PRAKTIKUM 3

Konfigurasi Firewall [iptables]

A.TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep dasar firewall
2. Mahasiswa mampu melakukan proses filtering menggunakan iptables

B.DASAR TEORI

Firewall adalah sistem atau sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan. Secara prinsip, firewall dapat dianggap sebagai sepasang mekanisme : yang pertama memblok lalu lintas, yang kedua mengijinkan lalu lintas jaringan. Firewall dapat digunakan untuk melindungi jaringan anda dari serangan jaringan oleh pihak luar, namun firewall tidak dapat melindungi dari serangan yang tidak melalui firewall dan serangan dari seseorang yang berada di dalam jaringan anda, serta firewall tidak dapat melindungi anda dari program-program aplikasi yang ditulis dengan buruk.

Secara umum, firewall biasanya menjalankan fungsi:

- Analisa dan filter paket

  Data yang dikomunikasikan lewat protokol di internet, dibagi atas paket-paket. Firewall dapat menganalisa paket ini, kemudian memperlakukannya sesuai kondisi tertentu. Misal, jika ada paket a maka akan dilakukan b. Untuk filter paket, dapat dilakukan di Linux tanpa program tambahan.
- Bloking isi dan protokol

  Firewall dapat melakukan bloking terhadap isi paket, misalnya berisi applet Jave, ActiveX, VBScript, Cookie.
- Autentikasi koneksi dan enkripsi

Firewall umumnya memiliki kemampuan untuk menjalankan enkripsi dalam autentikasi identitas user, integritas dari satu session, dan melapisi transfer data dari intipan pihak lain. Enkripsi yang dimaksud termasuk DES, Triple DES, SSL, IPSEC, SHA, MD5, BlowFish, IDEA dan sebagainya.

Secara konseptual, terdapat dua macam firewall yaitu :

- Network level

  Firewall network level mendasarkan keputusan mereka pada alamat sumber, alamat tujuan dan port yang terdapat dalam setiap paket IP. Network level firewall sangat cepat dan sangat transparan bagi pemakai. Application level firewall biasanya adalah host yang berjalan sebagai proxy server, yang tidak mengijinkan lalu lintas antar jaringan, dan melakukan logging dan auditing lalu lintas yang melaluinya
- Application level.

  Application level firewall menyediakan laporan audit yang lebih rinci dan cenderung lebih memaksakan model keamanan yang lebih konservatif daripada network level firewall. Firewall ini bisa dikatakan sebagai jembatan. Application-Proxy Firewall biasanya berupa program khusus, misal squid

C.TUGAS PENDAHULUAN

1. Sebutkan dan jelaskan dengan singkat apa yang disebut dengan konsep firewall ?
2. Sebutkan fasilitas iptables yang ada di linux !
3. Jelaskan perbedaan chain input, forward, output dari iptables ?

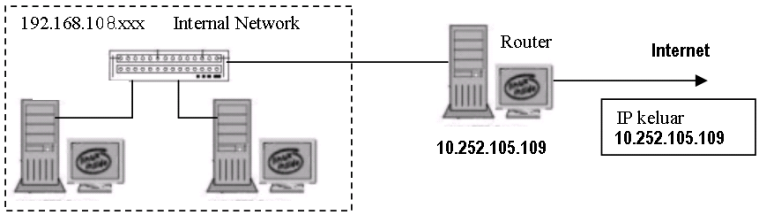
D.PERCOBAAN

Percobaan 1

1. Bangun desain jaringan sebagai berikut :

   Diasumsikan jairngan internal 192.168.108.0/24 dan jaringan internet 10.252.105.0/24

   IP Jaringan internet adalah IP dari jaringan EEPIS.



2. Setting komputer sebagai router (PC1) sbb :
   - Setting IP terkoneksi ke dua jaringan (jaringan internal dan internet)
     - Eth0 → 10.252.105.109 Bcast:10.252.105.255 Mask:255.255.255.0
       - IP pertama adalah IP yang terkoneksi ke jaringan EEPIS
     - Eth0:1 → 192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
       - IP Kedua adalah IP yang dibuat sebagai jaringan local

   - Setting default router supaya bisa terkoneksi jaringan internet (seluruh jaringan eepis dianggap sebagai jaringan internet)
     - # route add default gw <no_IP_GW>
     - # route add default gw 10.252.105.1

   - Setting ip_forward supaya router bisa memford data
     - #echo 1 > /proc/sys/net/ipv4/ip_forward

   - Setting menggunakan NAT
     - # iptables –t nat –A POSTROUTING –s *IP_number_sumber* -d 0/0 –j MASQUERADE

     NB : untuk mengetahui sudah terinstall : #iptables –t nat -nL
3. Setting komputer client sbb :
   - Client1
     - Setting IP

       Dengan IP:192.168.108.10 Bcast:192.168.108.255 Mask:255.255.255.0
     - Setting Gateway ke IP router 192.168.108.1

       route add –net default gw 192.168.108.1
   - Client2
     - Setting IP

Dengan IP:192.168.108.5 Bcast:192.168.108.255 Mask:255.255.255.0

- Setting Gateway ke IP router 192.168.108.1

  route add –net default gw 192.168.108.1

- Computer Internet
  - Setting dengan menggunakan no_ip yang diberikan oleh admin eepis, untuk mempermudah jalankan dhclient dari terminal (misal mendapat IP 10.252.105.109)

4. Lakukan test konektifitas
   - Router
     - ping 192.168.108.10, ping 10.252.105.1, ping 10.252.105.109, ping 202.154.178.3 (no ip DNS Server)

   - Client
     - ping 10.252.105.109, ping 192.168.108.5, ping 192.168.108.20, ping 10.252.105.1, ping 202.154.178.2

5. Pada komputer internet lakukan installasi web, ftp dan telnet

   #apt-get install apache2 proftpd telnetd
6. Lakukan koneksi di sisi client untuk mengakses web, telnet dan ftp, dan pastikan berhasil.
7. Dari komputer Router buat rule rule firewall sebagai berikut :
   - Setting memblok Client1 supaya tidak bisa mengakses telnet dan FTP sedangkan client2 diperbolehkan
   - Client1 dan client2 boleh akses web
     - #iptables –A FORWARD –s 192.168.108.0/24 –d 0/0 –p tcp --dport www -j ACCEPT
     - #iptables –A FORWARD –s 192.168.108.5/24 –d 0/0 –p tcp --dport telnet,ftp -j ACCEPT

- #iptables –A FORWARD –s 192.168.108.10/24 –d 0/0 –p tcp --dport telnet,ftp -j DROP
- #iptables–restore, iptables-save

8. Ceklah rule firewall yang telah anda buat

   #iptables –nL

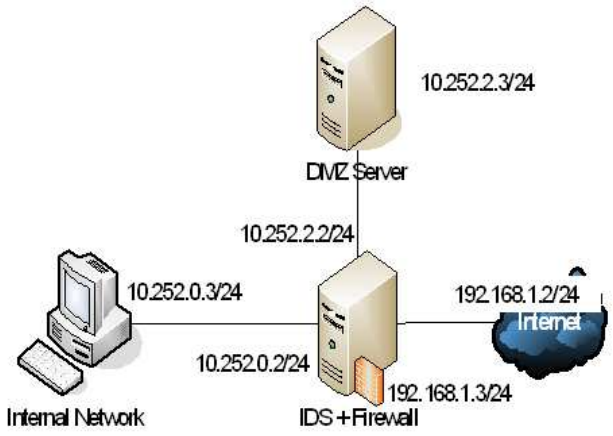
   atau

   #iptables –t nat –nL

9. Lakukan koneksi lagi ke web, telnet dan ftp pada client1 dan client2, catat hasilnya dan harus sesuai dengan rule, jika tidak sesuai ganti nomor urut rule firewall yang anda masukkan dan pastikan rule terpenuhi
10. Buat kesimpulan dari praktikum anda.

Percobaan 2 :

a. Buat desain jaringan sbb :



b. Bangun Jaringan dan konfigurasi sendiri seperti gambar diatas.
c. Install web server, FTP Server, dan Telnet pada jaringan DMZ server

   Untuk instalasi webserver, FTP server dan telnet

   # apt-get install apache2 proftpd telnetd

d. Buat statefull firewall :
   i. New state diperbolehkan dari internet ke DMZ

ii. New state tidak diperbolehkan dari internet ke IDS+firewall dan internal
iii. New state diperbolehkan dari internal ke DMZ dan IDS+Firewall
iv. New State tidak diperbolehkan dari DMZ Server ke internal, Firewall dan internet
v. New state tidak diperbolehkan dari firewall ke internal network

e. Buat jaringan 192.168.1.2 bisa akses web, ftp tapi tidak bisa akses telnet
f. Buat jaringan 192.168.1.2 tidak boleh melakukan perintah ping ke DMZ server
g. Buat jaringan internal bisa akses web, ftp dan telnet
h. Ceklah rule firewall yang telah anda buat
   #iptables –nL atau #iptables –t nat -nL

E. Daftar Pertanyaan

1. Berikan kesimpulan hasil praktikum yang anda lakukan.
2. Apa command iptables untuk melakukan blocking terhadap http ?
3. Apa command iptables untuk melakukan blocking terhadap MAC address tertentu ?
4. Apa saja command iptables yang dibuat jika kita hanya memperbolehkan ssh yang jalan di jaringan ?
5. Bagaimana jika yang diperbolehkan adalah ssh, web dan email ?
6. Bagaimana untuk blocking command ping ?