Vilniaus Gedimino technikos universitetas

Elektronikos fakultetas

Kompiuterijos ir ryšių technologijų katedra

Informacijos ir sistemų apsauga

Modulis ELKRM17209

Laboratorinio darbo nr. 3 ataskaita

Atliko: TETfm-20 grupės magistrantas
Saulius Krasuckas
Tikrino: doc. dr. Eimantas Garšva

VILNIUS, 2021

Darbo Tikslas

✓ Patikrinti tinklo nustatymus.

✓ Susipažinti su `iptable` sintakse.

✓ Nustatyti paprastą tarpsegmentinį ekraną.

Trumpas atlikto darbo aprašymas

1. Virtualaus kompiuterio konfigūracija

Tikrinu IP adresus.

Tikrinu maršrutizacijos lentelę.

Pataisau `interfaces` failą ir palyginu su ankstesne versija.

Aktyvuoju pakeistus nustatymus.

Abu IP adresai, prašomi LD3, nurodyti.

Vieninteliai vartai pagal nutylėjimą yra `192.168.10.254`, kaip ir prašo LD3 aprašas.

2. Tinklo paslaugų tikrinimas

Diegiu grafinę priemonę `sysvconfig`.

- Programinės įrangos valdymo įrankis neranda minimos priemonės.
- Įrankio paieškos apibendrinimas:
  - įrankis `chkservice` gana tiksliai atitinka `sysvconfig`;
  - puikiai veikia su SystemD *Init*-mechanizmu;
  - tik nerodo tarnybų priklausomybių nuo *Runlevels* (arba nuo *targets*, kalbant SystemD terminais).

SSH serverio instaliavimas.

Tą patį pakartojau ir kaimyniniame kompiuteryje.

3. Tinklo paslaugų tikrinimas

Teikiamos tinklo paslaugos.

Jungiuosi prie kaimyno per SSH.

Stebiu paslaugų būvio pasikeitimą.

Palyginimui įrašiau komandos išvesti abu kartus į skirtingus failus.
Tuomet pasinaudojau įrankiu `diff -u`.

Iš tinklinių (ne *Unix-socket*) prisijungimų atsirado du nauji įrašai:

```
tcp        0      0 192.168.10.14:51672     192.168.10.13:22        TIME_WAIT
tcp        0      0 192.168.10.14:51674     192.168.10.13:22        ESTABLISHED
```

- Pirmasis iš jų yra rodo mano pirmą bandymą prisijungti (nepavykusi autentikacija ir nutrūkęs ryšys).
- Antrasis iš jų yra rodo antrą, sėkmingą bandymą prisijungti.

4. Kaimyno skenavimas

Rezultatai:

```
osboxes@ldvm1:~$ sudo nmap -sS -P0 -n -F 192.168.10.13
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-04 20:37 EEST
Nmap scan report for 192.168.10.13
Host is up (0.00067s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:7A:D0:B7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

- Kaimyno kompiuteryje matau prieinamą tik vieną paslaugą / tarnybą:
  - SSH

Taip pat nuskenavau ir savo kompiuterį iš kaimyninio kompiuterio:
(kadangi žiniatinklis paruoštas tik savajame)

```
osboxes@ldvm2:~$ sudo nmap -sS -P0 -n -F 192.168.10.14
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-05 07:23 EDT
Nmap scan report for 192.168.10.14
Host is up (0.0013s latency).
Not shown: 97 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 0.97 seconds
```

- Savajame kompiuteryje matau prieinamas jau tris paslaugas / tarnybas:
  - SSH
  - HTTP
  - HTTPS

5. Paketų persiuntimo įjungimas

Įjungiu persiuntimą faile.

Peržiūriu įkeltus modulius.

Nustatau automatinį poros modulių užkrovimą.

Nerperkraudamas kompiuterio nustatau šias vertes tiesioges.

Patikrinu.

Nustatymas įvyko, o `iptable_nat` modulis įkeltas į branduolio erdvę (kartu su dar penkiais moduliais).

6. `iptables` patikrinimas

Peržiūriu nustatymus pagal nutylėjimą.

Uždraudžiu įeinančius paketus.

Išbandau draudimą, veikia.

Ryšys iš kaimyninio kompiuterio nebeužsimezga, įvyksta *Timeout*.

Žiūriu, kaip pasikeitė nustatymai.

Atsirado viena nauja eilutė: `DROP all -- anywhere anywhere`

Išvalau `iptables`.

Patikrinu ICMP pingą iš kaimyninio kompiuterio.

Uždraudžiu ICMP protokolą.

Tikrinu, ar atsirado taisyklė:

```
osboxes@ldvm1:~$ diff -u debug/{09,11}*.txt
--- "debug/09.iptables_iki_bandym\305\263.txt"  2021-07-04 22:08:14.293905599 +0300
+++ "debug/11.iptables_po_ICMP_taisykl\304\227s.txt"    2021-07-04 22:45:28.062899693
+0300
@@ -1,5 +1,6 @@
 Chain INPUT (policy ACCEPT)
 target     prot opt source               destination
+DROP       icmp --  anywhere             anywhere

 Chain FORWARD (policy ACCEPT)
 target     prot opt source               destination
```

Tikrinu ją, veikia.

Kompiuteris į ICMP pingą nebeatsako.

Išvalau `iptables`.

7. Kompiuterio apsaugojimas nuo resursus išnaudojančio ICMP srauto

Paleidžiu `ping` srautą į virtualų kompiuterį.

Stebiu, kaip vykdoma komanda:

```
64 bytes from 192.168.10.14: icmp_seq=1 ttl=64 time=0.439 ms
64 bytes from 192.168.10.14: icmp_seq=2 ttl=64 time=0.567 ms
64 bytes from 192.168.10.14: icmp_seq=3 ttl=64 time=0.745 ms
64 bytes from 192.168.10.14: icmp_seq=4 ttl=64 time=0.568 ms
```

Sustabdau srautą `Ctrl+C` pagalba:

```
^C
--- 192.168.10.14 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.439/0.579/0.745/0.112 ms
```

Nustatau apribojimą 1 šalt./s:

- Deja, virtualaus kompiuterio reakcija į *ping* srautą nepasikeitė.
  Įtarimų sukėlė `-j ACCEPT` ir `Chain INPUT (policy ACCEPT)`.
- Papildau, kad `iptables` atmestų visus ICMP paketus, neatitikusius šios taisyklės.

Vėl paleidžiu *ping* srautą.

```
[p@localhost Saulius-Krasuckas]$ ping 192.168.10.14
PING 192.168.10.14 (192.168.10.14) 56(84) bytes of data.
64 bytes from 192.168.10.14: icmp_seq=2 ttl=64 time=0.771 ms
64 bytes from 192.168.10.14: icmp_seq=4 ttl=64 time=0.665 ms
64 bytes from 192.168.10.14: icmp_seq=6 ttl=64 time=0.623 ms
64 bytes from 192.168.10.14: icmp_seq=8 ttl=64 time=0.636 ms
^C
--- 192.168.10.14 ping statistics ---
8 packets transmitted, 4 received, 50% packet loss, time 7000ms
rtt min/avg/max/mdev = 0.623/0.673/0.771/0.066 ms
```

Dabar iš aštuonių paketų per 7s atkeliavo tik 4 (50%).
Kompiuteris atmeta kas antrą ICMP paketą.
Panašu, kad įeinančio ICMP srauto ribojimas dabar veikia.

Išvalau `iptables`.

8. *Telnet* uždraudimas

Registruoju *Telnet* užklausas žurnale ir jų neleidžiu.

Kreipiuosi iš realaus į savo virtualų kompiuterį *Telnet* protokolu.

Peržiūriu įrašus jo žurnale.

```
osboxes@ldvm1:~$ tail -0f /var/log/syslog
Jul  5 10:00:26 ldvm1 kernel: [ 7539.021434] TELNET ATTEMPT: IN=enp0s8 OUT=
MAC=08:00:27:40:2c:f6:0a:00:27:00:00:00:08:00 SRC=192.168.10.254 DST=192.168.10.14
LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=46720 DF PROTO=TCP SPT=52720 DPT=23 WINDOW=29200
RES=0x00 SYN URGP=0
```

Kreipiuosi iš kaimyno į savo virtualų kompiuterį *Telnet* protokolu.

```
osboxes@ldvm2:~$ time telnet 192.168.10.14
Trying 192.168.10.14...
telnet: Unable to connect to remote host: Connection refused

real    0m0.013s
user    0m0.006s
sys     0m0.005s
```

Užklausa atmetama iškart.

O žurnalas vėl pasipildė:

```
Jul  5 10:04:18 ldvm1 kernel: [ 7765.363946] TELNET ATTEMPT: IN=enp0s8 OUT=
MAC=08:00:27:40:2c:f6:08:00:27:7a:d0:b7:08:00 SRC=192.168.10.13 DST=192.168.10.14
LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=1374 DF PROTO=TCP SPT=39398 DPT=23 WINDOW=64240
RES=0x00 SYN URGP=0
```

9. Automatinė taisyklių keltis

Sukuriu direktoriją taisyklėms saugoti.

Sukonfigūruoju `iptables`:

- išvalau buvusius nustatymus.
- nustatau taisykles pagal nutylėjimą.

Patikrinu konfigūraciją.

Įrašau konfigūraciją į failą.

Sukuriu failą `myfirewall`.

Kopijuoju į paleidimo sritį.

Suteikiu paleidimo teises.

Scenarijaus veikimas.

```
osboxes@ldvm1:~$ /etc/init.d/myfirewall
Usage: /etc/init.d/myfirewall {start|stop|show}

osboxes@ldvm1:~$ /etc/init.d/myfirewall show
Current firewall rules:
Failed to list table names in /proc/net/ip_tables_names: Permission denied

osboxes@ldvm1:~$ sudo /etc/init.d/myfirewall show
Current firewall rules:
# Generated by iptables-save v1.8.4 on Mon Jul  5 12:52:52 2021
*filter
:INPUT DROP [46:5323]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [991:138573]
-A INPUT -d 192.168.10.14/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -d 192.168.10.14/32 -p tcp -m tcp --dport 443 -j ACCEPT
COMMIT
# Completed on Mon Jul  5 12:52:52 2021
# Generated by iptables-save v1.8.4 on Mon Jul  5 12:52:52 2021
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [3:304]
:POSTROUTING ACCEPT [3:304]
COMMIT
# Completed on Mon Jul  5 12:52:52 2021
```

Patikrinu, ar scenarijus išvalo taisykles:

```
osboxes@ldvm1:~$ sudo /etc/init.d/myfirewall stop
Stopping firewall (flushing rules)

osboxes@ldvm1:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Įkeliu reikiamas `iptables` taisykles:

```
osboxes@ldvm1:~$ sudo /etc/init.d/myfirewall start
Starting firewall (iptables)
```

Tikrinu jų veikimą.

- HTTP paslauga nebeprieinama:

```
[p@localhost Saulius-Krasuckas]$ time curl -k http://192.168.10.14
curl: (7) Failed connect to 192.168.10.14:80; Connection timed out

real    2m7.277s
user    0m0.005s
sys     0m0.019s
```

Klientinė programa `curl` po 2 min. sulaukia *Timeout*.

- o HTTPS paslauga vis dar prieinama išorei:

```
[p@localhost Saulius-Krasuckas]$ time curl -k https://192.168.10.14
<html> ldvm1 (kompiuterio vardas) </html>

real    0m0.186s
user    0m0.108s
sys     0m0.066s
```

Perkaunu virtualų kompiuterį.

Pataisau scenarijaus automatinį startą (žr. prie sunkumų).

Patikrinu iptables taisykles – dabar jau užsikrovė:

```
osboxes@ldvm1:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             ldvm1                tcp dpt:ssh
ACCEPT     tcp  --  anywhere             ldvm1                tcp dpt:https

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Patikrinu taisyklių veikimą.

- HTTPS užklausa praleidžiama:

```
[p@localhost ~]$ curl -k https://192.168.10.14
<html> ldvm1 (kompiuterio vardas) </html>
```

- HTTP užklausa atmetama:

```
[p@localhost ~]$ curl -m 10 http://192.168.10.14
curl: (28) Connection timed out after 10001 milliseconds
```

- `iptables` taisyklės veikia.

10. Apsaugoto kompiuterio skenavimas

Skenuoju kaimyną pagal ketvirtą žingsnį:

- Rezultatas identiškas.
  Taip dėl to, kad tiek žiniatinklį, tiek tarpsegmentinį ekraną konfigūravau savame kompiuteryje, o ne kaimyininiame.
- Dėl to skenuoju savo kompiuterį iš kaimyninio.

Palyginu matomas paslaugas savame kompiuteryje:

```
osboxes@ldvm2:~$ sudo nmap -sS -P0 -n -F 192.168.10.14 > debug/02.ldvm1-paslaugos-
įjungus-tarpsegmentinį-ekraną.txt
osboxes@ldvm2:~$ diff -u debug/{01,02}*
  ...
 Nmap scan report for 192.168.10.14
-Host is up (0.00068s latency).
-Not shown: 97 closed ports
+Host is up (0.00064s latency).
+Not shown: 98 filtered 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)
```

Matyti, jog savojo kompiuterio prievadas `80/TCP`, skirtas HTTP paslaugai, tapo nebeprieinamas išorėje.

Laboratorinis darbas atliktas

Iškilę sunkumai ir pastebėti netikslumai

1. Virtualaus kompiuterio konfigūracija

Diegiu grafinę priemonę `sysvconfig`:

```
osboxes@ldvm1:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.10.254  0.0.0.0         UG    0      0        0 enp0s8
default         10.0.2.2        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      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
```

- Nustatymai ne visai atitinka LD aprašą:
  - 1. Vietoj `eth*` tinklo sąsajų vardų Linux naudoja `enp0s*` vardus.
    (šiame darbe naudojamas branduolys `5.8.0-59-generic`)
    Palieku kaip yra.
  - 2. Trūksta `10.10.10.x` adreso (nes LD2 buvo uždėtas rankomis, o po to OS perkrauta).
  - 3. OS turi du vartus pagal nutylėjimą:
    - vienas pasiekiamas per `enp0s3`, *NAT* tipo tinklo sąsają (su automatiniu IP adresu);
    - kitas pasiekiamas per `enp0s8`, *Host-only* tipo tinklo sąsają.

      ```
      Atsekiau, kad pirmuosius vartus sukonfigūruoja _NetworkManager_ įrankis,
      sukurdamas dedikuotą tinklo prisijungimą
      (tam atskirą tinklo valdymo abstrakciją):


      osboxes@ldvm1:~$ nmcli connection show
      NAME                UUID                                  TYPE      DEVICE
      Wired connection 1  2c671148-b52a-4426-9325-d35a52967e3c  ethernet  enp0s3

      osboxes@ldvm1:~$ nmcli connection show id "Wired connection 1" | grep 10.0.2.2
      IP4.GATEWAY:                            10.0.2.2
      IP4.ROUTE[1]:                           dst = 0.0.0.0/0, nh = 10.0.2.2, mt =
      100
      DHCP4.OPTION[23]:                       routers = 10.0.2.2
      ```

- Nereikalingus vartus pagal nutylėjimą bandau išmest būtent per *NetworkManager* kartu su minimu abstrakčiu tinklo prisijungimu:

```
osboxes@ldvm1:~$ sudo nmcli connection delete "Wired connection 1"
Connection 'Wired connection 1' (2c671148-b52a-4426-9325-d35a52967e3c) successfully
deleted.
```

- Tikrinu maršrutizacijos lentelę:

```
osboxes@ldvm1:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.10.254  0.0.0.0         UG    0      0        0 enp0s8
10.10.10.0      0.0.0.0         255.255.255.0   U     0      0        0 enp0s8
link-local      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
```

2. Tinklo paslaugų tikrinimas

Diegiu grafinę priemonę `sysvconfig`.

```
osboxes@ldvm1:~$ sudo apt-get install sysvconfig
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package sysvconfig
```

- Programinės įrangos valdymo įrankis neranda minimos priemonės.
  - Mėginu atnaujinti programų sąrašus:

```
osboxes@ldvm1:~$ sudo apt-get update
0% [Working]
Err:1 http://security.ubuntu.com/ubuntu focal-security InRelease
  Temporary failure resolving 'security.ubuntu.com'
Err:2 http://us.archive.ubuntu.com/ubuntu focal InRelease
  Temporary failure resolving 'us.archive.ubuntu.com'
Err:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
  Temporary failure resolving 'us.archive.ubuntu.com'
Err:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
  Temporary failure resolving 'us.archive.ubuntu.com'
Reading package lists... Done
W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/focal/InRelease
Temporary failure resolving 'us.archive.ubuntu.com'
W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/focal-
updates/InRelease  Temporary failure resolving 'us.archive.ubuntu.com'
W: Failed to fetch http://us.archive.ubuntu.com/ubuntu/dists/focal-
backports/InRelease  Temporary failure resolving 'us.archive.ubuntu.com'
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/focal-
security/InRelease  Temporary failure resolving 'security.ubuntu.com'
W: Some index files failed to download. They have been ignored, or old ones used
instead.
```

- Paaiškėja, kad pašalinus vartus pagal nutylėjimą `10.0.2.2`, nustojo veikti interneto ryšys.
  Jis veikdavo per tinklo sąsają `enp0s3`, kuri VirtualBox sistemoje yra *NAT* tipo (skirta išėjimui į internetą).
- Kadangi dabar ėmė veikti tik vartai per `192.168.10.254` (priklausantys Host OS), teko konfigūruoti maršrutizavimą + įjungti *NAT* mechanizmą jau Host OS pusėje būtent šiai Guest tinklo sąsajai (o ne įprastinei).
  (Neaprašau Host OS veiksmų, tai nebūtinai Linux sistema)
- Sąrašų atnaujinimas vėl veikia:

```
osboxes@ldvm1:~$ sudo apt-get update
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
  ...
Get:21 http://us.archive.ubuntu.com/ubuntu focal-backports/universe Translation-
en [2,060 B]
Get:22 http://us.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11
Metadata [1,780 B]
Get:23 http://us.archive.ubuntu.com/ubuntu focal-backports/universe amd64 c-n-f
Metadata [288 B]
Fetched 4,078 kB in 10s (391 kB/s)
Reading package lists... Done
```

- Turbūt vertėtų įtraukti tokį patikslinimą į laboratorinio darbo aprašą.
  (apie reikiamą *VirtualBox* tinklo sąsajos tipą + maršrutizavimą tarp Host ir Guest OS)
- Tęsiu `sysvconfig` diegimą. Tokio paketo *Ubuntu 20.04.2* neturi:

```
osboxes@ldvm1:~$ sudo apt-get install sysvconfig
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package sysvconfig

osboxes@ldvm1:~$ apt search sysvconfig
Sorting... Done
Full Text Search... Done
```

- Panašu, kad šis įrankis iš Ubuntu pašalintas 2009-09-11:
  https://superuser.com/questions/96040/did-sysvconfig-disappear-in-ubuntu-9-10
- Taip pat dabar neveikia ir `sysvconfig` atitikmenys, dar veikę po jo pašalinimo: `sysv-rc-conf`, `rcconf`:
  https://askubuntu.com/questions/1043248/rcconf-package-alternative-in-bionic-beaver

    - Panašu, kad jie nebeveikia nuo 2015 m., kai OS atsirado `systemd` mechanizmas. Ir tai kėlė nepatogumų žmonėms, atnaujinantiems Ubuntu jau net nuo versijos `14.04`: https://askubuntu.com/questions/1106216/ubuntu-18-04-cant-install-sysv-rc-conf-package-for-managing-startup-services#comment1824791_1106217
    - Galbūt reikėtų pagal tai irgi patikslinti LD3 aprašą?
- Ieškau atitikmenų darbui su SystemD mechanizmu.

  Jeigu pakanka tik patikrinti tarnybų būsenas, tiks komanda `systemctl`:

```
osboxes@ldvm1:~$ systemctl list-unit-files --type=service --all

----8><------------------------------------------------------------------------
----------------------><8----
UNIT FILE                                   STATE           VENDOR PRESET
accounts-daemon.service                     enabled         enabled
acpid.service                               disabled        enabled
alsa-restore.service                        static          enabled
alsa-state.service                          static          enabled
alsa-utils.service                          masked          enabled
anacron.service                             enabled         enabled
apache-htcacheclean.service                 disabled        enabled
apache-htcacheclean@.service                disabled        enabled
apache2.service                             enabled         enabled
apache2@.service                            disabled        enabled
apparmor.service                            enabled         enabled
apport-autoreport.service                   static          enabled
apport-forward@.service                     static          enabled
apport.service                              generated       enabled
apt-daily-upgrade.service                   static          enabled
apt-daily.service                           static          enabled
autovt@.service                             enabled         enabled
avahi-daemon.service                        enabled         enabled
lines 1-19
----8><------------------------------------------------------------------------
----------------------><8----
```

  Šitaip lengva filtruoti tarnybas pagal vardus (jų šablonus):

```
osboxes@ldvm1:~$ systemctl list-unit-files --type=service --all *Manager*
UNIT FILE                                   STATE   VENDOR PRESET
dbus-org.freedesktop.ModemManager1.service enabled enabled
ModemManager.service                        enabled enabled
NetworkManager-dispatcher.service           enabled enabled
NetworkManager-wait-online.service          enabled enabled
NetworkManager.service                      enabled enabled

5 unit files listed.
```

- Tarnybų valdymui susirandu įrankį `serman2`: https://aur.archlinux.org/packages/serman

- Pasiimu jį iš GitHub:

```
osboxes@ldvm1:~$ mkdir src

osboxes@ldvm1:~$ cd src/

osboxes@ldvm1:~$ git clone https://github.com/baoboa/serman
Cloning into 'serman'...
remote: Enumerating objects: 41, done.
remote: Total 41 (delta 0), reused 0 (delta 0), pack-reused 41
Unpacking objects: 100% (41/41), 32.70 KiB | 985.00 KiB/s, done.
```

- Išsibandau įrankį:

```
osboxes@ldvm1:~/src$ sudo serman/serman.py

----8><----------------------------------------------------------------------------
-------------------------><8----
Commands|  Services
————————┼———————————————————————————————————————————————————————————————————————
————————————————————————————————
enable  |  getty@tty2.service
running ● ▲
restart |  getty@tty6.service
running ● ▲
start   |  gpu-manager.service
dead
status  |  graphical.target
dead
        |  grub-common.service
exited ●
        |  grub-initrd-fallback.service
dead
        |  halt.target
        |  hibernate.target
        |  home.mount
mounted ●
        |  hwclock.service
        |  hybrid-sleep.target
        |  ifup@.service
        |  ifup@enp0s8.service
exited ● ▲
        |  ifupdown-pre.service
exited ●
        |  ifupdown-wait-online.service
————————┼———————————————————————————————————————————————————————————————————————
————————————————————————————————
query service status (display output with F2)
[press F3 for help]
```

- Deja, įrankis `serman2` turi trūkumų:
  - Ne visada teisingai nuskaito tarnybų `Enabled` būseną.

    - Taip pat šios būsenos perjungimui (ir kitiems veiksmams) naudoja ne visai intuityvų UI:
        - pagalba kviečiama klavišu `F3`;
        - veiksmo tipas pasirenkamas kairiame stulpelyje, tarnybos – sąraše dešinėje;
        - tarp jų persijungiama klavišais `Right`, `Left`;
        - tarnybas veiksmui įvykdyti reikia pasirinkti klavišu `Space`;
        - veiksmas įvykdomas klavišu `Enter`;
        - rezultatas pasižiūrimas klavišus `F3` atskirame vaizde;
        - grįžtama į pradinį vaizdą paspaudus `Enter`;
        - programa uždaroma paspaudus `Ctrl-C`;
        - užuominos (angl. *Hint*) eilutė pradingsta po pirmojo vaizdo perjungimo ir grįžimo.
    - Taip pat įrankis rodo ne tik tarnybų (`.service`), bet ir kitų SystemD vienetų būsenas:
        - `.automount`
        - `.device`
        - `.mount`
        - `.path`
        - `.scope`
        - `.slice`
        - `.socket`
        - `.swap`
        - `.target`
        - `.timer`
- Susirandu kitą įrankį, `chkservice`
    - Diegiu:

```
osboxes@ldvm1:~$ apt-cache search chkservice
chkservice - Tool for managing systemd units
osboxes@ldvm1:~$
osboxes@ldvm1:~$ sudo apt-get install chkservice
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  chkservice
0 upgraded, 1 newly installed, 0 to remove and 159 not upgraded.
Need to get 41.3 kB of archives.
After this operation, 188 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 chkservice amd64
0.3-1build1 [41.3 kB]
Fetched 41.3 kB in 1s (58.7 kB/s)
Selecting previously unselected package chkservice.
(Reading database ... 192778 files and directories currently installed.)
Preparing to unpack .../chkservice_0.3-1build1_amd64.deb ...
Unpacking chkservice (0.3-1build1) ...
Setting up chkservice (0.3-1build1) ...
Processing triggers for man-db (2.9.1-1) ...
```

- Išbandau `chkservice`:

```
osboxes@ldvm1:~/src$ sudo chkservice

----8><----------------------------------------------------------------------------
--------------------------><8----
 Failed: Connection reset by peer

  -m-     kbd.service                                    kbd.service
  [x]  >  kerneloops.service                             Tool to automatically
collect and submit kernel crash
  [x]  =  keyboard-setup.service                         Set the console
keyboard layout
  [s]  =  kmod-static-nodes.service                      Create list of static
device nodes for the current ker
  [s]     kmod.service
/lib/systemd/system/kmod.service
  [s]  =  logrotate.service                              Rotate log files
> [x]  =  ModemManager.service                          Modem Manager
<
  [s]  =  man-db.service                                 Daily man-db
regeneration
  [s]     modprobe@.service
/lib/systemd/system/modprobe@.service
  [s]  =  modprobe@drm.service                           Load Kernel Module drm
  [s]  =  motd-news.service                              Message of the Day
  [x]  >  mysql.service                                  MySQL Community Server
  [x]     NetworkManager-dispatcher.service
/lib/systemd/system/NetworkManager-dispatcher.service
  [x]  =  NetworkManager-wait-online.service             Network Manager Wait
Online
  [x]  >  NetworkManager.service                         Network Manager
  [x]  =  netplan-ovs-cleanup.service                    OpenVSwitch
configuration for cleanup

                                                        92/533
----8><----------------------------------------------------------------------------
--------------------------><8----
```

- Norint uždrausti tarnybą ir paspaudus `Space`, gaunu klaidą `Failed: Connection reset by peer`.
  Taip yra dėl klaidos programoje: https://github.com/linuxenko/chkservice/issues/12
- Imu pataisytą programos kodą iš GitHub: https://github.com/nufeng1999/chkservice

```
osboxes@ldvm1:~$ cd src

osboxes@ldvm1:~/src$ git clone https://github.com/nufeng74/chkservice.git
Cloning into 'chkservice'...
remote: Enumerating objects: 424, done.
remote: Counting objects: 100% (7/7), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 424 (delta 1), reused 4 (delta 1), pack-reused 417
Receiving objects: 100% (424/424), 98.22 KiB | 1.51 MiB/s, done.
Resolving deltas: 100% (264/264), done.

osboxes@ldvm1:~/src$ cd chkservice
osboxes@ldvm1:~/src/chkservice$ mkdir build
osboxes@ldvm1:~/src/chkservice$ cd build

osboxes@ldvm1:~/src/chkservice/build$ cmake -DCMAKE_INSTALL_PREFIX=/usr ..

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

sudo snap install cmake  # version 3.20.5, or
sudo apt  install cmake  # version 3.16.3-1ubuntu1

See 'snap info cmake' for additional versions.
```

- Diegiu kūrimo priemones:

```
osboxes@ldvm1:~/src/chkservice/build$ sudo apt-get install cmake g++ libsystemd-
dev libncurses-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  cmake-doc ninja-build g++-multilib ncurses-doc
The following NEW packages will be installed:
  cmake g++ libncurses-dev libsystemd-dev
0 upgraded, 4 newly installed, 0 to remove and 153 not upgraded.
Need to get 0 B/4,256 kB of archives.
After this operation, 22.6 MB of additional disk space will be used.
Selecting previously unselected package cmake.
(Reading database ... 196958 files and directories currently installed.)
Preparing to unpack .../cmake_3.16.3-1ubuntu1_amd64.deb ...
Unpacking cmake (3.16.3-1ubuntu1) ...
Selecting previously unselected package g++.
Preparing to unpack .../g++_4%3a9.3.0-1ubuntu2_amd64.deb ...
Unpacking g++ (4:9.3.0-1ubuntu2) ...
Selecting previously unselected package libncurses-dev:amd64.
Preparing to unpack .../libncurses-dev_6.2-0ubuntu2_amd64.deb ...
Unpacking libncurses-dev:amd64 (6.2-0ubuntu2) ...
Selecting previously unselected package libsystemd-dev:amd64.
Preparing to unpack .../libsystemd-dev_245.4-4ubuntu3.7_amd64.deb ...
Unpacking libsystemd-dev:amd64 (245.4-4ubuntu3.7) ...
Setting up libncurses-dev:amd64 (6.2-0ubuntu2) ...
Setting up g++ (4:9.3.0-1ubuntu2) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto
mode
Setting up cmake (3.16.3-1ubuntu1) ...
Setting up libsystemd-dev:amd64 (245.4-4ubuntu3.7) ...
Processing triggers for man-db (2.9.1-1) ...
```

- Kompiliuoju įrankį:

```
osboxes@ldvm1:~/src/chkservice/build$ cmake ..
-- The C compiler identification is GNU 9.3.0
-- The CXX compiler identification is GNU 9.3.0
-- Check for working C compiler: /usr/bin/cc
-- Check for working C compiler: /usr/bin/cc -- works
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Detecting C compile features
-- Detecting C compile features - done
-- Check for working CXX compiler: /usr/bin/c++
-- Check for working CXX compiler: /usr/bin/c++ -- works
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Detecting CXX compile features
-- Detecting CXX compile features - done
-- DEBUG mode disabled
-- Local build
-- Found PkgConfig: /usr/bin/pkg-config (found version "0.29.1")
-- Checking for module 'libsystemd'
--   Found libsystemd, version 245
-- Checking for module 'ncurses'
--   Found ncurses, version 6.2.20200212
-- Configuring done
-- Generating done
-- Build files have been written to: /home/osboxes/src/chkservice/build

osboxes@ldvm1:~/src/chkservice/build$ make chkservice
Scanning dependencies of target CHKSYSTEMD
[ 10%] Building CXX object src/CMakeFiles/CHKSYSTEMD.dir/chk-systemd.cpp.o
[ 20%] Building CXX object src/CMakeFiles/CHKSYSTEMD.dir/chk-systemd-utils.cpp.o
[ 30%] Linking CXX static library libCHKSYSTEMD.a
[ 30%] Built target CHKSYSTEMD
[ 40%] Building CXX object src/CMakeFiles/CHKCTL.dir/chk-ctl.cpp.o
[ 50%] Linking CXX static library libCHKCTL.a
[ 50%] Built target CHKCTL
[ 60%] Building CXX object src/CMakeFiles/CHKUI.dir/chk-wmain.cpp.o
  ...
[ 70%] Building CXX object src/CMakeFiles/CHKUI.dir/chk-wutils.cpp.o
[ 80%] Linking CXX static library libCHKUI.a
[ 80%] Built target CHKUI
[ 90%] Building CXX object src/CMakeFiles/chkservice.dir/chkservice.cpp.o
[100%] Linking CXX executable chkservice
[100%] Built target chkservice
```

- Išbandau pataisymą:

```
osboxes@ldvm1:~/src/chkservice/build$ ll src/chkservice
-rwxrwxr-x 1 osboxes osboxes 94344 Jul  4 15:27 src/chkservice*

osboxes@ldvm1:~/src/chkservice/build$ sudo src/chkservice
----8><---------------------------------------------------------------------
-------------------------><8----


  [x]  >  irqbalance.service                              irqbalance daemon
  -m-     kbd.service                                     kbd.service
  [x]  >  kerneloops.service                              Tool to automatically
collect and submit kernel crash
  [x]  =  keyboard-setup.service                          Set the console
keyboard layout
  [s]  =  kmod-static-nodes.service                       Create list of static
device nodes for the current ker
  [s]     kmod.service
/lib/systemd/system/kmod.service
  [s]  =  logrotate.service                               Rotate log files
> [ ]     ModemManager.service
/lib/systemd/system/ModemManager.service                <
  [s]  =  man-db.service                                  Daily man-db
regeneration
  [s]     modprobe@.service
/lib/systemd/system/modprobe@.service
  [s]  =  modprobe@drm.service                            Load Kernel Module drm
  [s]  =  motd-news.service                               Message of the Day
  [x]  >  mysql.service                                   MySQL Community Server
  [x]     NetworkManager-dispatcher.service
/lib/systemd/system/NetworkManager-dispatcher.service
  [x]  =  NetworkManager-wait-online.service              Network Manager Wait
Online
  [x]  >  NetworkManager.service                          Network Manager

                                                         91/532
----8><---------------------------------------------------------------------
-------------------------><8----
```

Ties `ModemManager` paspaudus `Space`, tarnyba dabar išsijungia jau iškart.

- `chkservice` trūkumai:
  - Nevystomas, autorės apleistas.
  - Nevisai intuityvus TUI (*Text User Interface*);
    - Pagalbos klavišas `?`;
    - Paieška randa tik pirmą rezultatą;
    - Neaprašytas būsenos stulpelis:
      - `=` – sustabdyta tarnyba;
      - `>` – veikianti tarnyba.

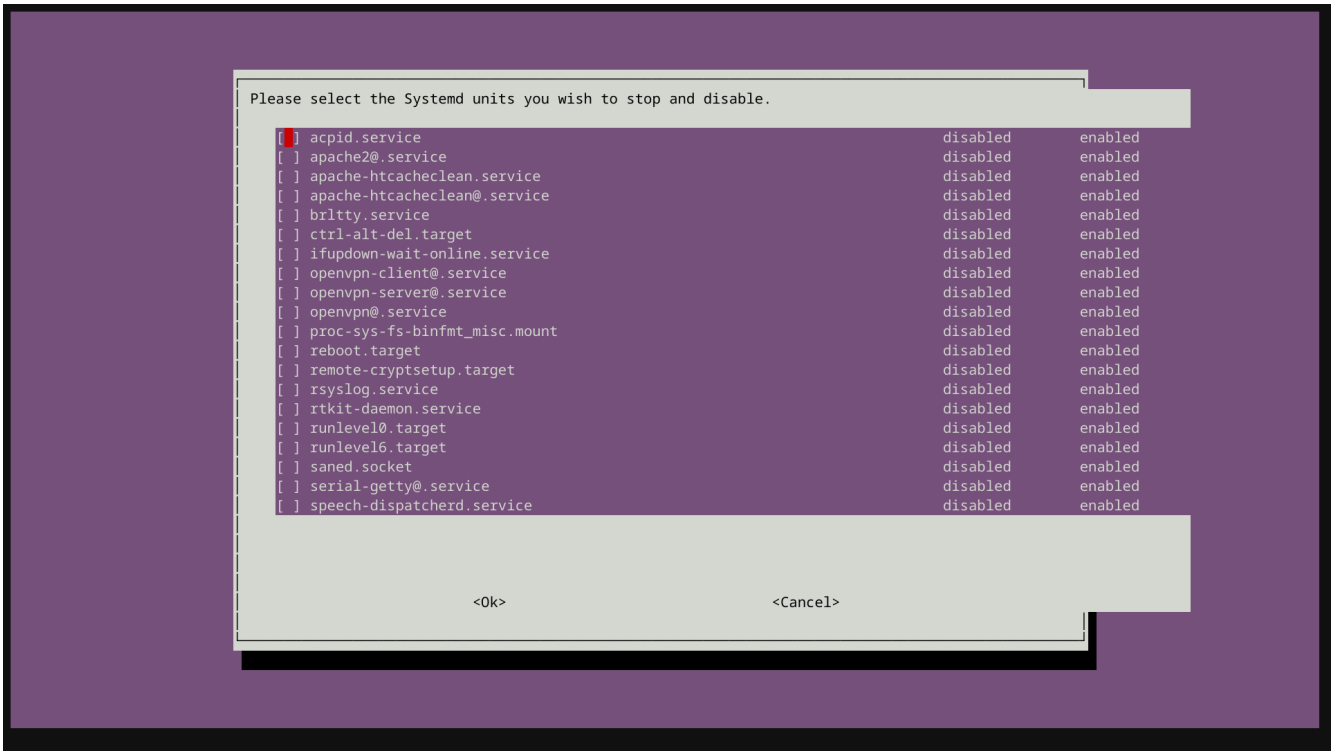
- Susirandu dar vieną įrankį, `systemctl-ui`.
  - Pasiimu jį iš GitHub:

```
osboxes@ldvm1:~/src$ git clone https://github.com/mpbcode/systemctl-ui
Cloning into 'systemctl-ui'...
remote: Enumerating objects: 7, done.
remote: Total 7 (delta 0), reused 0 (delta 0), pack-reused 7
Unpacking objects: 100% (7/7), 14.05 KiB | 1.76 MiB/s, done.
```

  - Diegiu Lua interpretatorių:

```
osboxes@ldvm1:~/src$ sudo apt-get install lua5.3
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  lua5.3
0 upgraded, 1 newly installed, 0 to remove and 153 not upgraded.
Need to get 0 B/110 kB of archives.
After this operation, 414 kB of additional disk space will be used.
Selecting previously unselected package lua5.3.
(Reading database ... 197606 files and directories currently installed.)
Preparing to unpack .../lua5.3_5.3.3-1.1ubuntu2_amd64.deb ...
Unpacking lua5.3 (5.3.3-1.1ubuntu2) ...
Setting up lua5.3 (5.3.3-1.1ubuntu2) ...
update-alternatives: using /usr/bin/lua5.3 to provide /usr/bin/lua (lua-
interpreter) in auto mode
update-alternatives: using /usr/bin/luac5.3 to provide /usr/bin/luac (lua-
compiler) in auto mode
Processing triggers for man-db (2.9.1-1) ...
```

  - Tikrinu įrankį:



- Deja, jis rodo tik uždraustas (*Disabled*) tarnybas: https://github.com/mpbcode/systemctl-ui/issues/1

3. Tinklo paslaugų tikrinimas

Sunkumų neaptikta.

4. Kaimyno skenavimas

Sunkumų neaptikta.

Gal tik toks neaiškumas iš 2LD, kuriuose tiksliai kompiuteriuose reikėjo diegti žiniatinklio ir DB paslaugas.

5. Paketų persiuntimo įjungimas

Sunkumų neaptikta.

6. `iptables` patikrinimas

Sunkumų neaptikta.

7. Kompiuterio apsaugojimas nuo resursus išnaudojančio ICMP srauto

Nustatau apribojimą 1 šalt./s

- Deja, virtualaus kompiuterio reakcija į *ping* srautą nepasikeitė.
  Įtarimų sukėlė `-j ACCEPT` ir `Chain INPUT (policy ACCEPT).`
- Papildau, kad `iptables` atmestų visus ICMP paketus, neatitikusius šios taisyklės:

```
osboxes@ldvm1:~$ sudo iptables -A INPUT -p icmp -j DROP
osboxes@ldvm1:~$ sudo iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             limit: avg 1/sec burst
1
DROP       icmp --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
```

- Vėl paleidžiu *ping* srautą:

```
[p@localhost Saulius-Krasuckas]$ ping 192.168.10.14
PING 192.168.10.14 (192.168.10.14) 56(84) bytes of data.
64 bytes from 192.168.10.14: icmp_seq=2 ttl=64 time=0.771 ms
64 bytes from 192.168.10.14: icmp_seq=4 ttl=64 time=0.665 ms
64 bytes from 192.168.10.14: icmp_seq=6 ttl=64 time=0.623 ms
64 bytes from 192.168.10.14: icmp_seq=8 ttl=64 time=0.636 ms
^C
--- 192.168.10.14 ping statistics ---
8 packets transmitted, 4 received, 50% packet loss, time 7000ms
rtt min/avg/max/mdev = 0.623/0.673/0.771/0.066 ms
```

8. *Telnet* uždraudimas

- Tačiau tai yra užklausų ne uždraudimas, o tik jų registravimas. Uždraudimui reikėtų papildomos taisyklės su `-j DROP`.
- Uždraudžiu *Telnet* užklausas iš tikrųjų:

```
osboxes@ldvm1:~$ sudo iptables -A INPUT -d 192.168.10.14 -p tcp --dport 23 -j DROP
osboxes@ldvm1:~$ sudo iptables --list
[sudo] password for osboxes:
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
LOG        tcp  --  anywhere             ldvm1                tcp dpt:telnet LOG
level warning prefix "TELNET ATTEMPT: "
DROP       tcp  --  anywhere             ldvm1                tcp dpt:telnet

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

- Kreipiuosi iš kaimyninio kompiuterio į savo virtualųjį:

```
osboxes@ldvm2:~$ time telnet 192.168.10.14
Trying 192.168.10.14...
telnet: Unable to connect to remote host: Connection timed out

real    2m9.458s
user    0m0.003s
sys     0m0.008s
```

- Šįkart užklausa trunka ilgai, ir irgi nesėkminga.
- Dabar virtualiojo kompiuterio žurnalas pasipildė net septyniais įrašais apie užklausą:

```
osboxes@ldvm1:~$ tail -0f /var/log/syslog
Jul  5 10:13:59 ldvm1 tracker-store[1682]: OK
Jul  5 10:13:59 ldvm1 systemd[997]: tracker-store.service: Succeeded.
Jul  5 10:14:06 ldvm1 kernel: [ 8339.632492] TELNET ATTEMPT: IN=enp0s8 OUT=
MAC=08:00:27:40:2c:f6:0a:00:27:00:00:00:08:00 SRC=192.168.10.254 DST=192.168.10.14
LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=9577 DF PROTO=TCP SPT=52736 DPT=23 WINDOW=29200
RES=0x00 SYN URGP=0
Jul  5 10:14:07 ldvm1 kernel: [ 8340.609642] TELNET ATTEMPT: IN=enp0s8 OUT=
MAC=08:00:27:40:2c:f6:0a:00:27:00:00:00:08:00 SRC=192.168.10.254 DST=192.168.10.14
LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=9578 DF PROTO=TCP SPT=52736 DPT=23 WINDOW=29200
RES=0x00 SYN URGP=0
Jul  5 10:14:09 ldvm1 kernel: [ 8342.562629] TELNET ATTEMPT: IN=enp0s8 OUT=
MAC=08:00:27:40:2c:f6:0a:00:27:00:00:00:08:00 SRC=192.168.10.254 DST=192.168.10.14
LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=9579 DF PROTO=TCP SPT=52736 DPT=23 WINDOW=29200
RES=0x00 SYN URGP=0
Jul  5 10:14:13 ldvm1 kernel: [ 8346.473122] TELNET ATTEMPT: IN=enp0s8 OUT=
MAC=08:00:27:40:2c:f6:0a:00:27:00:00:00:08:00 SRC=192.168.10.254 DST=192.168.10.14
LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=9580 DF PROTO=TCP SPT=52736 DPT=23 WINDOW=29200
RES=0x00 SYN URGP=0
Jul  5 10:14:21 ldvm1 kernel: [ 8354.294072] TELNET ATTEMPT: IN=enp0s8 OUT=
MAC=08:00:27:40:2c:f6:0a:00:27:00:00:00:08:00 SRC=192.168.10.254 DST=192.168.10.14
LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=9581 DF PROTO=TCP SPT=52736 DPT=23 WINDOW=29200
RES=0x00 SYN URGP=0
Jul  5 10:14:38 ldvm1 kernel: [ 8369.935750] TELNET ATTEMPT: IN=enp0s8 OUT=
MAC=08:00:27:40:2c:f6:0a:00:27:00:00:00:08:00 SRC=192.168.10.254 DST=192.168.10.14
LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=9582 DF PROTO=TCP SPT=52736 DPT=23 WINDOW=29200
RES=0x00 SYN URGP=0
Jul  5 10:15:10 ldvm1 kernel: [ 8401.219388] TELNET ATTEMPT: IN=enp0s8 OUT=
MAC=08:00:27:40:2c:f6:0a:00:27:00:00:00:08:00 SRC=192.168.10.254 DST=192.168.10.14
LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=9583 DF PROTO=TCP SPT=52736 DPT=23 WINDOW=29200
RES=0x00 SYN URGP=0
Jul  5 10:17:02 ldvm1 CRON[1816]: (root) CMD (   cd / && run-parts --report
/etc/cron.hourly)
```

- Tad panašu, kad dabar ji tikrai atmetama (ir todėl kartojama).

9. Automatinė taisyklių keltis

- Patikrinu iptables taisykles – deja, jos neužsikrovė:

```
osboxes@ldvm1:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

- Iš patirties žinau, kad automatiniam scenarijaus startui reikalinga papildoma simbolinė nuoroda.
  Ji turi būti `/etc/init.d/rc?.d` direktorijoje, kur `?` atitinka pageidaujamą *Runlevel*.
- Nustatau dabartinį *Runlevel*:

  ```
  osboxes@ldvm1:~$ runlevel
  N 3
  ```

- Patikrinu reikiamą direktoriją:

```
osboxes@ldvm1:~$ ll /etc/rc3.d/
total 16
drwxr-xr-x   2 root root  4096 Jul  3 01:07 ./
drwxr-xr-x 132 root root 12288 Jul  5 12:20 ../
lrwxrwxrwx   1 root root    29 Jun 30 12:08 K01apache-htcacheclean ->
../init.d/apache-htcacheclean*
lrwxrwxrwx   1 root root    27 Mar  7 00:02 K01speech-dispatcher ->
../init.d/speech-dispatcher*
lrwxrwxrwx   1 root root    15 Mar  7 00:02 S01acpid -> ../init.d/acpid*
lrwxrwxrwx   1 root root    17 Mar  7 00:02 S01anacron -> ../init.d/anacron*
lrwxrwxrwx   1 root root    17 Jun 30 12:08 S01apache2 -> ../init.d/apache2*
lrwxrwxrwx   1 root root    16 Mar  7 00:02 S01apport -> ../init.d/apport*
lrwxrwxrwx   1 root root    22 Mar  7 00:02 S01avahi-daemon -> ../init.d/avahi-
daemon*
lrwxrwxrwx   1 root root    19 Mar  7 00:02 S01bluetooth -> ../init.d/bluetooth*
lrwxrwxrwx   1 root root    26 Mar  7 00:02 S01console-setup.sh ->
../init.d/console-setup.sh*
lrwxrwxrwx   1 root root    14 Mar  7 00:02 S01cron -> ../init.d/cron*
lrwxrwxrwx   1 root root    14 Mar  7 00:02 S01cups -> ../init.d/cups*
lrwxrwxrwx   1 root root    22 Mar  7 00:02 S01cups-browsed -> ../init.d/cups-
browsed*
lrwxrwxrwx   1 root root    14 Mar  7 00:02 S01dbus -> ../init.d/dbus*
lrwxrwxrwx   1 root root    14 Mar  7 00:02 S01gdm3 -> ../init.d/gdm3*
lrwxrwxrwx   1 root root    21 Mar  7 00:02 S01grub-common -> ../init.d/grub-common*
lrwxrwxrwx   1 root root    20 Mar  7 00:02 S01irqbalance -> ../init.d/irqbalance*
lrwxrwxrwx   1 root root    20 Mar  7 00:02 S01kerneloops -> ../init.d/kerneloops*
lrwxrwxrwx   1 root root    15 Jun 30 12:08 S01mysql -> ../init.d/mysql*
lrwxrwxrwx   1 root root    17 Mar  7 00:02 S01openvpn -> ../init.d/openvpn*
lrwxrwxrwx   1 root root    18 Mar  7 00:02 S01plymouth -> ../init.d/plymouth*
lrwxrwxrwx   1 root root    37 Mar  7 00:02 S01pulseaudio-enable-autospawn ->
../init.d/pulseaudio-enable-autospawn*
lrwxrwxrwx   1 root root    15 Mar  7 00:02 S01rsync -> ../init.d/rsync*
lrwxrwxrwx   1 root root    17 Mar  7 00:02 S01rsyslog -> ../init.d/rsyslog*
lrwxrwxrwx   1 root root    15 Mar  7 00:02 S01saned -> ../init.d/saned*
lrwxrwxrwx   1 root root    23 Mar  7 00:02 S01spice-vdagent -> ../init.d/spice-
vdagent*
lrwxrwxrwx   1 root root    13 Jun 29 11:37 S01ssh -> ../init.d/ssh*
lrwxrwxrwx   1 root root    29 Mar  7 00:02 S01unattended-upgrades ->
../init.d/unattended-upgrades*
lrwxrwxrwx   1 root root    15 Mar  7 00:02 S01uuidd -> ../init.d/uuidd*
lrwxrwxrwx   1 root root    32 Mar  7 00:15 S01virtualbox-guest-utils ->
../init.d/virtualbox-guest-utils*
lrwxrwxrwx   1 root root    18 Mar  7 00:02 S01whoopsie -> ../init.d/whoopsie*
```

- Čia kuriu simbolinę nuorodą:

```
osboxes@ldvm1:~$ sudo ln -sv /etc/init.d/myfirewall /etc/rc3.d/S99myfirewall
'/etc/rc3.d/S99myfirewall' -> '/etc/init.d/myfirewall'
```

- Dar sykį perkraunu virtualų kompiuterį:

```
osboxes@ldvm1:~$ sudo reboot
Connection to 192.168.10.14 closed by remote host.
Connection to 192.168.10.14 closed.
```

10. Apsaugoto kompiuterio skenavimas

- Skenuoju kaimyną, bet gaunu klaidą:

```
osboxes@ldvm2:~$ sudo nmap -sS -P0 -n -F --max_rtt_timeout 6 192.168.10.14
nmap: unrecognized option '--max_rtt_timeout'
See the output of nmap -h for a summary of options.
```

- Tikrinu `nmap` versiją:

```
osboxes@ldvm2:~$ nmap --version
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1d nmap-libssh2-1.8.2 libz-1.2.11 libpcre-
8.39 libpcap-1.9.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Pasirinktosios `iptables` komandos aprašymas

Komandą (o tiksliau tris beveik identiškas) pasirinkau iš šių pavyzdžių:

https://www.thegeekstuff.com/2011/06/iptables-rules-examples/#:~:text=11.%20Load%20Balance%20Incoming%20Web%20Traffic

```
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter
0 --every 3 --packet 0 -j DNAT --to-destination 192.168.1.101:443
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter
0 --every 3 --packet 1 -j DNAT --to-destination 192.168.1.102:443
iptables -A PREROUTING -i eth0 -p tcp --dport 443 -m state --state NEW -m nth --counter
0 --every 3 --packet 2 -j DNAT --to-destination 192.168.1.103:443
```

Originaliose komandose yra klaida:

tūksta nurodytos lentelės `nat`, nes kitaip komanda bando rašyti į `filter` lentelę, ir joje neranda grandinės `PREROUTING`.

Taigi, komandas pataisau:

```
iptables -t nat -A PREROUTING -i eth0 <...>
iptables -t nat -A PREROUTING -i eth0 <...>
iptables -t nat -A PREROUTING -i eth0 <...>
```

Ši komanda naudoja nestandartinį `iptables` modulį `state` (angl. *Extension module*). Jis aprašytas čia: https://www.netfilter.org/documentation/HOWTO/netfilter-extensions-HOWTO-3.html#ss3.9

- Šios komandos papildo `nat` lentelę.
- Lentelė naudojama maršrutizavimo sprendimų priėmimui (taisymui).
- Kiekviena ši komanda:
  - tikrina, ar paketas ateina per tinklo sąsają `eth0`;
  - tikrina, ar jo transportinis protokolas yra TCP;
  - tikrina, ar paskirties prievadas yra HTTPS (443/TCP);
  - įjungia modulį `state` (angl. *Extension module*);
  - tikrina, ar tai nauja TCP sesija;
  - įjungia modulį `nth`;

    - pasirenka skaitiklį #0;
    - nustato skaitiklio #0 talpą = 3;
    - tikrina, ar paketo numeris skaitiklyje yra vienas iš trijų:
        - = 0
        - = 1
        - = 2
    - ir jei šios sąlygos patenkintos, komanda nurodo tokį paketą nukreipti į vieną iš trijų IP adresų (pagal paketo numerį nurodytame skaitiklyje):
        - 192.168.1.101
        - 192.168.1.102
        - 192.168.1.103
    - … pritaikant paketui atitinkamą `Destination NAT` transliaciją.
    - … ir išlaikant tą patį paskirties prievadą (*Destination port*) – `443/TCP`.

Kiekvienos šios komandos tikslas – gaunamą HTTPS srautą po lygiai (paketų skaičiaus atžvilgiu) ir iš eilės (angl. *Round-robin*) išskirstyti į tris HTTPS gavėjus. Pvz.:

- žiniatinklio serverius,
- Proxy serverius,
- L7 ugniasienes
- ar kitus su HTTPS apdorojančius tinklo įrenginius.

Kitaip sakant, tikslas – atlikti HTTPS apkrovos paskirstymą (angl. *Load balancing*) tarp trijų tinklo mazgų.