Topic: iptables: Setting Up a Firewall

The iptables utility builds and manipulates network packet filtering rules in the Linux Kernel. You can use iptables to set up a firewall to protect your system from malicious users.

Login:
- user: root
- password: iaisthebestever

- Run chkconfig to cause iptables to start when the system comes up:
  - /sbin/chkconfig iptables on
  - iptables –L, “list contents of your iptables”
  - service iptables save
  - write down your observations

- Resetting iptables: if you have a problem with firewall rules, you can return packet processing rules in the kernel to the default states without rebooting by giving the following commands:
  - iptables - -flush && iptables - -delete-chain
  - iptables –L; new rule should be in your iptables.
  - write down your observations.

- Allow loopback access. This rule must come before the rules denying port access!!
  - iptables -A INPUT -i lo -p all -j ACCEPT - Essential rule so your computer to be able to access itself through the loopback interface
  - iptables -A OUTPUT -o lo -p all -j ACCEPT
  - iptables –L; new rule should be in your iptables.
  - write down your observations.

- Block NSF, port 2049, udp and tcp packets
  - iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 2049 -j DROP
  - iptables -A INPUT -p udp -s 0/0 -d 0/0 --dport 2049 -j DROP - Block NFS
  - iptables –L; new rule should be in your iptables.
  - write down your observations.

- Block X windows, port 6000 to 6009
  - iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 6000:6009 -j DROP
  - iptables –L; new rule should be in your iptables.
  - write down your observations.

- Block X windows font server, port 7100
  - iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 7100 -j DROP

- Block printer port, 515 for tcp and udp
  - iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 515 -j DROP
  - iptables -A INPUT -p udp -s 0/0 -d 0/0 --dport 515 -j DROP
  - iptables –L; new rule should be in your iptables.
  - write down your observations.
• Block Sun rpc/NFC, port 111 for tcp and udp
  o iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 111 -j DROP
  o iptables -A INPUT -p udp -s 0/0 -d 0/0 --dport 111 -j DROP
  o iptables -L ; new rule should be in your iptables.
  o write down your observations.

• Deny network packets which claim to be from your loopback interface (127.0.0.1)
  o iptables -A INPUT -p all -s 127.0.0.1 -i eth0 -j DROP
  o iptables –L ; new rule should be in your iptables.
  o write down your observations.

Another approach to firewalls is to drop everything and then grant access to each port you may need.

• Flush your iptables
  o iptables -F
  o iptables –L

• Allow self access by loopback interface
  o iptables -A INPUT -i lo -p all -j ACCEPT
  o iptables -A OUTPUT -o lo -p all -j ACCEPT
  o iptables –L ; new rule should be in your iptables.
  o write down your observations.

• Accept established connections
  o iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
  o iptables –L ; new rule should be in your iptables.
  o write down your observations.

• Reject-with tcp-reset
  o iptables -A INPUT -p tcp --tcp-option ! 2 -j REJECT
  o iptables –L ; new rule should be in your iptables.
  o write down your observations.

• Open ftp port
  o iptables -A INPUT -p tcp -i eth0 --dport 21 -j ACCEPT
  o iptables –L ; new rule should be in your iptables.
  o write down your observations.

• Open secure shell port
  o iptables -A INPUT -p udp -i eth0 --dport 21 -j ACCEPT
  o iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT
  o iptables -A INPUT -p udp -i eth0 --dport 22 -j ACCEPT
  o iptables –L ; new rule should be in your iptables.
  o write down your observations.

• Open HTTP port
  o iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT
  o iptables -A INPUT -p udp -i eth0 --dport 80 -j ACCEPT
  o iptables –L ; new rule should be in your iptables.
  o write down your observations.
• Accept local network Samba connection
  o **iptables** -A INPUT -p tcp --syn -s 192.168.100.0/24 --destination-port 139 -j ACCEPT
  o **iptables** –L ; new rule should be in your iptables.
  o write down your observations.

• Drop all other connection attempts. Only connections defined above are allowed.
  o **iptables** -P INPUT DROP
  o **iptables** –L ; new rule should be in your iptables.
  o write down your observations.

• Save your iptables
  o **iptables-save**

• restore your iptables
  o **iptables-restore**