Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 3A

Aim: To study installation and configuration of Linux Kernel firewall iptables.

Theory:
A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. Firewalls can be either hardware orsoftware but the ideal configuration will consist of both. In addition to limiting access to yourcomputer and network, a firewall is also useful for allowing remote access to a private networkthrough secure authentication certificates and logins. Software firewalls are installed on yourcomputer and can be customized which gives administrator control over its function and protectionfeatures. A software firewall will protect computer from outside attempts to control or gain access. Setting up a good firewall is an essential step to take in securing any modern operating system.Most Linux distributions ship with a few different firewall tools that can be used to configurefirewalls. Iptables is a standard firewall included in most Linux distributions by default. It isactually a front end to the kernel-level netfilter hooks that can manipulate the Linux network stack.It works by matching each packet that crosses the networking interface against a set of rules todecide what to do.

IPTABLES : TABLES and CHAINS
Iptables command allows the system administrators to manage incoming and outgoing traffics. IPtables contains set of tables, tables consists of chains and chains consists of rules. The iptables firewall operates by comparing network traffic against a set of rules. The rules define the characteristics that a packet must have to match the rule, and the action that should be taken for matching packets. There are many options to establish which packets match a specific rule. i.e. packet protocol type, the source or destination address or port, the interface that is being used, its relation to previous packets. When the defined pattern matches, the action that takes place is calleda target. A target can be a final policy decision for the packet, such as accept, or drop. These rules are organized into groups called chains. A chain is a set of rules that a packet is checked against sequentially. When the packet matches one of the rules, it executes the associated action and is not checked against the remaining rules in the chain.

IPTables has the following 3 built-in tables.
1. Filter Table
Filter is default table for iptables. So, if you don't define you own table, you'll be using filter table. Iptables's filter table has the following built-in chains.

•INPUT chain
•OUTPUT chain
•FORWARD chain

2. NAT table
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 ipaddress 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

A user can create chains as needed. There are three chains defined by default. They are:
•INPUT: This chain handles all packets that are addressed to your server.
•OUTPUT: This chain contains rules for traffic created by your server.
•FORWARD: This chain is used to deal with traffic destined for other servers that are not created on your server. This chain is basically a way to configure your server to route requests to other machines.

Usage of Iptables
An iptable command-line utility can be followed by an argument denoting the command to execute. To add a new rule to a chain, you use -A . Use -D to remove it, and -R to replace it. The -s option specifies the source address attached to the packet, -d specifies the destination address, and the -j option specifies the target of the rule. The ACCEPT target will allow a packet to pass. The -i option now indicates the input device and can be used only with the INPUT and FORWARD chains. The -o option indicates the output device and can be used only for OUTPUT and FORWARD chains.

Conclusion: Hence we have successfully studied commands that are commonly used when configuring an iptables firewall and also configured a linux machine as Firewall(iptables). iptables is a very flexible tool that allows to mix and match the commands with different options to match specific needs .