KUBH/GH Network Training Network_Administration_101

Day 4

Ashish Belwase
& CE-IV

Training Contents

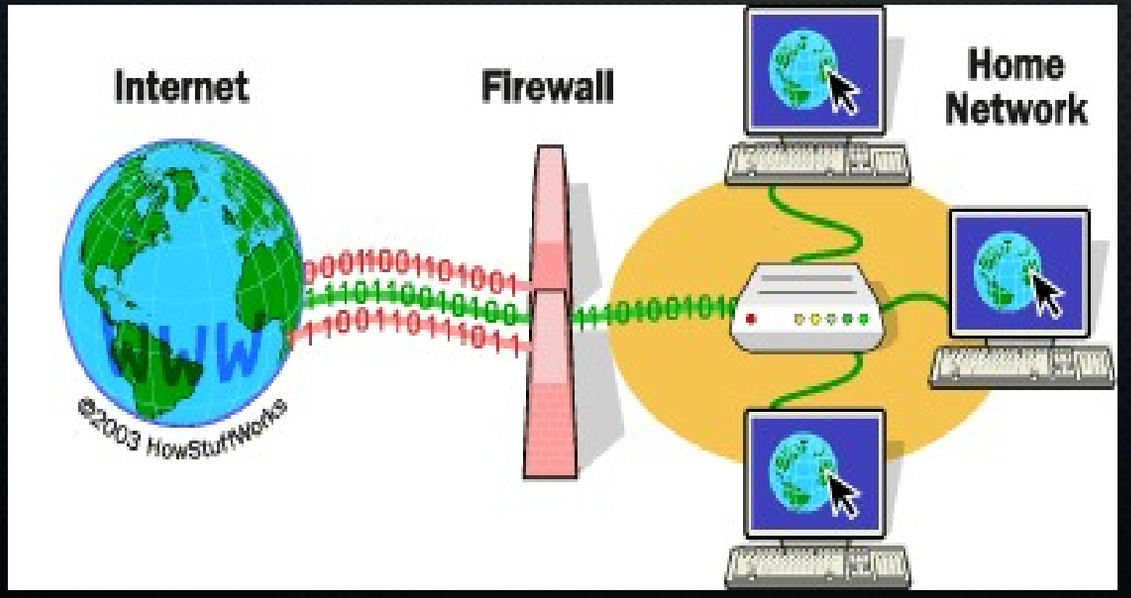
- Introduction to Networking [1]
- Clamping & Network Devices[2]
- Centos Installation & Basic Linux Commands[3]
- Commands & Configuring Network[3]
- DHCP Server[2]
- Bandwith Management [1]
- DNS & Proxy Server[2]
- Web & FTP Server[1]
- Securing Server with Firewall & NAT [2]
- Job Scheduling, Monitoring & Bash Scripting [3]
- Remote Network Administration[1]
- Mikrotik-First Time Access[1]
- IP,DHCP,NAT (masquerade) [1]
- Wrap-up[1]

Day 4

- Firewall
- Iptables
- NAT
- Job Scheduling
- Bash Scripting

Firewall

- Controls the incoming and outgoing network traffic based on applied rules.
- Helps to create trusted and secured network
- Prevents hackers, viruses, and worms that try to reach your computer over the Internet
-



iptables

- A linux kernel tool to manipulate firwall
- Uses the chains (matched against traffic)and rules it store
- Uses table to hold chains of rules
- 3 Predefined chain
  - INPUT - All packets destined for the host computer.
  - OUTPUT - All packets originating from the host computer.
  - FORWARD - All packets neither destined for nor originating from the host computer, but passing through (routed by) the host computer. This chain is used if you are using your computer as a router.
-

iptables

- Display iptables rules
  - Sudo Iptables -L
  - Sudo iptables -L INPUT -n --line-numbers
- Delete a rule
  - iptables -D INPUT 4 #4 is line number
- Block/Allow an IP
  - iptables -A INPUT -s 192.168.1.11-j DROP
  - iptables -A INPUT -s 192.168.0.0/24 -j DROP #block whole subnet
-

iptables

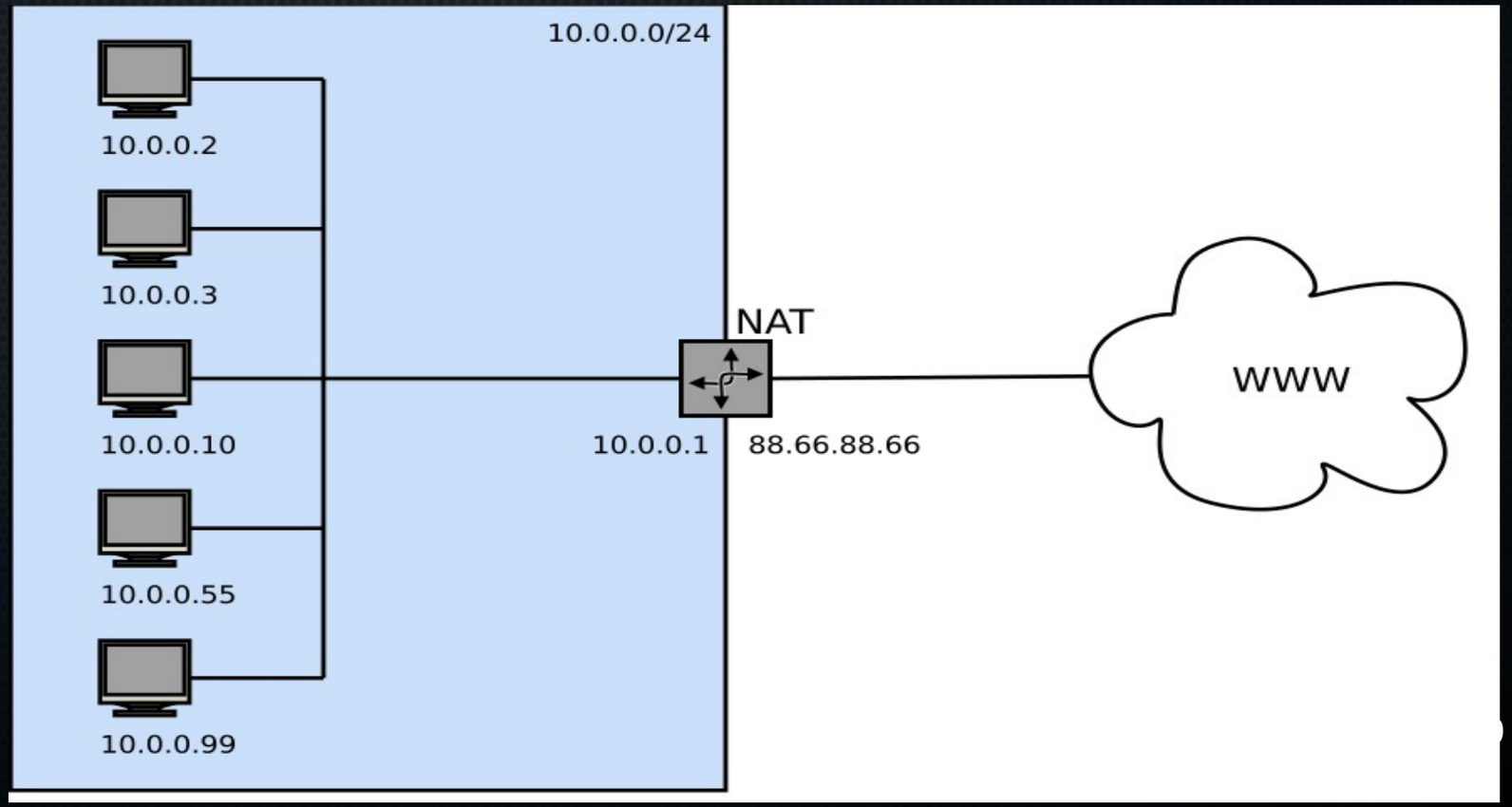
- Block/Allow port 80
  - iptables -A INPUT -p tcp --dport 80 -j DROP
  - iptables -A INPUT -i eth1 -p tcp --dport 80 -j DROP
- Block/Allow a port for specific IP
  - iptables -A INPUT -p tcp -s 1.2.3.4 --dport 80 -j DROP
  - iptables -A INPUT -i eth1 -p tcp -s 192.168.1.0/24 --dport 80 -j DROP

iptables

- Block www.facebook.com
  - First find IP of facebook
    - host -t a www.facebook.com
  - Find CIDR (Classless interdomain routing)
    - whois 69.171.228.40 | grep CIDR
  - Now DROP with iptables
    - iptables -A OUTPUT -p tcp -d 69.171.224.0/19 -j DROP
  - Also domain names can be used to block
    - iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP
    - iptables -A OUTPUT -p tcp -d facebook.com -j DROP

NAT (Network Address Translation)

- Mapping of one IP Address to Another
- Provides a type of firewallby hiding internal IP addresses
- Port Forwarding
-



NAT (Network Address Translation)

- Configuring NAT with iptables
  - Flush all chains
    - iptables --flush
    - iptables --table nat --flush
    - iptables --delete-chain
    - iptables --table nat --delete-chain

NAT (Network Address Translation)

- Configuring NAT with iptables
  - Forward the port
    - echo 1 > /proc/sys/net/ipv4/ip_forward
  - Masquerade
    - iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
  - Forward
    - iptables -A FORWARD -i eth1 -j ACCEPT
-

Limit SSH Access

- Limit SSH Access by hosts
  - /etc/hosts.allow
  - sshd: 192.168.1.30
  - sshd: ALL: DENY
-

Job Scheduling

- Automatic Execution of programs
- Cron jobs : Crontab -e
- Format : Minute Hour Day Month Day_Of_Week Command
- Run p1 program every four hours
  - 0 4 * * * p1
- Runs backup at 10:00 p.m. every Friday night:
  - 0 22 * * 5 /usr/local/scripts/backup
- send out an e-mail at 4:01 a.m. on April 1 (whatever day may be):
  - 1 4 1 4 * /bin/mail dad@domain.com < /home/abgeek/mail_text
  -

Monitoring Network

- iftop -i eth1 -bnB
- Arp -i
- Netstat -antu
- Nmap
- Wireshark
- bmon

Bash Scripting

- Every tool may not be available so admins have to create their own scripts
-