Lab 3

Aim: Use of iptables in linux to create firewalls.

Objectives: To study how to create and destroy firewall security parameters.

Outcomes: The learner will be able to:-

- Recognize the need for having a security on host side by controlling incoming / outgoing traffic using the acquired skills and knowledge.
- Design rules for the INPUT/OUTPUT/FORWARD chain.

Hardware / Software Required: Linux

Theory:

IPtables are the tables provided by the Linux kernel firewall (implemented as different Netfilter modules) and the chains and rules it stores. Different kernel modules and programs are currently used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

iptables requires elevated privileges to operate and must be executed by user root, otherwise it fails to function. On most Linux systems, iptables is installed as /usr/sbin/iptables and documented in its man pages which can be opened using man iptables when installed. It may also be found in /sbin/iptables, but since iptables is more like a service rather than an "essential binary", the preferred location remains /usr/sbin.

1. To drop all traffic:

sudo iptables -P INPUT DROP

sudo iptables -P OUTPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -L -v –n

2. Only Block Incoming Traffic

To drop all incoming / forwarded packets, but allow outgoing traffic,

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT

sudo iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT

sudo iptables -L -v –n

3. Block Outgoing IPaddress host -t a hostname

sudo iptables -A OUTPUT -d outgoing ipaddress -j DROP

4. Block or Allow ICMP ping request

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP/ACCEPT

Conclusion:

There are many other firewall utilities and some that may be easier, but iptables is a good learning tool, if only because it exposes some of the underlying netfilter structure and because it is present in so many systems.

Questions:

Submit the screenshots of your lab and the answers to the below questions in a document file (.doc/.pdf)

.1 Describe various types of firewalls.

2. Find another GUI tools to create firewalls.