

KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

Virtualios infrastruktūros sauga

T120M144

Laboratorinio darbo Nr. 2 ataskaita

VMware ESXi

Atliko: IFM-1/3 gr.

Stud. Eligijus Kiudys

Patikrino:

Kaunas, 2022

Laboratorinis darbas Nr. 2.

Tinklo kūrimas naudojant WMware ESXi hypervizorių

Darbo tikslas

Naudojant WMware ESXi technologiją sukurti virtualių mašinų tinklą.

Darbo priemonės

1. WMware ESXi hypervizorius
2. VShpere klientas
3. Windows. Linux atvaizdai
4. Microsoft File Checksum Integrity Verifier arba Linux MD5SUM / SHA1SUM (kontrolinių sumų skaičiavimas)
5. VMware Player arba VirtualBox
6. Putty (ssh prisijungimui), WinSCP (failų parsisiuntimui naudojant ssh protokolą).
7. FTP prieiga (ISO atvaizdai – ISO katalogas; FCIV – TOOLS katalogas). Prisijungimo vardas: anonymous

Darbo uždaviniai

1. Naudojant WMware/VirtualBox aplinką sukurti 2 virtualias mašinas (viena jų privalo būti WMware ESXi tarnybinėje stotyje).
2. Identifikuoti ir apskaičiuoti kontrolines sumas failus, kurie aprašomi ataskaitoje.
3. Aptikti pėdsakus virtualioje mašinoje.
4. Pateikti darbo rezultatų išvadas.

Darbo planas

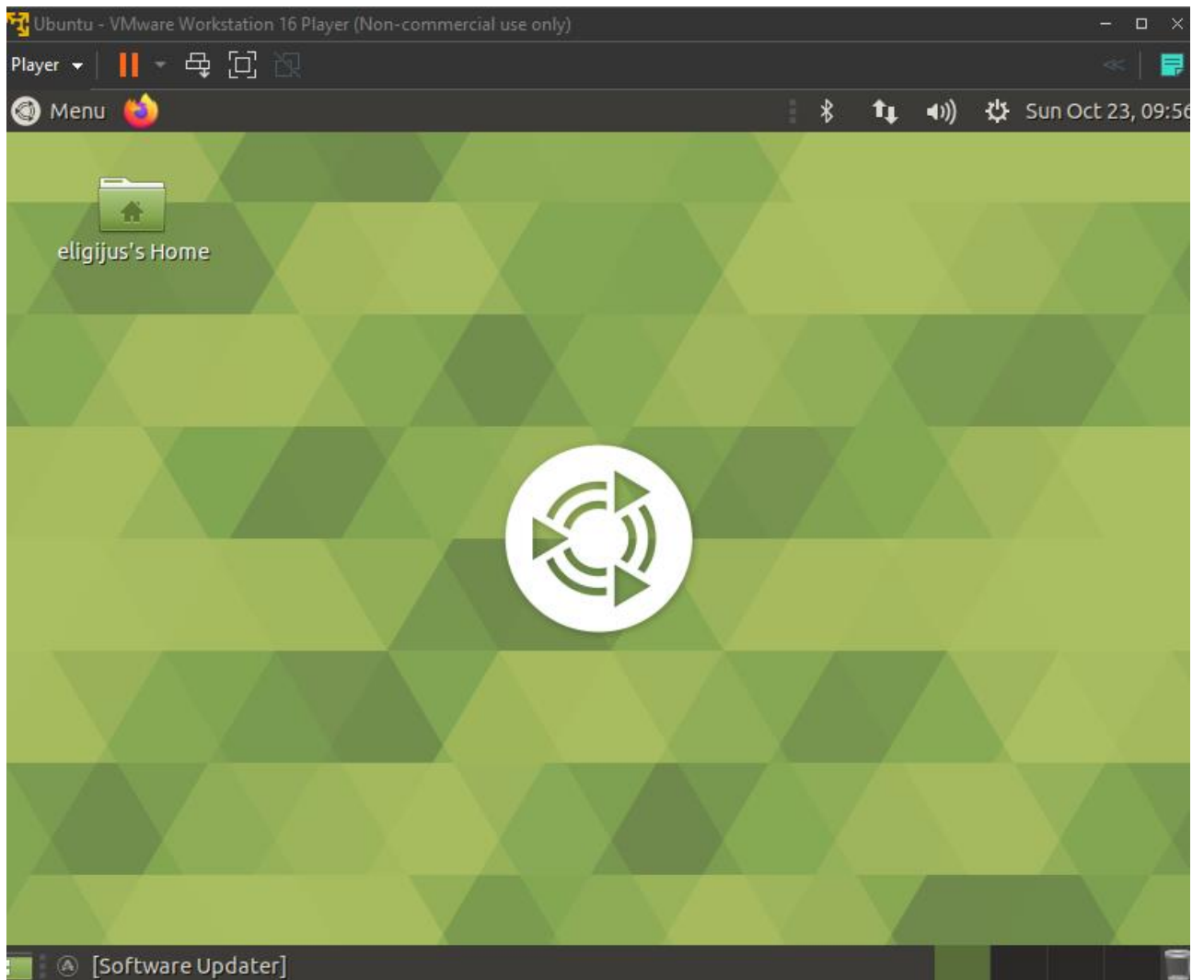
1. Naudojant VMware ESXi ir VMware Player sukurti 2 (arba 3) virtualias mašinas. Jei dirbama klasėje, naudoti KTU ESXi tarnybinę stotį (arba VMware Player). Potinklio kūrimo IP struktūra: **192.168.XX.Y/255.255.255.0** (XX – studento pažymėjimo paskutiniai du skaičiai; Y – bet koks skaičius nuo 2 iki 254; Gateway – 192.168.XX.1)
2. Gauti *.vmdk disko atvaizdus
3. Apskaičiuoti kontrolines (VMDK)
4. Identifikuoti vartotoją ir pademonstruoti informaciją apie vartotoją.
5. Pateikti išvadas

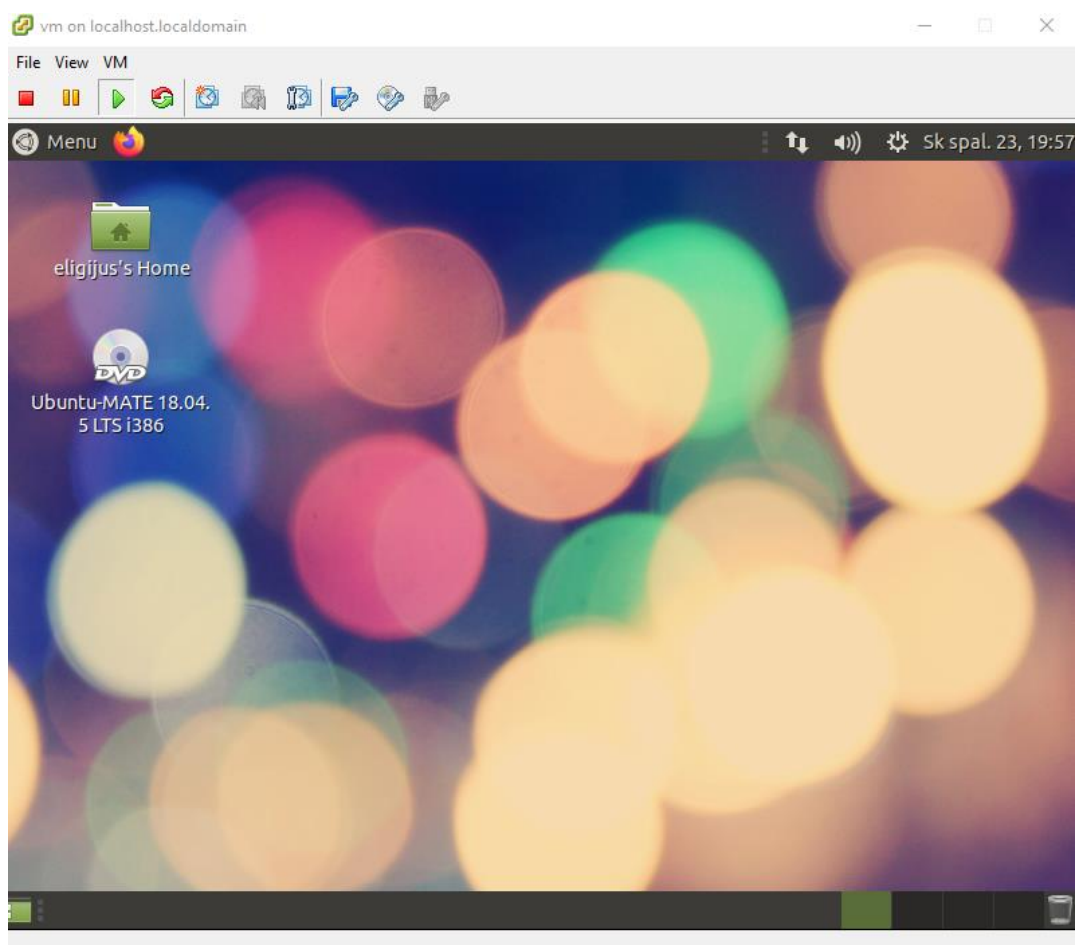
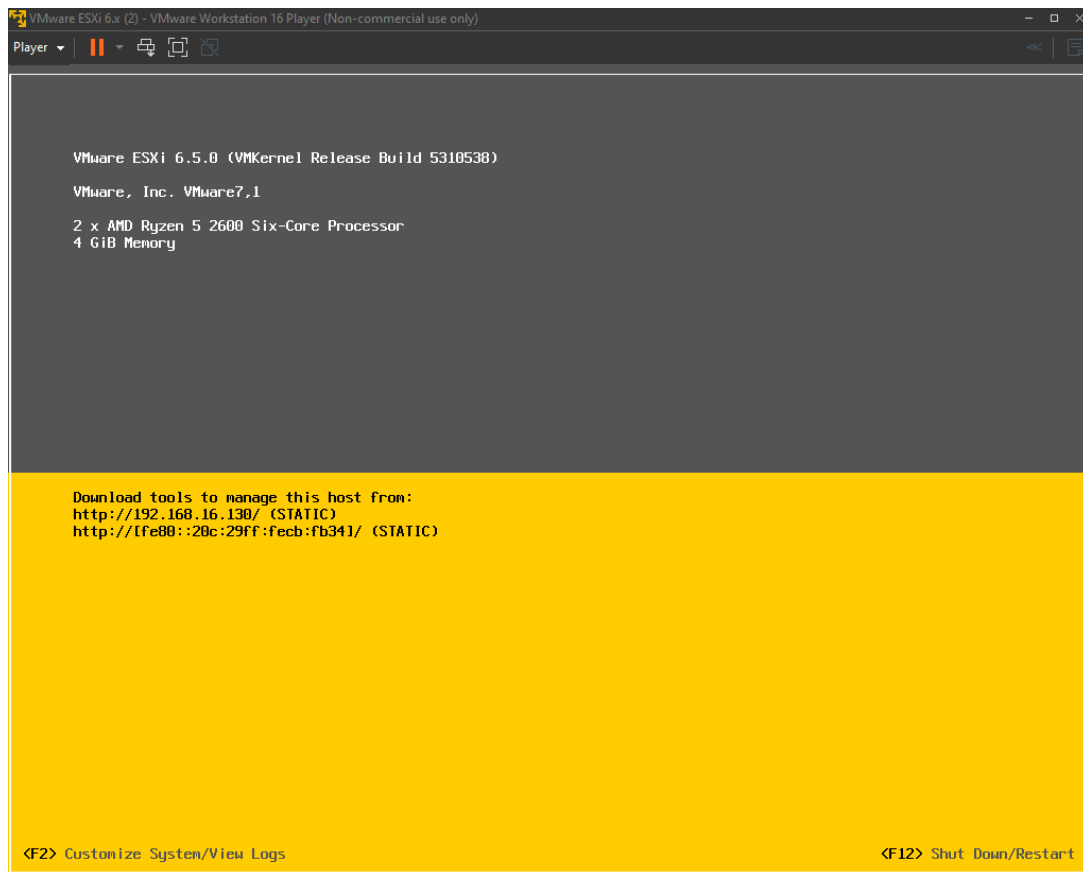
Darbo eiga

- Nurodykite savo studento pažymėjimo numerį: C1616_____
- Nustatykite savo virtualaus potinklio adresą: **192.168.XX.Y/ 255.255.255.0**
- Įdiekite virtualias mašinas naudodami VMware ESXi hypervizoriaus technologiją.
- Virtualių mašinų vartotojo vardas turi būti studento vardas (jei atliekate nuotoliniu būdu, sąlyga netaikoma).

Pademonstruoti

Buvo sukurtos iš viso trys virtualios mašinos pirmoji mašina Ubuntu mate, antroji virtualis mašina Vmware esxi 6.5 ir trčioji virtuali mašina buvo sukurta antroje virtualiojoje mašinoje.





Sukonfigūruotas tinklas

Sukūrus virtualias mašinas buvo sukoinfigūruotas jų tinklas, su specifiniais ip adresais.

```
C:\Users\Eligijus>ping 192.168.16.130

Pinging 192.168.16.130 with 32 bytes of data:
Reply from 192.168.16.130: bytes=32 time<1ms TTL=64
Reply from 192.168.16.130: bytes=32 time<1ms TTL=64
Reply from 192.168.16.130: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.16.130:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Eligijus>ping 192.168.16.131

Pinging 192.168.16.131 with 32 bytes of data:
Reply from 192.168.16.131: bytes=32 time=1ms TTL=64
Reply from 192.168.16.131: bytes=32 time<1ms TTL=64
Reply from 192.168.16.131: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.16.131:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\Eligijus>ping 192.168.16.132

Pinging 192.168.16.132 with 32 bytes of data:
Reply from 192.168.16.132: bytes=32 time=27ms TTL=64
Reply from 192.168.16.132: bytes=32 time=15ms TTL=64
Reply from 192.168.16.132: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.16.132:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 27ms, Average = 16ms
Control-C
^C
C:\Users\Eligijus>
```

```
elinijus's Home
• eligijus@ubuntu: ~
File Edit View Search Terminal Help

    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 541 bytes 44343 (44.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 541 bytes 44343 (44.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eligijus@ubuntu:~$ ping 192.168.16.130
PING 192.168.16.130 (192.168.16.130) 56(84) bytes of data.
64 bytes from 192.168.16.130: icmp_seq=1 ttl=64 time=1.57 ms
64 bytes from 192.168.16.130: icmp_seq=2 ttl=64 time=0.418 ms
^C
--- 192.168.16.130 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.418/0.994/1.570/0.576 ms
eligijus@ubuntu:~$ ping 192.168.16.131
PING 192.168.16.131 (192.168.16.131) 56(84) bytes of data.
64 bytes from 192.168.16.131: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 192.168.16.131: icmp_seq=2 ttl=64 time=0.685 ms
^C
--- 192.168.16.131 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.685/0.860/1.035/0.175 ms
eligijus@ubuntu:~$
```

```
Menu
• eligijus@eligijus-virtual-machine: ~
File Edit View Search Terminal Help

    loop txqueuelen 1000 (Local Loopback)
    RX packets 886 bytes 64590 (64.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 886 bytes 64590 (64.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

U
eligijus@eligijus-virtual-machine:~$ ping 192.168.16.130
PING 192.168.16.130 (192.168.16.130) 56(84) bytes of data.
64 bytes from 192.168.16.130: icmp_seq=1 ttl=64 time=1.85 ms
64 bytes from 192.168.16.130: icmp_seq=2 ttl=64 time=0.447 ms
^C
--- 192.168.16.130 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.447/1.152/1.857/0.705 ms
eligijus@eligijus-virtual-machine:~$ ping 192.168.16.132
PING 192.168.16.132 (192.168.16.132) 56(84) bytes of data.
64 bytes from 192.168.16.132: icmp_seq=1 ttl=64 time=1.10 ms
64 bytes from 192.168.16.132: icmp_seq=2 ttl=64 time=0.606 ms
64 bytes from 192.168.16.132: icmp_seq=3 ttl=64 time=0.669 ms
^C
--- 192.168.16.132 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2023ms
rtt min/avg/max/mdev = 0.606/0.794/1.107/0.222 ms
eligijus@eligijus-virtual-machine:~$
```

Virtualių mašinių nustatymai

Edit settings - vm (ESXi 6.5 virtual machine)

CPU	1	
Memory	1024	MB
Hard disk 1	16	GB
SCSI Controller 0	LSI Logic Parallel	
Network Adapter 1	VM Network	<input checked="" type="checkbox"/> Connect
Floppy drive 1	Use existing floppy image	
CD/DVD Drive 1	Datastore ISO file	
Status	<input checked="" type="checkbox"/> Connect at power on	
CD/DVD Media	[datastore1] ubuntu-mate-18.04.5-desktop-i386.iso Browse...	
Virtual Device Node	IDE controller 1	Master

Save Cancel

Hardware

Options

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	30 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Add...

Remove

Device status

☐ Connected

☒ Connect at power on

Connection

☐ Use physical drive:

Auto detect

☒ Use ISO image file:

C:\Users\Eligjus\Downloads\ubuntu-mate-18.04.5-

✕

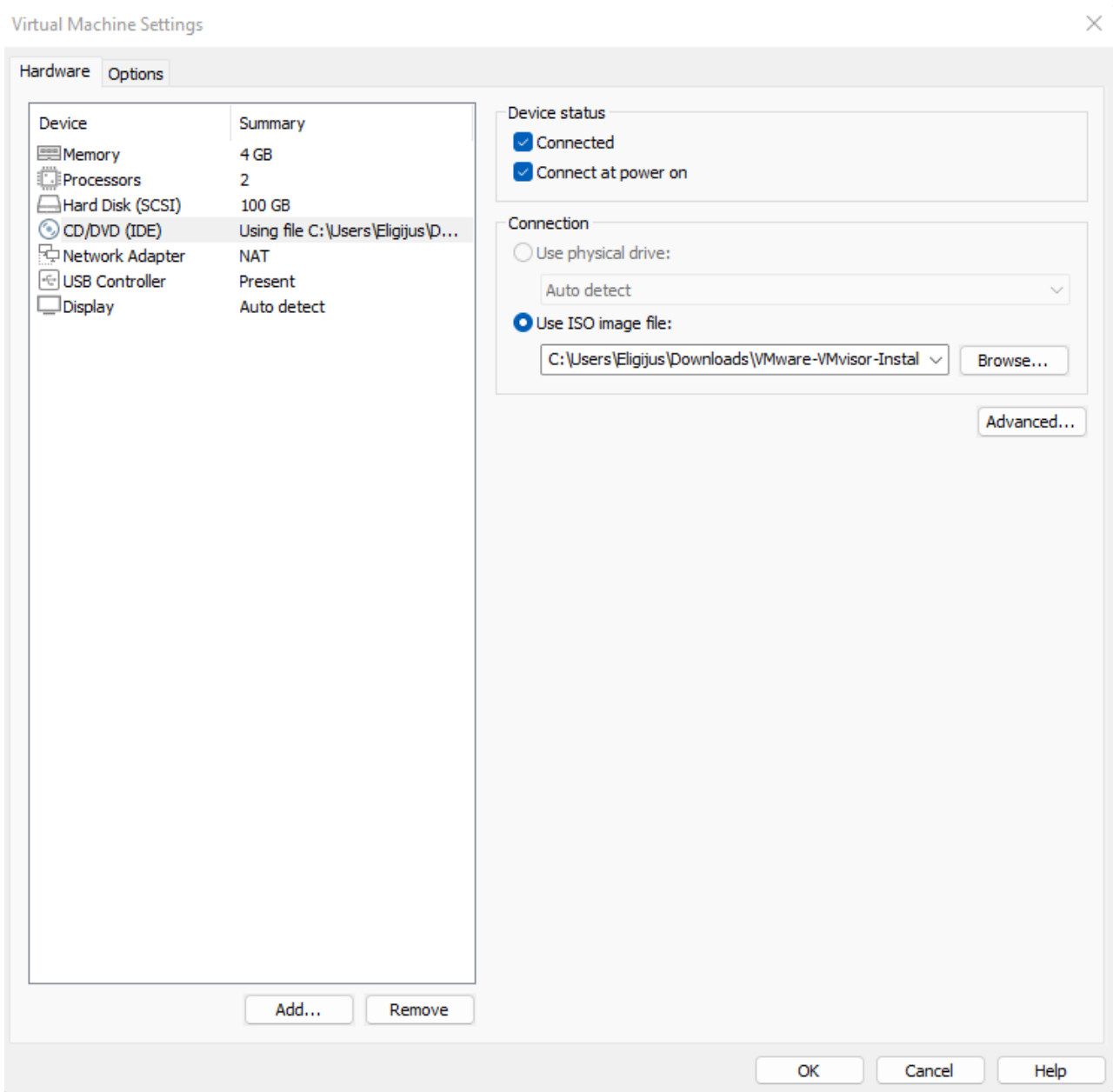
Browse...

Advanced...

OK

Cancel

Help



Tinklo adresai

1 lentelė

Eil. Nr.	Virtuali mašina	IP adresas
1	ESXi 6.5	192.168.16.130
2	Ubuntu mate (ESXi viduje)	192.168.16.131
3	Ubuntu mate	192.168.16.132

Hypervizoriaus failai

```
C:\Users\Eligijus>certutil -hashfile "C:\Users\Eligijus\Documents\Virtual Machines\Ubuntu\Ubuntu.vmdk" SHA256
SHA256 hash of C:\Users\Eligijus\Documents\Virtual Machines\Ubuntu\Ubuntu.vmdk:
0a962e864066763fa3fb77620e05f24f84fa8d0e858b44467cd0a1442afdf2d1
CertUtil: -hashfile command completed successfully.
```

```

vm-flat.vmdk  vm.vmdk      vm.vmx      vmware-3.log  vmware-5.log  vmware-7.log
vm.nvram      vm.vmsd      vmware-2.log vmware-4.log  vmware-6.log  vmware.log
[root@localhost:/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm] sha256sum vm-flat.vmdk
f1a712abbbb44ff37d924b53890371c28c00a4a80a32c3fe87f00a57c6594e5b  vm-flat.vmdk

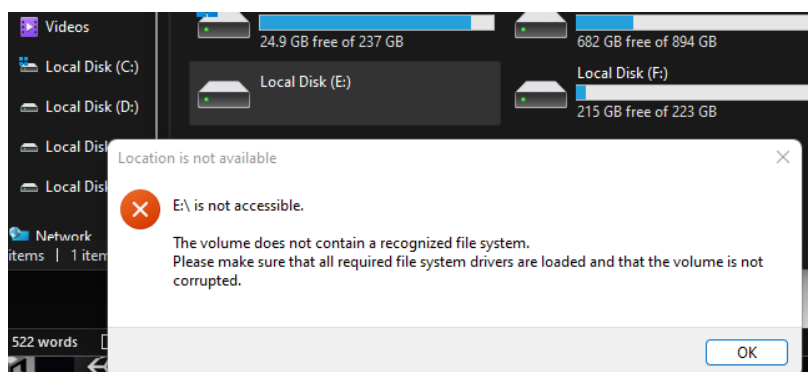
```

2 lentelė

Ei l. N r.	Failo pavadinimas**	Virtualios mašinos namų katalogas	Failo dydis	Failo data	Failo kontrolinė suma *
1	vm.nvram	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	9 KB	10/23/2022	
2	vm.vmdk	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	1 KB	10/23/2022	
3	vm.vmsd	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	0 KB	10/18/2022	
4	vm.vmx	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	3 KB	10/23/2022	
5	vm-flat.vmdk	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	2097 152 KB	10/23/2022	f1a712abbbb44ff37d924b53890371c28c00a4a80a32c3fe87f00a57c6594e5b
6	vmware.log	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	192 KB	10/23/2022	
7	vmware.log-1	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	237 KB	10/18/2022	
8	vmware.log-2	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	168 KB	10/19/2022	
9	vmware.log-3	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	191 KB	10/23/2022	
10	vmware.log-4	/vmfs/volumes/634d4b0d-	167 KB	10/23/2022	

		6b8c5444-c6fa-000c29cbfb34/vm/			
1	vmware.log-5	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	166 KB	10/23/2022	
1	vmware.log-6	/vmfs/volumes/634d4b0d-6b8c5444-c6fa-000c29cbfb34/vm/	191 KB	10/23/2022	

Virtualaus disko prijungimo pademonstravimas



Linux diskas neatsidaro per Windows operacinę sistemą.

Virtualių diskų (VMDK) kontrolinių sumų perskaičiavimas, po disko prisijungimo ir peržiūros

```
C:\Users\Eligijus>certutil -hashfile "C:\Users\Eligijus\Documents\634d4b0d-6b8c5444-c6fa-000c29cbfb34\vm\vm-flat.vmdk" SHA256
SHA256 hash of C:\Users\Eligijus\Documents\634d4b0d-6b8c5444-c6fa-000c29cbfb34\vm\vm-flat.vmdk:
f1a712abbbb44ff37d924b53890371c28c00a4a80a32c3fe87f00a57c6594e5b
CertUtil: -hashfile command completed successfully.

C:\Users\Eligijus>certutil -hashfile "C:\Users\Eligijus\Documents\Virtual Machines\Ubuntu\Ubuntu.vmdk" SHA256
SHA256 hash of C:\Users\Eligijus\Documents\Virtual Machines\Ubuntu\Ubuntu.vmdk:
58fcf01ac562b10523604436af47f18de3615f86a3376514d7a6fd065beef1c8
CertUtil: -hashfile command completed successfully.

C:\Users\Eligijus>
```

3 lentelė

Eil. Nr.	Failo (VMDK) pavadinimas	Failo (VMDK) kontrolinė suma
1	vm-flat.vmdk	f1a712abbbb44ff37d924b53890371c28c00a4a80a32c3fe87f00a57c6594e5b
2	Ubuntu.vmdk	58fcf01ac562b10523604436af47f18de3615f86a3376514d7a6fd065beef1c8

Vartotojo identifikavimas

UbuntuVirtualus - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Data Sources

vm-flat.vmdk_1 Host

vm-flat.vmdk

vol1 (Unallocated: 0-2047)

vol2 (Linux (0x83): 2048-33552383)

\$OrphanFiles (11473)

\$Unalloc (14)

bin (199)

boot (12)

cdrom (8)

dev (15)

etc (303)

home (3)

lib (27)

lost+found (2)

media (5)

mnt (2)

opt (2)

proc (2)

root (6)

run (23)

sbin (295)

snap (9)

srv (2)

sys (2)

tmp (17)

usr (10)

var (16)

vol3 (Unallocated: 33552384-33554431)

Data Views

File Views

Metadata (15)

Operating System Information (2)

Web Bookmarks (9)

Web Cookies (6)

Web Form Autofill (4)

Listing

/img_vm-flat.vmdk/vol_vol2/etc

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
profile			2	2018-04-09 14:10:28 EEST	2022-10-18 14:04:52 EEST	2022-10-23 19:20:31 EEST	2022-10-18 14:04:5
protocols			1	2016-12-26 03:56:39 EET	2022-10-18 14:04:52 EEST	2016-12-26 03:56:39 EET	2022-10-18 14:04:5
request-key.d			2	2020-08-07 02:00:04 EEST	2022-10-18 14:24:24 EEST	2022-10-23 19:19:11 EEST	2022-10-18 14:24:2
rmt			1	2017-07-21 17:35:22 EEST	2022-10-18 14:04:52 EEST	2017-07-21 17:35:22 EEST	2022-10-18 14:04:5
rpc			1	2016-12-26 03:56:39 EET	2022-10-18 14:04:52 EEST	2016-12-26 03:56:39 EET	2022-10-18 14:04:5
rsyslog.conf			1	2018-01-30 17:52:13 EET	2022-10-18 14:04:52 EEST	2022-10-23 19:19:17 EEST	2022-10-18 14:04:5
securetty			1	2018-01-25 17:09:22 EET	2022-10-18 14:04:52 EEST	2022-10-23 19:19:42 EEST	2022-10-18 14:04:5
sedrmcSgo			2	2022-10-18 14:16:46 EEST	2022-10-18 14:16:46 EEST	2022-10-18 14:16:46 EEST	2022-10-18 14:16:4
sensors3.conf			1	2017-04-05 23:07:33 EEST	2022-10-18 14:04:52 EEST	2022-10-23 19:19:19 EEST	2022-10-18 14:04:5
services			1	2016-12-26 03:56:39 EET	2022-10-18 14:04:52 EEST	2022-10-23 19:19:29 EEST	2022-10-18 14:04:5
shadow			1	2022-10-18 14:13:11 EEST	2022-10-18 14:13:11 EEST	2022-10-23 19:19:18 EEST	2022-10-18 14:13:1
shadow-			2	2022-10-18 14:13:11 EEST	2022-10-18 14:13:11 EEST	2022-10-18 14:13:11 EEST	2022-10-18 14:13:1

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File

whoopsie*:18480:0:99999:7:::
kernoops*:18480:0:99999:7:::
saned*:18480:0:99999:7:::
nm-openvpn*:18480:0:99999:7:::
avahi*:18480:0:99999:7:::
colord*:18480:0:99999:7:::
hplip*:18480:0:99999:7:::
geodue*:18480:0:99999:7:::
pulse*:18480:0:99999:7:::
eligijus:\$6\$LT02vStt\$OxdjbgllwwK2dhiMrOt4goe2LjFfzG0YX3NgADLnToscJ347yL3rH.C12rIJ1TrQ54oMTLPpoq04NUzFomddMo1:19283:0:99999:7:::
-----METADATA-----

4 lentelė

Eil. Nr.	Reikšmė	Informacija
1	Vartotojo vardas:	eligijus
2	Vartotojo prisijungimas:	2022-10-23 19:19:18 EEST
3	Vartotojo slaptažodis:	\$6\$LT02vStt\$OxdjbgllwwK2dhiMrOt4goe2LjFfzG0YX3NgADLnToscJ347yL3rH.C12rIJ1TrQ54oMTLPpoq04NUzFomddMo

UbuntuVirtualus - Autopsy 4.19.3

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing
/img_vm-flat.vmdk/vol2/etc

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
profile			2	2018-04-09 14:10:28 EEST	2022-10-18 14:04:52 EEST	2022-10-23 19:20:31 EEST	2022-10-18 14:04:5
protocols			1	2016-12-26 03:56:39 EET	2022-10-18 14:04:52 EEST	2016-12-26 03:56:39 EET	2022-10-18 14:04:5
request-key.d			2	2020-08-07 02:00:04 EEST	2022-10-18 14:24:24 EEST	2022-10-23 19:19:11 EEST	2022-10-18 14:24:2
rmt			1	2017-07-21 17:35:22 EEST	2022-10-18 14:04:52 EEST	2017-07-21 17:35:22 EEST	2022-10-18 14:04:5
rpc			1	2016-12-26 03:56:39 EET	2022-10-18 14:04:52 EEST	2016-12-26 03:56:39 EET	2022-10-18 14:04:5
rsyslog.conf			1	2018-01-30 17:52:13 EET	2022-10-18 14:04:52 EEST	2022-10-23 19:19:17 EEST	2022-10-18 14:04:5
securetty			1	2018-01-25 17:09:22 EET	2022-10-18 14:04:52 EEST	2022-10-23 19:19:42 EEST	2022-10-18 14:04:5
sedrMcSgo			2	2022-10-18 14:16:46 EEST	2022-10-18 14:16:46 EEST	2022-10-18 14:16:46 EEST	2022-10-18 14:16:4
sensors3.conf			1	2017-04-05 23:07:33 EEST	2022-10-18 14:04:52 EEST	2022-10-23 19:19:19 EEST	2022-10-18 14:04:5
services			1	2016-12-26 03:56:39 EET	2022-10-18 14:04:52 EEST	2022-10-23 19:19:29 EEST	2022-10-18 14:04:5
shadow			1	2022-10-18 14:13:11 EEST	2022-10-18 14:13:11 EEST	2022-10-23 19:19:18 EEST	2022-10-18 14:13:1
shadow-			2	2022-10-18 14:13:11 EEST	2022-10-18 14:13:11 EEST	2022-10-18 14:13:11 EEST	2022-10-18 14:13:1

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File

whoopsie:*:18480:0:99999:7:::
kernoops:*:18480:0:99999:7:::
saned:*:18480:0:99999:7:::
nm-openvpn:*:18480:0:99999:7:::
avahi:*:18480:0:99999:7:::
colord:*:18480:0:99999:7:::
hplip:*:18480:0:99999:7:::
geodue:*:18480:0:99999:7:::
pulse:*:18480:0:99999:7:::
eligijus:\$6\$LT02vStt\$0xdjbgllwwK2dhiMrOt4goe2LjFfZG0YX3NgADLnToscJ347yL3rH.C12rIJ1TrQ54oMTLPpoq04NUzFomddMo1:19283:0:99999:7:::

-----METADATA-----

4 lentelė

Eil. Nr.	Reikšmė	Informacija
1	Vartotojo vardas:	eligijus
2	Vartotojo prisijungimas:	2022-10-23 19:35:21 EEST
3	Vartotojo slaptažodis:	\$6\$LT02vStt\$0xdjbgllwwK2dhiMrOt4goe2LjFfZG0YX3NgADLnToscJ347yL3rH.C12rIJ1TrQ54oMTLPpoq04NUzFomddMo

Išvados

Virtualias mašinas pavyko sėkmingai sukonfigūruoti, didelių problemų neiškilo. Per tinklą virtualios mašinos gali pasiekti viena kitą. Taip pat buvo pastebėta, kad disko kontrolinė suma nesikeičia prieš paleidžiant virtualią mašiną ir po jos paleidimo. Atlikus virtualių diskų poėmį pamačiau, kad galima išgauti daug informacijos. Naudojant linux sistemos disko poėmį pavyko gauti tik maišų slaptažodį. Galima atskirti, kad slaptažodžiai yra vienodi, kaip ir buvo nustatyta įrašant operacines sistemas. Paėmus slaptažodžius iš abiejų diskų jie nesiskiria.

Darbo rezultatų vertinimas
(pildo dėstytojas)

5 lentelė

Vertinimas (balais)	Galimas maksimalus vertinimo balas	Vertinimo objektas	Pastabos
	5	Sukurtos ir sujungtos į bendrą potinklį 2 virtualios mašinos	Privalomai, viena mašina turi būti įdiegta į ESXi
	3	Apskaičiuotos kontrolinės vmdx sumos	Kiekviena virtuali mašina vertinama vienu balu
	2	Surinkta informacija apie vartotoją	Balai už informaciją apie vartotoją ir jo slaptažodį
	10		