3 laboratorinis darbas

Debian Linux tinklo paslaugų tyrimas

Darbo tikslas: išbandyti Debian Linux elementariąsias tinklo paslaugas ir paruošti tarnybinę stotį tolesniems tinklo saugumo tyrimams.

**Darbo eiga:**

1. Patikrinkite kokios tinklo sąsajos yra virtualiame kompiuterye: *ifconfig –a*, kokie tinklo sąsajų pavadinimai? Kokie pasirenkami tinklo sąsajos parametrai: *ifconfig --help*.

Nustatykite tinklo adresą: *ifconfig eth0 192.168.10.1X netmask 255.255.255.0*

Komandos parametrai: *up* – aktyvuoja sąsają (jei nenurodyta įjungta pagal nutylėjimą),

*down* – išjungia sąsają,

*netmask <addr>* tinklo kaukė,

*broadcast [addr]* tinklo pačiajuostės užklausos adresas.

*hw <type> <addr>* aparatinių adresų nustatymas pavyzdžiui MAC.

Patikrinkite ar pavyko sukonfigūruoti tinklo sąsają.

1. Nustatykite tinklo vartus, arba maršrutą pagal nutylėjimą: *route add default gw 192.168.10.254*

*gw* raktas sako, kad po jo einantis IP adresas yra tarptinkliniai vartai į kuriuos turi būti siunčiami visi ne tam tinklui skirti paketai tolimesnei maršrutizacijai. Patikrinkite ar vartai nustatyti: *route –a*.

1. Aukščiau aprašytu būdu nustačius tinklo adresą, jis po kompiuterio perkrovimo neišliks. Perkraukite virtualų kompiuterį ir patikrinkite šį teiginį. Pagrindinius tinklo nustatymus reiktų nustatyti */etc/network/interfaces* faile. Čia galima nustatyti IP adresą, maršrutizavimo informaciją ir kt., apie galimybes galima sužinoti *man interfaces*. Naudosime statinę IP adresaciją, todėl naudodami *nano* */etc/network/interfaces* nustatykite tokią:

*iface eth0 inet static*

*address 192.168.10.1X*

*netmask 255.255.255.0*

*gateway 192.168.10.254*

 Tinklo sąsaja bus aktyvuota perkrovus kompiuterį, arba įvykdžius komandą *ifup eth0*.

1. Nustatykite kompiuterio vardą komanda *hostname kompiuterio\_vardas,* toks nustatymas perkrovus kompiuterį neišliks, todėl kompiuterio vardą įrašykite į failą */etc/hostname*, patikrinkite ar vardas pasikeitė*: hostname.*

Nustatykite vardų išspendimo tarnybines stotis, redaguodami */etc/resolv.conf*. Naudokite tekstų redaktorių vi, nano ar kt.:

*nameserver 193.219.146.19*

*nameserver 193.219.146.2*

Yra du būdai nustatyti vardų išsprendimo tarnybines stotis: rankiniu būdu redaguoti /etc/resolv.conf (*man resolv.conf*), arba naudoti *resolvconf* komandą. Jei naudojama resolvconf komanda galinti dinamiškai redaguoti vardų išsprendimo informaciją, */etc/resolv.conf* pakeičiamas simboline nuoroda į */etc/resolvconf/run/resolv.conf*. Jei naudojamas *resolvconf* rankiniu būdu redaguoti *resolv.conf* failo nereiktų, nes šis bus perrašytas, jei reikia įtraukti statinį įrašą, tai reikia padaryti */etc/network/interfaces* faile, pvz.: *dns-nameservers 12.34.56.78 12.34.56.79*

1. Nustatykite maršrutą į hipotetinį tinklą per kaimyninį kompiuterį *route add -net 172.18.X.0 netmask 255.255.255.0 gw 192.168.10.(1X-1)*, išbandykite jį *traceroute 172.18.X.ą*.

Raktas *–net* reiškia kad tai maršrutas į visą tinklą, o raktas *–host* reikštų, kad maršrutas skirtas konkrečiam tinklo mazgui.

1. Aprašykite reikalingas vidaus vardų sąsajas su IP adresais.

*/etc/hosts* faile galima statiškai užduoti tinklo mazgų vardus, papildykite šį failą kaimyninio kompiuterio IP adresu su vardu kaimynas: *192.168.10.****(1X-1)***  *kaimynas*

Išbandykite ar išsprendžia nustatytą vardą *ping kaimynas* .

1. Tinklo plokštė gali turėti kelis pilnaverčius tinklo adresus (alias). Nustatykite antrąjį adresą tinklo plokštei *ifconfig eth0:1 10.10.10.X/24*. Patikrinkite ar adresas nusistatė *ipconfig –a*. Išbandykite ar šis funkcionuoja siųsdami *ping* užklausas kaimyno kompiuterio antrąjam IP adresui.
2. Debian linux turi patogią ir efektyvią programinės įrangos valdymo priemonę Apt-get. Peržiūrėkite šaltinių sąrašą: *cat /etc/apt/sources.list* . Susipažinkite su apt-get raktais, *apt-get –help*, perskaitykite šio įrankio aprašymą: <http://www.ubuntu.lt/render/Articles;aid,39> . Atnaujinkite programų sąrašus *apt-get update* , instaliuokite tinklo skenerį nmap: *apt-get install nmap*, instaliavimo metu gali tekti atnaujinti kelias bibliotekas.
3. Susipažinkite su nmap galimybėmis *man nmap* ir skenuokite kaimyninį kompiuterį ***nmap -sS -O 192.168.10.(1X-1)* Išsiaiškinkite ką reiškia gautas atsakymas.**
4. **Instaliuokite tekstinę žiniatiklio naršyklę links, *apt-get install links* ir žiniatinklio paslaugą su duomenų baze ir kitais įrankiais kurie bus reikalingi tolimesniuose laboratoriniuose darbuose (ką reiškia naudojamas \):**

*apt-get install apache-ssl apache-common libapache-mod-php4 \*

*mysql-server mysql-common mysql-client php4-mysql \*

*libnet1 libnet1-dev libpcre3 libpcre3-dev autoconf automake1.9 \*

*libpcap0.8 libpcap0.8-dev libmysqlclient15-dev \*

*php4-gd php4-pear libphp-adodb vim gcc make \*

*php4-cli libtool libssl-dev gcc-4.1 g++*

1. **Peržiūrėkite apache konfigūracinį failą *cat /etc/apache-ssl/httpd.conf*. Iš kokių dalių jis susideda, kaip nustatoma kokius puslapius reikia atversti kreipiantis į žiniatinklio serverį? Šakninėje serverio dokumentų direktorijoje sukurkite žiniatinklio failą: *cd /var/www, echo “<html> kompiuterio vardas </html>” > index.php*. Išbandykite ar atidaromas jūsų žiniatinklio puslapis naudodamiesi realaus kompiuterio naršykle, atkreipkite dėmesį, kad nudojamas saugus žiniatinklo protokolas https.**
2. **Peržiūrėkite kompiuteryje vykstančius procesus *ps –aux*. Kokios komandos ps galimybės: *man ps*. Peržiūrėkite tik žiniatinklio procesą *ps –aux | grep apache*. Pažiūrėkite kokie procesai daugiausia naudoja kompiuterio resursus *top*, iš atsidarosio lango išeikite naudodami *q*. Išsiaiškinkite ką rodo top komanda: *man top*.**
3. **Skenuokite kaimyno kompiuterio atvirus prievadus, kaip pasikeitė situacija nuo pirmojo skenevimo?**

**Atakaitos turinys:**

1. Darbo tikslas
2. Tumpas atlikto darbo aprašymas ir atsakymai į klausimus
3. Duotos komandos aprašymas
4. Išvados