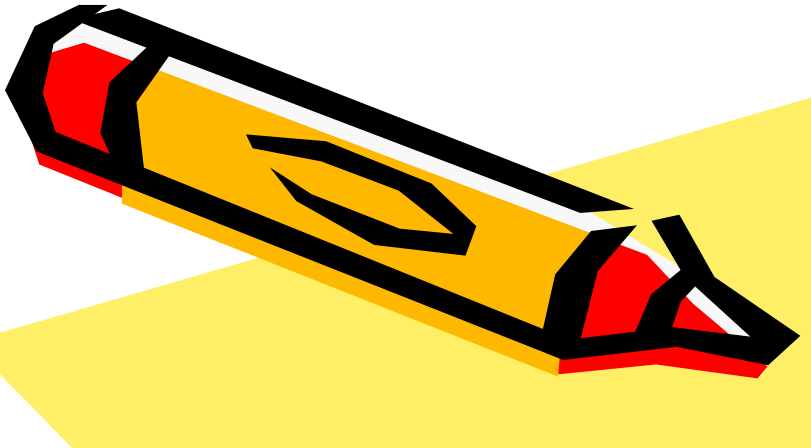


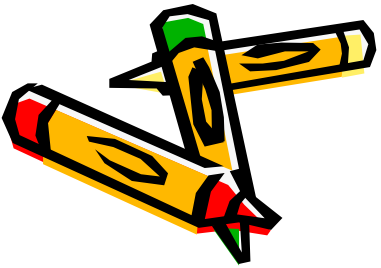
NAT & IPTables

From ACCEPT to MASQUERADE

Tim(othy) Clark (eclipse)

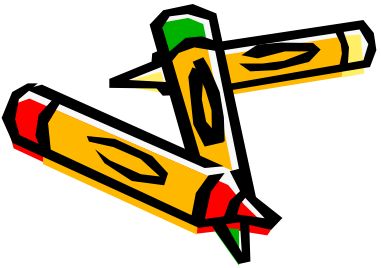
NAT

- IPv4 Hack
- One external IP for a whole network
- Used commonly in home routers
- All external traffic goes through the router



IPTABLES

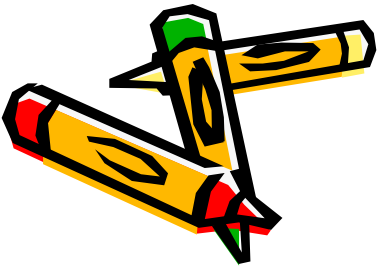
- Packet Filtering
- Packet Manipulation
- Creates firewalls
- NATs
- Cool stuff



Command Structure

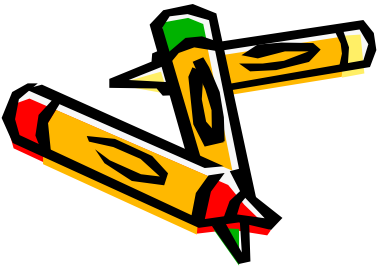
IPTABLES –A INPUT –s 137.44.10.0/24 –j DROP

- "-A chain" adds rules to a chain
- This is followed by a match
- And then an action
- Can match on lost of things
- Can ACCEPT, DROP or jump to a user defined chain



Tables, Chains and Rules

- Tables define basic usage
- Chains contain rules that are checked till one is executed
- Different built in chains execute in different paces
- Rules execute actions on packets that match the condition.

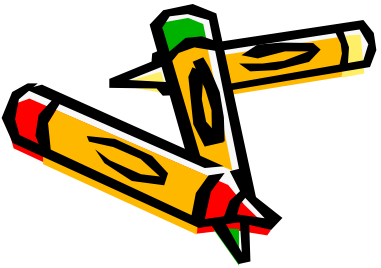


Example Traversal

Source: 137.44.10.6

-A INPUT -s 137.44.10.0/24 -j DROP
-A INPUT -s 137.44.0.0/16 -j ACCEPT
-P INPUT DROP

Incoming Packet

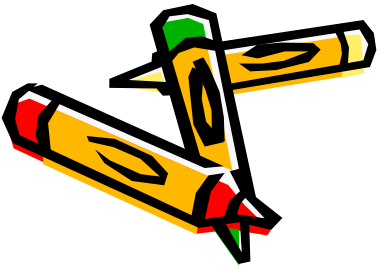


Example Traversal

Source: 137.44.195.83

-A INPUT -s 137.44.10.0/24 -j DROP
-A INPUT -s 137.44.0.0/16 -j ACCEPT
-P INPUT DROP

Matching Packet



Example Traversal

Source: 64.233.183.104

-A INPUT -s 137.44.10.0/24 -j DROP
-A INPUT -s 137.44.0.0/16 -j ACCEPT
-P INPUT DROP

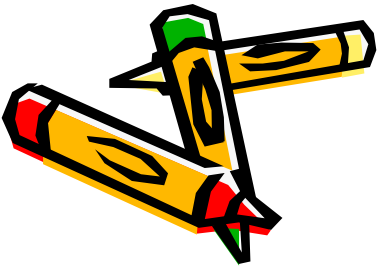
Incoming Packet

Connection Tracking

- Detects replies to sent packets
- Matching module
- NEW is starting a new connection
- ESTABLISHED is for existing connections
- RELATED is for new connections related to existing ones

Masquerade

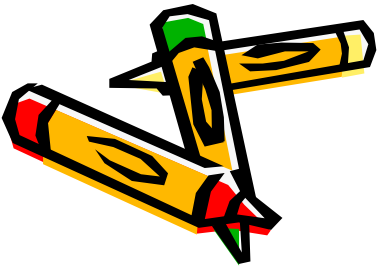
- Used in the prerouting chain of the nat table
- Makes NAT work
- Changes destination and source addressed as appropriate



Example Masq Code

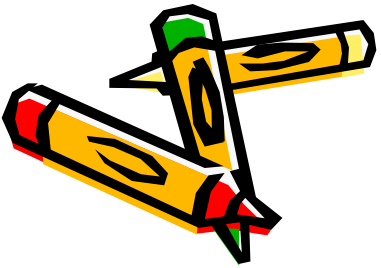
- Internal interface is eth1
- External interface is eth0
- Example configuration:

```
iptables –P INPUT DROP
iptables -P FORWARD DROP
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables –A FORWARD -i eth1 -j ACCEPT
iptables –t nat -A POSTROUTING -o eth0 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```



Useful Bits

- iptables-save stores the configuration in a file
- iptables-restore restores the configuration from a file
- Easily write scripts to restore it
- iptables has a good manual page



Any Questions?