

1. – 3.A.

```

osboxes@osboxes: ~
File Edit View Search Terminal Help

osboxes@osboxes:~$ sudo ufw enable
Firewall is active and enabled on system startup
osboxes@osboxes:~$ sudo ufw status
Status: active
osboxes@osboxes:~$ sudo ufw show raw
IPV4 (raw):
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts    bytes target     prot opt in     out     source            destination
   164    17826 ufw-before-logging-input all -- *      *        0.0.0.0/0        0.0.0.0/0

   164    17826 ufw-before-input all -- *      *        0.0.0.0/0        0.0.0.0/0
   114     8784 ufw-after-input all -- *      *        0.0.0.0/0        0.0.0.0/0
   103     7817 ufw-after-logging-input all -- *      *        0.0.0.0/0        0.0.0.0/0

   103     7817 ufw-reject-input all -- *      *        0.0.0.0/0        0.0.0.0/0
   103     7817 ufw-track-input all -- *      *        0.0.0.0/0        0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts    bytes target     prot opt in     out     source            destination
    0         0 ufw-before-logging-forward all -- *      *        0.0.0.0/0        0.0.0.0/0

    0         0 ufw-before-forward all -- *      *        0.0.0.0/0        0.0.0.0/0
    0         0 ufw-after-forward all -- *      *        0.0.0.0/0        0.0.0.0/0
    0         0 ufw-after-logging-forward all -- *      *        0.0.0.0/0        0.0.0.0/0

    0         0 ufw-reject-forward all -- *      *        0.0.0.0/0        0.0.0.0/0
    0         0 ufw-track-forward all -- *      *        0.0.0.0/0        0.0.0.0/0

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts    bytes target     prot opt in     out     source            destination
   44     5270 ufw-before-logging-output all -- *      *        0.0.0.0/0        0.0.0.0/0

   44     5270 ufw-before-output all -- *      *        0.0.0.0/0        0.0.0.0/0
    5       374 ufw-after-output all -- *      *        0.0.0.0/0        0.0.0.0/0
    5       374 ufw-after-logging-output all -- *      *        0.0.0.0/0        0.0.0.0/0

    5       374 ufw-reject-output all -- *      *        0.0.0.0/0        0.0.0.0/0
    5       374 ufw-track-output all -- *      *        0.0.0.0/0        0.0.0.0/0

Chain ufw-after-forward (1 references)
  pkts    bytes target     prot opt in     out     source            destination

Chain ufw-after-input (1 references)
  pkts    bytes target     prot opt in     out     source            destination
    3       234 ufw-skip-to-policy-input udp -- *      *        0.0.0.0/0        0.0.0.0/0
  udp dpt:137
    1       229 ufw-skip-to-policy-input udp -- *      *        0.0.0.0/0        0.0.0.0/0
  udp dpt:138
    0         0 ufw-skip-to-policy-input tcp -- *      *        0.0.0.0/0        0.0.0.0/0
  tcp dpt:139
    0         0 ufw-skip-to-policy-input tcp -- *      *        0.0.0.0/0        0.0.0.0/0
  tcp dpt:445
    0         0 ufw-skip-to-policy-input udp -- *      *        0.0.0.0/0        0.0.0.0/0
  udp dpt:67
    0         0 ufw-skip-to-policy-input udp -- *      *        0.0.0.0/0        0.0.0.0/0
  udp dpt:68
    7       504 ufw-skip-to-policy-input all -- *      *        0.0.0.0/0        0.0.0.0/0
  ADDRTYPE match dst-type BROADCAST

Chain ufw-after-logging-forward (1 references)
  pkts    bytes target     prot opt in     out     source            destination
    0         0 LOG all -- *      *        0.0.0.0/0        0.0.0.0/0
/min burst 10 LOG flags 0 level 4 prefix "[UFW BLOCK]"
limit: avg 3

Chain ufw-after-logging-input (1 references)
  pkts    bytes target     prot opt in     out     source            destination

```

```

osboxes@osboxes:~$ sudo ufw allow http
Rule added
Rule added (v6)
osboxes@osboxes:~$ sudo ufw allow https
Rule added
Rule added (v6)
osboxes@osboxes:~$ sudo ufw status
Status: active

To Action From
--
80/tcp ALLOW Anywhere
443/tcp ALLOW Anywhere
80/tcp (v6) ALLOW Anywhere (v6)
443/tcp (v6) ALLOW Anywhere (v6)

osboxes@osboxes:~$ sudo ufw deny ftp
Rule added
Rule added (v6)
osboxes@osboxes:~$ sudo ufw status
Status: active

To Action From
--
80/tcp ALLOW Anywhere
443/tcp ALLOW Anywhere
21/tcp DENY Anywhere
80/tcp (v6) ALLOW Anywhere (v6)
443/tcp (v6) ALLOW Anywhere (v6)
21/tcp (v6) DENY Anywhere (v6)

osboxes@osboxes:~$ sudo ufw deny outgoing 25
ERROR: Need 'to' or 'from' clause
osboxes@osboxes:~$ sudo ufw deny out 25
Rule added
Rule added (v6)
osboxes@osboxes:~$ sudo ufw status
Status: active

To Action From
--
80/tcp ALLOW Anywhere
443/tcp ALLOW Anywhere
21/tcp DENY Anywhere
80/tcp (v6) ALLOW Anywhere (v6)
443/tcp (v6) ALLOW Anywhere (v6)
21/tcp (v6) DENY Anywhere (v6)
25 DENY OUT Anywhere
25 (v6) DENY OUT Anywhere (v6)

osboxes@osboxes:~$ sudo ufw deny from 15.15.15.51
Rule added
osboxes@osboxes:~$ sudo ufw status
Status: active

To Action From
--
80/tcp ALLOW Anywhere
443/tcp ALLOW Anywhere
21/tcp DENY Anywhere
Anywhere DENY 15.15.15.51
80/tcp (v6) ALLOW Anywhere (v6)
443/tcp (v6) ALLOW Anywhere (v6)
21/tcp (v6) DENY Anywhere (v6)
25 DENY OUT Anywhere
25 (v6) DENY OUT Anywhere (v6)

osboxes@osboxes:~$

```

B.

1.

```
osboxes@osboxes:~$ clamscan /home

----- SCAN SUMMARY -----
Known viruses: 6985448
Engine version: 0.102.2
Scanned directories: 1
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 13.716 sec (0 m 13 s)
osboxes@osboxes:~$
```

2.

```
osboxes@osboxes: ~
File Edit View Search Terminal Help
osboxes@osboxes:~$ sudo apt-get update && sudo apt-get upgrade
Hit:1 http://dl.google.com/linux/chrome/deb stable InRelease
Hit:2 http://repository.spotify.com stable InRelease
Hit:3 http://archive.ubuntu.com/ubuntu bionic InRelease
Hit:4 http://archive.canonical.com/ubuntu bionic InRelease
Hit:5 http://archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:6 http://archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:7 http://security.ubuntu.com/ubuntu bionic-security InRelease
Ign:8 http://packages.linuxmint.com tina InRelease
Hit:9 http://packages.linuxmint.com tina Release
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
  casper fwupd fwupdate fwupdate-signed netplan.io
The following packages will be upgraded:
osboxes@osboxes:~$ sudo apt-get remove google-chrome-stable
[sudo] password for osboxes:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  google-chrome-stable
0 upgraded, 0 newly installed, 1 to remove and 5 not upgraded.
After this operation, 235 MB disk space will be freed.
Do you want to continue? [Y/n] Y
(Reading database ... 267689 files and directories currently installed.)
Removing google-chrome-stable (81.0.4044.138-1) ...
update-alternatives: using /usr/bin/firefox to provide /usr/bin/x-www-browser
(x-www-browser) in auto mode
update-alternatives: using /usr/bin/firefox to provide /usr/bin/gnome-www-brow
(gnome-www-browser) in auto mode
Processing triggers for desktop-file-utils (0.23+linuxmint6) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for gnome-menus (3.13.3-11ubuntu1.1) ...
Processing triggers for mime-support (3.60ubuntu1) ...
osboxes@osboxes:~$
```


3. Valitsin salasanapolitiikan muokkaamisen ja turvattomien protokollien käytöstä poistamisen



```
osboxes@osboxes: ~  
File Edit View Search Terminal Help  
[1/2] /etc/pam.d/common-password  
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.  
# To take advantage of this, it is recommended that you configure any  
# local modules either before or after the default block, and use  
# pam-auth-update to manage selection of other modules. See  
# pam-auth-update(8) for details.  
  
# here are the per-package modules (the "Primary" block)  
password [success=1 default=ignore] pam_unix.so obscure sha512  
# here's the fallback if no module succeeds  
password requisite pam_deny.so  
# prime the stack with a positive return value if there isn't one already;  
# this avoids us returning an error just because nothing sets a success code  
# since the modules above will each just jump around  
password required pam_permit.so  
# and here are more per-package modules (the "Additional" block)  
password optional pam_gnome_keyring.so  
password optional pam_ecryptfs.so  
# end of pam-auth-update config  
  
password sufficient pam_unix.so use auththok md5 shadow remember=13  
password requisite pam_cracklib.so ucredit=-1 lcredit=-1 ocredit=-1  
  
# for private user groups, i. e. the uid is the same as gid, and username is  
# the same as the primary group name: for these, the user permissions will be  
# used as group permissions, e. g. 022 will become 002.  
#  
# Prefix these values with "0" to get octal, "0x" to get hexadecimal.  
#  
ERASECHAR 0177  
KILLCHAR 025  
UMASK 022  
  
# Password aging controls:  
#  
# PASS_MAX_DAYS Maximum number of days a password may be used.  
# PASS_MIN_DAYS Minimum number of days allowed between password changes.  
# PASS_WARN_AGE Number of days warning given before a password expires.  
#  
PASS_MAX_DAYS 99999  
PASS_MIN_DAYS 7  
PASS_WARN_AGE 7  
  
# Min/max values for automatic uid selection in useradd  
#  
UID_MIN 1000  
UID_MAX 60000  
# System accounts  
[ Search Wrapped ]  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo M-A Mark Text  
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line M-E Redo M-G Copy Text  
osboxes@osboxes:~$ sudo apt-get --purge remove xinetd nis yp-tools tftpd atftdp tftpd-hpa telnetd rsh-server rsh-redone-  
server  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
E: Unable to locate package atftdp  
osboxes@osboxes:~$
```