Building a Router with iptables

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe *iptables* and its functions.
2. Configure packet forwarding in Linux.
3. Configure NAT routing in *iptables*

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Building a Router with iptables
    - Introduction to *iptables*
    - Packet forwarding
    - Network Address Translation
- Introduction to *iptables*
    - Firewall designed for the Linux kernel
    - Used by most distros
    - Features
        - Routing
        - NAT
        - Filtering
        - Logging
        - Redirecting
- Firewall conflicts
    - Front-ends
        - There are many "front-ends" for iptables
            - Uncomplicated Firewall (UFW)
        - Can co-exist with *iptables*
    - Firewalls
        - There are other firewalls
            - *firewalld*
            - *nftables*
        - Generally cannot co-exist with *iptables*
    - Disable UFW
        - `sudo ufw disable`
- Packet Forwarding
    - The Linux kernel does not allow packets to move between interfaces
    - Blocked for security
    - Can be enabled
        1. `sudoedit /etc/sysctl.conf`
        2. Uncomment `net.ipv4.ip_forward=1`
        3. Reload with `sysctl -p`
- *iptables* Configuration
    - Ephemeral
        - Not written to disk by default
        - Changes are lost when the service stops

    - Persistent
        - Writes the changes to disk
        - `/etc/iptables/`
    - `sudo apt install iptable-persistent`
- *iptables* Rules
    - `cat /etc/iptables/rules.v4`
    - Processing Chains
        - Input: Traffic destined for the localhost
        - Output: Traffic leaving the localhost
        - Forward: Traffic being routed elsewhere
- Enabling NAT
    - Configure NAT rule
        - `sudo iptables -t nat -A POSTROUTING -j MASQUERADE`
        - `sudo iptables -t nat -s 10.222.0.0/24 -A POSTROUTING -j MASQUERADE`
    - Save configuration
        - `sudo iptables-save | sudo tee /etc/iptables/rules.v4`
- Follow up tasks
    - Port forwarding
    - Firewall rules