Practical Work
2.12.2015

Firewall configuration in Linux - Iptables

Introduction:

Iptables is an extensible packet identification framework used by Netfilter in the Linux kernel. It is used to set up the firewall and filter packets, as well as setting up NAT (Network Address Translation) and forwarding.

Step 1: Boot into a Linux environment

Boot up from the Ubuntu Live-CD and open a console for root (the administrator). Check that the wireless connection is working (if it isn't supported, you can try connecting using the wired interface). Check the iptables configuration using the command:

```
iptables -L
```

The default should be an empty ruleset with default policy of ACCEPT.

Step 2: Clearing rules

At any point, rules can be cleared using the -F, -X and -Z switches (see the manpage, *man iptables*, for further information).

Step 3: Setting up the default rules

Before changing the default rules, it is best to always enable loopback connections:

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

Set the default rule to be DROP. After this point no connections will be possible.

```
iptables -P OUTPUT DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP
```

Step 4: Enabling through services/protocols

Enable connections based on the port using the following template (eg: HTTP):

```
iptables -A INPUT  -i $IFACE -p tcp --sport 80 -m state \
        --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o $IFACE -p tcp --dport 80 -m state \
        --state NEW,ESTABLISHED -j ACCEPT
```

Note that *$IFACE* refers to the name of the interface (usually *eth0* or *eth1*). Since internet access will be very limited without DNS resolution available, it is best to also enable this service (notice that DNS uses both udp and tcp):

```
iptables -A INPUT -i $IFACE -p udp --sport 53 -m state \
        --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o $IFACE -p udp --dport 53 -m state \
        --state NEW,ESTABLISHED -j ACCEPT
```

Step 5: Enabling FTP

The FTP protocol uses a few more ports than the basic (21) one. Active FTP transfers take effect over port 20, while passive transfers take place on any port number greater than 1023. The *RELATED* state allows one to set rules that will only allow through connections related to previously accepted ports (eg: ftp/21):

```
iptables -A INPUT  -i $IFACE -p tcp --sport 20      -m state \
        --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -o $IFACE -p tcp --dport 20   -m state \
        --state ESTABLISHED -j ACCEPT
iptables -A INPUT  -i $IFACE -p tcp --sport 1024:65535 --dport 1024:65535 \
        -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -o $IFACE -p tcp --sport 1024:65535 --dport 1024:65535 \
        -m state --state ESTABLISHED,RELATED -j ACCEPT
```

However... is there any particular problem or side-effect to the above ACCEPT rules?

Step 6: Save the rules

Use *iptables-save* with a file redirect to store your firewall configuration:

```
iptables-save > yourname.iptables
```

<u>Deliverables:</u>

Iptables configuration file (output of iptables-save). This assignment is not marked, so no submission is required.

<u>Further Reference:</u>

Useful commands: *ifconfig*, *netstat*, */etc/services* (service reference).

http://www.netfilter.org/documentation/index.html#documentation-howto