Ishita Hardasmalani

C14-2103058

EXPERIMENT NO. 9

Aim: Design of personal Firewall using Iptables

Theory:

All packets inspected by iptables pass through a sequence of built-in tables (queues) for processing. Each of these queues is dedicated to a particular type of packet activity and is controlled by an associated packet transformation/filtering chain.

1. Filter Table

Filter is default table for iptables.

Iptables's filter table has the following built-in chains.

- INPUT chain – Incoming to firewall. For packets coming to the local server.
- OUTPUT chain – Outgoing from firewall. For packets generated locally and going out of the local server.
- FORWARD chain – Packet for another NIC on the local server. For packets routed through the local server.

2. NAT Table

This table is consulted when a packet that creates a new connection is encountered.
Iptable's NAT table has the following built-in chains.

- PREROUTING chain – Alters packets before routing. i.e Packet translation happens immediately after the packet comes to the system (and before routing). This helps to translate the destination ip address of the packets to something that matches the routing on the local server. This is used for DNAT (destination NAT).
- POSTROUTING chain – Alters packets after routing. i.e Packet translation happens when the packets are leaving the system. This helps to translate the source ip address of the packets to something that might match the routing on the destination server. This is used for SNAT (source NAT).
- OUTPUT chain – NAT for locally generated packets on the firewall.

3. Mangle Table

Iptables's Mangle table is for specialized packet alteration. This alters QOS bits in the TCP header. Mangle table has the following built-in chains.

- PREROUTING chain
- OUTPUT chain
- FORWARD chain
- INPUT chain
- POSTROUTING chain

4. Raw Table

Iptable's Raw table is for configuration exemptions. Raw table has the following built-in chains.

- PREROUTING chain
- OUTPUT chain

5. Security Table

This table is used for Mandatory Access Control (MAC) networking rules, such as those enabled by the SECMARK and CONNSECMARK targets. Mandatory Access Control is implemented by Linux Security Modules such as SELinux. The security table is called after the filter table, allowing any Discretionary Access Control (DAC) rules in the filter table to take effect before MAC rules. This table provides the following built-in chains: INPUT (for packets coming into the box itself), OUTPUT (for altering locally-generated packets before routing), and FORWARD (for altering packets being routed through the box).

Chains

Tables consist of *chains*, Rules are combined into different chains. The kernel uses chains to manage packets it receives and sends out. A chain is simply a checklist of rules which are lists of rules which are followed in order. The rules operate with an if-then -else structure.

Input – This chain is used to control the behaviour for incoming connections. For example, if a user attempts to SSH into your PC/server, iptables will attempt to match the IP address and port to a rule in the input chain.

Forward – This chain is used for incoming connections that aren't actually being delivered locally. Think of a router – data is always being sent to it but rarely actually destined for the router itself; the data is just forwarded to its target.

Output – This chain is used for outgoing connections. For example, if you try to ping howtogeek.com, iptables will check its output chain to see what the rules are regarding ping and howtogeek.com before making a decision to allow or deny the connection attempt.

Targets:

ACCEPT: Allow packet to pass through the firewall.

DROP: Deny access by the packet.

REJECT: Deny access and notify the server.

QUEUE: Send packets to user space.

RETURN: jump to the end of the chain and let the default target process it

iptables command Switch	Description
-L	Listing of rules present in the chain
-n	Numeric output of addresses and ports
-v	Displays the rules in verbose mode
-t <-table->	If you don't specify a table, then the filter table is assumed. As discussed before, the possible built-in tables include: filter, nat, mangle
-j <target>	Jump to the specified target chain when the packet matches the current rule.
-A	Append rule to end of a chain
-F	Flush. Deletes all the rules in the selected table
-p <protocol-type>	Match protocol. Types include, icmp, tcp, udp, and all
-s <ip-address>	Match source IP address
-d <ip-address>	Match destination IP address
-i <interface-name>	Match "input" interface on which the packet enters.
-o <interface-name>	Match "output" interface on which the packet exits

Steps:-

1. Get root access: $ sudo su root
2. # apt-get install iptables

Commands:-

1. To see the list of iptables rules

iptables -L

. Initially it is empty

2. To block outgoing traffic to a particular destination for a specific protocol from a machine

Syntax: iptables -I OUTPUT -s <your ip> -d <neighbour ip> -p <protocol> -j <action>

Open one terminal and Ping the neighbour. Let the ping run.

#ping 192.168.208.6

Open another terminal and run the iptables command

iptables -I OUTPUT -s 192.168.208.18 -d 192.168.208.6 -p icmp -j DROP

2. To allow outgoing traffic to a particular destination for a specific protocol from a machine

iptables -I OUTPUT -s 192.168.208.18 -d 192.168.208.6 -p icmp -j ACCEPT

3. To block outgoing traffic to a particular destination for a specific protocol from a machine for sometime

iptables -I OUTPUT -s 192.168.208.18 -d 192.168.208.6 -p icmp -j REJECT

Allow the traffic again by using ACCEPT instead of REJECT

4. To block incoming traffic from particular destination for a specific protocol to machine

Syntax: iptables -I INPUT -s <neighbour ip> -d <firewall ip> -p <protocol> -j <action>

Open one terminal and Ping the neighbour. Let the ping run.

#ping 192.168.208.6

Open another terminal and run the iptables command

 # iptables -I INPUT -s 192.168.208.6 -d 192.168.208.18 -p icmp -j DROP

5. To allow incoming traffic from particular destination for a specific protocol to machine

Syntax: iptables -I INPUT -s <neighbour ip> -d <firewall ip> -p <protocol> -j <action>

Open another terminal and run the iptables command

 # iptables -I INPUT -s 192.168.208.6 -d 192.168.208.18 -p icmp -j ACCEPT

Check the ping status on the other terminal

6. To clear the rules in iptables

iptables -F

7. To block specific URL from machine

 # iptables -t filter -I OUTPUT -m string --string facebook.com -j REJECT --algo kmp

It will block facebook.com by performing string matching. The algorithm used for string matching is KMP.

If we change target *from REJECT to ACCEPT*, the site can be visited again.

Observations:

1. In case of OUTPUT chain, for DROP and REJECT chain, at source machine we get two different messages.

   For DROP – 'Operation Not Permitted'. Here No acknowledgement is provided.

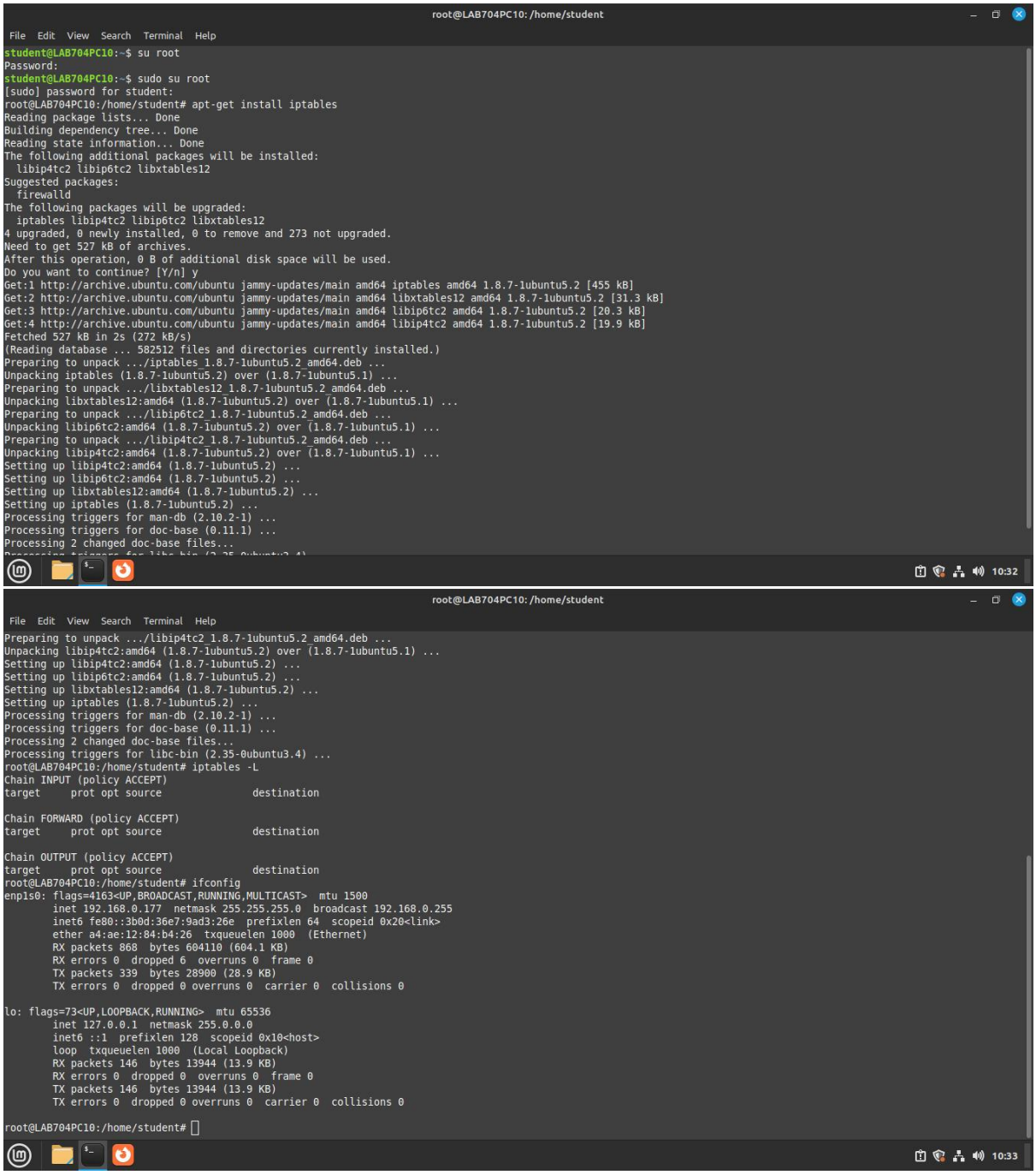
   For REJECT – 'Destination Port Unreachable'. Here acknowledgement is given.

2. In case of INPUT chain for DROP and REJECT chain at source machine we get two different responses as follows:

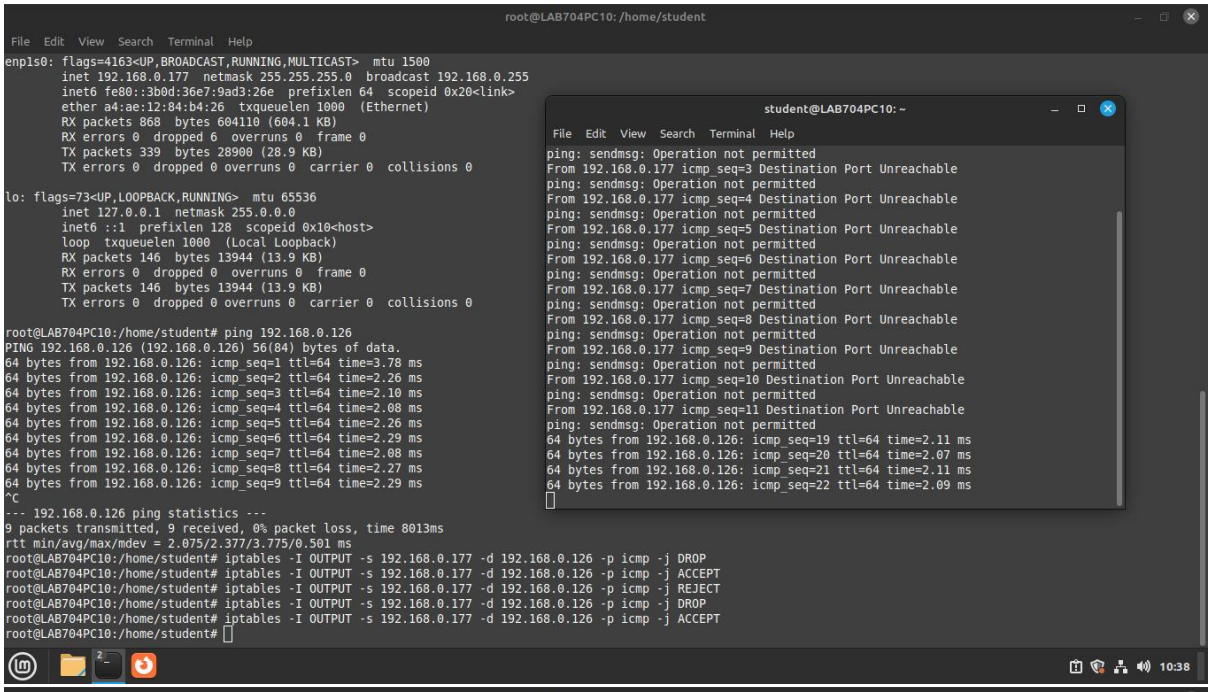
   For DROP – No message. Here No acknowledgement is provided.

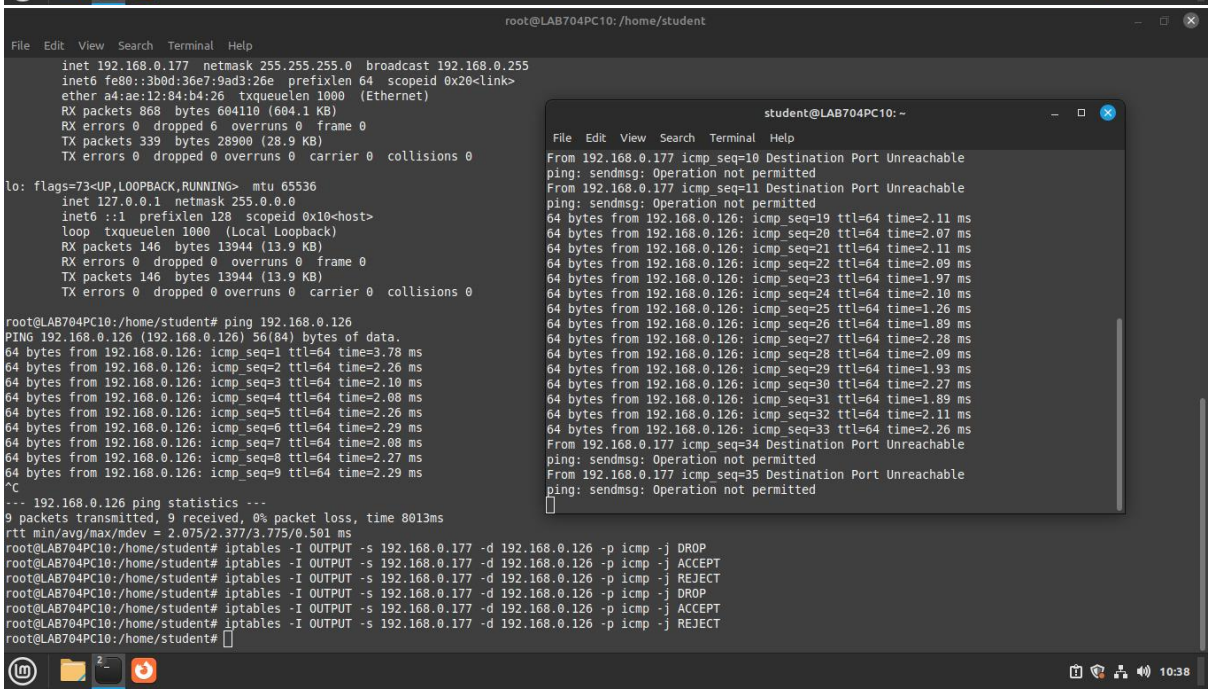
   For REJECT – 'Destination Port Unreachable'. Here acknowledgement is given.

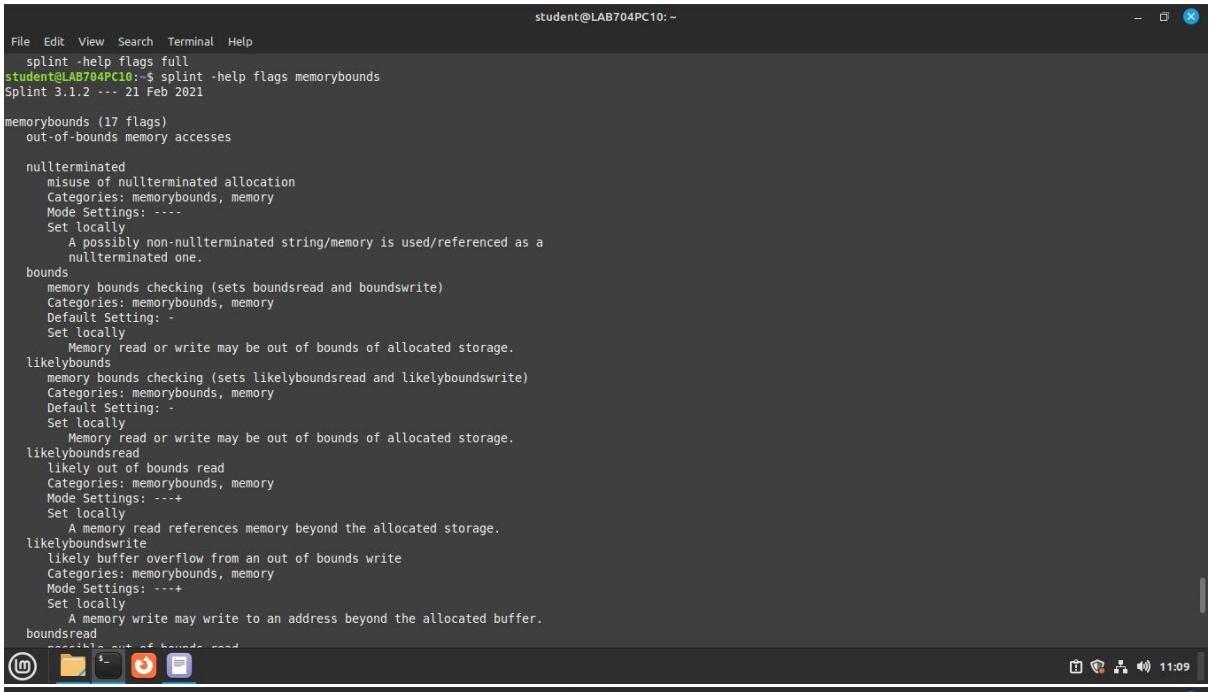
Output:

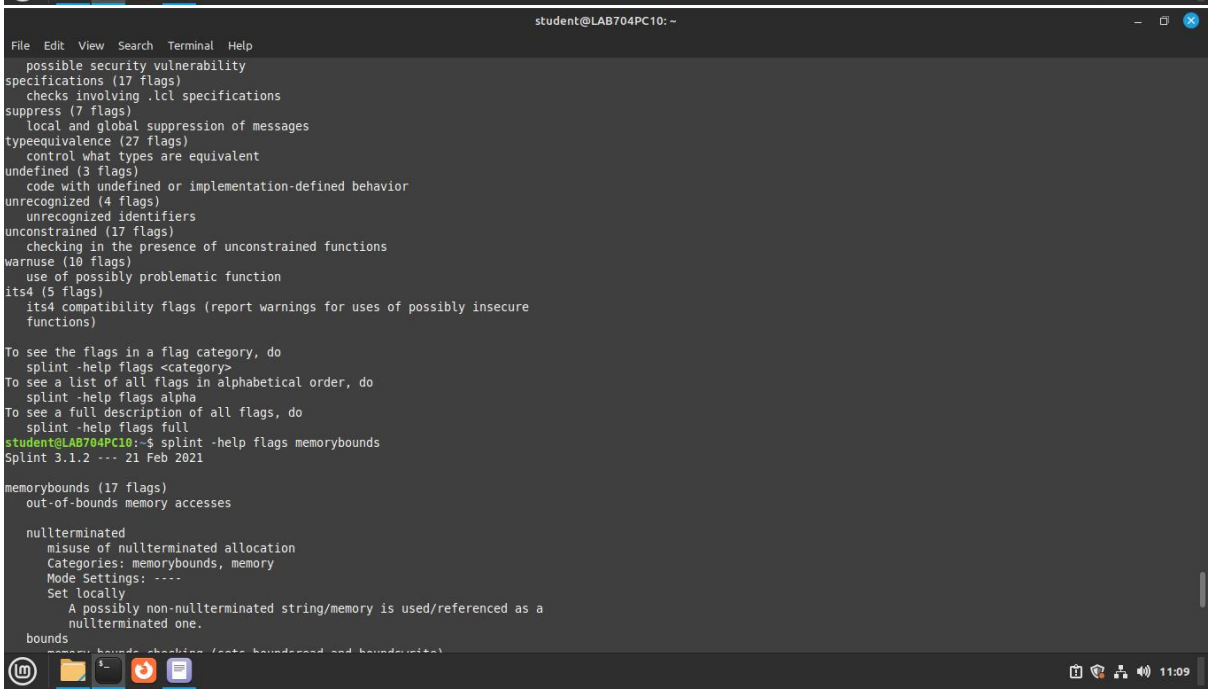

root@LAB704PC10: /home/student
File Edit View Search Terminal Help
student@LAB704PC10:~$ su root
Password:
student@LAB704PC10:~$ sudo su root
[sudo] password for student:
root@LAB704PC10:/home/student# apt-get install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libip4tc2 libip6tc2 libxtables12
Suggested packages:
firewalld
The following packages will be upgraded:
iptables libip4tc2 libip6tc2 libxtables12
4 upgraded, 0 newly installed, 0 to remove and 273 not upgraded.
Need to get 527 kB of archives.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 iptables amd64 1.8.7-1ubuntu5.2 [455 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libxtables12 amd64 1.8.7-1ubuntu5.2 [31.3 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip6tc2 amd64 1.8.7-1ubuntu5.2 [20.3 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip4tc2 amd64 1.8.7-1ubuntu5.2 [19.9 kB]
Fetched 527 kB in 2s (272 kB/s)
(Reading database ... 582512 files and directories currently installed.)
Preparing to unpack .../iptables_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking iptables (1.8.7-1ubuntu5.2) over (1.8.7-1ubuntu5.1) ...
Preparing to unpack .../libxtables12_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking libxtables12:amd64 (1.8.7-1ubuntu5.2) over (1.8.7-1ubuntu5.1) ...
Preparing to unpack .../libip6tc2_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking libip6tc2:amd64 (1.8.7-1ubuntu5.2) over (1.8.7-1ubuntu5.1) ...
Preparing to unpack .../libip4tc2_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking libip4tc2:amd64 (1.8.7-1ubuntu5.2) over (1.8.7-1ubuntu5.1) ...
Setting up libip4tc2:amd64 (1.8.7-1ubuntu5.2) ...
Setting up libip6tc2:amd64 (1.8.7-1ubuntu5.2) ...
Setting up libxtables12:amd64 (1.8.7-1ubuntu5.2) ...
Setting up iptables (1.8.7-1ubuntu5.2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for doc-base (0.11.1) ...
Processing 2 changed doc-base files...
10:32

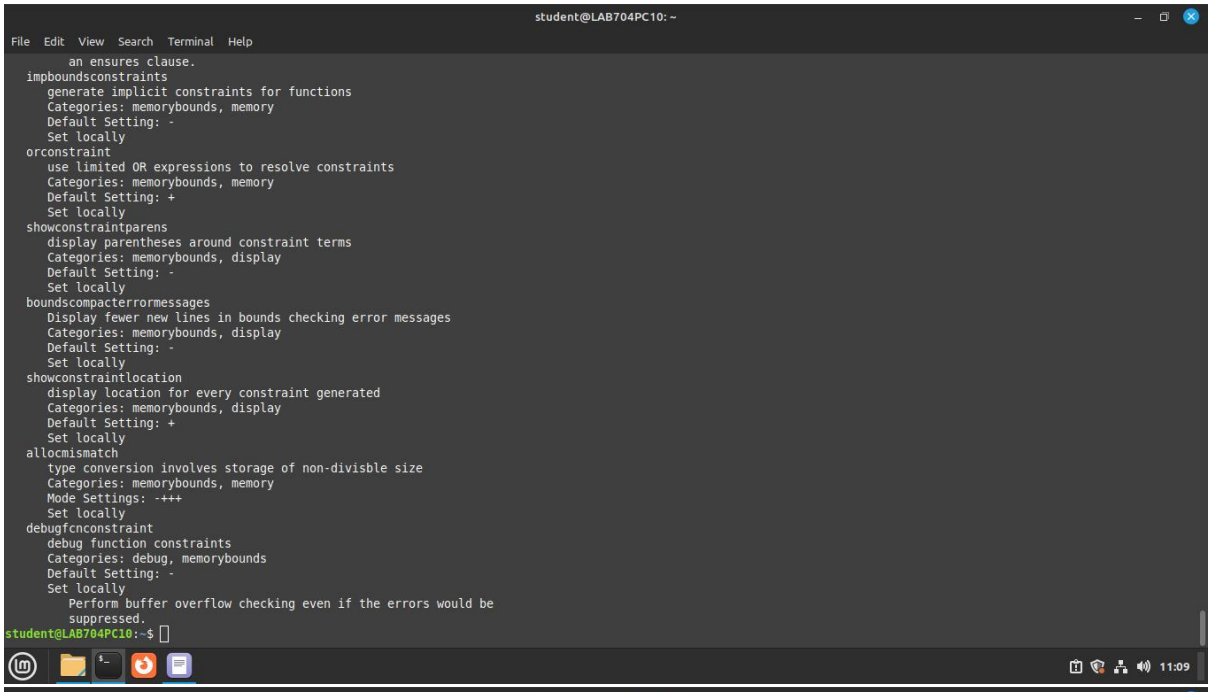
root@LAB704PC10: /home/student
File Edit View Search Terminal Help
Preparing to unpack .../libip4tc2_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking libip4tc2:amd64 (1.8.7-1ubuntu5.2) over (1.8.7-1ubuntu5.1) ...
Setting up libip4tc2:amd64 (1.8.7-1ubuntu5.2) ...
Setting up libip6tc2:amd64 (1.8.7-1ubuntu5.2) ...
Setting up libxtables12:amd64 (1.8.7-1ubuntu5.2) ...
Setting up iptables (1.8.7-1ubuntu5.2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for doc-base (0.11.1) ...
Processing 2 changed doc-base files...
Processing triggers for libc-bin (2.35-0ubuntu3.4) ...
root@LAB704PC10:/home/student# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
root@LAB704PC10:/home/student# ifconfig
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.177 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::3b0d:36e7:9ad3:26e prefixlen 64 scopeid 0x20<link>
ether a4:ae:12:84:b4:26 txqueuelen 1000 (Ethernet)
RX packets 868 bytes 604110 (604.1 KB)
RX errors 0 dropped 6 overruns 0 frame 0
TX packets 339 bytes 28900 (28.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 146 bytes 13944 (13.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 146 bytes 13944 (13.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@LAB704PC10:/home/student#
10:33

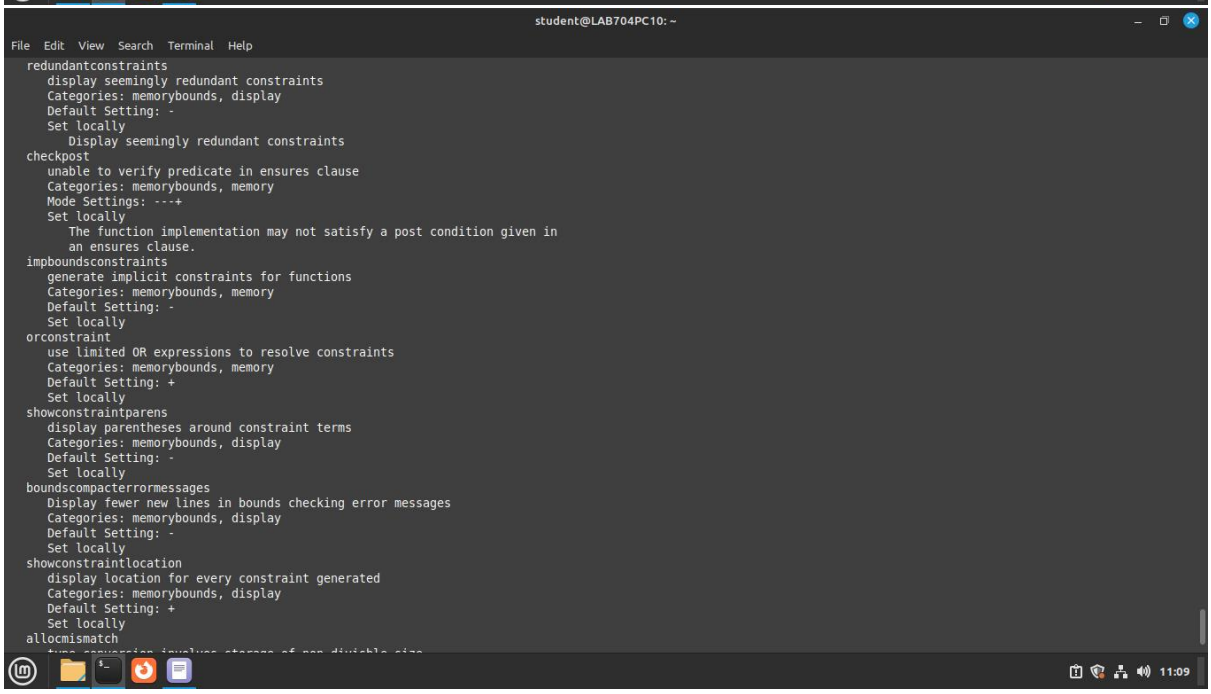

root@LAB704PC10: /home/student
File Edit View Search Terminal Help
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.177 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::3b0d:36e7:9ad3:26e prefixlen 64 scopeid 0x20<link>
ether a4:ae:12:84:b4:26 txqueuelen 1000 (Ethernet)
RX packets 868 bytes 604110 (604.1 KB)
RX errors 0 dropped 6 overruns 0 frame 0
TX packets 339 bytes 28900 (28.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 146 bytes 13944 (13.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 146 bytes 13944 (13.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@LAB704PC10:/home/student# ping 192.168.0.126
PING 192.168.0.126 (192.168.0.126) 56(84) bytes of data.
64 bytes from 192.168.0.126: icmp_seq=1 ttl=64 time=3.78 ms
64 bytes from 192.168.0.126: icmp_seq=2 ttl=64 time=2.26 ms
64 bytes from 192.168.0.126: icmp_seq=3 ttl=64 time=2.10 ms
64 bytes from 192.168.0.126: icmp_seq=4 ttl=64 time=2.08 ms
64 bytes from 192.168.0.126: icmp_seq=5 ttl=64 time=2.26 ms
64 bytes from 192.168.0.126: icmp_seq=6 ttl=64 time=2.29 ms
64 bytes from 192.168.0.126: icmp_seq=7 ttl=64 time=2.08 ms
64 bytes from 192.168.0.126: icmp_seq=8 ttl=64 time=2.27 ms
64 bytes from 192.168.0.126: icmp_seq=9 ttl=64 time=2.29 ms
^C
--- 192.168.0.126 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 2.075/2.377/3.775/0.501 ms
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j DROP
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j ACCEPT
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j REJECT
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j DROP
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j ACCEPT
root@LAB704PC10:/home/student#
student@LAB704PC10: ~
File Edit View Search Terminal Help
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=3 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=4 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=5 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=6 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=7 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=8 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=9 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=10 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=11 Destination Port Unreachable
ping: sendmsg: Operation not permitted
64 bytes from 192.168.0.126: icmp_seq=19 ttl=64 time=2.11 ms
64 bytes from 192.168.0.126: icmp_seq=20 ttl=64 time=2.07 ms
64 bytes from 192.168.0.126: icmp_seq=21 ttl=64 time=2.11 ms
64 bytes from 192.168.0.126: icmp_seq=22 ttl=64 time=2.09 ms
10:38

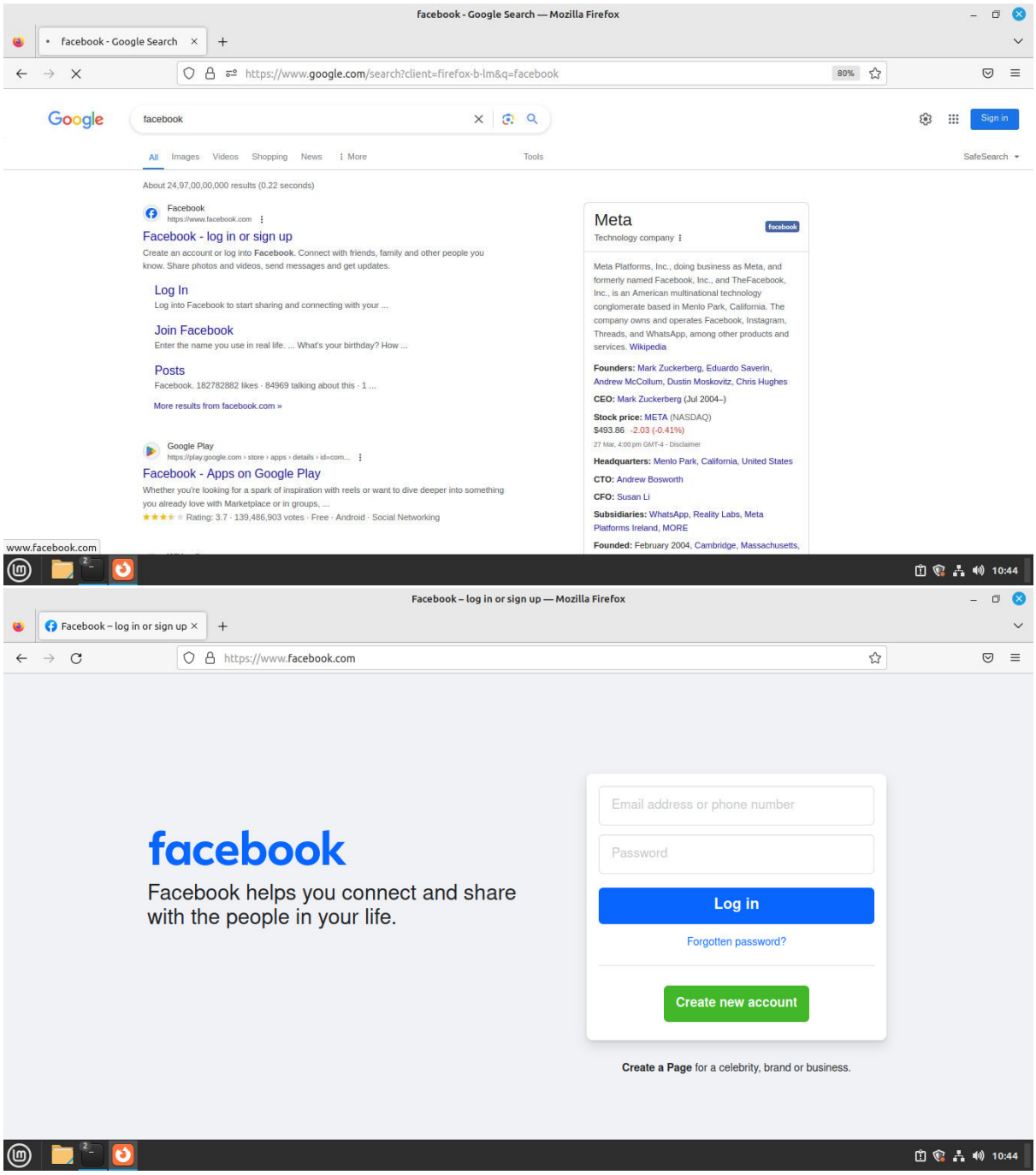

root@LAB704PC10: /home/student
File Edit View Search Terminal Help
inet 192.168.0.177 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::3b0d:36e7:9ad3:26e prefixlen 64 scopeid 0x20<link>
ether a4:ae:12:84:b4:26 txqueuelen 1000 (Ethernet)
RX packets 868 bytes 604110 (604.1 KB)
RX errors 0 dropped 6 overruns 0 frame 0
TX packets 339 bytes 28900 (28.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 146 bytes 13944 (13.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 146 bytes 13944 (13.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@LAB704PC10:/home/student# ping 192.168.0.126
PING 192.168.0.126 (192.168.0.126) 56(84) bytes of data.
64 bytes from 192.168.0.126: icmp_seq=1 ttl=64 time=3.78 ms
64 bytes from 192.168.0.126: icmp_seq=2 ttl=64 time=2.26 ms
64 bytes from 192.168.0.126: icmp_seq=3 ttl=64 time=2.10 ms
64 bytes from 192.168.0.126: icmp_seq=4 ttl=64 time=2.08 ms
64 bytes from 192.168.0.126: icmp_seq=5 ttl=64 time=2.26 ms
64 bytes from 192.168.0.126: icmp_seq=6 ttl=64 time=2.29 ms
64 bytes from 192.168.0.126: icmp_seq=7 ttl=64 time=2.08 ms
64 bytes from 192.168.0.126: icmp_seq=8 ttl=64 time=2.27 ms
64 bytes from 192.168.0.126: icmp_seq=9 ttl=64 time=2.29 ms
^C
--- 192.168.0.126 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 2.075/2.377/3.775/0.501 ms
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j DROP
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j ACCEPT
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j REJECT
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j DROP
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j ACCEPT
root@LAB704PC10:/home/student# iptables -I OUTPUT -s 192.168.0.177 -d 192.168.0.126 -p icmp -j REJECT
root@LAB704PC10:/home/student#
student@LAB704PC10: ~
File Edit View Search Terminal Help
From 192.168.0.177 icmp_seq=10 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=11 Destination Port Unreachable
ping: sendmsg: Operation not permitted
64 bytes from 192.168.0.126: icmp_seq=19 ttl=64 time=2.11 ms
64 bytes from 192.168.0.126: icmp_seq=20 ttl=64 time=2.07 ms
64 bytes from 192.168.0.126: icmp_seq=21 ttl=64 time=2.11 ms
64 bytes from 192.168.0.126: icmp_seq=22 ttl=64 time=2.09 ms
64 bytes from 192.168.0.126: icmp_seq=23 ttl=64 time=1.97 ms
64 bytes from 192.168.0.126: icmp_seq=24 ttl=64 time=2.10 ms
64 bytes from 192.168.0.126: icmp_seq=25 ttl=64 time=1.26 ms
64 bytes from 192.168.0.126: icmp_seq=26 ttl=64 time=1.89 ms
64 bytes from 192.168.0.126: icmp_seq=27 ttl=64 time=2.28 ms
64 bytes from 192.168.0.126: icmp_seq=28 ttl=64 time=2.09 ms
64 bytes from 192.168.0.126: icmp_seq=29 ttl=64 time=1.93 ms
64 bytes from 192.168.0.126: icmp_seq=30 ttl=64 time=2.27 ms
64 bytes from 192.168.0.126: icmp_seq=31 ttl=64 time=1.89 ms
64 bytes from 192.168.0.126: icmp_seq=32 ttl=64 time=2.11 ms
64 bytes from 192.168.0.126: icmp_seq=33 ttl=64 time=2.26 ms
From 192.168.0.177 icmp_seq=34 Destination Port Unreachable
ping: sendmsg: Operation not permitted
From 192.168.0.177 icmp_seq=35 Destination Port Unreachable
ping: sendmsg: Operation not permitted
10:38


student@LAB704PC10: ~
File Edit View Search Terminal Help
splint -help flags full
student@LAB704PC10:~$ splint -help flags memorybounds
Splint 3.1.2 --- 21 Feb 2021
memorybounds (17 flags)
out-of-bounds memory accesses
nullterminated
misuse of nullterminated allocation
Categories: memorybounds, memory
Mode Settings: ----
Set locally
A possibly non-nullterminated string/memory is used/referenced as a
nullterminated one.
bounds
memory bounds checking (sets boundsread and boundswrite)
Categories: memorybounds, memory
Default Setting: -
Set locally
Memory read or write may be out of bounds of allocated storage.
likelybounds
memory bounds checking (sets likelyboundsread and likelyboundswrite)
Categories: memorybounds, memory
Default Setting: -
Set locally
Memory read or write may be out of bounds of allocated storage.
likelyboundsread
likely out of bounds read
Categories: memorybounds, memory
Mode Settings: ---+
Set locally
A memory read references memory beyond the allocated storage.
likelyboundswrite
likely buffer overflow from an out of bounds write
Categories: memorybounds, memory
Mode Settings: ---+
Set locally
A memory write may write to an address beyond the allocated buffer.
boundsread
11:09


student@LAB704PC10: ~
File Edit View Search Terminal Help
possible security vulnerability
specifications (17 flags)
checks involving .lcl specifications
suppress (7 flags)
local and global suppression of messages
typeequivalence (27 flags)
control what types are equivalent
undefined (3 flags)
code with undefined or implementation-defined behavior
unrecognized (4 flags)
unrecognized identifiers
unconstrained (17 flags)
checking in the presence of unconstrained functions
warnuse (10 flags)
use of possibly problematic function
its4 (5 flags)
its4 compatibility flags (report warnings for uses of possibly insecure
functions)
To see the flags in a flag category, do
splint -help flags <category>
To see a list of all flags in alphabetical order, do
splint -help flags alpha
To see a full description of all flags, do
splint -help flags full
student@LAB704PC10:~$ splint -help flags memorybounds
Splint 3.1.2 --- 21 Feb 2021
memorybounds (17 flags)
out-of-bounds memory accesses
nullterminated
misuse of nullterminated allocation
Categories: memorybounds, memory
Mode Settings: ----
Set locally
A possibly non-nullterminated string/memory is used/referenced as a
nullterminated one.
bounds
11:09


student@LAB704PC10: ~
File Edit View Search Terminal Help
an ensures clause.
impboundsconstraints
generate implicit constraints for functions
Categories: memorybounds, memory
Default Setting: -
Set locally
orconstraint
use limited OR expressions to resolve constraints
Categories: memorybounds, memory
Default Setting: +
Set locally
showconstraintparens
display parentheses around constraint terms
Categories: memorybounds, display
Default Setting: -
Set locally
boundscompacterrormessages
Display fewer new lines in bounds checking error messages
Categories: memorybounds, display
Default Setting: -
Set locally
showconstraintlocation
display location for every constraint generated
Categories: memorybounds, display
Default Setting: +
Set locally
allocmismatch
type conversion involves storage of non-divisble size
Categories: memorybounds, memory
Mode Settings: -+++
Set locally
debugfcnconstraint
debug function constraints
Categories: debug, memorybounds
Default Setting: -
Set locally
Perform buffer overflow checking even if the errors would be
suppressed.
student@LAB704PC10:~$
11:09


student@LAB704PC10: ~
File Edit View Search Terminal Help
redundantconstraints
display seemingly redundant constraints
Categories: memorybounds, display
Default Setting: -
Set locally
Display seemingly redundant constraints
checkpost
unable to verify predicate in ensures clause
Categories: memorybounds, memory
Mode Settings: ---+
Set locally
The function implementation may not satisfy a post condition given in
an ensures clause.
impboundsconstraints
generate implicit constraints for functions
Categories: memorybounds, memory
Default Setting: -
Set locally
orconstraint
use limited OR expressions to resolve constraints
Categories: memorybounds, memory
Default Setting: +
Set locally
showconstraintparens
display parentheses around constraint terms
Categories: memorybounds, display
Default Setting: -
Set locally
boundscompacterrormessages
Display fewer new lines in bounds checking error messages
Categories: memorybounds, display
Default Setting: -
Set locally
showconstraintlocation
display location for every constraint generated
Categories: memorybounds, display
Default Setting: +
Set locally
allocmismatch
11:09


facebook - Google Search — Mozilla Firefox
facebook - Google Search
https://www.google.com/search?client=firefox-b-lm&q=facebook
80%
Google
facebook
Sign in
All Images Videos Shopping News More Tools SafeSearch
About 24,97,00,00,000 results (0.22 seconds)
Facebook
https://www.facebook.com
Facebook - log in or sign up
Create an account or log into Facebook. Connect with friends, family and other people you know. Share photos and videos, send messages and get updates.
Log In
Log into Facebook to start sharing and connecting with your ...
Join Facebook
Enter the name you use in real life. ... What's your birthday? How ...
Posts
Facebook. 182782882 likes · 84969 talking about this · 1 ...
More results from facebook.com »
Google Play
https://play.google.com › store › apps › details › id=com...
Facebook - Apps on Google Play
Whether you're looking for a spark of inspiration with reels or want to dive deeper into something you already love with Marketplace or in groups, ...
Rating: 3.7 · 139,486,903 votes · Free · Android · Social Networking
Meta
Technology company
facebook
Meta Platforms, Inc., doing business as Meta, and formerly named Facebook, Inc., and TheFacebook, Inc., is an American multinational technology conglomerate based in Menlo Park, California. The company owns and operates Facebook, Instagram, Threads, and WhatsApp, among other products and services. Wikipedia
Founders: Mark Zuckerberg, Eduardo Saverin, Andrew McCollum, Dustin Moskovitz, Chris Hughes
CEO: Mark Zuckerberg (Jul 2004–)
Stock price: META (NASDAQ)
$493.86 -2.03 (-0.41%)
27 Mar, 4:00 pm GMT-4 - Disclaimer
Headquarters: Menlo Park, California, United States
CTO: Andrew Bosworth
CFO: Susan Li
Subsidiaries: WhatsApp, Reality Labs, Meta Platforms Ireland, MORE
Founded: February 2004, Cambridge, Massachusetts,
www.facebook.com
10:44

Facebook – log in or sign up — Mozilla Firefox
Facebook – log in or sign up
https://www.facebook.com
facebook
Facebook helps you connect and share with the people in your life.
Email address or phone number
Password
Log in
Forgotten password?
Create new account
Create a Page for a celebrity, brand or business.
10:44