Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Кафедра безпеки інформаційних систем та технологій

Лабораторна робота № 2

з навчальної дисципліни

« Спеціалізовані мови програмування та проектування електронних елементів і систем»

Виконав:

Студент групи КБ-41

Кравченко Є.М.

Перевірив:

Професор

Олійников Р.В.

Харків – 2021 р.

LABORATORY WORK #2

“SECURING LINUX SERVER WITH THE PACKET FILTER IPTABLES”

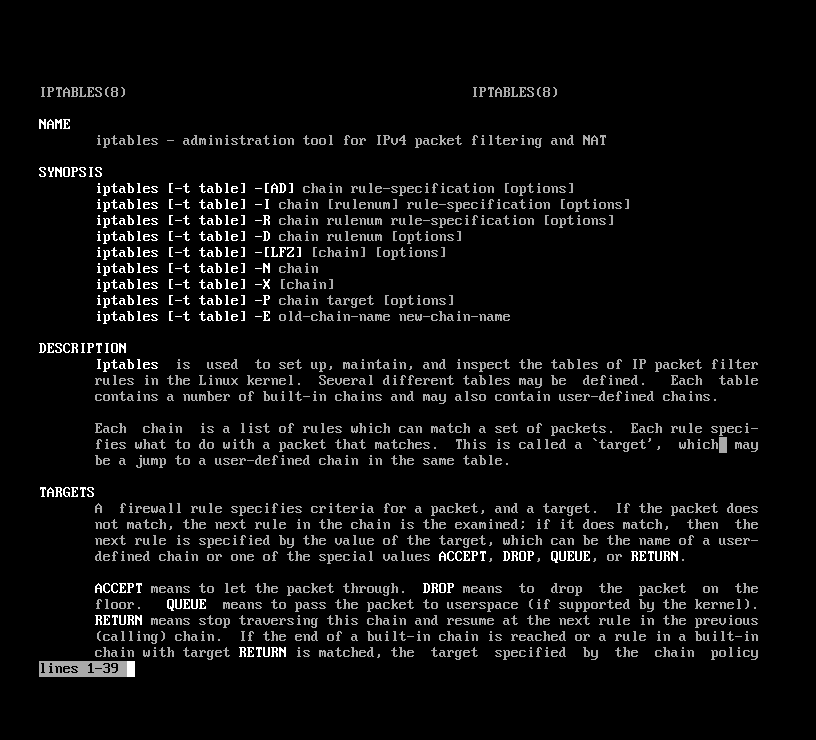
**1. Learning information about setting up rules for iptables in Linux.**

In the Linux command line type ‘reset’ command to prepare command line for viewing manual (help) pages:

reset

After preparing terminal, type ‘man iptables’ to view manual page on this utility.

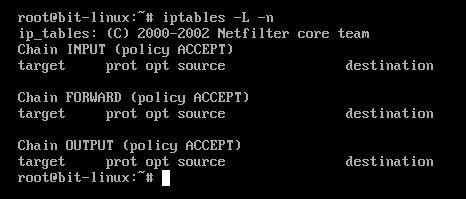
man iptables



**2. Setting prohibiting policy for networking traffic.**

View my current rules and iptables policy by typing

iptables –L -n



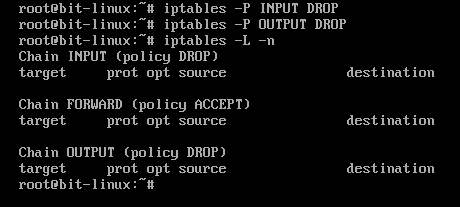
As I have read in the manual page, -L means listing of rules, -n means numerical format (typing without converting IP addresses to domain names, its greatly improves speed of rule displaying).

Change default policy to prohibiting. To do it, type

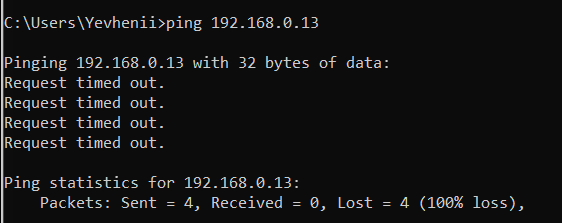
iptables –P INPUT DROP

iptables –P OUTPUT DROP

and check my new policy (like in previous example, “iptables -L -n”).



Check this by trying to access my Linux system from Windows by pinging, trying to browse and trying to establish telnet or ftp connection.



**3. Creating and testing rules for allowing http, ftp and telnet traffic to your Linux server.**

After setting up prohibiting policy, I need to add rules for enabling specific traffic (for allowing http, ftp and telnet access).

To add a rule, iptables command should have the following form:

iptables –A INPUT ………. –j ACCEPT

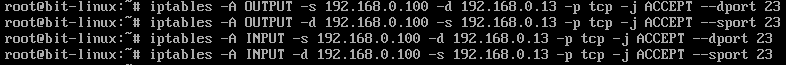
“-A INPUT” means adding (-A) a new rule to the INPUT chain. I can also use OUTPUT for adding a rule to the correspondent chain.

“-j ACCEPT” (be attentive to the case of letters) means that this is an enabling rule. If you want to create prohibiting rule, use “DROP” or “DENY” instead of “ACCEPT”.

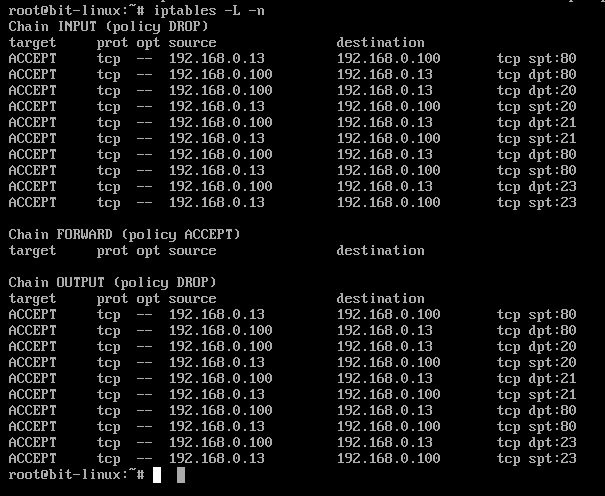
Between “-A INPUT” and “-j ACCEPT” there should be specification of source and destination IP addresses, selection of the protocol, specification of source and destination port numbers. If i want to select some range of port numbers, i use colon (“:”).

For exact specification of these parameters, read the manual page.





You need to enable http, ftp and telnet access from your Windows computer to your Linux server.

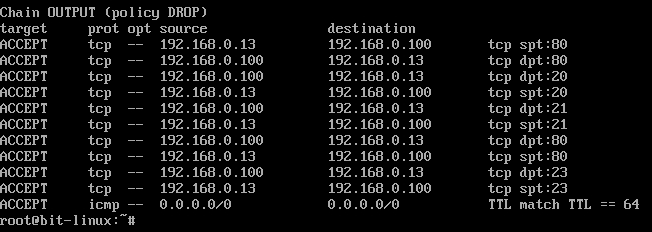


**4. Creating and testing rules for allowing pinging your Linux from other Linux servers, but disabling pinging from Windows.**

After enabling base protocols (http, ftp and telnet), add additional rule for enabling pinging your computer, but only from Linux computer all over network.

To enable ping, you need to enable icmp protocol.





To find a difference between Windows and Linux IP packets, try to look at TTL field.

After adding that rule to your INPUT and OUTPUT chains, your Windows won’t be able to ping your Linux, but other Linux computers will be able to ping your Linux IP address.

Conclusions

In this work it was learned information about setting up rules for iptables in Linux, set prohibiting policy for networking traffic (disabling all traffic which is not evidently permitted), created and testing rules for allowing http, ftp and telnet traffic to your Linux server and created and tested rules for allowing pinging Linux from other Linux servers, but disabling pinging from Windows.