

Vilniaus Gedimino technikos universitetas

Elektronikos fakultetas

Kompiuterijos ir ryšių technologijų katedra

Magistro tiriamasis darbas 2

Modulis ELKRM17203

Atliko: TETfm-20 grupės magistrantas

Saulius Krasuckas

Tikrino: doc. dr. Darius Guršnys

Darbo Tikslas

- ✓ Išbandyti Ubuntu Linux elementariąsias tinklo paslaugas.
- ✓ Paruošti tarnybinę stotį tolesniems tinklo saugumo tyrimams.

Trumpas atlikto darbo aprašymas

0. Infrastruktūros paruošimas

1. Ruošimo eiga

Laboratorinei infrastruktūrai paruošti pasirinkau VirtualBox virtualizavimo įrankį (hipervizorių). Host kompiuteris bus senokas HP EliteBook 8460p laptopas:

- CPU: i5-2520M @ 2.50GHz
- RAM: 3692 MiB (prieinami OS)
- Host OS bus CentOS 7.9.2009
- Guest OS bus Ubuntu 20.04.2 LTS

Pradinę VM konfigūraciją sukuriu savo Bash skripto

(<https://github.com/VGTU-ELF/TETfm-20/blob/48a7e7c30bc23b756cff9a1e53cdb0ce4e4c921f/Semestras-2/1-Informacijos-ir-sistem%C5%B3-apsauga/laboratoriniai-darbai/Saulius-Krasuckas/OLD-infra.sh#L54>) pagalba.

Jis parsisiunčia oficialių .vdi failą iš <https://sourceforge.net/projects/osboxes/files>, sukuria naują VM ir prijungia nurodytą diską.

Tuomet per Bootloader menu įrašau Linux branduolio argumentų eilutėje, kad jis atidarytų konsolę per ttyS0, virtualų Serial/UART įrenginį:

```
linux          <...> console=ttyS0,115200n8
```

Ir galiausiai jungiuosi į *Guest* konsolę iš *Host* kompiuterio per telnet :

```
telnet 127.0.0.1 23001
```

2. NIC konfigūravimas Host pusėje (NAT + Host-only)

Pagal nutylėjimą Virtualbox VM gauna NAT tipo virtualią tinklo sąsają: NIC 1: ... Attachment: NAT ...

VirtualBox dokumentacija (<https://www.virtualbox.org/manual/ch06.html#networkingmodes>) teigia:

“ The following table provides an overview of the most important networking modes.

Table 6.1. Overview of Networking Modes

Mode	VM → Host	VM ← Host	VM1 ↔ VM2	VM → Net/LAN	VM ← Net/LAN
Host-only	+	+	+	–	–
Internal	–	–	+	–	–
Bridged	+	+	+	+	+
NAT	+	Port forward	–	+	Port forward
NATservice	+	Port forward	+	+	Port forward

The following sections describe the available network modes in more detail.

Panašu, kad su ja iš *Host OS* aš *Guest OS* nepasieksiu paprastai ir saugiai.

Todėl VM konfigūracijoje pridedu papildomą tinklo interfeisą

(<https://github.com/VGTU-ELF/TETfm-20/blob/48a7e7c30bc23b756cff9a1e53cdb0ce4e4c921f/Semestras-2/1-Informacijos-ir-sistem%C5%B3-apsauga/laboratoriniai-darbai/Saulius-Krasuckas/OLD-infra.sh#L89>)

, bet jau Host-only tipo:

```
if [ -z "$HOSTONLY_IF" ]; then
    VBoxManage hostonlyif create
    VBoxManage list hostonlyifs | awk '/^Name/ {NEWEST_NIC=$2} END {print NEWEST_NIC}'
    | read HOSTONLY_IF
fi
VBoxManage hostonlyif ipconfig ${HOSTONLY_IF} --ip ${OAM_IP}
VBoxManage list hostonlyifs | awk '/'${HOSTONLY_IF}'/ {START=1} START && $0=="'
{START=0} START {print}'
```

Po šito VM gauna du interfeisus:

```
$ VBoxManage showvminfo VGTU-2021-IiSA-saukrs-LDVM1 | grep NIC.[12]
NIC 1:                                MAC: 080027EB204C, Attachment: NAT, Cable connected: on,
Trace: off (file: none), Type: 82540EM, Reported speed: 0 Mbps, Boot priority: 0,
Promisc Policy: deny, Bandwidth group: none
NIC 1 Settings:  MTU: 0, Socket (send: 64, receive: 64), TCP Window (send:64, receive:
64)
NIC 2:                                MAC: 080027B6C487, Attachment: Host-only Interface
'vboxnet0', Cable connected: on, Trace: off (file: none), Type: 82540EM, Reported
speed: 0 Mbps, Boot priority: 0, Promisc Policy: deny, Bandwidth group: none
```

1. Tinklo sąsajos

Tikrinu vardus.

Peržiūriu pasirenkamis sąsajų parametrus.

Peržiūriu sąsajų parametrus.

Nustatau tinklo adresą.

2. Tinklo vartai

Nustatau vartus.

Patikrinu; vartai nustatyti.

3. Statinės tinklo konfigūracijos įrašymas

Tinklo adresai prieš perkrovimą.

Po perkrovimo.

Surašau statinę konfigūraciją naudodamas `echo ... >> ...`.

Aktyvuoju tinklo konfigūraciją iš failo.

4. Kompiuterio vardas

Nustatau kompiuterio vardą.

Įrašau kompiuterio vardą į konfigūracinį failą.

Patikrinu — vardas pasikeitė.

Konfigūruoju vardų išsprendimo tarnybines stotis.

5. Standartiniai maršrutai

Nustatau maršrutą per kaimyną.

Išbandau jį.

6. Vidaus vardai.

Aprašau kaimyninį VM.

Vardo išsprendimas.

7. Keli tinklo adresai

Nustatau antrąjį tinklo adresą.

Patikrinu, nusistatė abiejuose kompiuteriuose.

Išbandau antrus IP adresus, veikia.

8. Programinės įrangos valdymas

Šaltinių sąrašas.

apt-get raktai.

Skaitau apt-get aprašymą. Puslapis

(<https://web.archive.org/web/20090321133431/https://ubuntu.lt/render/Articles;aid,39>) aprašo šias subkomandas:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get dist-upgrade
sudo apt-get install ...
sudo apt-get remove ...
sudo apt-get remove --purge ...
```

Atnaujinu programų sąrašus.

Instaliuoju nmap.

9. Įrankis nmap

Skenuoju kaimyną.

10. Žiniatinklio paslauga ir klientas

Instaliuoju links.

Instaliuoju žiniatinklio paslaugą, duomenų bazę ir kitus įrankius.

11. Žiniatinklio konfigūravimas

Peržiūriu konfigūracinį failą.

12. Vykdomi procesai

Peržiūriu kompiuteryje vykdomus procesus.

Tikrinimo metu veikė 195 procesai.

Peržvelgiu komandos ps galimybes.

Daug skaitymo, apibendrinu iškeliau rezultatuose.

Procesų peržiūra su top .

13. Prievadų skenavimas

Nuskenuoju kaimyno prievadus.

Sunkumai ir atsakymai į klausimus

0. Guest OS paruošimas

- Programinės įrangos diegimui reikėjo atnaujinti jos duomenų bazę:

```
$ sudo apt update
```

- Kitaip neišsidiegė bent jau openssh-server :

```
osboxes@osboxes:~$ sudo apt install openssh-server
sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 58 not upgraded.
Need to get 688 kB of archives.
After this operation, 6,010 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ncurses-term all 6.2-0ubuntu2 [249 kB]
Err:2 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-sftp-server amd64 1:8.2p1-4ubuntu0.1 404 Not Found [IP: 91.189.91.39 80]
Err:3 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-server amd64 1:8.2p1-4ubuntu0.1 404 Not Found [IP: 91.189.91.39 80]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ssh-import-id all 5.10-0ubuntu1 [10.0 kB]
Fetched 259 kB in 1s (204 kB/s)
E: Failed to fetch
http://us.archive.ubuntu.com/ubuntu/pool/main/o/openssh/openssh-sftp-server_8.2p1-4ubuntu0.1_amd64.deb 404 Not Found [IP: 91.189.91.39 80]
E: Failed to fetch
http://us.archive.ubuntu.com/ubuntu/pool/main/o/openssh/openssh-server_8.2p1-4ubuntu0.1_amd64.deb 404 Not Found [IP: 91.189.91.39 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
```

- Atnaujinu programinės įrangos duomenų bazę:

```

osboxes@osboxes:~$ sudo apt update
sudo apt update
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Get:5 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [254
kB]
...
Get:53 http://us.archive.ubuntu.com/ubuntu focal-backports/universe amd64
Packages [4,032 B]
Get:54 http://us.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11
Metadata [1,780 B]
Get:55 http://us.archive.ubuntu.com/ubuntu focal-backports/universe amd64 c-n-f
Metadata [224 B]
Fetched 8,419 kB in 14s (588 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
262 packages can be upgraded. Run 'apt list --upgradable' to see them.

```

- SSH serverio instaliavimas

- Ieškau programinės įrangos paketo:

```

osboxes@osboxes:~$ apt search ssh
Sorting...
Full Text Search...
4pane/focal 6.0-1build1 amd64
  four-pane detailed-list file manager

agent-transfer/focal 0.41-1ubuntu1 amd64
  copy a secret key from GnuPG's gpg-agent to OpenSSH's ssh-agent
...
zsnapped-rcmd/focal,focal 0.8.11h-1ubuntu2 all
  Remote sshd command checker for ZFS Snapshot Daemon

zssh/focal 1.5c.debian.1-7build2 amd64
  interactive file transfers over ssh

```

- Diegiu OpenSSH serverį:


```

osboxes@osboxes:~$ sudo apt install openssh-server
sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 261 not upgraded.
Need to get 1,100 kB/1,359 kB of archives.
After this operation, 6,010 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-client
amd64 1:8.2p1-4ubuntu0.2 [671 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-sftp-
server amd64 1:8.2p1-4ubuntu0.2 [51.5 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-server
amd64 1:8.2p1-4ubuntu0.2 [377 kB]
Fetched 1,100 kB in 3s (350 kB/s)
Preconfiguring packages ...
(Reading database ... 145074 files and directories currently installed.)
...
Setting up openssh-sftp-server (1:8.2p1-4ubuntu0.2) ...
Setting up openssh-server (1:8.2p1-4ubuntu0.2) ...

Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
3072 SHA256:q7is6Llfa0sm7vxlzTgNUUInZN0uRZ5EoRe1VPNEzNg root@osboxes (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:YG+pWX5P0RlrH0zmB0cPAxGQ0w5cpiE8HMISFrQ6xxA root@osboxes (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:SSYtj9I+qp5yLhXGL3AdbncN3l0nSbJ1C4cqQ2UzTkI root@osboxes (ED25519)

Progress: [ 90%] [#####.....]
Created symlink /etc/systemd/system/ssh.service →
/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service →
/lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
Processing triggers for systemd (245.4-4ubuntu3.4) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for ufw (0.36-6) ...

```

- Galbūt šitą žingsnį (aprašytą Moodle) verta apjungti su 2lab*.docx aprašytais žingsniais į bendrą tekstą?

1. Tinklo sąsajos

- Trūko ifconfig komandos, teko susiinstaliuoti paketą net-tools:

```
osboxes@osboxes:~$ ifconfig -a
```

Command 'ifconfig' not found, but can be installed with:

```
sudo apt install net-tools
```

```
osboxes@osboxes:~$ sudo apt install net-tools
```

```
[sudo] password for osboxes:
```

```
...
```

```
The following NEW packages will be installed:
```

```
net-tools
```

```
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
```

```
...
```

```
Progress: [ 80%] [#####.....]
```

- LD apraše nenurodyta, su kuriuo naudotoju (neprivilegiuotu ar root) reiktų leisti komandas. Dėl to leidau iš neprivilegiuoto, ir man gana daug sykių pritrūkavo teisių, prieš komandą tekdavo rašyti sudo .
- Tinklo sąsajų (interfeisų) pavadinimai yra enp0s3, enp0s8, lo.
- Pasirenkami sąsajų parametrai yra:

Usage:

```
ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
[add <address>[/<prefixlen>]]
[del <address>[/<prefixlen>]]
[[-]broadcast [<address>]] [[-]pointopoint [<address>]]
[netmask <address>] [dstaddr <address>] [tunnel <address>]
[outfill <NN>] [keepalive <NN>]
[hw <HW> <address>] [mtu <NN>]
[[-]trailers] [[-]arp] [[-]allmulti]
[multicast] [[-]promisc]
[mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
[txqueuelen <NN>]
[[-]dynamic]
[up|down] ...
```

- Patikrinu — tinklo adresas tikrai nustatytas:

```
osboxes@osboxes:~$ ifconfig enp0s8
```

```
ifconfig enp0s8
```

```
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.14 netmask 255.255.255.0 broadcast 192.168.10.255
    ether 08:00:27:b2:e7:9d txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 308 bytes 47526 (47.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Trūko dar vieno paketo: ifupdown

```
root@osboxes:~# ifup enp0s8
```

Command 'ifup' not found, but can be installed with:

```
apt install ifupdown          # version 0.8.35ubuntu1, or
apt install netscript-2.4     # version 5.5.3
```

```
root@osboxes:~# apt install ifupdown
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  rdnssd
The following NEW packages will be installed:
  ifupdown
0 upgraded, 1 newly installed, 0 to remove and 261 not upgraded.
Need to get 60.5 kB of archives.
After this operation, 234 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 ifupdown amd64
0.8.35ubuntu1 [60.5 kB]
Progress: [ 80%] [#####.....]
Fetched 60.5 kB in 1s (84.4 kB/s)
Selecting previously unselected package ifupdown.
Processing triggers for man-db (2.9.1-1) ...online.target.wants/networking.service →
/lib/systemd/system/networking.service.
```

2. Tinklo vartai

- Komanda `route -a` aprašyme netiksli. Reikėjo `route -n`:

```
osboxes@osboxes:~$ route -a
route -a
route: invalid option -- 'a'
Usage: route [-nNvee] [-FC] [<AF>]          List kernel routing tables
        route [-v] [-FC] {add|del|flush} ... Modify routing table for AF.

        route {-h|--help} [<AF>]            Detailed usage syntax for specified AF.
        route {-V|--version}                Display version/author and exit.

        -v, --verbose                        be verbose
        -n, --numeric                        don't resolve names
        -e, --extend                        display other/more information
        -F, --fib                            display Forwarding Information Base (default)
        -C, --cache                         display routing cache instead of FIB

...
```

3. Statinės tinklo konfigūracijos įrašymas

- Tekstų redaktorius `nano` nesivaldo per VirtualBox *Serial-over-Telnet* terminalinį prisijungimą:

```
osboxes@osboxes:~$ nano /etc/network/interfaces
(B[ Directory '/etc/network' is not writable ](B GNU nano 4.8
/etc/network/interfaces
(B^G(B^O(B^W(B^K(B^J(B^C(B^X(B^R(B^\(B^U(B^T(B^_(B Go To Line[2A[20A: ^X
^C^X^Z`^[^[^]^C^C^C
```

- Tekstų redaktorius `vi` pagal nutylėjimą net per SSH man veikia nekorektiškai:
 - Jei atsidarau failą, rodo tvarkingai:

```
root@osboxes:~# vi /etc/network/interfaces
face enp0s8 inet static
address 192.168.10.14
netmask 255.255.255.0
gateway 192.168.10.254
auto enp0s8
~
~
~
```

- Bet jei paspaudžiu `<Shift-O>` (*Open new line*), tekstas susigadina:

```
[>4;menp0s8 inet static

address 192.168.10.14
netmask 255.255.255.0
gateway 192.168.10.254
auto enp0s8
~
~
```

- Teko surašyti statinę konfigūraciją iš CLI:

```
osboxes@osboxes:~$ sudo -i
root@osboxes:~#
root@osboxes:~# echo 'iface enp0s8 inet static' >> /etc/network/interfaces
root@osboxes:~# echo 'address 192.168.10.14' >> /etc/network/interfaces
root@osboxes:~# echo 'netmask 255.255.255.0' >> /etc/network/interfaces
root@osboxes:~# echo 'gateway 192.168.10.254' >> /etc/network/interfaces
root@osboxes:~#
root@osboxes:~# cat /etc/network/interfaces
iface enp0s8 inet static
address 192.168.10.14
netmask 255.255.255.0
gateway 192.168.10.254
```

- Po perkrovimo tinklas vis tiek nesusikonfigūruoja:

```
osboxes@osboxes:~$ ifconfig enp0s8
enp0s8: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 08:00:27:b2:e7:9d txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Papildau konfigūraciją auto eilute:

```
root@osboxes:~# cat /etc/network/interfaces
auto enp0s8
```

```
iface enp0s8 inet static
address 192.168.10.14
netmask 255.255.255.0
gateway 192.168.10.254
```

- Po perkrovimo tinklas jau susikonfigūruoja automatiškai.
- Galbūt reikėtų šitą patikslinti LD apraše?

4. Kompiuterio vardas

- Komandinio apvalkalo eilutėje rodomas kompiuterio vardas nepasikeičia savaime. Tam naudotojui reikia persijungti iš naujo:

```
osboxes@osboxes:~$
osboxes@osboxes:~$ su - osboxes
Password:
osboxes@ldvm1:~$
```

- Pagal aprašą sukonfigūravus vardų išsprendimą, jis nustojo veikti:

```
osboxes@ldvm1:~$ ping www.google.lt
ping: www.google.lt: Temporary failure in name resolution
```

- Pastebėjau, kad srautas nenukeliauja nei vienu žingsniu iš mašinos:

```
osboxes@ldvm1:~$ ping 193.219.146.19
PING 193.219.146.19 (193.219.146.19) 56(84) bytes of data.
From 192.168.10.14 icmp_seq=1 Destination Host Unreachable
From 192.168.10.14 icmp_seq=2 Destination Host Unreachable
From 192.168.10.14 icmp_seq=3 Destination Host Unreachable
^C
--- 193.219.146.19 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4095ms
```

- Įtariau, kad tai įvyko dėl neveikiančiai sukonfigūruotų papildomų tinklo vartų — jie perima išorei skirtą tinklo srauto nukreipimą ir toliau niekur nenukreipia:

```
osboxes@ldvm1:~$ route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
0.0.0.0          192.168.10.254  0.0.0.0          UG      0      0      0 enp0s8
0.0.0.0          10.0.2.2        0.0.0.0          UG      20100  0      0 enp0s3
10.0.2.0         0.0.0.0         255.255.255.0    U       100    0      0 enp0s3
169.254.0.0      0.0.0.0         255.255.0.0      U       1000   0      0 enp0s8
192.168.10.0     0.0.0.0         255.255.255.0    U       0      0      0 enp0s8
```

- Veikimui atstatyti iš konfigūracijos pašalinau niekur nevedančius tinklo vartus:

```
osboxes@ldvm1:~$ sudo route delete default gw 192.168.10.254
sudo: unable to resolve host ldvm1: Temporary failure in name resolution
[sudo] password for osboxes:
osboxes@ldvm1:~$
```

- Tačiau duotos VU vardų išsprendimo tarnybinės stotys vis tiek lieka nepasiekiamios

```
osboxes@ldvm1:~$ ping 193.219.146.19
sboxes@ldvm1:~$ cat /etc/resolv.conf
nameserver 193.219.146.19
nameserver 193.219.146.2

PING 193.219.146.19 (193.219.146.19) 56(84) bytes of data.
From 193.219.94.140 icmp_seq=1 Destination Host Unreachable
^C

osboxes@ldvm1:~$ ping 193.219.146.2
PING 193.219.146.2 (193.219.146.2) 56(84) bytes of data.
From 193.219.94.140 icmp_seq=1 Destination Host Unreachable
From 193.219.94.140 icmp_seq=3 Destination Host Unreachable
^C
```

- Prisiminiau, kad jos neveikia jau keletą metų.
- Google susiradau
(https://www.litnet.lt/images/projektai/Sensorių_pradines_konfiguracijos_instrukcijos.pdf)
atnaujintas VU vardų išsprendimo tarnybinės stotis:

```
$ PDF=https://t.co/anBJLWY7f6
$ curl -L $PDF | pdftotext - - | grep -i DNS
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100  135k  100  135k    0     0   243k      0 --:--:-- --:--:-- --:--:--  243k
dns1=193.219.80.11
dns2=193.219.80.2
## DNS adresai
```

```
osboxes@ldvm1:~$ ping 193.219.80.11
PING 193.219.80.11 (193.219.80.11) 56(84) bytes of data.
64 bytes from 193.219.80.11: icmp_seq=2 ttl=63 time=94.8 ms
64 bytes from 193.219.80.11: icmp_seq=3 ttl=63 time=38.8 ms
^C
```

```
osboxes@ldvm1:~$ ping 193.219.80.2
PING 193.219.80.2 (193.219.80.2) 56(84) bytes of data.
64 bytes from 193.219.80.2: icmp_seq=1 ttl=63 time=38.8 ms
64 bytes from 193.219.80.2: icmp_seq=2 ttl=63 time=35.5 ms
^C
```

- Pagaliau radom pasiekiamas tarnybines stotis.
- Perkonfigūruoju jas į veikiančias:

```
osboxes@ldvm1:~$ sudo nano /etc/resolv.conf
sudo: unable to resolve host ldvm1: Temporary failure in name resolution
[sudo] password for osboxes:

osboxes@ldvm1:~$ cat /etc/resolv.conf
nameserver 193.219.80.11
nameserver 193.219.80.2
```

- Nėra komandos traceroute:

```
osboxes@ldvm1:~$ traceroute
```

Command 'traceroute' not found, but can be installed with:

```
sudo apt install inetutils-traceroute # version 2:1.9.4-11, or
sudo apt install traceroute           # version 1:2.1.0-2
```

- Teko įsidiegti:

```
osboxes@ldvm1:~$ sudo apt install traceroute
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  traceroute
0 upgraded, 1 newly installed, 0 to remove and 261 not upgraded.
...
update-alternatives: using /usr/sbin/tcptraceroute.db to provide
/usr/sbin/tcptraceroute (tcptraceroute) in auto mode
Processing triggers for man-db (2.9.1-1) ...
```

5. Standartiniai maršrutai

Veikia pagal aprašą, sunkumų neiškilo. Klausimai neužduoti.

6. Vidaus vardai:

Veikia pagal aprašą, sunkumų neiškilo. Klausimai neužduoti.

7. Keli tinklo adresai

Veikia pagal aprašą, sunkumų neiškilo. Klausimai neužduoti.

8. Programinės įrangos valdymas

- Deja, nuoroda <http://ubuntu.lt/render/Articles;aid,39> neveikia.
 - Teko susirasti kopiją Web-archyve:
<https://web.archive.org/web/20090321133431/https://ubuntu.lt/render/Articles;aid,39>

9. Įrankis nmap

- Gautas atsakymas reiškia:
 - buvo nuskenuoti 999 TCP transportinio protokolo prievadai;
 - kaimyniniame kompiuteryje rastas tik vienas atviras prievadas;
 - ten veikia tinklo paslauga SSH;
 - kompiuterio MAC adresas priklauso "Oracle VirtualBox" gamintojui.

10. Žiniatinklio paslauga ir klientas

- Deja, apraše duota diegimo komanda neveikia:


```

osboxes@ldvm1:~$ sudo apt-get install apache-ssl apache-common libapache-mod-php4 \
> mysql-server mysql-common mysql-client php4-mysql \
> libnet1 libnet1-dev libpcrc3 libpcrc3-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++
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package apache-ssl is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source

E: Package 'apache-ssl' has no installation candidate
E: Unable to locate package apache-common
E: Unable to locate package libapache-mod-php4
E: Unable to locate package php4-mysql
E: Unable to locate package automake1.9
E: Couldn't find any package by glob 'automake1.9'
E: Couldn't find any package by regex 'automake1.9'
E: Unable to locate package libmysqlclient15-dev
E: Unable to locate package php4-gd
E: Unable to locate package php4-pear
E: Unable to locate package php4-cli
E: Unable to locate package gcc-4.1
E: Couldn't find any package by glob 'gcc-4.1'
E: Couldn't find any package by regex 'gcc-4.1'

```

- Kadangi nežinia, kokios tiksliai naujos development įrankių versijos tiks, juos išimu iš sąrašo:
 - automake
 - gcc
- Juos įdiegsiu tada, kai jų prireiks.
- O likusių įrankių pavadinimus parenku su `apt search ...`:
 - apache2
 - libapache2-mod-php7.4
 - mysql-server
 - php7.4-mysql
 - default-libmysqlclient-dev
 - php7.4-gd
 - php-pear
 - php-cli

- Įdiegiu:

```
osboxes@ldvm1:~$ sudo apt-get install apache2 libapache2-mod-php7.4 \
mysql-server php7.4-mysql default-libmysqlclient-dev php7.4-gd \
php-pear php-cli
```

- Instaliavimo komandoje naudojamas \ simbolis reiškia, kad tolimesnis komandos tekstas nukeliamas į kitą eilutę.

11. Žiniatinklio konfigūravimas

- Peržiūrėti konfigūracinio failo nepavyksta dėl stipriai naujesnės Apache versijos:

```
osboxes@ldvm1:~$ cat /etc/apache-ssl/httpd.conf
cat: /etc/apache-ssl/httpd.conf: No such file or directory
```

- Sprendimas — paieškoti panašių failų naujuose paketuose:

```
osboxes@ldvm1:~$ dpkg --search /etc/apache2  
apache2, libapache2-mod-php7.4: /etc/apache2
```

```
osboxes@ldvm1:~$ dpkg --getfiles apache2 | grep /\.conf  
/etc/apache2/apache2.conf  
/etc/apache2/conf-available/charset.conf  
/etc/apache2/conf-available/localized-error-pages.conf  
/etc/apache2/conf-available/other-vhosts-access-log.conf  
/etc/apache2/conf-available/security.conf  
/etc/apache2/conf-available/serve-cgi-bin.conf  
/etc/apache2/mods-available/actions.conf  
/etc/apache2/mods-available/alias.conf  
/etc/apache2/mods-available/autoindex.conf  
/etc/apache2/mods-available/cache_disk.conf  
/etc/apache2/mods-available/cgid.conf  
/etc/apache2/mods-available/dav_fs.conf  
/etc/apache2/mods-available/deflate.conf  
/etc/apache2/mods-available/dir.conf  
/etc/apache2/mods-available/http2.conf  
/etc/apache2/mods-available/info.conf  
/etc/apache2/mods-available/ldap.conf  
/etc/apache2/mods-available/mime.conf  
/etc/apache2/mods-available/mime_magic.conf  
/etc/apache2/mods-available/mpm_event.conf  
/etc/apache2/mods-available/mpm_prefork.conf  
/etc/apache2/mods-available/mpm_worker.conf  
/etc/apache2/mods-available/negotiation.conf  
/etc/apache2/mods-available/proxy.conf  
/etc/apache2/mods-available/proxy_balancer.conf  
/etc/apache2/mods-available/proxy_ftp.conf  
/etc/apache2/mods-available/proxy_html.conf  
/etc/apache2/mods-available/reqtimeout.conf  
/etc/apache2/mods-available/setenvif.conf  
/etc/apache2/mods-available/ssl.conf  
/etc/apache2/mods-available/status.conf  
/etc/apache2/mods-available/userdir.conf  
/etc/apache2/ports.conf  
/etc/apache2/sites-available/000-default.conf  
/etc/apache2/sites-available/default-ssl.conf
```

- Pasirenku /etc/apache2/apache2.conf ir filtruoja jį taip:

```

osboxes@ldvm1:~$ cat /etc/apache2/apache2.conf | grep -C1 ^Include
# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

# Include list of ports to listen on
Include ports.conf

--
# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

```

- Konfigūracija susideda iš:
 - trijų <Directory ...> dalių:
 - <Directory />
 - <Directory /usr/share>
 - <Directory /var/www/>
 - vienos <FilesMatch ...> dalies, aprašančios .ht failus:
 - <FilesMatch "^\.ht">
 - daugelio .conf failų, įtraukiamų direktyva Include arba IncludeOptional:

```

/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf

```

- Deja, puslapis per https dar neatsidaro:

```
osboxes@ldvm1:/var/www$ links https://ldvm1
```

```
+
|
|
|
|
|
|
|
|
|
|
+----- Error -----
|
| Error loading https://ldvm1/:
|
| Connection refused
|
| [ Cancel ]
+-----
```

- Patikrinu Apache prievadus, trūksta 443/TCP (https):

```
osboxes@ldvm1:/var/www$ sudo netstat -4ltn | grep apache
tcp6      0      0 :::80          :::*           LISTEN
11795/apache2
```

- Įjungiu pagal suguglintą dokumentaciją:

```
osboxes@ldvm1:/var/www$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create
self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2

osboxes@ldvm1:/var/www$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'apache2.service'.
Authenticating as: osboxes.org,,, (osboxes)
Password:
==== AUTHENTICATION COMPLETE ====
```

- Patikrinu Apache prievadus dar sykį, 443/TCP jau veikia:

```
osboxes@ldvm1:/var/www$ sudo netstat -4lnp | grep apache
tcp6      0      0 :::80          :::*           LISTEN
17145/apache2
tcp6      0      0 :::443         :::*           LISTEN
17145/apache2
```

- Patikrinu su vietine naršykle, https dar neveikia:

```

+----- Error -----
|
| Error loading
|
|
| SSL error
|
|
| [ Cancel ]
|
+-----
```

- Patikrinu su CLI įrankiu wget :

```
osboxes@ldvm1:/etc/apache2/sites-enabled$ wget -S https://ldvm1
--2021-06-30 06:26:28-- https://ldvm1/
Resolving ldvm1 (ldvm1)... 192.168.10.14
Connecting to ldvm1 (ldvm1)|192.168.10.14|:443... connected.
OpenSSL: error:1408F10B:SSL routines:ssl3_get_record:wrong version number
Unable to establish SSL connection.
```

- Pagal klaidą suguglinu patarimą tikrinti 443/TCP prievadą be SSL. Be SSL veikia:

```

osboxes@ldvm1:~$ wget -S http://ldvm1:443
--2021-06-30 06:27:13-- http://ldvm1:443/
Resolving ldvm1 (ldvm1)... 192.168.10.14
Connecting to ldvm1 (ldvm1)|192.168.10.14|:443... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 200 OK
  Date: Wed, 30 Jun 2021 10:27:13 GMT
  Server: Apache/2.4.41 (Ubuntu)
  Last-Modified: Wed, 30 Jun 2021 09:08:33 GMT
  ETag: "2aa6-5c5f811269876"
  Accept-Ranges: bytes
  Content-Length: 10918
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html
Length: 10918 (11K) [text/html]
Saving to: 'index.html'

index.html                                100%
[=====>] 10.66K  --.-KB/s
in 0s

2021-06-30 06:27:13 (24.0 MB/s) - 'index.html' saved [10918/10918]

```

- Panašu, kad trūksta SSL-konfigūracinio failo. Tikrinu:

```

osboxes@ldvm1:/var/www$ ll /etc/apache2/sites-available/
total 20
drwxr-xr-x 2 root root 4096 Jun 30 05:08 ./
drwxr-xr-x 8 root root 4096 Jun 30 05:08 ../
-rw-r--r-- 1 root root 1332 Apr 13 2020 000-default.conf
-rw-r--r-- 1 root root 6338 Apr 13 2020 default-ssl.conf

osboxes@ldvm1:/var/www$ ll /etc/apache2/sites-enabled/
total 8
drwxr-xr-x 2 root root 4096 Jun 30 05:08 ./
drwxr-xr-x 8 root root 4096 Jun 30 05:08 ../
lrwxrwxrwx 1 root root 35 Jun 30 05:08 000-default.conf -> ../sites-
available/000-default.conf

```

- Trūksta, įtraukiu konfigūracinį failą rankomis:

```
osboxes@ldvm1:/etc/apache2/sites-enabled$ sudo ln -s ../sites-available/default-ssl.conf
```

```
osboxes@ldvm1:/etc/apache2/sites-enabled$ ll
total 8
drwxr-xr-x 2 root root 4096 Jun 30 06:21 ./
drwxr-xr-x 8 root root 4096 Jun 30 05:08 ../
lrwxrwxrwx 1 root root 35 Jun 30 05:08 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root 35 Jun 30 06:21 default-ssl.conf -> ../sites-available/default-ssl.conf
```

```
osboxes@ldvm1:~$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'apache2.service'.
Authenticating as: osboxes.org,,, (osboxes)
Password:
==== AUTHENTICATION COMPLETE ====
```

- Patikrinu; SSL lyg veikia, bet pyksta dėl SSL sertifikato:

```
osboxes@ldvm1:~$ wget -S https://ldvm1
--2021-06-30 06:31:39-- https://ldvm1/
Resolving ldvm1 (ldvm1)... 192.168.10.14
Connecting to ldvm1 (ldvm1)|192.168.10.14|:443... connected.
ERROR: cannot verify ldvm1's certificate, issued by 'CN=ubuntu':
  Self-signed certificate encountered.
ERROR: no certificate subject alternative name matches
  requested host name 'ldvm1'.
To connect to ldvm1 insecurely, use '--no-check-certificate'.
```

- Tikrinu su links:

```
osboxes@ldvm1:/var/www$ links https://ldvm1
```

```

+----- Invalid certificate -----
+-----+
|
|
| The server ldvm1 doesn't have a valid certificate. Do you
want to connect to it anyway? |
|
|
| [ No ] [ Yes ] [ Never ]
|
+-----+
+-----+
```

- Jau veikia:

Apache2 Ubuntu Default Page: It works (p1 of 2)

Ubuntu Logo Apache2 Ubuntu Default Page
It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems.

It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

...

- Bet panašu, kad rodomas ne mūsų sukurtas žiniatinklio failas, o Apache puslapis pagal nutylėjimą.
 - Tikrinu konfigūracijos failą:

```
osboxes@ldvm1:/etc/apache2/sites-enabled$ cat default-ssl.conf | grep -v -e  
'^[[[:space:]]*#'
```

```
<IfModule mod_ssl.c>  
  <VirtualHost _default_:443>  
    ServerAdmin webmaster@localhost  
  
    DocumentRoot /var/www/html  
  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
  
    SSLEngine on  
  
    SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem  
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key  
  
    <FilesMatch "\.(cgi|shtml|phtml|php)$">  
      SSLOptions +StdEnvVars  
    </FilesMatch>  
    <Directory /usr/lib/cgi-bin>  
      SSLOptions +StdEnvVars  
    </Directory>  
  
  </VirtualHost>  
</IfModule>
```

- Dar vienas LD aprašo netikslumas:
 - failą kūriau /var/www direktorijoje,
 - o su šia Apache versija reikia kurti /var/www/html direktorijoje.
- Perkeliu konfigūracinį failą:

```
osboxes@ldvm1:/etc/apache2/sites-enabled$ cd /var/www
```

```
osboxes@ldvm1:/var/www$ ll
```

```
total 16
drwxr-xr-x  3 root root 4096 Jun 30 05:57 ./
drwxr-xr-x 15 root root 4096 Jun 30 05:05 ../
drwxr-xr-x  2 root root 4096 Jun 30 05:08 html/
-rw-r--r--  1 root root   42 Jun 30 05:57 index.php
```

```
osboxes@ldvm1:/var/www$ ls -Al html
```

```
total 12
-rw-r--r--  1 root root 10918 Jun 30 05:08 index.html
```

```
osboxes@ldvm1:/var/www$ sudo mv -v index.php html/
renamed 'index.php' -> 'html/index.php'
```

```
osboxes@ldvm1:/var/www$ ls -Al
```

```
total 4
drwxr-xr-x  2 root root 4096 Jun 30 06:51 html
```

```
osboxes@ldvm1:/var/www$ ls -Al html
```

```
total 16
-rw-r--r--  1 root root 10918 Jun 30 05:08 index.html
-rw-r--r--  1 root root   42 Jun 30 05:57 index.php
```

- Bet to irgi nepakanka, turinys nepasikeitė.
- Galbūt .html failas turi prioritetą .php atžvilgiu. Pašalinu:

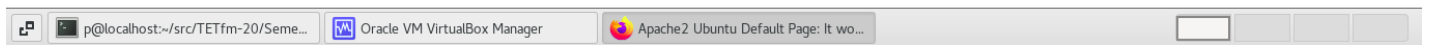
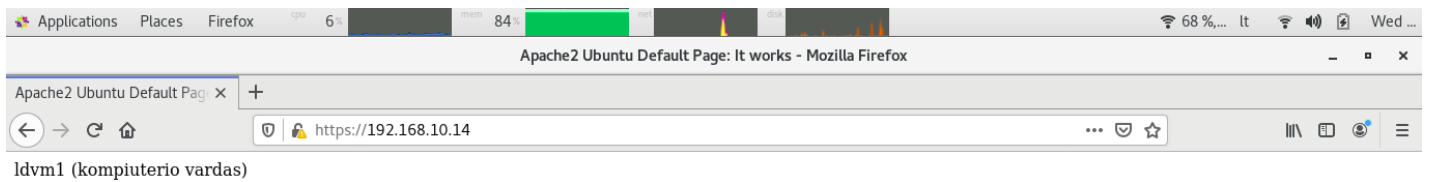
```
osboxes@ldvm1:/var/www$ sudo rm -v html/index.html
removed 'html/index.html'
```

- Patikrinu su `links`, pagaliau veikia!

```
osboxes@ldvm1:/var/www$ links https://ldvm1
```

ldvm1 (kompiuterio vardas)

Mano žiniatinklio puslapis atidaromas ir tikro kompiuterio naršyklėje:



12. Vykdomi procesai

- Komandos ps galimybės:
 - Komanda parodo OS procesų „fotografiją“.
 - Pagal nutylėjimą rodomi tik esamo naudotojo procesai.
 - Komanda geba rodymui atrinkti:
 - visus procesus;
 - tik aktyvius (nemiegančius) procesus;
 - tik su esamu terminalu susietus procesus;
 - procesus pagal nurodytą PID sąrašą;
 - procesus pagal nurodytą komandinę eilutę;
 - pagal proceso savininko grupę (RGID);
 - pagal proceso sesijos ID;
 - pagal procesų terminalo vardus;
 - pagal proceso savininko ID.
 - Komanda geba išvesti tokius proceso duomenis:
 - PID, PGID, SID, TTY;
 - proceso būseną;

- proceso žymės (*Flags*);
 - starto laiką;
 - vykdymo laiką;
 - komandinius argumentus;
 - SELinux *Security context*;
 - LWP gijų (*Threads*) skaičių;
 - LWP gijų ID;
 - signalų būsenas;
 - virtualios atminties būsenas;
 - CPU registrų būsenas;
 - aplinkos kintamuosius (*Environment variables*);
 - ir dar dalį kitų.
- Komanda geba išvesti duomenis skirtingais pavidalais:
 - kombinuojant skirtingus laukus;
 - tam yra keli skirtingi iš anksto nustatyti formatai (Long, Extra long, Jobs ir kt.);
 - keičiant išvedamų eilučių plotį;
 - keičiant išvedamų eilučių skaičių;
 - rodant tik naudotojo nurodytus laukus;
 - rūšiuojant išvestį pagal nurodytą lauką;
 - apjungiant procesus į hierarchiją (medį) pagal PPID;
 - įterpiant gijas tarp procesų;
 - įjungiant/išjungiant laukų antraštes;
 - ir dar keliais kitais.
- Procesai, kurie naudoja daugiausiai kompiuterio resursų:
 - pagal CPU:

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
241	root	0	-20	0	0	0	I	0.3	0.0	0:02.60	
kworker/1:1H-kblockd											
1052	osboxes	20	0	14116	2540	1840	S	0.3	0.3	0:02.47	sshd
7528	mysql	20	0	1741604	237416	6120	S	0.3	23.6	1:01.97	mysqld
17852	root	20	0	344220	54440	12364	S	0.3	5.4	1:26.96	
unattended-upgr											
17865	root	20	0	0	0	0	I	0.3	0.0	0:00.66	
kworker/u4:0-events_power_efficient											
19713	osboxes	20	0	20516	4032	3252	R	0.3	0.4	0:00.17	top
1	root	20	0	171048	7952	4088	S	0.0	0.8	0:08.11	systemd

o pagal Memory:

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
7528	mysql	20	0	1741604	229984	6104	S	0.3	22.9	1:02.20	mysqld
17852	root	20	0	344220	96800	56224	D	20.3	9.6	1:29.37	
unattended-upgr											
28602	osboxes	20	0	369752	22468	14712	S	0.0	2.2	0:00.10	tracker-store
26582	root	20	0	293720	16292	14336	S	0.0	1.6	0:00.07	
packagekitd											
662	root	20	0	775596	12832	3356	S	0.0	1.3	0:02.57	snappd
878	osboxes	39	19	520180	12196	6704	S	0.0	1.2	0:00.31	tracker-miner-f
303	root	19	-1	68212	11048	10172	S	0.0	1.1	0:01.00	systemd-journal
26973	root	20	0	313752	10652	9012	S	0.0	1.1	0:00.13	ModemManager

• Programa top:

- o Pateikia dinaminį sistemos (OS) vaizdą.
- o Pateikia sistemos informacijos reziumė:
 - sistemos laikrodį;
 - *Uptime*;
 - prisijungusių naudotojų sk.;
 - tris vidutines sistemines apkrovas (*System load*);
 - procesų skaičių:
 - kiek iš viso;
 - kiek veikia;
 - kiek „miega“;
 - kiek sustabdytų;

- kiek „zombių“.
- CPU laikus, skirtus:
 - *User* procesams;
 - branduolio užduotims;
 - prioritetų keitimui (*Niceness*);
 - ramybės būsenai (*Idle*);
 - aparatūros pertraukims (*Hardware interrupts*);
 - programinėms pertraukims (*Software interrupts*);
 - hiperizoriaus veiklai (*Host* + kitų *Guest OS* aptarnavimui).
- Pateikia procesų ir branduolio gijų sąrašą stulpeliais:
 - proceso identifikatorių PID;
 - proceso savininką (naudotoją);
 - proceso sisteminį prioritetą;
 - proceso prioriteto pataisymą (*Niceness*);
 - proceso Virt
 - proceso Resident
 - proceso Shared
 - proceso būseną;
 - proceso sunaudojamą CPU laiką %;
 - proceso sunaudojamą atminties apimtį %;
 - proceso vykdymo laiką;
 - proceso komandos pavadinimą.
- Rūšiuoja pagal pasirinktus stulpelius;

13. Prievadų skenavimas

- Kaimyno prievadų situacija nepasikeitė, nes jame nieko neinstaliavau.
 - Nelabai tiksli instrukcija LD apraše.
- Tačiau jei skenuoju iš kaimyno pirmąjį kompiuterį, situacija jau gerokai kita:
 - (Abu kompiuteriai sukurti iš bendro .vdi atvaizdo, todėl pradžioje jų tarnybos buvo identiškos)

```
osboxes@ldvm2:~$ sudo nmap -sS 192.168.10.14
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-30 09:09 EDT
Nmap scan report for 192.168.10.14
Host is up (0.00081s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 08:00:27:40:2C:F6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

- Matyti, kad atsirado du atviri prievadai (veikia nauja tarnyba): http ir https

Duotosios Linux tinklo komandos aprašymas: tcpdump

Tai tinklo srauto sniferis (paketų gaudyklė).

1. Įrankis skaito duomenų paketus (įprastai iš tinklo sąsajos) ir išveda jų dekoduoatą aprašymą.
2. Tai jis daro paketams, atitinkantiems užduotą filtrą.
3. Jei filtro nėra, nuskaitymi visi paketai iš eilės.
4. Jei filtras yra, jis konstruojamas kaip loginė išraiška (angl. *Boolean expression*)
5. Ir atitinka `pcap-filter` sintaksę.
6. Įprastai išvestyje paketo aprašymas talpinamas į vieną, atskirą eilutę.
7. Įprastai jis pradedamas paketo laiko žyma.
8. Jei nurodyta parinktis `-w`, paketų turinys įrašomas į atskirą failą (vėlesnei analizei).
9. Jei nurodyta parinktis `-r`, paketai ne iš tinklo sąsajos, bet iš failo, sukurto naudojant `-w`.
10. Jei nurodyta parinktis `-v`, paketai nuskaitymi iš tų failų, kurių vardai yra surašyti šiai parinkčiai priskirtame faile.
11. Jei nurodytos abi parinktys: tiek skaitymo iš failo, tiek rašymo į failą, atsiranda galimybė iš didžiulio *Capture* failo išsipjauti tik reikiamas srauto dalis.
12. Įrankis geba išvardinti:
 - a. gaudymui tinkamas sistemos tinklo sąsajos, `-D`;
 - b. sąsajos palaikomus *Data-link* tipus, `-L`;
13. Įrankis turi nuskaitymo valdymą pagal:
 - a. tinklo sąsajos vardą, `-i`;
 - b. tinklo sąsajos būseną (angl. *Promiscuous* arba ne), `-p`;
 - c. pagautų paketų skaičių, `-c`;
 - d. paketų keliavimo kryptį, `-Q`;
 - e. fiksuotą paketo pradžios fragmentą, `-s`;
 - f. išraišką, pateiktą atskirame faile, `-F` (praverčia, kai išraiškos apimtys labai išauga).
14. Įrankis turi išvesties valdymą:
 - a. išjungti laiko žymas arba pakeisti jų tipą, `-t`;
 - b. išjungti mazgų vardų išsprendimą, `-n`;

- c. įjungti Layer2 antraštes, -e ;
- d. įjungti Layer2 *Payload* išvestį ASCII formatu, -A (antraščių nutrynimą);
- e. įjungti buferizavimą kas eilutę, -l ;
- f. įjungti paketo numerio rodymą, -# ;
- g. įjungti tik trumpus paketų aprašymus, -q ;
- h. įjungti išplėstinius paketų aprašymus, -v ;
- i. įjungti absoliučius TCP sekų numerius, -S (vietoj santykinų);
- j. įjungti priverstinį tipą visų pagautų paketų dekodavime, -T ;
- k. įjungti šešioliktainį paketo rodymą, -x ;
- l. įjungti šešioliktainį ir ASCII rodymą, patalpintus greta, -X ;
- m. pradėti naują failą pagal pagautų duomenų apimtį (MB), -C ;
- n. pradėti naują failą pagal gaudymo trukmę (s), -F .

15. Ir dar kelios funkcijos.

Pavyzdys

Gaudymui tinkamos tinklinės sąsajos:

```
osboxes@ldvm1:~$ tcpdump -D
1.enp0s3 [Up, Running]
2.enp0s8 [Up, Running]
3.lo [Up, Running, Loopback]
4.any (Pseudo-device that captures on all interfaces) [Up, Running]
5.bluetooth-monitor (Bluetooth Linux Monitor) [none]
6.nflog (Linux netfilter log (NFLOG) interface) [none]
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
```

Viso srauto gaudymas per Ethernet sąsają enp0s3:

```

osboxes@ldvm1:~$ sudo tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes

13:11:35.318610 IP ldvm1.57894 > pugot.canonical.com.ntp: NTPv4, Client, length 48
13:11:35.320401 IP ldvm1.42866 > one.one.one.one.domain: Flags [S], seq 548142022, win 64240, options [mss 1460,sackOK,TS val 2727199959 ecr 0,nop,wscale 7,tfo cookiereq,nop,nop], length 0
13:11:35.503655 IP one.one.one.one.domain > ldvm1.42866: Flags [S.], seq 433792001, ack 548142023, win 65535, options [mss 1460], length 0
13:11:35.504691 IP ldvm1.42866 > one.one.one.one.domain: Flags [.], ack 1, win 64240, length 0
13:11:35.504781 IP ldvm1.42866 > one.one.one.one.domain: Flags [P.], seq 1:45, ack 1, win 64240, length 44 37324+ PTR? 4.94.189.91.in-addr.arpa. (42)
13:11:35.505093 IP one.one.one.one.domain > ldvm1.42866: Flags [.], ack 45, win 65535, length 0
13:11:35.539035 IP pugot.canonical.com.ntp > ldvm1.57894: NTPv4, Server, length 48
...
13:11:36.540981 IP ldvm1.42866 > one.one.one.one.domain: Flags [.], ack 189, win 64052, length 0
^C
17 packets captured

```

Tik vieno tinklo mazgo srauto gaudymas per kitą Ethernet sąsają:

```

osboxes@ldvm1:~$ sudo tcpdump -i enp0s8 host kaimynas
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes

13:13:14.220174 IP kaimynas > ldvm1: ICMP echo request, id 6, seq 1, length 64
13:13:14.220232 IP ldvm1 > kaimynas: ICMP echo reply, id 6, seq 1, length 64
13:13:16.035415 IP kaimynas > ldvm1: ICMP echo request, id 6, seq 2, length 64
13:13:16.035500 IP ldvm1 > kaimynas: ICMP echo reply, id 6, seq 2, length 64
13:13:17.419338 IP kaimynas > ldvm1: ICMP echo request, id 6, seq 3, length 64
13:13:17.419440 IP ldvm1 > kaimynas: ICMP echo reply, id 6, seq 3, length 64
13:13:20.046245 ARP, Request who-has kaimynas tell ldvm1, length 28
13:13:20.047002 ARP, Reply kaimynas is-at 08:00:27:7a:d0:b7 (oui Unknown), length 46
13:13:20.108060 ARP, Request who-has ldvm1 tell kaimynas, length 46
13:13:20.108097 ARP, Reply ldvm1 is-at 08:00:27:40:2c:f6 (oui Unknown), length 28
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel

```

Viso potinklio srauto gaudymas išjungus vardų išsprendimą ir paketų laiko žymas:

```
osboxes@ldvm1:~$ sudo tcpdump -i enp0s8 -n -t net 192.168.10.0/24 and not tcp port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
IP 192.168.10.13.56204 > 192.168.10.14.443: Flags [S], seq 2018303758, win 64240,
options [mss 1460,sackOK,TS val 3668928396 ecr 0,nop,wscale 7], length 0
IP 192.168.10.14.443 > 192.168.10.13.56204: Flags [S.], seq 3166645553, ack 2018303759,
win 65160, options [mss 1460,sackOK,TS val 1348531861 ecr 3668928396,nop,wscale 7],
length 0
IP 192.168.10.13.56204 > 192.168.10.14.443: Flags [.], ack 1, win 502, options
[nop,nop,TS val 3668928397 ecr 1348531861], length 0
IP 192.168.10.13.56204 > 192.168.10.14.443: Flags [P.], seq 1:372, ack 1, win 502,
options [nop,nop,TS val 3668928398 ecr 1348531861], length 371
IP 192.168.10.14.443 > 192.168.10.13.56204: Flags [.], ack 372, win 507, options
[nop,nop,TS val 1348531862 ecr 3668928398], length 0
IP 192.168.10.14.443 > 192.168.10.13.56204: Flags [P.], seq 1:1281, ack 372, win 507,
options [nop,nop,TS val 1348531869 ecr 3668928398], length 1280
IP 192.168.10.13.56204 > 192.168.10.14.443: Flags [.], ack 1281, win 501, options
[nop,nop,TS val 3668928405 ecr 1348531869], length 0
IP 192.168.10.13.56204 > 192.168.10.14.443: Flags [P.], seq 372:452, ack 1281, win 501,
options [nop,nop,TS val 3668928407 ecr 1348531869], length 80
IP 192.168.10.13.56204 > 192.168.10.14.443: Flags [FP.], seq 452:476, ack 1281, win
501, options [nop,nop,TS val 3668928407 ecr 1348531869], length 24
IP 192.168.10.14.443 > 192.168.10.13.56204: Flags [.], ack 452, win 507, options
[nop,nop,TS val 1348531873 ecr 3668928407], length 0
IP 192.168.10.14.443 > 192.168.10.13.56204: Flags [P.], seq 1281:1552, ack 477, win
507, options [nop,nop,TS val 1348531876 ecr 3668928407], length 271
IP 192.168.10.13.56204 > 192.168.10.14.443: Flags [R], seq 2018304235, win 0, length 0
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel
```

Tik TCP paketų gaudymas per OAM tinklo sąsają:

```
osboxes@ldvm1:~$ sudo tcpdump -i enp0s8 tcp -w ldvm-tcp-srautas.pcap
tcpdump: listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
^Z
[1]+  Stopped                  sudo tcpdump -i enp0s8 tcp -w ldvm-tcp-srautas.pcap

osboxes@ldvm1:~$ fg
sudo tcpdump -i enp0s8 tcp -w ldvm-tcp-srautas.pcap
^C
142 packets captured
143 packets received by filter
0 packets dropped by kernel

osboxes@ldvm1:~$ ls -l ldvm-tcp-srautas.pcap
-rw-r--r-- 1 tcpdump tcpdump 21572 Jun 30 13:24 ldvm-tcp-srautas.pcap
```

Įrašytų į failą paketų skaičiaus patikrinimas

```
osboxes@ldvm1:~$ sudo -u tcpdump tcpdump -r ldvm-tcp-srautas.pcap | wc -l  
reading from file ldvm-tcp-srautas.pcap, link-type EN10MB (Ethernet)  
142
```

Minimalus pirmųjų keturių paketų dekodavimas:

```
sboxes@ldvm1:~$ sudo -u tcpdump tcpdump -r ldvm-tcp-srautas.pcap -t -n -q -c 4  
reading from file ldvm-tcp-srautas.pcap, link-type EN10MB (Ethernet)  
IP 192.168.10.14.22 > 192.168.10.8.40606: tcp 124  
IP 192.168.10.8.40606 > 192.168.10.14.22: tcp 0  
IP 192.168.10.8.40606 > 192.168.10.14.22: tcp 36  
IP 192.168.10.14.22 > 192.168.10.8.40606: tcp 124
```

Viso darbo išvados

1. Laboratorinį darbą #2 (LD2) atlikti pavyko pilnai, tačiau kilo gana daug kliūčių.
2. Ko gero pagrindinė to priežastis: noras viską daryti be GUI, naudojant tik CLI įrankius.
 - a. Dėl šio mano reikalavimo teko LD atlikimą pradėti nuo LD2, o LD1 dar laukia eilėje.
3. Tam reikėjo pramokti *VirtualBox* įrankį ir suskriptinti automatinį VM kūrimą su tinkama konfigūracija:
 - a. Antra tinklo sąsaja pageidautina *Host-only* tipo (skirta OAM: Operation, Administration, Management).
 - b. Bendras *.vdi* disko atvaizdas, iš kurio galiu pakelti norimai daug VM neužimant Host talpyklos dubliuotomis *.vdi* kopijomis.
 - c. Kiekvienai VM parinkau po 2 virtualius CPU ir po 1024 MiB RAM (mano Host turi prieinamus 3.7 GiB RAM).
 - d. Tam pasirinkau mano naudojamą CentOS Linux ir man žinomą *Bash* kalbą.
 - e. Tai užtruko kelias paras: 150 *Commits*, [OLD-infra.sh](https://github.com/VGTU-ELF/TETfm-20/commits/48a7e7c30bc23b756cff9a1e53cdb0ce4e4c921f/Semestras-2/1-Informacijos-ir-sistem%C5%B3-apsauga/laboratoriniai-darbai/Saulius-Krasuckas/OLD-infra.sh)
(<https://github.com/VGTU-ELF/TETfm-20/commits/48a7e7c30bc23b756cff9a1e53cdb0ce4e4c921f/Semestras-2/1-Informacijos-ir-sistem%C5%B3-apsauga/laboratoriniai-darbai/Saulius-Krasuckas/OLD-infra.sh>)
4. Antra kliūčių priežastis: LD aprašas skirtas senesnei Ubuntu versijai (turbūt 18.04):
 - a. Dėl OS versijų skirtumo dalis programinių įrankių buvo sudiegti naujesnės versijos (pvz. PHP7 vietoj PHP4).
 - b. O dalies (*Development*) įrankių diegimą atidėjau iki tyrimų, kuomet įrankių prireiks tiesiogiai.