

# Network Protocols

## Internet Control Message Protocol (ICMP)

# ICMP overview

- Primarily used for error and status messages
- Some security monkeys are really afraid of ICMP
  - We could point and laugh at that them
  - But lets be grown up and rational about ICMP
- ICMP is kind of like many protocols in one
  - All ICMP messages have 3 common fields
  - TYPE, CODE, CHECKSUM
  - Otherwise ICMP messages can vary widely

# By way of example...

- Extract of my standard iptables ruleset:

```
# icmp ingress / egress  
  
-p icmp --icmp-type echo-reply -j ACCEPT  
-p icmp --icmp-type destination-unreachable -j ACCEPT  
-p icmp --icmp-type echo-request -j ACCEPT  
-p icmp --icmp-type time-exceeded -j ACCEPT  
-p icmp --icmp-type parameter-problem -j ACCEPT  
-p icmp -j DROP
```

# ICMP echo / echo reply

- This is the heart of the infamous “ping”
- ID and sequence numbers match ping to reply
- The variable length data is “echoed” back

# ICMP destination unreachable

- Returned to a sender by a router, host or firewall
  - Host, net, protocol, port unreachables
  - Administratively prohibited
  - Fragmentation needed and DF was set
    - Filtering has caused problems – thx monkeys
  - And some more, but not typically very common
- Includes original IP header + 64 bits
  - This can be handy for debugging

# ICMP time exceeded

- Almost always a TTL has expired
  - Fragmentation reassembly expired, rare
- Perhaps you're doing a traceroute?
- Perhaps there is a routing loop?
- You again get IP header + 64 bits

# ICMP parameter problem

- I don't think I've ever seen this in practice
- Could probably do w/o it, but seems harmless
  - I'm a little more liberal in what I accept
- Some sort of datagram header processing error

# Other ICMP messages of note

- Source quench
  - ineffective as congestion control knob
- Redirect
  - You want to know if you're getting them
  - But you don't want them!
- Timestamp, netmask , etc. requests
  - These just seem to be information leaks to me