Na *clientovi* spustite *Firefox*, ak v ňom máte nastavený *proxy* server, zrušte toto nastavenie. V okne *Firefoxu* zobrazte testovaciu stránku web servera *Apache* bežiaceho na *serveri*.

37. Na *clientovi* si príkazom **yum install ftp** nainštalujte *FTP* klienta.
38. Na *clientovi* sa z terminálu pripojte pomocou protokolu *FTP* na *server* príkazom **ftp server**, ako prihlasovacie meno použite *anonymous*, heslo môže byť ľubovoľné. Príkazom **dir** si zobrazte obsah priečinka, v ktorom sa nachádzate na *FTP* serveri.
39. Na *serveri* spustite príkaz **netstat -tpn**, z výpisu zistite, z akého zdrojového portu sa *client* pripojil na *FTP* server. Dátové *FTP* spojenie nevidíte, tiež nevidíte aktívne spojenie protokolom *HTTP.*
40. Na *clientovi* zavrite *firefox* a ukončite aj *FTP* spojenie.
41. Na *serveri* otvorte druhý terminál a spusťte v ňom príkaz **tcpdump -i ens192**.
42. Na *clientovi* si v okne *firefoxu* zobrazte webovú stránku *servera*.
43. Na *serveri* z výpisu získaného programom *tcpdump* zistite číslo zdrojového portu, z ktorého sa *client* pripojil na webový server počítača *server*.
44. Na *clientovi* sa z terminálu pripojte pomocou protokolu *FTP* na *server* príkazom **ftp server**, ako prihlasovacie meno použite *anonymous*, heslo môže byť ľubovoľné. Príkazom **dir** si zobrazte obsah priečinka, v ktorom sa nachádzate na *FTP* serveri. Presuňte sa po priečinka *pub* a vypíšte jeho obsah.
45. Z výpisu získaného programom *tcpdump* zistite číslo zdrojového portu, z ktorého sa *client* pripojil na *FTP* server počítača *server*. Tiež identifikujte, na akých portoch prebiehalo dátové *FTP* spojenie.
46. Na *clientovi* zavrite *firefox* a ukončite aj *FTP* spojenie.
47. Na *clientovi* zistite informácie o *FTP* serveri príkazom **telnet server 21**. Spojenie potom ukončite.
48. Z *clienta* zistite otvorené *TCP* porty na *serveri* v rozsahu 20-30 príkazom **nmap -sT -p 20-30 server**.
49. Z *clienta* príkazom **nmap -sT -p 20-23,25,80,443 server** zistite, ktoré zo zvolených *TCP* portov sú na *serveri* otvorené.
50. Na *serveri* zapnite firewall príkazom **systemctl start firewalld.service**. Z *clienta* príkazom **nmap -sT -p 20-23,25,80,443 server** zistite, ktoré zo zvolených *TCP* portov sú na *serveri* otvorené. Porovnajte ich z predchádzajúcim výpisom.
51. Príkazom **nmap -sT server** zistite, ktoré *TCP* porty sú na *serveri* otvorené.

52. Na *serveri* si príkazom **netstat -ltpn** overte, že služby *ftp* a *http* čakajú na pripojenie klientov. Pokúste sa z *clienta* pripojiť pomocou protokolov *HTTP* a *FTP* na *server*, nepodarí sa to lebo spojenie blokuje firewall.
53. Na *serveri* odstráňte používateľský účet *slanina.*