Computer Science CSCI 251

Systems and Networks

Dr. Peter Walsh
Department of Computer Science
Vancouver Island University
peter.walsh@viu.ca

Cyber Security

- Social Engineering
  - *countermeasures:* training
- Application Software Vulnerabilities
  - buffer overflow, input validation
  - *countermeasures:* keep up with patches
- Malicious Software
  - virus, worm, ransom-ware, bots
  - *countermeasures:*
    antivirus software (e.g., `ClamAV`)
    packet filtering (e.g., `iptables`)
- Default Software Configurations
  - often useful rather than secure with well-known passwords such as `admin` and `default`
  - *countermeasures:* password-protect services

Cyber Security cont.

Goal: identify vulnerabilities before they can be exploited.

- Latest Security Threats
  - Linux Security (`linuxsecurity.com`)
  - SEI Insights (`insights.sei.cmu.edu/`)
- Penetration Testing
  - Kali Linux (kali.org)

Packet Filtering Firewalls

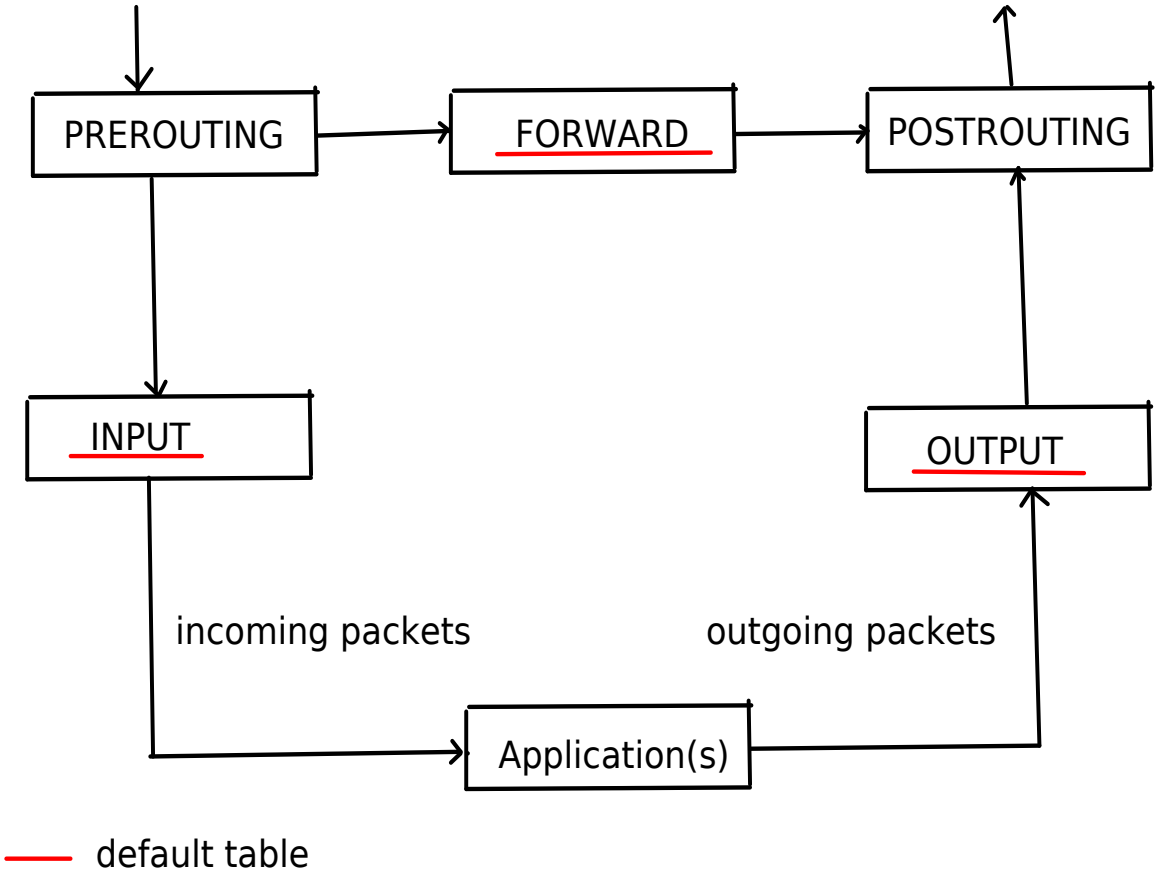
Packet filtering provides controlled access to packets to/from a network.

- Netfilter
  - kernel module that supports packet filtering, state management and NAT
- Iptables
  - user-land user-interface to Netfilter

Iptables Built-In Tables/Chains

- Filter Table
  - INPUT Chain
  - FORWARD Chain
  - OUTPUT Chain
- NAT Table
  - PREROUTING Chain
  - POSTROUTING Chain
  - ...
- Mangle Table
  - PREROUTING Chain
  - POSTROUTING Chain
  - ...

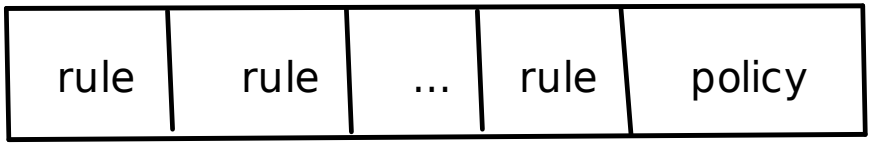
Iptables Packet Flow



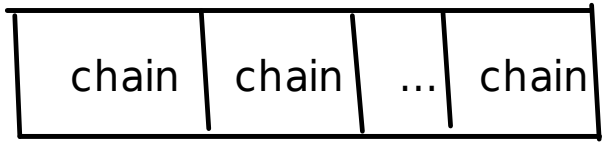
Iptables Table/Chain/Rule Structure

Rule

Chain



Table



Iptables Sample Usage

- List Rules
  - `iptables -L`
- Flush Rules
  - `iptables -F`
- Zero Packet and Byte Count
  - `iptables -Z`
    `iptables -L -v`
- Set Default Policy
  - `iptables -P INPUT DROP`
- Rule Append (Drop ICMP Packets)
  - `iptables -A INPUT -p icmp -j DROP`
- Rule Delete (Drop ICMP Packets)
  - `iptables -D INPUT -p icmp -j DROP`
- Rule Append (Accept ssh connections)
  - `iptables -A INPUT -p tcp --dport 22 -j ACCEPT`

Iptables Rule Persistence

- Save and Restore Rules (Debian/Ubuntu)
  - `iptables-save > /etc/iptables/rules.v4`
  - `iptables-restore < /etc/iptables/rules.v4`
- Install `iptables-persistent` Package
  - `apt-get update`

    `apt-get install iptables-persistent`
  - on boot, rules will be restored from rules.v4

Iptables Basic Firewall

```
# Generated by iptables-save v1.8.4
...
*filter
:INPUT DROP [6:284]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [514:6336925]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
COMMIT
...
```

Additional Network Tools

- Network Mapper
  - `apt-get update`
    `apt-get install nmap`
  - sample Usage
    `nmap -p 7075 192.168.1.72`
    `nmap -p 1-65535 localhost`
    `nmap -p 7075 -sU localhost`
    `nmap -p 7075 -sT localhost`
- Wireshark
  - `apt-get update`
    `apt-get install wireshark`

Multi-Homed Host Firewall With DMZ