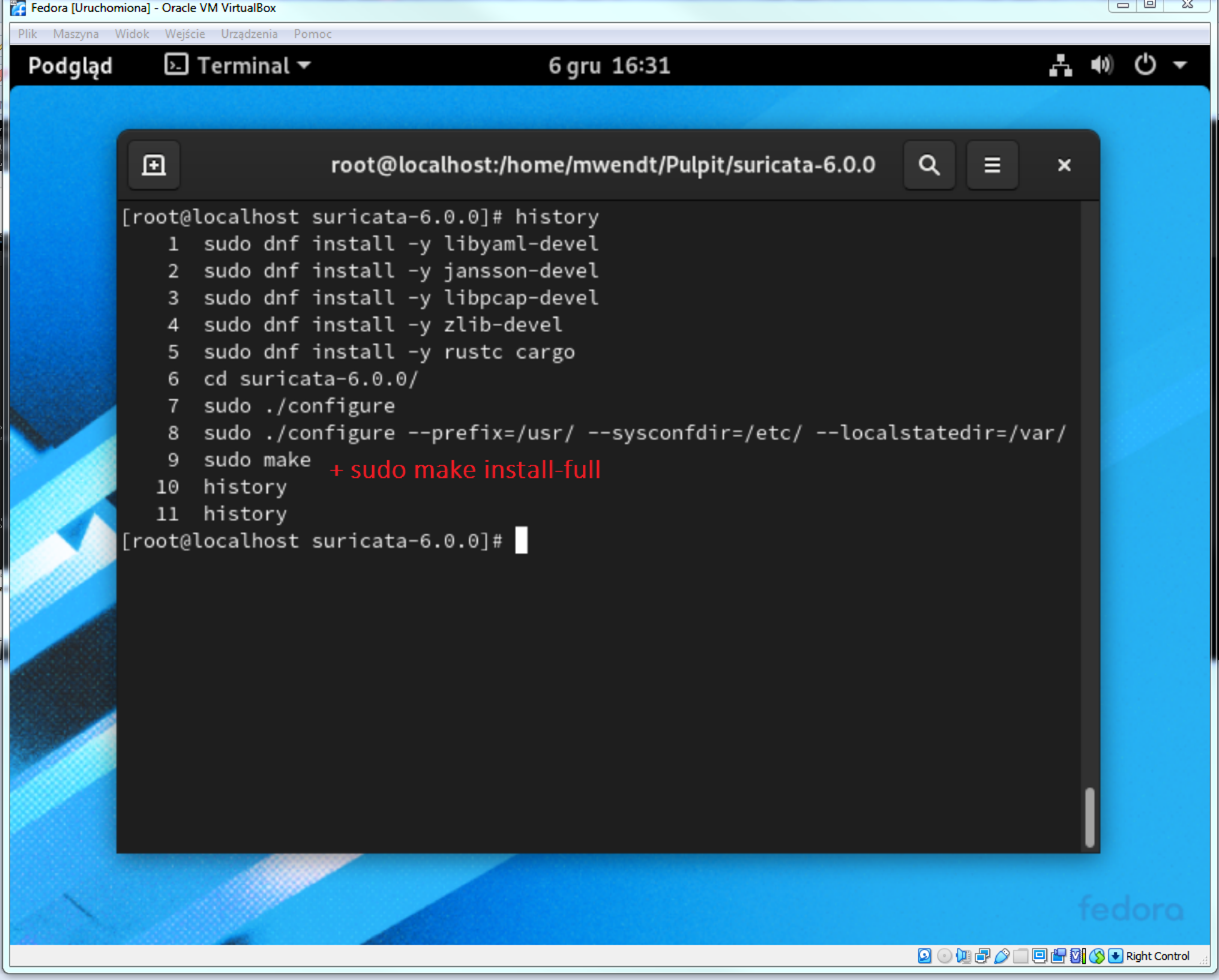
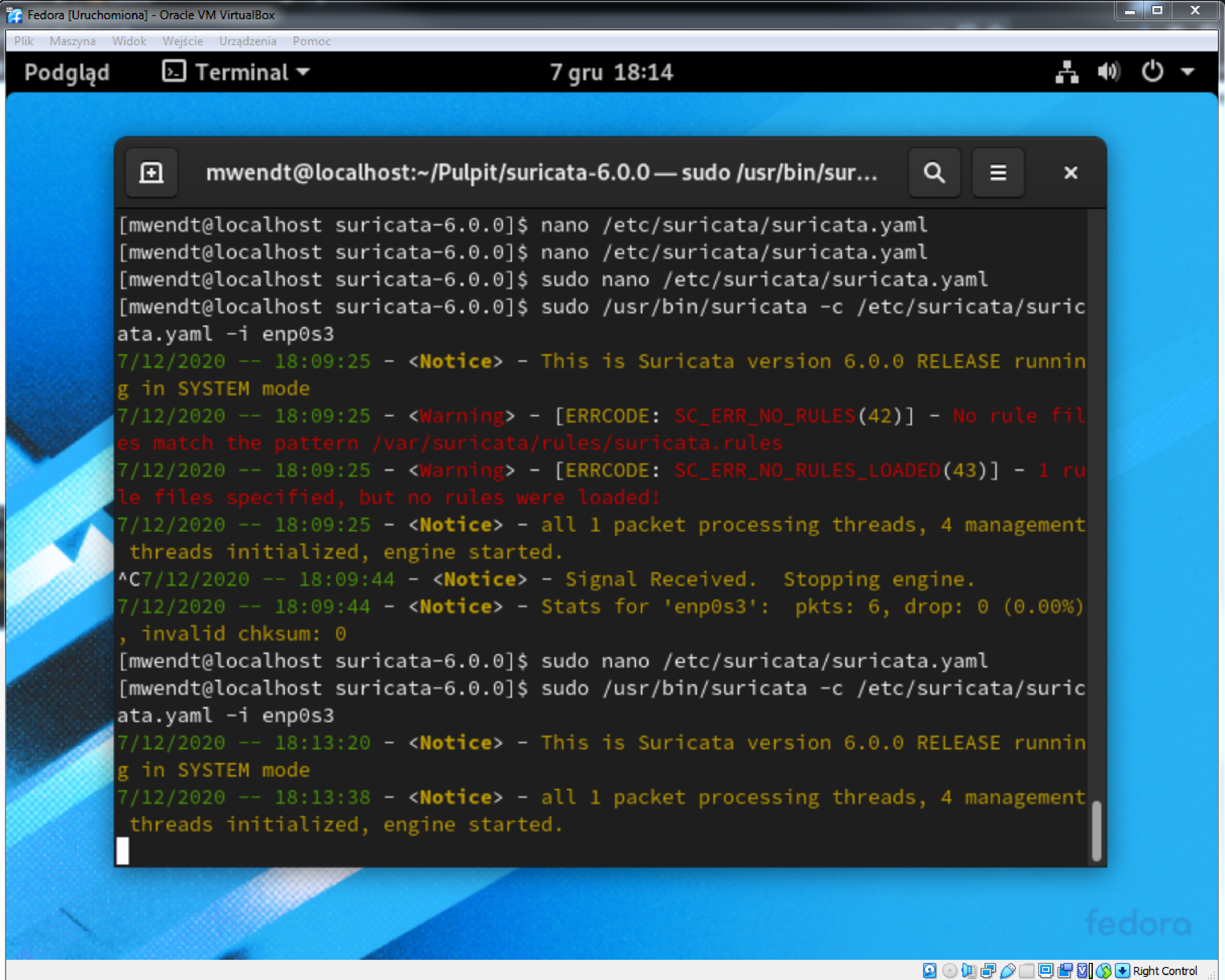
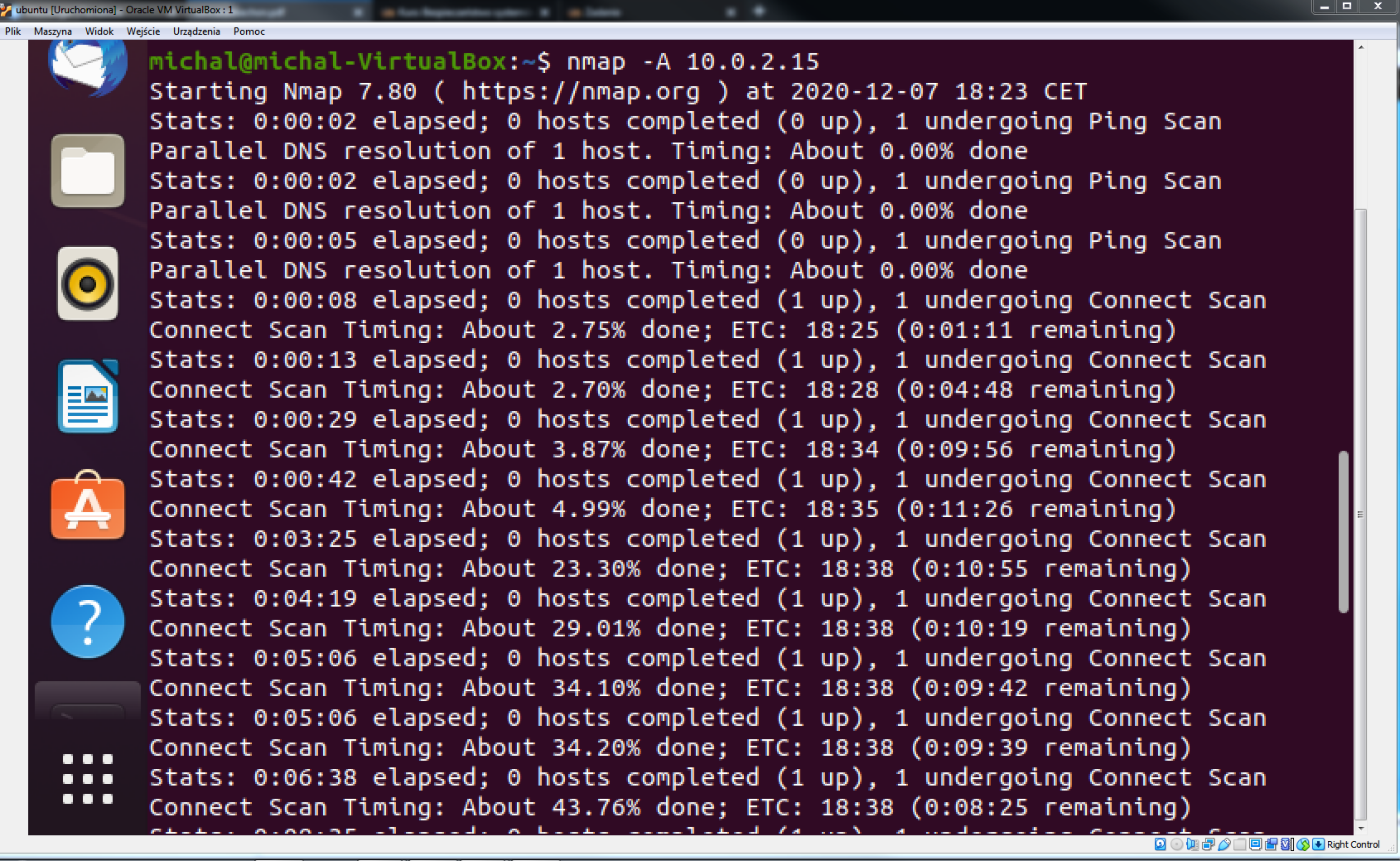

Fedora [Uruchomiona] - Oracle VM VirtualBox
Plik
Maszyna
Widok
Wejście
Urządzenia
Pomoc
Podgląd
Terminal
6 gru 16:31
root@localhost:/home/mwendt/Pulpit/suricata-6.0.0
fedora
Right Control

```
[root@localhost suricata-6.0.0]# history
    1  sudo dnf install -y libyaml-devel
    2  sudo dnf install -y jansson-devel
    3  sudo dnf install -y libpcap-devel
    4  sudo dnf install -y zlib-devel
    5  sudo dnf install -y rustc cargo
    6  cd suricata-6.0.0/
    7  sudo ./configure
    8  sudo ./configure --prefix=/usr/ --sysconfdir=/etc/ --localstatedir=/var/
    9  sudo make
   10  history
   11  history
[root@localhost suricata-6.0.0]# 
```

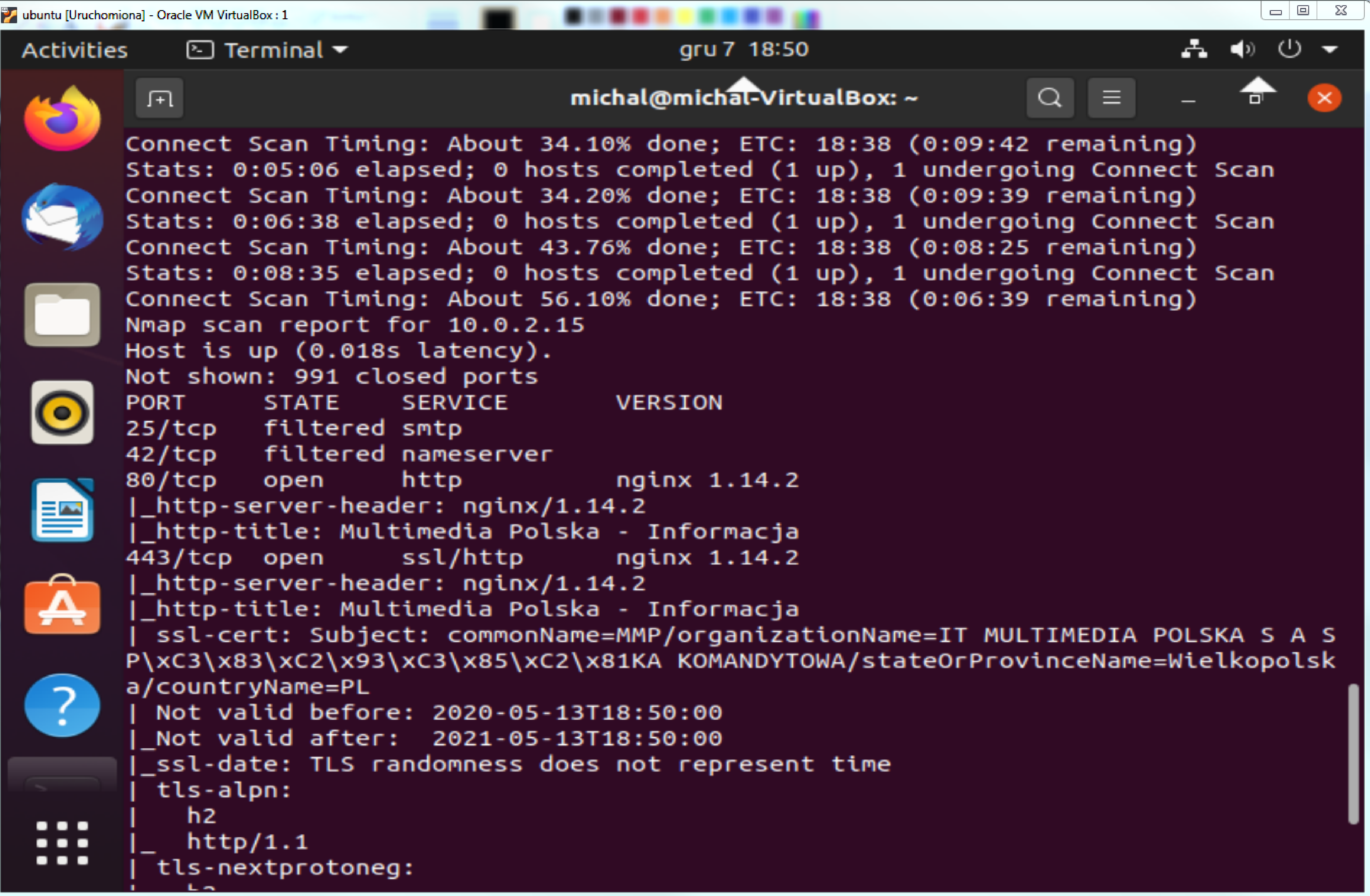
+ sudo make install-full


Fedora [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc
Podgląd
Terminal
7 gru 18:14
mwendt@localhost:~/Pulpit/suricata-6.0.0 — sudo /usr/bin/sur...
fedora
Right Control

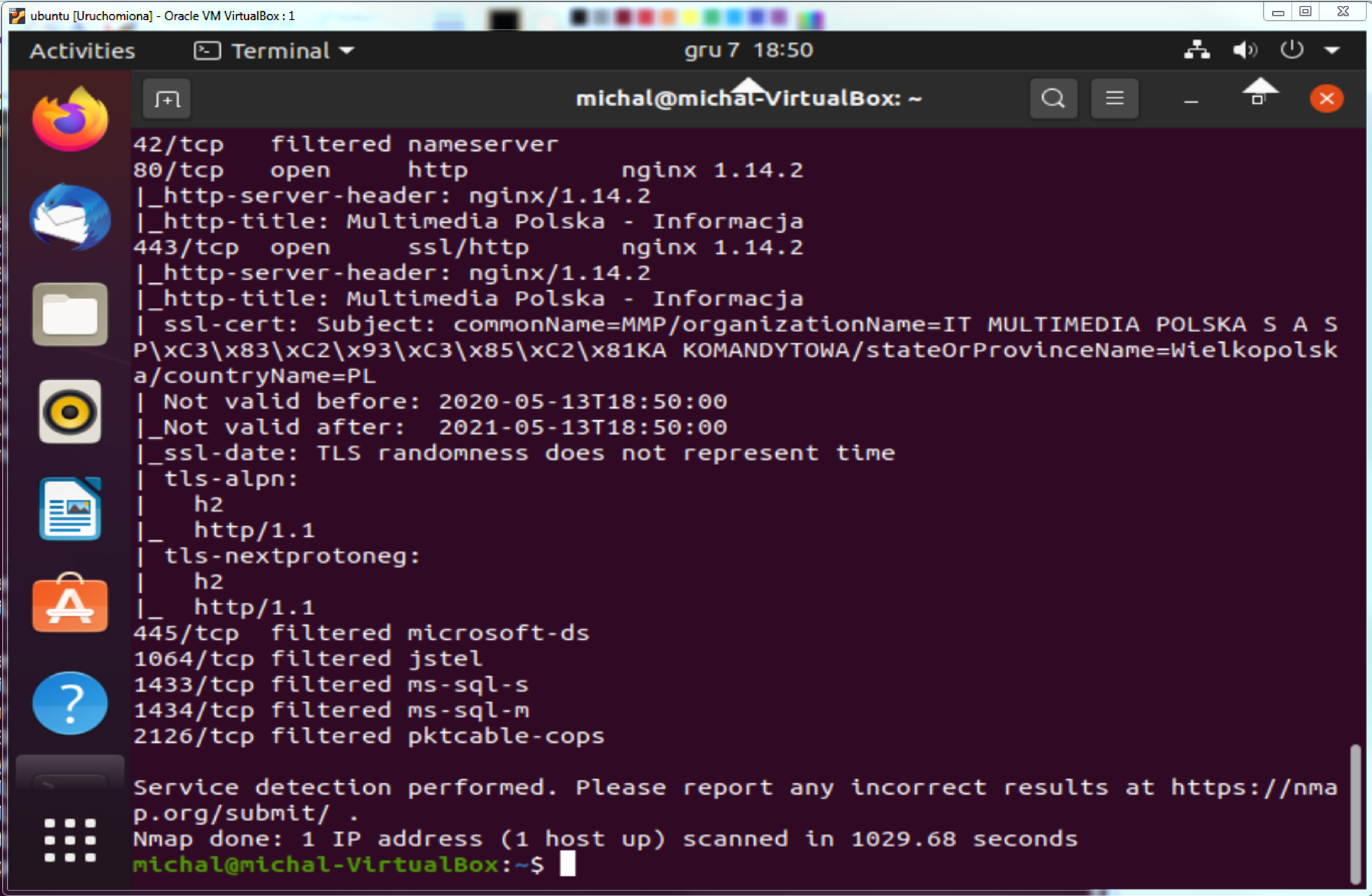
```
[mwendt@localhost suricata-6.0.0]$ nano /etc/suricata/suricata.yaml
[mwendt@localhost suricata-6.0.0]$ nano /etc/suricata/suricata.yaml
[mwendt@localhost suricata-6.0.0]$ sudo nano /etc/suricata/suricata.yaml
[mwendt@localhost suricata-6.0.0]$ sudo /usr/bin/suricata -c /etc/suricata/suric
ata.yaml -i enp0s3
7/12/2020 -- 18:09:25 - <Notice> - This is Suricata version 6.0.0 RELEASE runnin
g in SYSTEM mode
7/12/2020 -- 18:09:25 - <Warning> - [ERRCODE: SC_ERR_NO_RULES(42)] - No rule fil
es match the pattern /var/suricata/rules/suricata.rules
7/12/2020 -- 18:09:25 - <Warning> - [ERRCODE: SC_ERR_NO_RULES_LOADED(43)] - 1 ru
le files specified, but no rules were loaded!
7/12/2020 -- 18:09:25 - <Notice> - all 1 packet processing threads, 4 management
 threads initialized, engine started.
^C7/12/2020 -- 18:09:44 - <Notice> - Signal Received.  Stopping engine.
7/12/2020 -- 18:09:44 - <Notice> - Stats for 'enp0s3':  pkts: 6, drop: 0 (0.00%)
, invalid chksum: 0
[mwendt@localhost suricata-6.0.0]$ sudo nano /etc/suricata/suricata.yaml
[mwendt@localhost suricata-6.0.0]$ sudo /usr/bin/suricata -c /etc/suricata/suric
ata.yaml -i enp0s3
7/12/2020 -- 18:13:20 - <Notice> - This is Suricata version 6.0.0 RELEASE runnin
g in SYSTEM mode
7/12/2020 -- 18:13:38 - <Notice> - all 1 packet processing threads, 4 management
 threads initialized, engine started.
```



```
michal@michal-VirtualBox:~$ nmap -A 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-07 18:23 CET
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 2.75% done; ETC: 18:25 (0:01:11 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 2.70% done; ETC: 18:28 (0:04:48 remaining)
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 3.87% done; ETC: 18:34 (0:09:56 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 4.99% done; ETC: 18:35 (0:11:26 remaining)
Stats: 0:03:25 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 23.30% done; ETC: 18:38 (0:10:55 remaining)
Stats: 0:04:19 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 29.01% done; ETC: 18:38 (0:10:19 remaining)
Stats: 0:05:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 34.10% done; ETC: 18:38 (0:09:42 remaining)
Stats: 0:05:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 34.20% done; ETC: 18:38 (0:09:39 remaining)
Stats: 0:06:38 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 43.76% done; ETC: 18:38 (0:08:25 remaining)
```

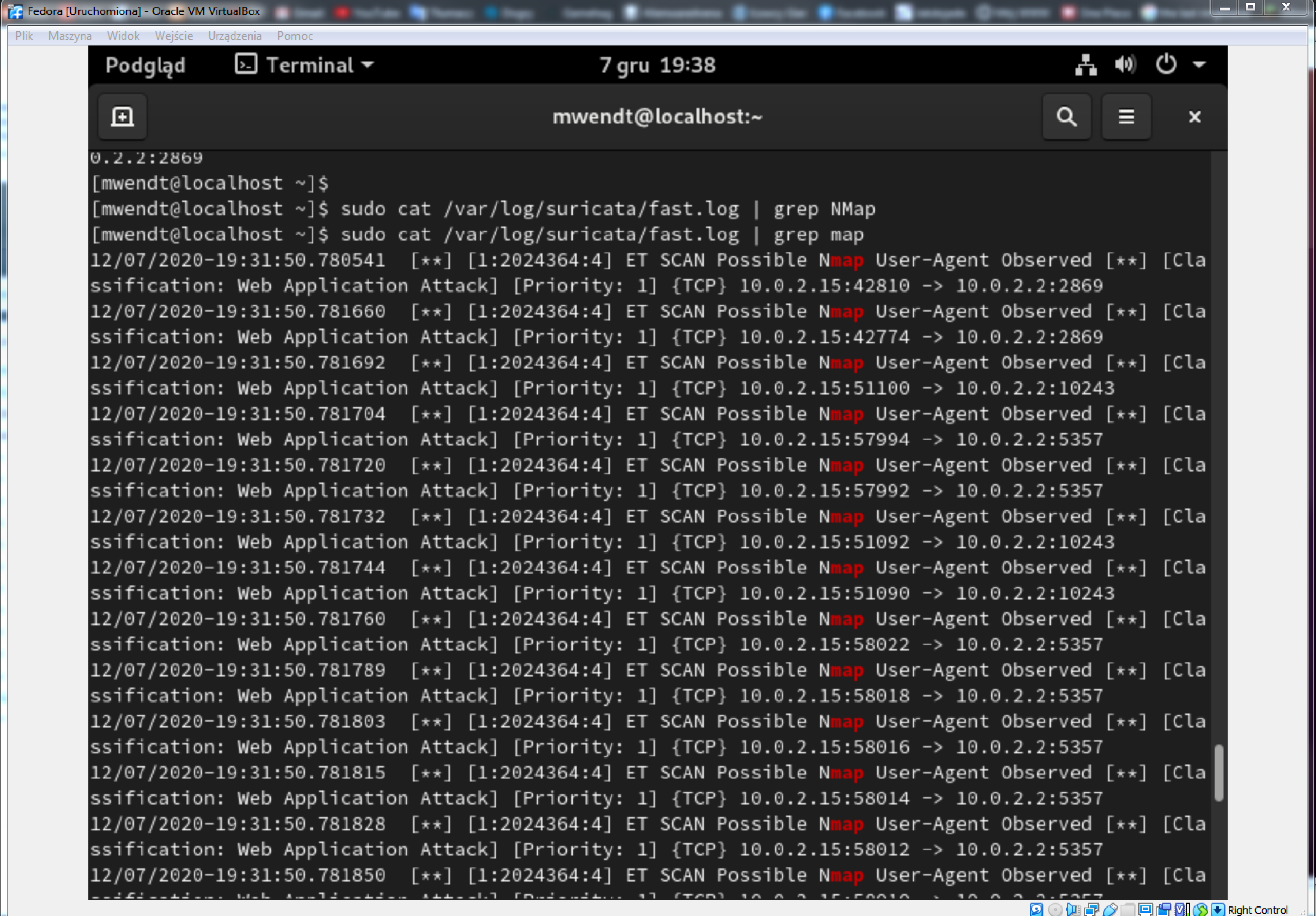

ubuntu [Uruchomiona] - Oracle VM VirtualBox : 1
Activities
Terminal
gru 7 18:50
michal@michal-VirtualBox: ~

```
Connect Scan Timing: About 34.10% done; ETC: 18:38 (0:09:42 remaining)
Stats: 0:05:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 34.20% done; ETC: 18:38 (0:09:39 remaining)
Stats: 0:06:38 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 43.76% done; ETC: 18:38 (0:08:25 remaining)
Stats: 0:08:35 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 56.10% done; ETC: 18:38 (0:06:39 remaining)
Nmap scan report for 10.0.2.15
Host is up (0.018s latency).
Not shown: 991 closed ports
PORT     STATE    SERVICE       VERSION
25/tcp   filtered smtp
42/tcp   filtered nameserver
80/tcp   open     http          nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Multimedia Polska - Informacja
443/tcp  open     ssl/http      nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Multimedia Polska - Informacja
| ssl-cert: Subject: commonName=MMP/organizationName=IT MULTIMEDIA POLSKA S A S
P\xC3\x83\xC2\x93\xC3\x85\xC2\x81KA KOMANDYTOWA/stateOrProvinceName=Wielkopolsk
a/countryName=PL
| Not valid before: 2020-05-13T18:50:00
|_Not valid after:  2021-05-13T18:50:00
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
| tls-nextprotoneg:
```


ubuntu [Uruchomiona] - Oracle VM VirtualBox : 1
Activities
Terminal
gru 7 18:50
michal@michal-VirtualBox: ~

```
42/tcp   filtered nameserver
80/tcp   open     http          nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Multimedia Polska - Informacja
443/tcp  open     ssl/http      nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Multimedia Polska - Informacja
| ssl-cert: Subject: commonName=MMP/organizationName=IT MULTIMEDIA POLSKA S A S
P\xC3\x83\xC2\x93\xC3\x85\xC2\x81KA KOMANDYTOWA/stateOrProvinceName=Wielkopolsk
a/countryName=PL
| Not valid before: 2020-05-13T18:50:00
|_Not valid after:  2021-05-13T18:50:00
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
| tls-nextprotoneg:
|   h2
|_  http/1.1
445/tcp  filtered microsoft-ds
1064/tcp filtered jstel
1433/tcp filtered ms-sql-s
1434/tcp filtered ms-sql-m
2126/tcp filtered pktcable-cops

Service detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1029.68 seconds
michal@michal-VirtualBox:~$ 
```



```
0.2.2:2869
[mwendt@localhost ~]$
[mwendt@localhost ~]$ sudo cat /var/log/suricata/fast.log | grep NMap
[mwendt@localhost ~]$ sudo cat /var/log/suricata/fast.log | grep map
12/07/2020-19:31:50.780541  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:42810 -> 10.0.2.2:2869
12/07/2020-19:31:50.781660  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:42774 -> 10.0.2.2:2869
12/07/2020-19:31:50.781692  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:51100 -> 10.0.2.2:10243
12/07/2020-19:31:50.781704  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:57994 -> 10.0.2.2:5357
12/07/2020-19:31:50.781720  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:57992 -> 10.0.2.2:5357
12/07/2020-19:31:50.781732  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:51092 -> 10.0.2.2:10243
12/07/2020-19:31:50.781744  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:51090 -> 10.0.2.2:10243
12/07/2020-19:31:50.781760  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:58022 -> 10.0.2.2:5357
12/07/2020-19:31:50.781789  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:58018 -> 10.0.2.2:5357
12/07/2020-19:31:50.781803  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:58016 -> 10.0.2.2:5357
12/07/2020-19:31:50.781815  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:58014 -> 10.0.2.2:5357
12/07/2020-19:31:50.781828  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
ssification: Web Application Attack] [Priority: 1] {TCP} 10.0.2.15:58012 -> 10.0.2.2:5357
12/07/2020-19:31:50.781850  [**] [1:2024364:4] ET SCAN Possible Nmap User-Agent Observed [**] [Cla
```