Edinburgh Napier UNIVERSITY

Networked Services

Firewall tests using masking

Module Leader: Dr Gordon Russell

Lecturers: G. Russell

Edinburgh Napier UNIVERSITY

Masks

- In rules such as

iptables -A INPUT -s 192.168.0.0/16 -j DROP

- The source ip mask can be specified as a quad dotted mask:

iptables -A INPUT -s 192.168.0.0/255.255.0.0 -j DROP

- The mask can be any sort of bitmask, not just a valid network VLSM.

- Block any host with a 0 in the last octet..

iptables -A INPUT -s 0.0.0.0/0.0.0.255 -j DROP

Edinburgh Napier UNIVERSITY

Optimization using masks

- Consider this problem:
  - Write one or more rules which will block TCP port 80 traffic from 10.0.0.0 to 10.0.0.255 if the last octet is even.
  - Use only 1 rule and use bitmasks to perform the optimization.
- Even numbers have 0 is the LSB.
- To be in 10.0.0.0/24 the first 24 bits are important to prove it.
- So bits 25 to 31 are irrelevant (Don't Care).
- Last octet must be 00000001, or simply 1.

-s 10.0.0.0/255.255.255.1 –j DROP

Edinburgh Napier UNIVERSITY

Optimization using masks

- Consider this problem:
  - Write one or more rules which will block TCP port 80 traffic from 10.0.0.0 to 10.0.0.31 and from 10.0.0.36 to 10.0.0.255. Accept all other traffic in 10.0.0.0/24.
  - Use only 2 rules and use bitmasks to perform the optimization.
- One way to look at this is drop all in 10.0.0.0/24 except .32 to .35.
- 32 is 00100000 and 35 is 00100011
  - Bottom 2 LSBs are Don't Care…

-s 10.0.0.32/255.255.255.252 –j ACCEPT

-s 10.0.0.0/255.255.255.0 –j DROP

Edinburgh Napier UNIVERSITY

Optimization using masks

- Consider this problem:
  - Write one or more rules which will block TCP port 80 traffic from 10.0.0.0 to 10.0.0.127, except 10.0.0.11-10.0.0.15 which are accepted.
  - Use only 3 rules and use bitmasks to perform the optimization.
- 10.0.0.0/255.255.255.127 takes care of the first test
- 11-15 in binary is 1011 – 1111.
  - 1100-1111 if part of this range (where the 2 LSBs are Don't Care), leaving just 1011.

-s 10.0.0.12/255.255.255.252 –j ACCEPT

-s 10.0.0.11/255.255.255.255 –j ACCEPT

-s 10.0.0.0/255.255.255.127 –j DROP

Edinburgh Napier UNIVERSITY

Discussion

- You need to write a set of rules which permit 10.0.0.0-10.0.0.59 to be accepted, and all other 10.0.0.0/24 IP numbers to be rejected.
- You should do this in 3 rules.