Uncomplicated Firewall

Primers

- OSI Models
  - 7: Application
  - 6: Presentation
  - 5: Session
  - 4: Transport
  - 3: Network
  - 2: Datalink
  - 1: Physical
- Can write rules for 7, 6, 5, 4 but not 3, 2, 1

Linux firewall

- Packet comes in off the wire, picked up by the NIC
- Passed to kernel: Netfilter
- Parsed by firewall rules: iptables
- sent to user space: (web traffic)

UFW and IPTables

- iptables is the utility to write rules for NetFilters to use

    - kind of complicated to use
    - see talk about iptables (RITSEC - IPTABLES)
- UFW is frontend for iptables

How to use UFW?

- ufw enable/disable - Turn off or on
- ufw reload - reload the rules, usually ran after making a change
- ufw reset - disable the firewall, rest to installation defaults
- ufw logging on/off - low, medium, high, full
- ufw default|deny|allow|reject|incoming|outgoing|routed - specify the default policy for the direction of the traffic
- ufw status verbose|numbered - show all ufw firewall rules and state (enabled|disabled)

Writing rules

- ufw allow port|protocol - ufw allow 22/tcp
- ufw allow service - ufw allow smpt

- ufw allow in|out port/service - ufw allow in http
- ufw deny|reject
- ufw deny proto tcp 80 to any port 80
    - ufw deny proto|tcp|udp to destination port
- ufw deny proto tcp from 10.0.0.1/8 to 192.178.178.2/24 port 3306

UFW app|list|info|update

- creating rules can also be called from /etc/services/.
- If the service exists there, the string can be used in a firewall rule

---

Deny vs. Reject

- Deny drops traffic quietly//ignores it.
- Reject lets the sender know the traffic was dropped intentionally.

Rule Management

- ufw status numbered

- ufw delete `<rule>`
- ufw delete numbered
- ufw insert n `<rule>`
- When adding rules, your rule will be appended to end of the list

---

Remote Boxes

- ufw --dry run
  - show changes to be made, but will not apply them
- ufw reload; sleep 20; ufw disable
  - dont firewall yourself off from a remote box.