Lab Class 4 - IPTables

References:

- manual iptables
- Linux: 25 Iptables Netfilter Firewall Examples For New SysAdmins
- 10 iptables rules to help secure your Linux box, By Jack Wallen
- Linux NAT in Four Steps using iptables, By Frank Wiles
- BCP 38 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

---

Assignment 1

1. See how to flush all `iptables` rules and save it in a script (bash) file (`iptables-save` and `iptables-restore`)

2. In this exercise we will configure the Fedora Workstation and Windows machines to use the Fedora Server as gateway on the internal net interface. The firewall will run on the Fedora Server machine.

    1. EnableIP forwarding on this machine

        > Use `echo 1 > /proc/sys/net/ipv4/ip_forward` or `sysctl net.ipv4.ip_forward=1` and NAT. See `MASQUERADE` on the `iptables` manual and the tutorial.

        - The Fedora Server machine must have the network interfaces configured as described in the Assignment from Class 1.
        - You must enable NAT where `192.168.0.0/24` is the outside and `172.10.X.0/24` the inside.
        - Are the last two `ACCEPT` rules for *NATing* needed if the default policy is `ACCEPT`?

    2. On the Fedora Workstation and Windows machines the address for the group's net (`172.10.X.0/24`) should have been configured on the previous exercise. Disable the other interface (`192.168.0.0/24`) on the Windows and Fedora Workstation machines (use `ifconfig`, `ip link` or the graphical user interface in Linux and the graphical interface in Windows).

        The default gateway on both machines should now be the `172.10.X.1` address of the Fedora Server. In Windows you can use the graphical interface or `route`. In Linux you can use the `route` command or `ip route` or the graphical user interface.

    3. The DNS server need not be configured if only IP addresses are used, otherwise you can add `192.168.0.1` to the DNS Server setting (i.e., **Host** address).

    4. Test the configurations by pinging to `192.168.0.1` in all the configured machines.

3. We will now restrict access to the outside. Only the following services will be allowed to go through from the Windows and Fedora Workstation machines:

    - Domain Name system (DNS)
    - SSH
    - SMTP
    - HTTP/HTTPS
        - All other traffic should be blocked (default policy for the `FORWARD` chain is `DROP`, and what about other chains?).
        - Test it by assessing a blocked (e.g. IMAP, FTP) and an allowed service. Consult the Linux Firewalls book scripts and adapt them accordingly. **Note:** Recall the last two rules for NAT and see if you need any.

4. On the Fedora Server machine it should be possible to initiate any connection (with no restriction). However, it should only ACCEPT connections on port `22` (i.e., for SSH). It should answer to `ICMP-ECHO request`` from the inside and outside, but all other` ICMP` messages should be dropped.

5. Install an httpd server on the Windows or Fedora Workstation machines. Install the firewall rules as to redirect connections to Fedora Server on port `80` to the newly installed `httpd server`. See rule 5 from the reference of Jack Wallen. Test it with the Kali machine, that should still have the `192.168.0.0/24` interface on.

6. The DoS attack targeting an anti-spam site used open DNS servers and the possibility of spoofing source addresses. The DNS amplification attack can be avoided (as other spoofing attacks) following the Best Current Practice (BCP) 38.

    - Setup an `iptables` rule on the Fedora Server (which is the router of our controlled domain) to follow the best practice (see the anti-spoofing of the Linux Firewalls book scripts).
    - Test it analysing the traffic with `tcpdump` on the Fedora Server on interface `192.168.0.0/24` before and after activating the filter.
    - Use `nmap` to send packets with a spoofed source address.

- To recover the normal network configurations you can run the dhclient in Linux (on the interfaces or restart the network or restart the machines) and turn on/off the interface in Windows or with ipconfig/ifconfig.

NetFilter Paths and Lab Network

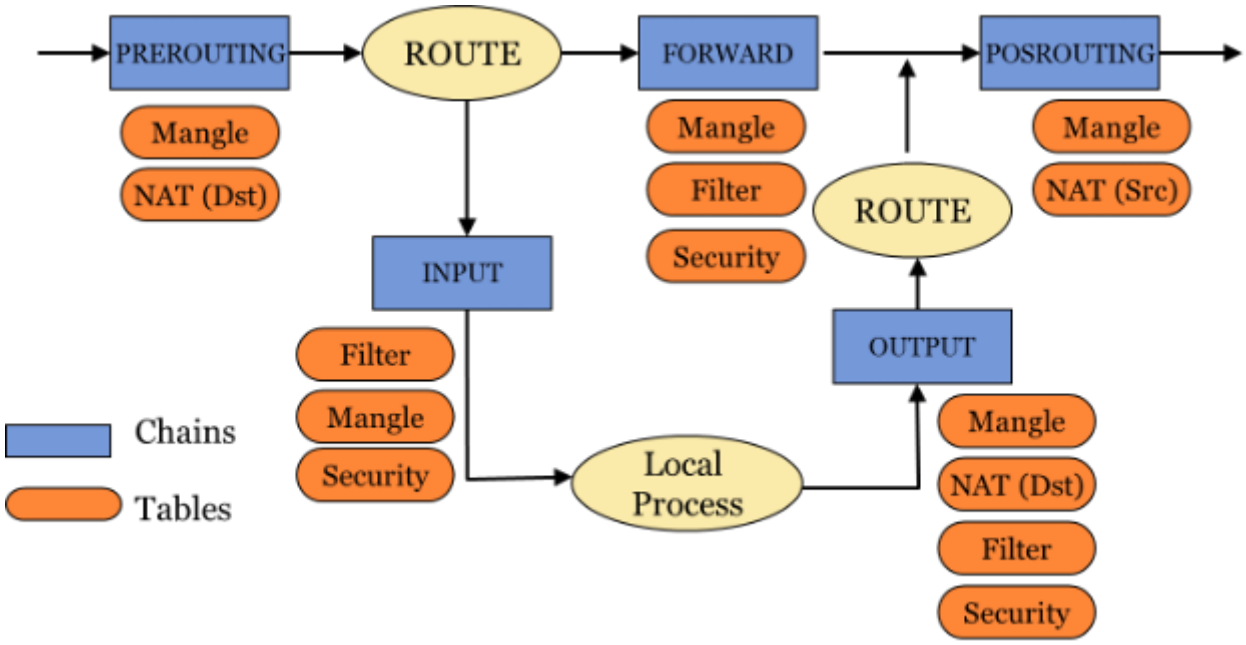

Figure 1 - Netfilter paths

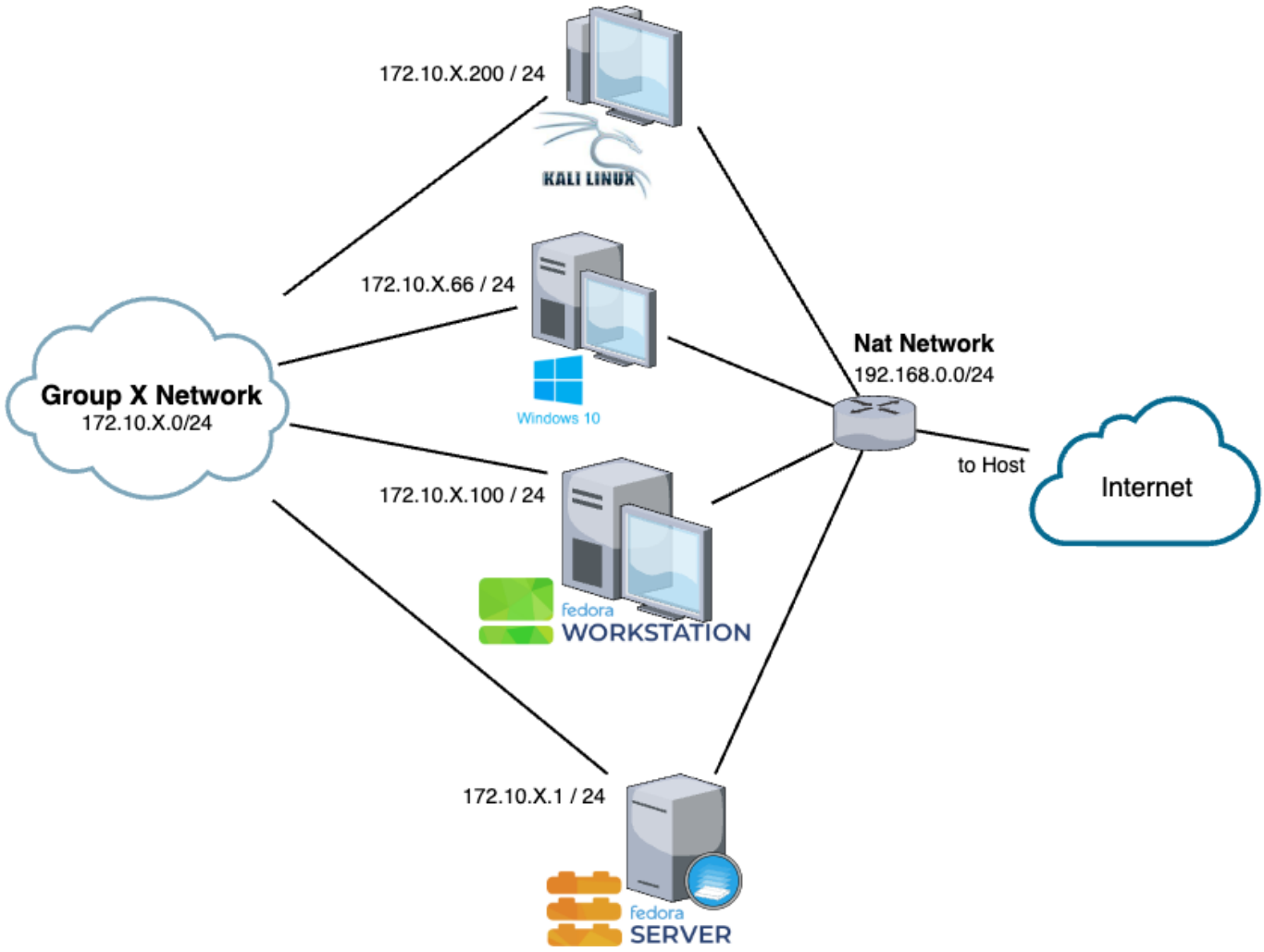

Figure 2 - Network Organization