tulemüür

ufw
https://help.ubuntu.com/community/UFW
https://help.ubuntu.com/community/Gufw
https://help.ubuntu.com/lts/serverguide/firewall.html
https://kuutorvaja.eenet.ee/wiki/Iptables_puust_ja_punaseks
tulemüüri loeng

Käesolevaga tegeleme tarkvaralise tulemüüriga. Praktikas rakendatakse sageli riistvaralist tulemüüri. Enne tulemüüri sätetega tegelemist tasub teha (seisvast) VMist hetktõmmis (*snapshot*).

uuendame serveris ka tarkvara:
sudo apt update && sudo apt upgrade && sudo apt clean

olek:
sudo ufw status verbose (detailsem)
sudo ufw status numbered #kui on sisse lülitatud
sudo ufw status
sudo ufw show added

hetkel kehtivad reeglid
sudo iptables -L
grep DEFAULT_ /etc/default/ufw

enne tulemüüri sisselülitamist keelame kogu siseneva liikluse
sudo ufw default deny (vaikimisi rakendatakse sisenevale liiklusele)
täpsemalt saab:
sudo ufw default allow outgoing
sudo ufw default deny incoming

„*oksa läbisaagimine, millel istutakse*" ehk iseendal SSH-ligipääsu äravõtmine - keelame kogu siseneva liikluse ja aktiveerime tulemüüri enne kui SSH pordi lubame...

lubame ssh
sudo ufw allow ssh

praktikas turvalisem lisada - takistame rünnakud SSH pordile (⩾6 päringut 30 s jooksul):
sudo ufw limit ssh (ka: *sudo ufw limit 22/tcp*)
sudo ufw limit from 205.184.2.4 to tcp 22 (konkreetne IP)
sudo ufw limit 2022/tcp comment 'SSH port rate limit' (SSH mittestandardse 2022 pordi peal)

man ufw
ufw supports connection rate limiting, which is useful for protecting against brute-force login attacks. When a limit rule is used, ufw will normally allow the connection but will deny connections if an IP address attempts to initiate 6 or more connections within 30 seconds. See http://www.debian-administration.org/articles/187 for details.

kiire (`-F` *fast mode*) avatud portide skaneerimine (teisest virtuaalmasinast, vajadusel paigaldada nmap):
`nmap -F 192.168.56.xxx` (üks IP)
`nmap -F 192.168.56.0/24` (terve võrgusegment)

vaatame, mis on lisatud (ka siis kui tulemüür ei ole aktiivne)
sudo ufw show added

ufw musta nimekirja panemine
failis /etc/ufw/before.rules

```
## blacklist section
# block just 192.168.xxx.xxx (e.g. host)
-A ufw-before-input -s 192.168.5.101 -j DROP
# block 184.105.*.*
-A ufw-before-input -s 184.105.0.0/16 -j DROP
# don't delete the 'COMMIT' line or these rules won't be processed
COMMIT
```

millise pordi peal töötab SSH?
cat /etc/services | grep ssh - vaikimisi port
grep Port /etc/ssh/sshd_config - antud masinas kasutuselolev port (vaikimisi port on välja kommenteeritud)

kasutatakse failis */etc/services* esimeses veerus olevaid nimetusi, näiteks veebiserveri lubamiseks
sudo ufw allow http (või ka sudo ufw allow 80/tcp)
sudo ufw allow https (või ka sudo ufw allow 443/tcp)

kustutamine (ka siis kui tulemüür ei ole aktiivne):
sudo ufw delete allow http #kui oli lubatud
sudo ufw delete deny http #kui oli keelatud

konkreetse pordi/protokolli lubamine:
sudo ufw allow 22/tcp

kui SSH kaudu ligipääs lubatud siis aktiveerime tulemüüri (vastasel korral ei pääse üle võrgu SSH'ga enam ligi peale tulemüüri aktiveerimist - võib tähendada probleemi):
sudo ufw enable

rakenduste profiilid:
sudo ufw app list
serveris on üldjuhul olemas vaid OpenSSH profiil

vaatame infot:
sudo ufw app info OpenSSH

algsätete taastamine
sudo ufw reset

Graafiline liides ufw'le - gufw (tööjaamas):
sudo apt update && sudo apt install gufw && sudo apt clean

Harjutus
Kopeerime *desktop* masinast valmisprofiili serverisse. Selleks paigaldame ka *desktop* masinasse ufw ja ka gufw (ufw GUI). Profiili saab kopeerida (NB! veendu enne failinimedes ja otsiteekonnas):
/etc/gufw/app_profiles/samba.jhansonxi -> *desktop* masinas
/etc/ufw/applications.d/samba (faililaiend ei ole oluline) -> serveris

Kopeerimiseks võib kasutada ka graafilist liidest (Nautilus failihaldur) või siis käsurida:
scp /etc/gufw/app_profiles/samba.jhansonxi kasutaja@server:/etc/ufw/applications.d/samba

lubame Samba konkreetsest sisevõrgust (host-only võrguliides):
sudo ufw --dry-run allow from 192.168.56.0/24 to any app Samba #simuleerime
sudo ufw allow from 192.168.56.0/24 to any app Samba #rakendame
Samba (sisuliselt MS Windowsi kohtvõrk) lubamine kogu maailmale ei ole hea mõte tulenevalt selle protokolli turvaprobleemidest. Samuti ei ole hea mõte avalikus võrgus seda lubada - pigem üle VPNi sisevõrgus.

Harjutamise eesmärgil võib valida veel mõne profiili **/etc/gufw/app_profiles/** kaustast ja serverisse kopeerida.

vaatame olekut kus numbrid ridadel ees:
sufo ufw status numbered

reegli kustutamiseks:
sudo ufw delete 2 (asenda number õigega, vastata y kinnitamiseks)

kustutamine (ka siis kui tulemüür ei ole aktiivne):
sudo ufw delete allow http #kui oli lubatud
sudo ufw delete deny http #kui oli keelatud

ping'i keelamine
`sudo cp /etc/ufw/before.rules /etc/ufw/before.rules_backup` #varukoopia

asendame lubamise keelamisega:
`sudo sed -i '/ufw-before-input.*icmp/s/ACCEPT/DROP/g' /etc/ufw/before.rules` #ettevaatust! sed on võimas käsk

sisuliselt asendatakse
```
# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT
```

sellega:
```
 # ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j DROP
-A ufw-before-input -p icmp --icmp-type source-quench -j DROP
-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP
-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP
-A ufw-before-input -p icmp --icmp-type echo-request -j DROP
```

laadime tulemüüri reeglid peale muutmist uuesti:
`sudo ufw reload`

või kui oli keelatud siis lubame:
sudo ufw enable

netstat
liidesed: netstat -i

ruutimine: netstat -rn
UG – up, gateway
UH – up, route to single host (and not a network)
man route -> Flags

netstat -tlnp #tcp, listening, numeric, program
netstat -ulnp #udp, listening, numeric, program
netstat -tulnp #tcp, udp, listening, numeric, program
netstat -a #kõik ühendused
lisainfo: *man netstat*

VPN
Siin on vajalik tulemüüris IP protokoll 47 ja 1723/tcp port lubada. Ruuter peaks lisaks lubama ka *VPN Passthrough* ja seda PPTP, IPsec ja L2TP osas - seda just NAT'i tõttu.

/etc/ufw/before.rules
-A ufw-before-input -p 47 -j ACCEPT
-A ufw-before-output -p 47 -j ACCEPT
-A ufw-before-input -p tcp -s 0.0.0.0/0 --sport 1723 -j ACCEPT
-A ufw-before-output -p tcp -d 0.0.0.0/0 --dport 1723 -j ACCEPT

sama iptables'iga:
iptables -I INPUT -p 47 -m state --state ESTABLISHED -j ACCEPT
iptables -I OUTPUT -p 47 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -p tcp --sport 1723 -m state --state ESTABLISHED -j ACCEPT
iptables -I OUTPUT -p tcp --dport 1723 -m state --state NEW,ESTABLISHED -j ACCEPT

teenused

SystemV süsteemis asuvad /etc/rc<level>.d/ kataloogis, S on start ja K on kill ehk siis kas teenus käivitatakse või pannakse seisma - tegemist on symlink'idega. Lisainfo käivitustasemete kohta.
Teenuste haldamine /etc/init.d/<teenus> , nt /etc/init.d/networking ja parameetrid tavaliselt start, stop, restart, status

Ubuntus
ajutiselt lubamine (näide):
sudo service apache2 start | status | stop | restart

Upstart'i puhul esmalt määrame käsitsi hallatavaks, tekitades .override faili:
sudo echo manual > /etc/init/SERVICE.override
nt: sudo echo manual > /etc/init/apache2.override
Kui taas vajadus automaatse halduse järele siis kustutada .override fail
sudo rm /etc/init/apache2.override

Pisut graafilisem on sysv-rc-conf kus saab +/- märkidega reguleerida teenuste käivitumist erinevatel töötasemetel (*runlevel*).

systemd
vaatame versiooni: **systemd -version**
info käivitamisest: **systemd-analyze**
ajalises plaanis: **systemd-analyze blame** (abiinfo: **systemd-analyze -h** ja ka **man systemd-analyze**)

Teha kindlaks, millised 3 teenust võtavad kõige rohkem aega.

systemd päringutest väljumiseks q, abiinfo h (kasutatakse less'i)

mis on süsteemis olemas:
systemctl list-unit-files
systemctl list-units
ebaõnnestunud teenused: **systemctl --failed**

haldamine:
systemctl start name.service
systemctl stop name.service
systemctl restart name.service
systemctl reload name.service
systemctl status name.service
systemctl enable name.service
systemctl disable name.service

vaatame kas teenus on lubatud, aktiivne
systemctl is-enabled name.service
systemctl is-active name.service

info teenuse kohta
systemctl show name.service

keelame (mask) ja lubame (unmask) teenuse käivitamise:
systemctl mask name.service
systemctl unmask name.service
… enne kui teenust lubada/keelata saab tuleb *mask* eemaldada. Väljumiseks q.

Lisalugemist systemd kohta Arch Linuxi wikist.