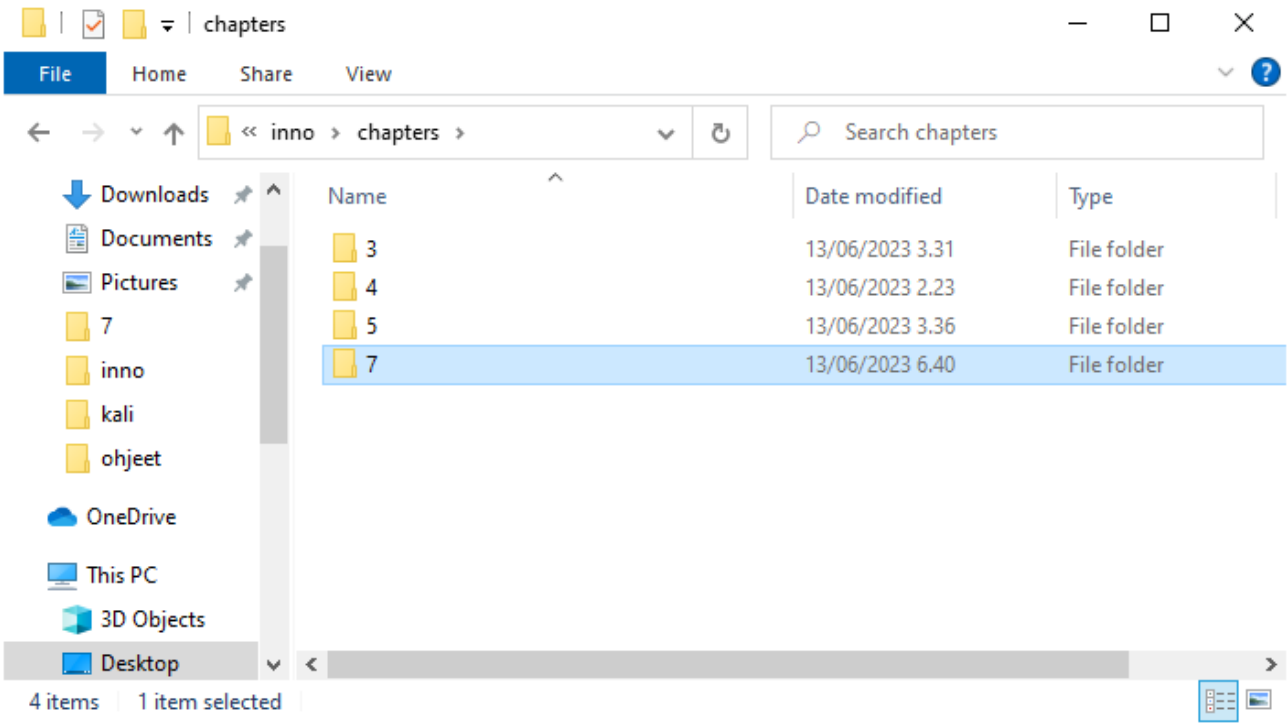
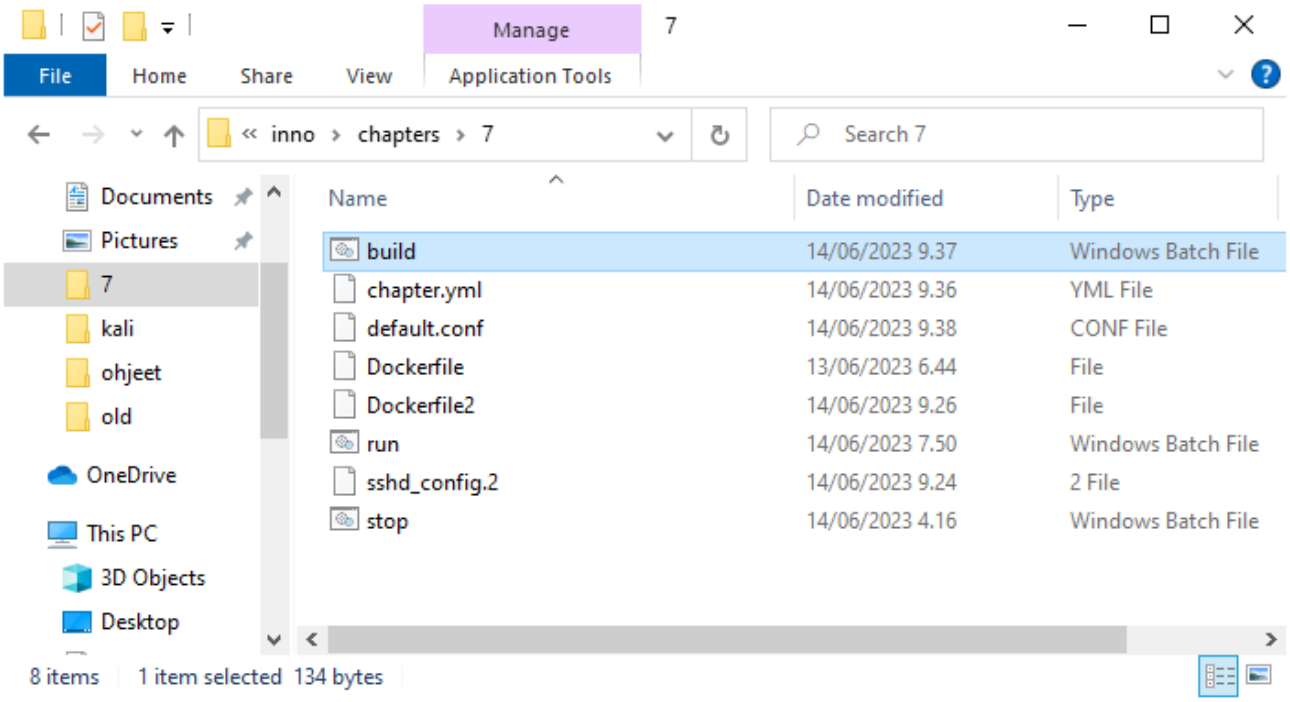
“chapter7”

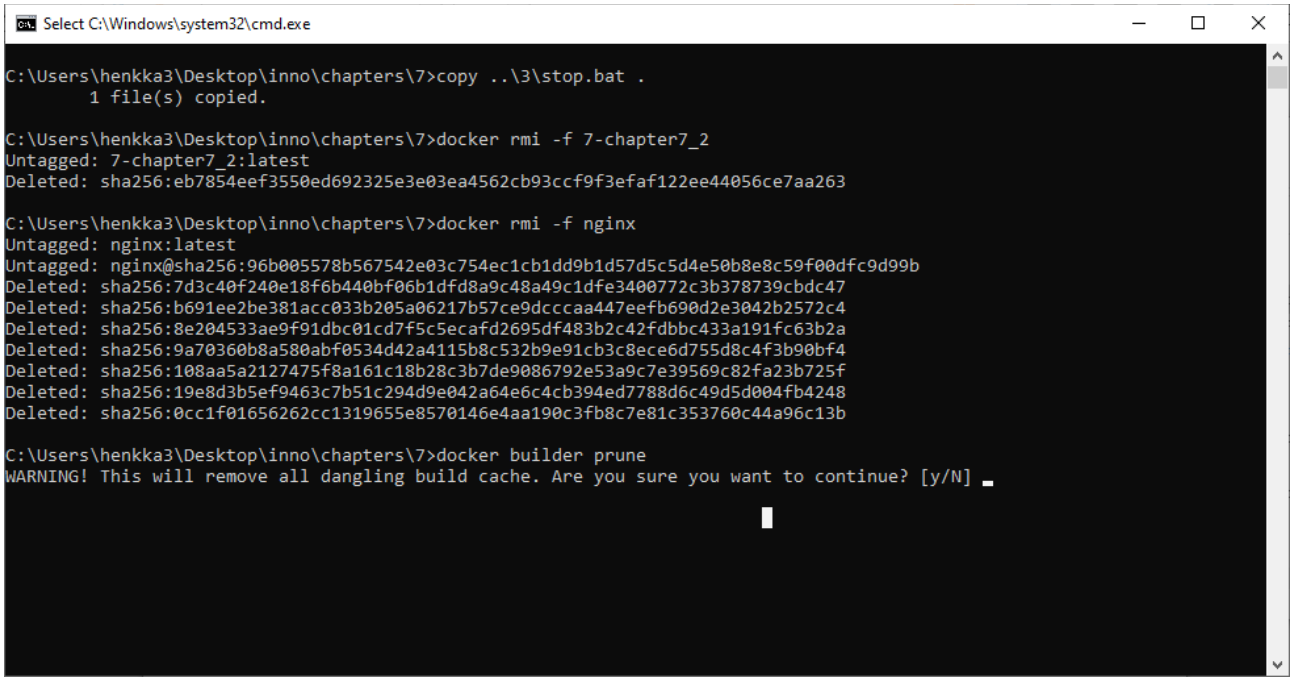
Koskapa Dockeria käytettäessä käyttöjärjestelmän ydinosat ovat samat kaikille konteille, ja verkkoyhteyksistä vastaava koodi myös(ainakin jossain määrin), käyttöjärjestelmän tunnistamisen yrittäminen vähemmän kiinnostavaa. Mutta voidaan yrittää tunnistaa mikä sovellus on ajossa missäkin portissa.
Em. tunnistaminen onkin kai pointti tässä: https://nmap.org/book/vscan.html .

7.1. kontin rakennus

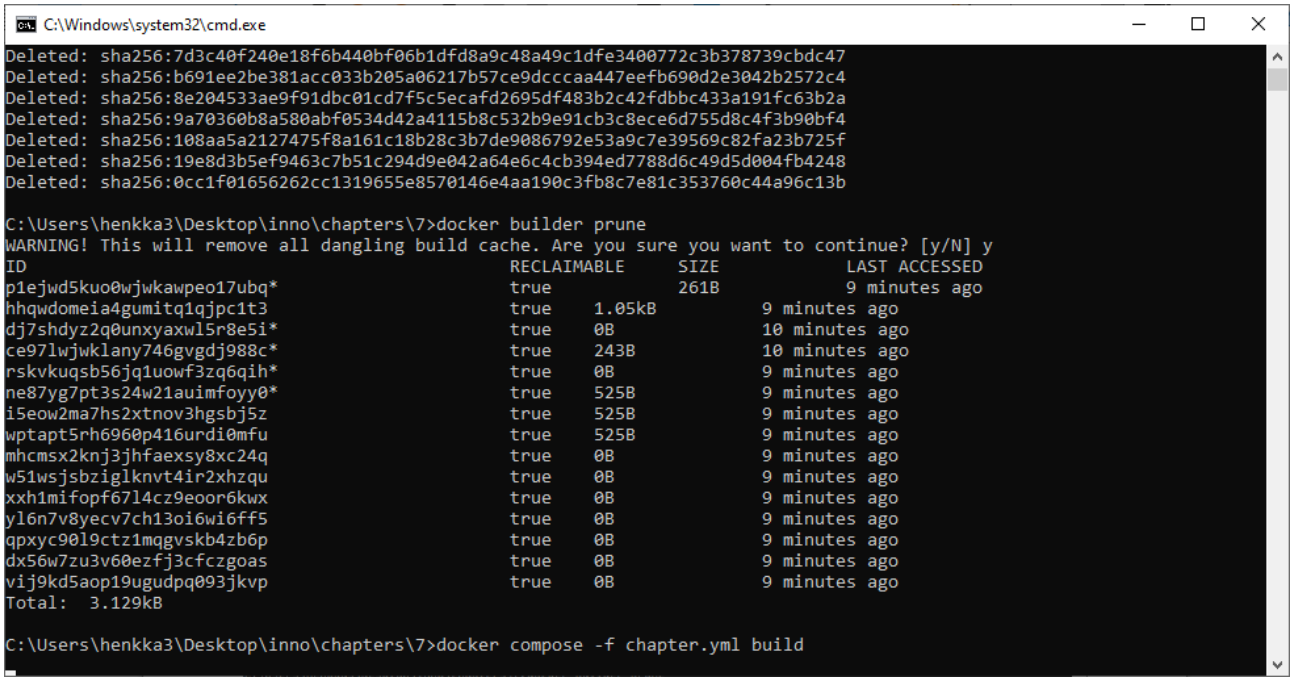


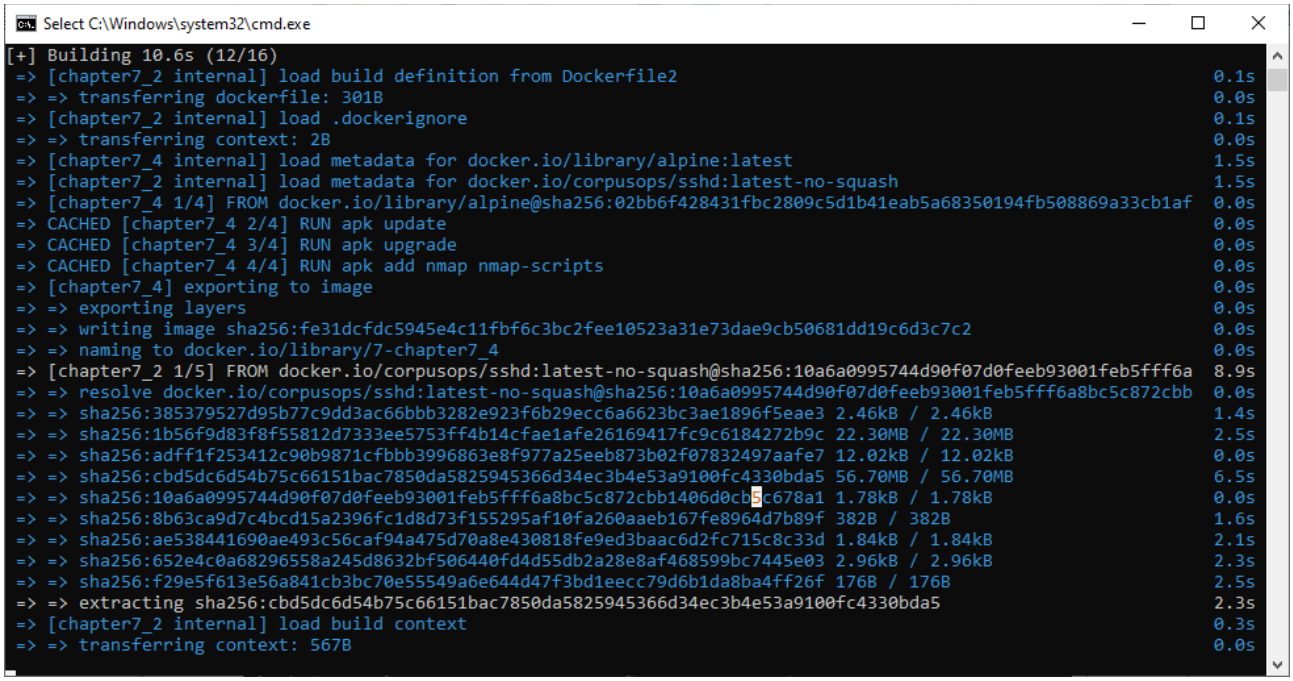
Eli tuplaklikataan inno/chapters/7/build.bat.


Manage
7
File
Home
Share
View
Application Tools
« inno › chapters › 7
Search 7
Documents
Pictures
7
kali
ohjeet
old
OneDrive
This PC
3D Objects
Desktop
Name
Date modified
Type
build
14/06/2023 9.37
Windows Batch File
chapter.yml
14/06/2023 9.36
YML File
default.conf
14/06/2023 9.38
CONF File
Dockerfile
13/06/2023 6.44
File
Dockerfile2
14/06/2023 9.26
File
run
14/06/2023 7.50
Windows Batch File
sshd_config.2
14/06/2023 9.24
2 File
stop
14/06/2023 4.16
Windows Batch File
8 items
1 item selected 134 bytes

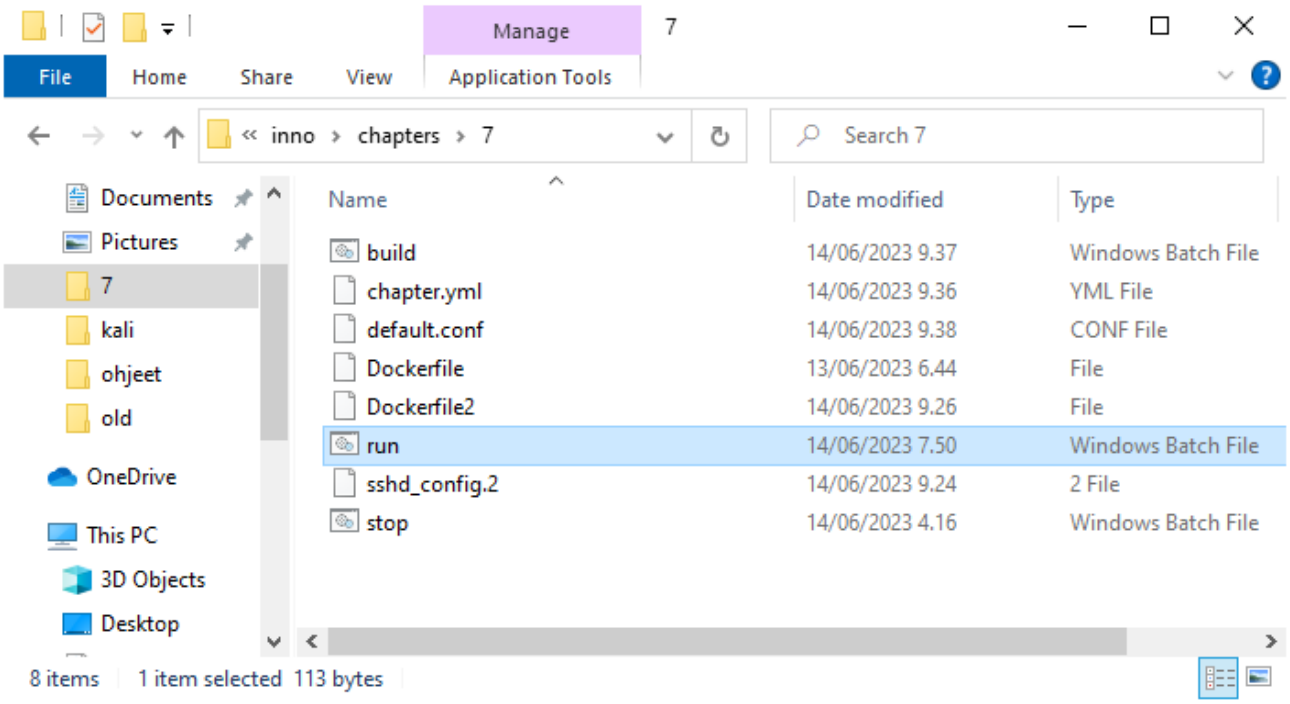

Select C:\Windows\system32\cmd.exe
C:\Users\henkka3\Desktop\inno\chapters\7>copy ..\3\stop.bat .
1 file(s) copied.
C:\Users\henkka3\Desktop\inno\chapters\7>docker rmi -f 7-chapter7_2
Untagged: 7-chapter7_2:latest
Deleted: sha256:eb7854eef3550ed692325e3e03ea4562cb93ccf9f3efaf122ee44056ce7aa263
C:\Users\henkka3\Desktop\inno\chapters\7>docker rmi -f nginx
Untagged: nginx:latest
Untagged: nginx@sha256:96b005578b567542e03c754ec1cb1dd9b1d57d5c5d4e50b8e8c59f00dfc9d99b
Deleted: sha256:7d3c40f240e18f6b440bf06b1dfd8a9c48a49c1dfe3400772c3b378739cbdc47
Deleted: sha256:b691ee2be381acc033b205a06217b57ce9dcccaa447eefb690d2e3042b2572c4
Deleted: sha256:8e204533ae9f91dbc01cd7f5c5ecafd2695df483b2c42fdbbc433a191fc63b2a
Deleted: sha256:9a70360b8a580abf0534d42a4115b8c532b9e91cb3c8ece6d755d8c4f3b90bf4
Deleted: sha256:108aa5a2127475f8a161c18b28c3b7de9086792e53a9c7e39569c82fa23b725f
Deleted: sha256:19e8d3b5ef9463c7b51c294d9e042a64e6c4cb394ed7788d6c49d5d004fb4248
Deleted: sha256:0cc1f01656262cc1319655e8570146e4aa190c3fb8c7e81c353760c44a96c13b
C:\Users\henkka3\Desktop\inno\chapters\7>docker builder prune
WARNING! This will remove all dangling build cache. Are you sure you want to continue? [y/N]

y+enter

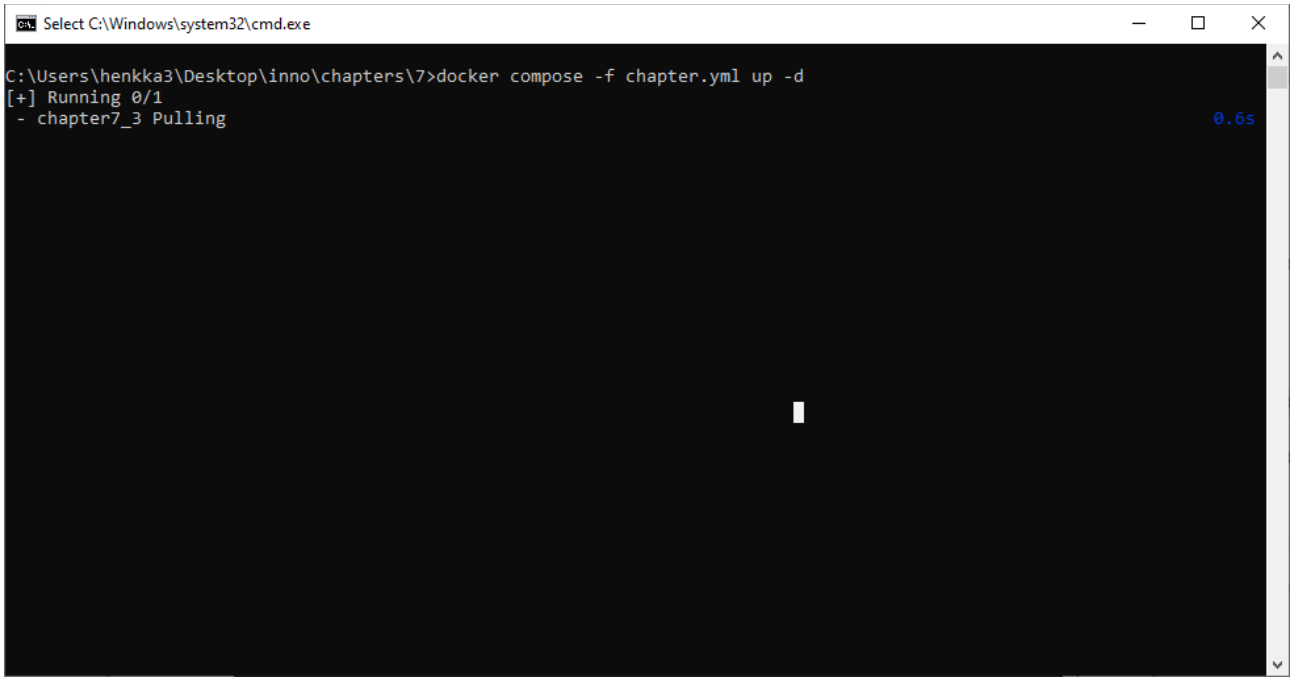

C:\Windows\system32\cmd.exe
Deleted: sha256:7d3c40f240e18f6b440bf06b1dfd8a9c48a49c1dfe3400772c3b378739cbdc47
Deleted: sha256:b691ee2be381acc033b205a06217b57ce9dcccaa447eefb690d2e3042b2572c4
Deleted: sha256:8e204533ae9f91dbc01cd7f5c5ecafd2695df483b2c42fdbbc433a191fc63b2a
Deleted: sha256:9a70360b8a580abf0534d42a4115b8c532b9e91cb3c8ece6d755d8c4f3b90bf4
Deleted: sha256:108aa5a2127475f8a161c18b28c3b7de9086792e53a9c7e39569c82fa23b725f
Deleted: sha256:19e8d3b5ef9463c7b51c294d9e042a64e6c4cb394ed7788d6c49d5d004fb4248
Deleted: sha256:0cc1f01656262cc1319655e8570146e4aa190c3fb8c7e81c353760c44a96c13b
C:\Users\henkka3\Desktop\inno\chapters\7>docker builder prune
WARNING! This will remove all dangling build cache. Are you sure you want to continue? [y/N] y
ID RECLAIMABLE SIZE LAST ACCESSED
p1ejwd5kuo0wjwkawpeo17ubq* true 261B 9 minutes ago
hhqwdomeia4gumitq1qjpc1t3 true 1.05kB 9 minutes ago
dj7shdyz2q0unxyaxwl5r8e5i* true 0B 10 minutes ago
ce97lwjwklany746gvgdj988c* true 243B 10 minutes ago
rskvkuqsb56jq1uowf3zq6qih* true 0B 9 minutes ago
ne87yg7pt3s24w21auimfoyy0* true 525B 9 minutes ago
i5eow2ma7hs2xtnov3hgsbj5z true 525B 9 minutes ago
wptapt5rh6960p416urdi0mfu true 525B 9 minutes ago
mhcmsx2knj3jhfaexsy8xc24q true 0B 9 minutes ago
w51wsjsbziglknvt4ir2xhzqu true 0B 9 minutes ago
xxh1mifopf67l4cz9eoor6kwx true 0B 9 minutes ago
yl6n7v8yecv7ch13oi6wi6ff5 true 0B 9 minutes ago
qpxyc90l9ctz1mqgvskb4zb6p true 0B 9 minutes ago
dx56w7zu3v60ezfj3cfczgoas true 0B 9 minutes ago
vij9kd5aop19ugudpq093jkvp true 0B 9 minutes ago
Total: 3.129kB
C:\Users\henkka3\Desktop\inno\chapters\7>docker compose -f chapter.yml build

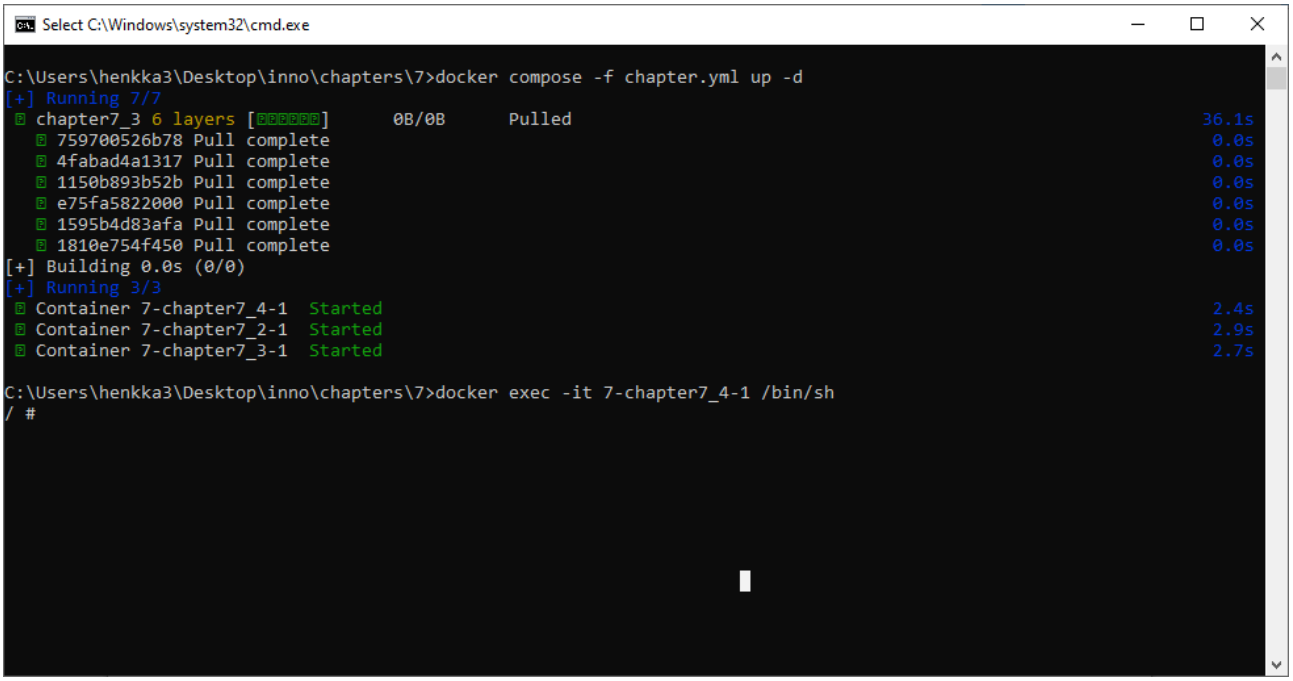

Select C:\Windows\system32\cmd.exe
[+] Building 10.6s (12/16)
=> [chapter7_2 internal] load build definition from Dockerfile2 0.1s
=> => transferring dockerfile: 301B 0.0s
=> [chapter7_2 internal] load .dockerignore 0.1s
=> => transferring context: 2B 0.0s
=> [chapter7_4 internal] load metadata for docker.io/library/alpine:latest 1.5s
=> [chapter7_2 internal] load metadata for docker.io/corpusops/sshd:latest-no-squash 1.5s
=> [chapter7_4 1/4] FROM docker.io/library/alpine@sha256:02bb6f428431fbc2809c5d1b41eab5a68350194fb508869a33cb1af 0.0s
=> CACHED [chapter7_4 2/4] RUN apk update 0.0s
=> CACHED [chapter7_4 3/4] RUN apk upgrade 0.0s
=> CACHED [chapter7_4 4/4] RUN apk add nmap nmap-scripts 0.0s
=> [chapter7_4] exporting to image 0.0s
=> => exporting layers 0.0s
=> => writing image sha256:fe31dcfdc5945e4c11fbf6c3bc2fee10523a31e73dae9cb50681dd19c6d3c7c2 0.0s
=> => naming to docker.io/library/7-chapter7_4 0.0s
=> [chapter7_2 1/5] FROM docker.io/corpusops/sshd:latest-no-squash@sha256:10a6a0995744d90f07d0feeb93001feb5fff6a 8.9s
=> => resolve docker.io/corpusops/sshd:latest-no-squash@sha256:10a6a0995744d90f07d0feeb93001feb5fff6a8bc5c872cbb 0.0s
=> => sha256:385379527d95b77c9dd3ac66bbb3282e923f6b29ecc6a6623bc3ae1896f5eae3 2.46kB / 2.46kB 1.4s
=> => sha256:1b56f9d83f8f55812d7333ee5753ff4b14cfae1afe26169417fc9c6184272b9c 22.30MB / 22.30MB 2.5s
=> => sha256:adff1f253412c90b9871cfbbb3996863e8f977a25eeb873b02f07832497aafe7 12.02kB / 12.02kB 0.0s
=> => sha256:cbd5dc6d54b75c66151bac7850da5825945366d34ec3b4e53a9100fc4330bda5 56.70MB / 56.70MB 6.5s
=> => sha256:10a6a0995744d90f07d0feeb93001feb5fff6a8bc5c872cbb1406d0cb5c678a1 1.78kB / 1.78kB 0.0s
=> => sha256:8b63ca9d7c4bcd15a2396fc1d8d73f155295af10fa260aaeb167fe8964d7b89f 382B / 382B 1.6s
=> => sha256:ae538441690ae493c56caf94a475d70a8e430818fe9ed3baac6d2fc715c8c33d 1.84kB / 1.84kB 2.1s
=> => sha256:652e4c0a68296558a245d8632bf506440fd4d55db2a28e8af468599bc7445e03 2.96kB / 2.96kB 2.3s
=> => sha256:f29e5f613e56a841cb3bc70e55549a6e644d47f3bd1eecc79d6b1da8ba4ff26f 176B / 176B 2.5s
=> => extracting sha256:cbd5dc6d54b75c66151bac7850da5825945366d34ec3b4e53a9100fc4330bda5 2.3s
=> [chapter7_2 internal] load build context 0.3s
=> => transferring context: 567B 0.0s

7.2. ajo

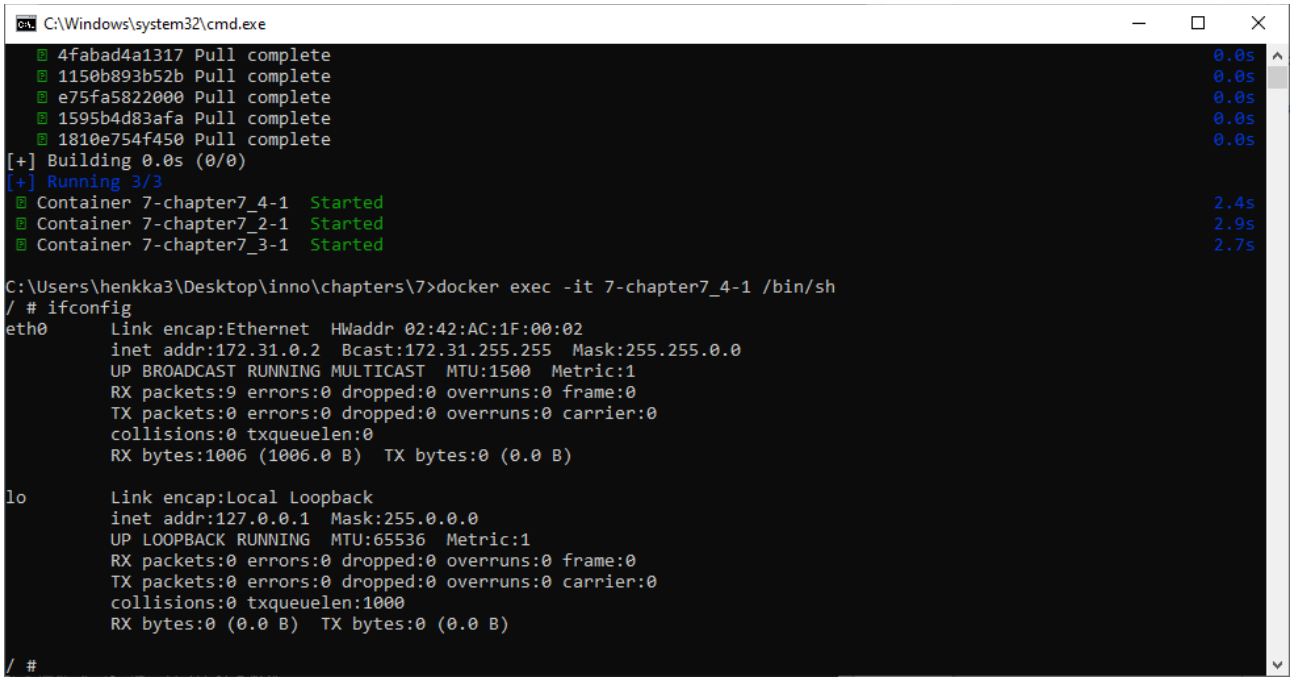


Eli tuplaklikataan inno/chpaters/7/run.bat .





ensin ifconfig



Sitten nmap -v -T5 -p0- -sT ip/maski.

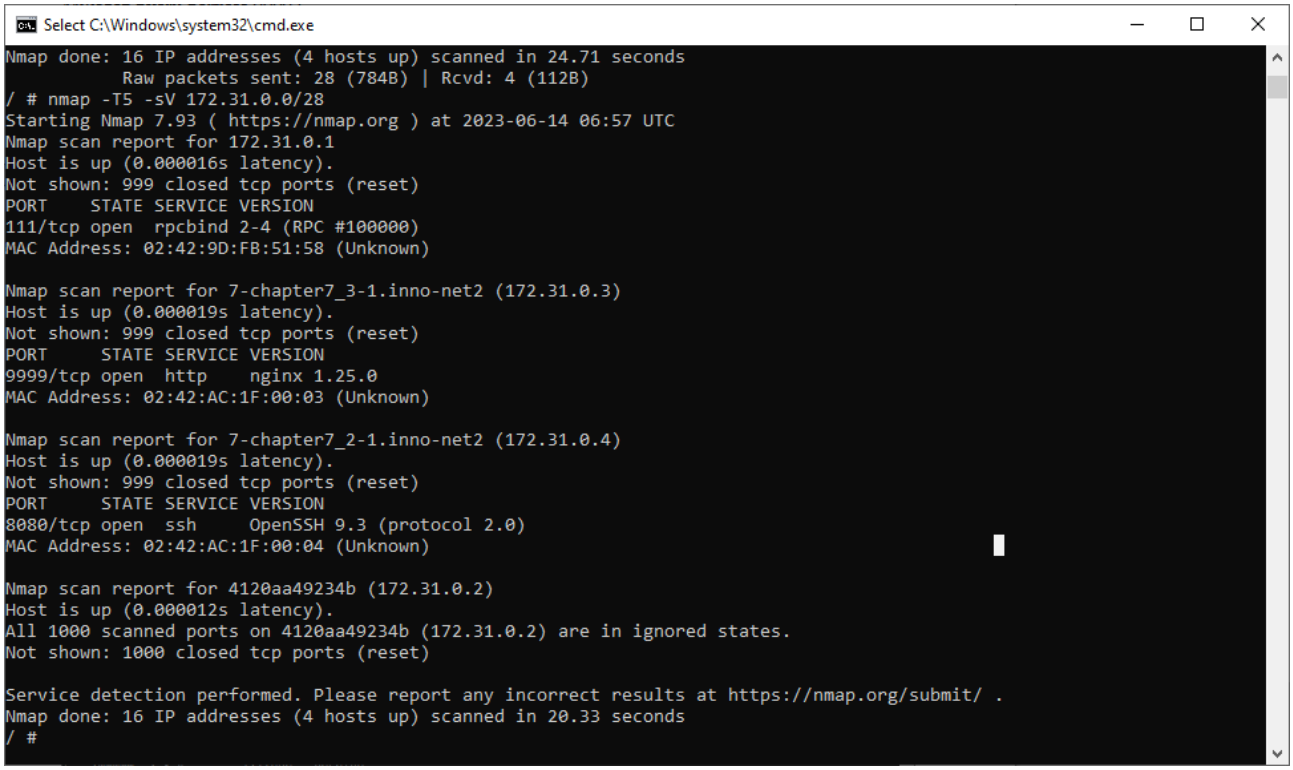
```
C:\Windows\system32\cmd.exe
[+] Running 3/3
 ⠿ Container 7-chapter7_4-1  Started
 ⠿ Container 7-chapter7_2-1  Started
 ⠿ Container 7-chapter7_3-1  Started

C:\Users\henkka3\Desktop\inno\chapters\7>docker exec -it 7-chapter7_4-1 /bin/sh
/ # ifconfig
eth0      Link encap:Ethernet  HWaddr 02:42:AC:1F:00:02
          inet addr:172.31.0.2  Bcast:172.31.255.255  Mask:255.255.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1006 (1006.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

/ # nmap -v -T5 -p0- -sT 172.31.0.0/28
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-14 06:54 UTC
Initiating ARP Ping Scan at 06:54
Scanning 15 hosts [1 port/host]
Completed ARP Ping Scan at 06:54, 1.17s elapsed (15 total hosts)
Initiating Parallel DNS resolution of 3 hosts. at 06:54
```

```
Select C:\Windows\system32\cmd.exe
58595/tcp open  unknown
MAC Address: 02:42:9D:FB:51:58 (Unknown)

Nmap scan report for 7-chapter7_3-1.inno-net2 (172.31.0.3)
Host is up (0.00058s latency).
Not shown: 65535 closed tcp ports (conn-refused)
PORT     STATE SERVICE
9999/tcp open  abyss
MAC Address: 02:42:AC:1F:00:03 (Unknown)

Nmap scan report for 7-chapter7_2-1.inno-net2 (172.31.0.4)
Host is up (0.00063s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
10514/tcp open  unknown
MAC Address: 02:42:AC:1F:00:04 (Unknown)

Initiating Connect Scan at 06:54
Scanning 4120aa49234b (172.31.0.2) [65536 ports]
Completed Connect Scan at 06:54, 2.34s elapsed (65536 total ports)
Nmap scan report for 4120aa49234b (172.31.0.2)
Host is up (0.00017s latency).
All 65536 scanned ports on 4120aa49234b (172.31.0.2) are in ignored states.
Not shown: 65536 closed tcp ports (conn-refused)

Read data files from: /usr/bin/../share/nmap
Nmap done: 16 IP addresses (4 hosts up) scanned in 24.71 seconds
           Raw packets sent: 28 (784B) | Rcvd: 4 (112B)
/ #
```

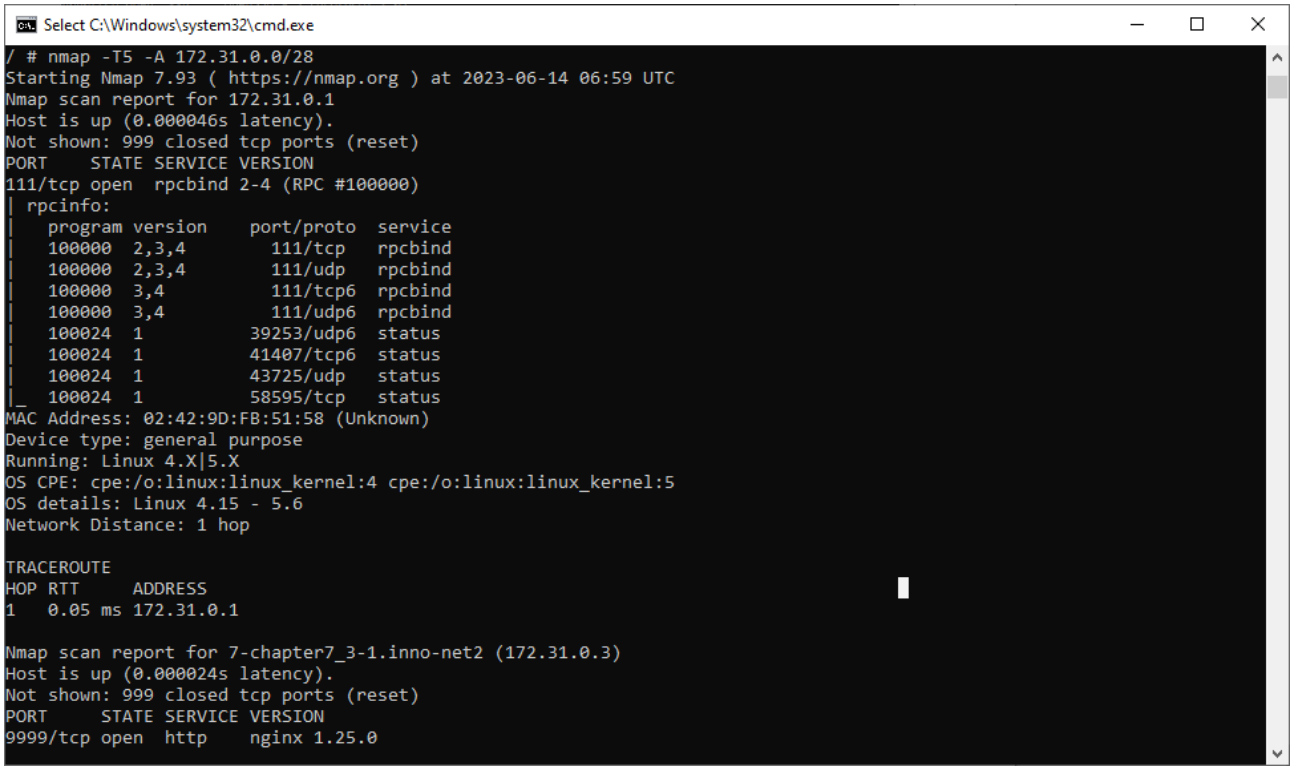
Mikähän pyörii portissa 9999?
Ja onko portissa 8080 nimenomaan http-proxy?

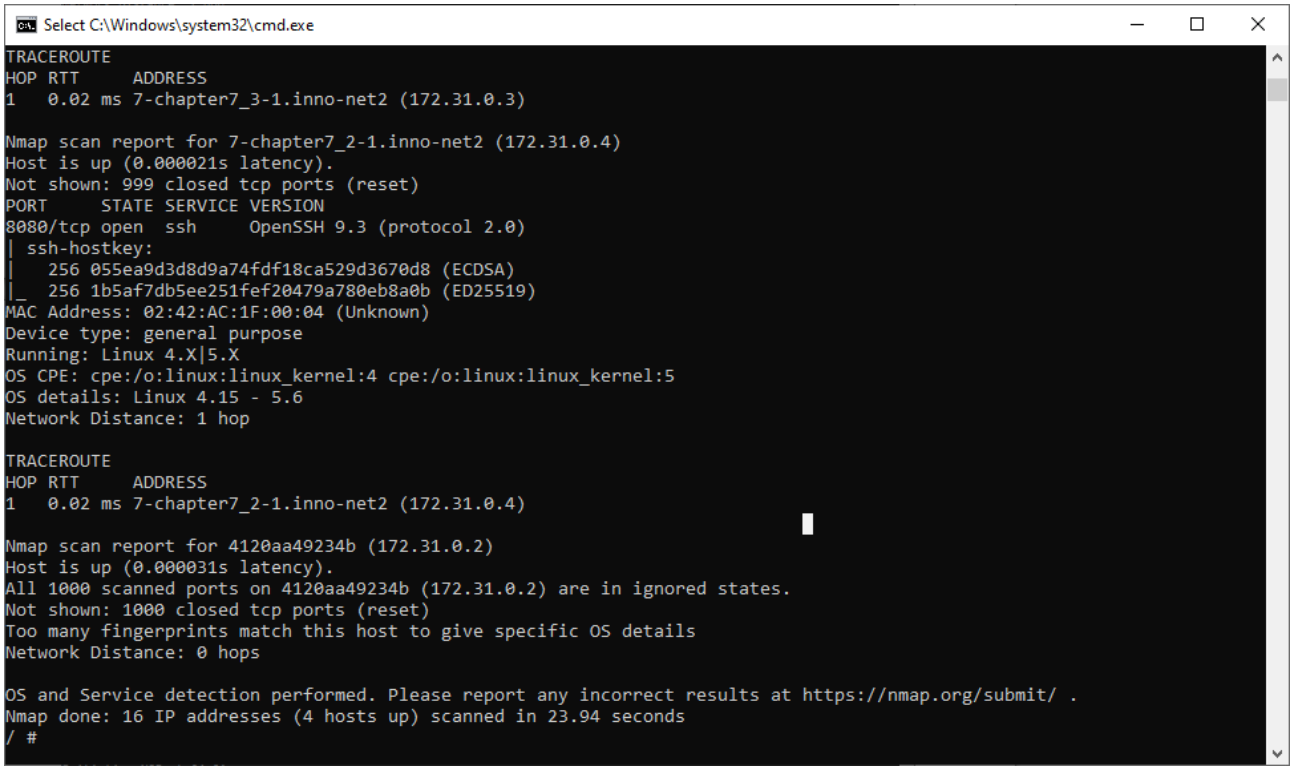
Selvitetään asia https://nmap.org/book/vscan.html mukaillen. Eli nmap -sV ip/maski .

Käytetään skannaukseen Alpine-konttia koska Devuaniin ei ollut ohjeita tehdessä saatavilla pakettia nmap-scripts mitä esim. “-sV”-optio vaatii.

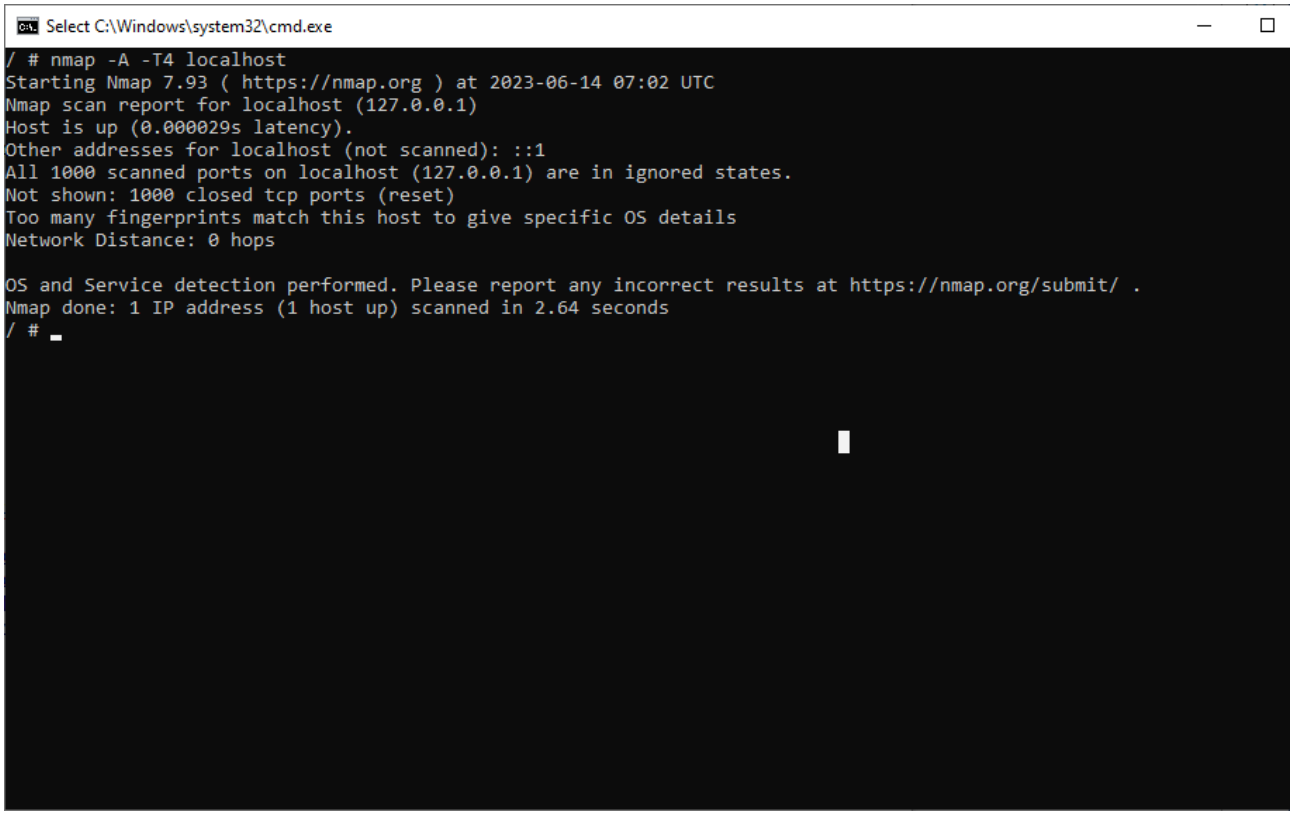


Komennolla “nmap -A ip/maski” lisätietoja.

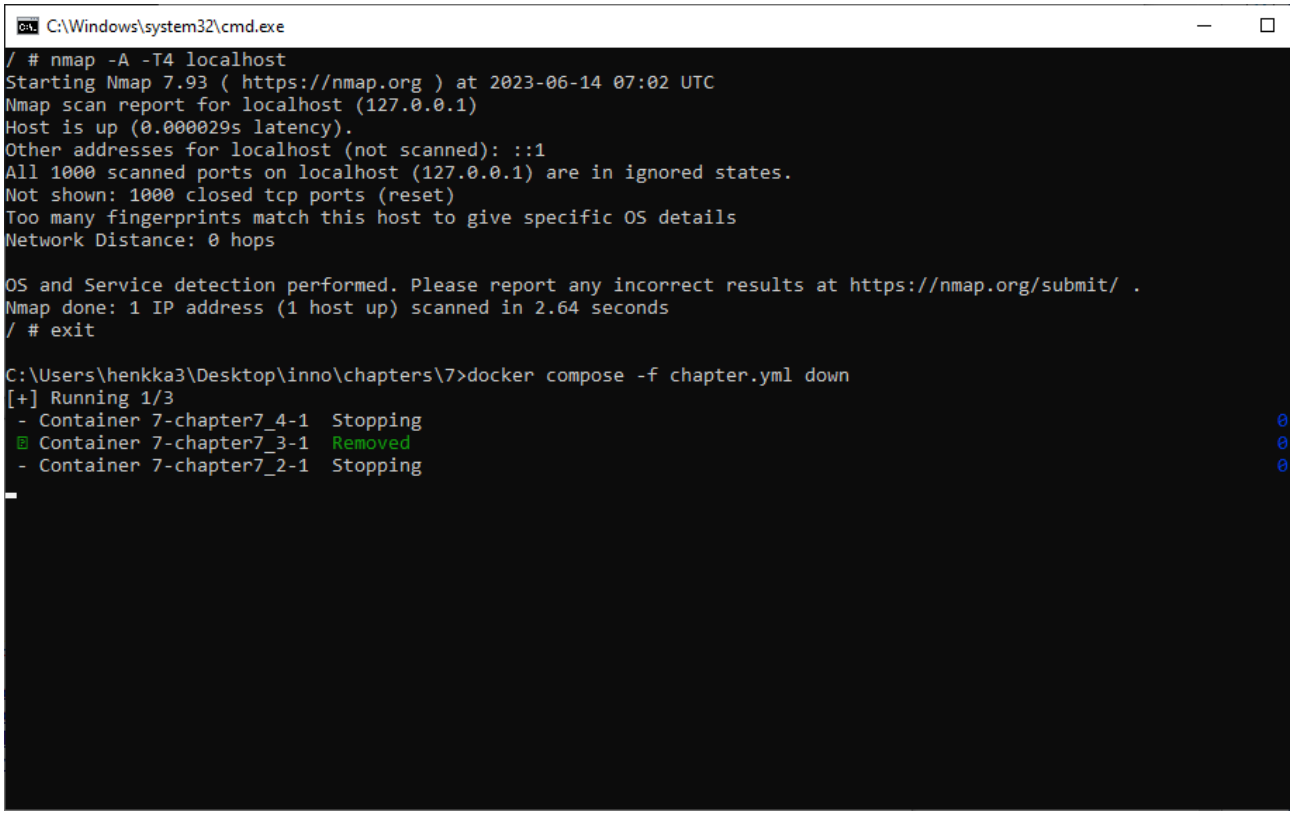




nmap -A -T4 localhost



7.3.exit



Kuten aiemmin, exit:illä ulos kontista.

7.4.

Muutamia linkkejä:

https://stackoverflow.com/questions/56871370/nse-failed-to-initialize-the-script-engine
https://stackoverflow.com/questions/56446898/nmap-could-not-locate-nse-main-lua
https://github.com/nmap/nmap/issues/2596
https://superuser.com/questions/1008977/nmap-wont-run-any-scripts

liittyy siihen miksi skannaavana konttina yleensä Alpine.

7.5.

Yritys lavastaa dns-servo johonkin muuhun porttiin kuin 53 ei ensimmäisillä yrityksillä onnistunut. Saattaa olla windows-alustan ominaisuus tai sitten ei.