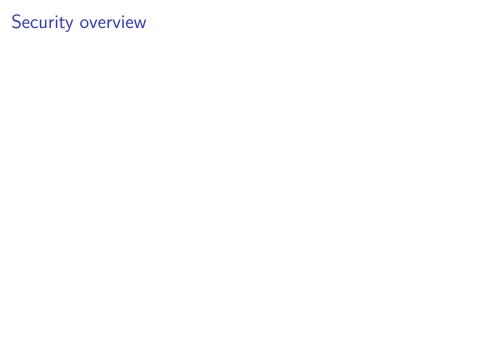
## **CSET 2200**

Access Control Lists

# Review

### This week

- Security themed
- ACL
- ► NAT



#### Access Control Lists

- Allow you to filter packets
- ▶ Support layer 2, 3 and 4
- ▶ We'll focus on 3 and 4

### **ACL**

- ► Applied to an interface
- ► Seperate filter for inbound and outbound

# ACL (contd)

- Matches packets based on ACL entries
- Entries can be deny or allow
- ► First match wins

#### Cisco ACLs

- 2 common types
- Standard (Source IP)
- ► Extended (Source and Dest, Layer 4)
- Names or Numbered

### Standard ACLs

- Only match source address
- ► Can match a host or a group of hosts

#### Wildcard mask

- One is don't care bit
- Zero must match
- Somewhat opposite of subnet mask
- Doesn't need to be contigious

# Example with Standard ACL

### Extended ACL

- Allows you to match layer 4 items
- Specify the protocol, source dest ip
- Also specify the protocol specific detail

#### Match TCP and UDP

- Can match port
- Range of ports also supported
- Supports friendly names of many services
- ▶ gt, lt, range, eq

# Creating ACLs

- Numbered ACL can only be appended
- Named can be edited
- Use Sequence number to insert into ACL

# Apply ACL

▶ ip access group command

## Useful ACL commands

sh access-list
sh ip access-list
sh ip interface

### Demonstration

# Questions

#### Wed - NAT

 $\blacktriangleright \ \, https://en.wikipedia.org/wiki/Network\_address\_translation$