Iptables

Se doreste crearea unui firewall stateful pentru sistem Linux folosit ca Desktop. Pe acesta nu ruleaza servere, iar utilizatorul poate comunica cu orice serviciu extern.

stergerea tuturor regulitor din tabelul filter din toate CHAIN-urile
iptables -F
permitere trafic loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
permitea tuturor pachetelor generate de host (starea NEW,ESTABLISHED si RELATED)
iptables -A OUTPUT -m state –state NEW,ESTABLISHED,RELATED -j ACCEPT
permitea pachetelor care se intorc catre host si nu reprezinta initializarea unei conexiuni(starea ESTABLISHED si RELATED)
iptables -A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT
setare policy DROP pe INPUT si OUTPUT. Pachetele care nu sunt prinse de cele 2 reguli de mai sus sunt dropate
iptables -P INPUT DROP
iptables -P OUTPUT DROP

Filtrarea dupa MAC

iptables -F
permitere trafic loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
frame-urile cu mac-ul sursa specificat sunt permite pe INPUT
iptables -A INPUT -i eth0 -m mac –mac-source 00 :1A :92 :96 :18 :58 -j ACCEPT
policy pe INPUT este DROP (restul frame-urilor sunt filtrate)
iptables -P INPUT DROP
pe output se poate lasa policy ACCEPT
iptables -P OUTPUT ACCEPT

Tema :

1. Blocarea conexiunilor catre host cu exceptia SSH. Traficul outbound si raspunsul la acesta este permis.

iptables -F
iptables -A INPUT -p tcp –dport 22 -j ACCEPT
iptables -A INPUT -m state –state ESTABLISHED, RELATED -j ACCEPT

iptables -A OUTPUT -m state –state NEW,ESTABLISHED, RELATED -j ACCEPT
iptables -P INPUT DROP
iptables -P OUTPUT DROP
2. Logarea de pachete

Cerinta :
se doreste logarea tuturor pachetele de tip HTTP care sunt generate de host in vederea analizarii ulterioare a site-urilor vizitate sau pentru analiza continutului headerelor acestora.

se foloseste targetul LOG –log-level specifica facilitatea syslog folosita –log-prefix specifica un string care se va gasi in fata fiecarui pachet logat pentru o identificare mai usoara
iptables -A OUTPUT -p tcp –dport 80 -j LOG –log-level info –log-prefix "HTTP generat de host"

3. Se doreste crearea unui firewall pentru un server din LAN.
Cerinte :
- pe host ruleaza server ssh (tcp/22), http (tcp/80), https (tcp/443), smtp (tcp/25), pop (tcp/110), imap (tcp/143) si dns (dns/53). Toate aceste servicii si doar acestea trebuie sa fie accesibile userilor din LAN
- firewall-ul trebuie sa dropeze si sa logheze pachetele invalide
- serverul poate accesa pe internet doar servere web (pentru update) si dns (pentru query iterative sau pentru a folosi un forwarder)

TCP_IN_LAN="22 25 80 110 143 443"
UDP_IN_LAN="53"

TCP_OUT_WAN="80"
UDP_OUT_WAN="53"

stergere orice regula din toate tabelele de pe toate chainurile
iptables -t filter -F
iptables -t nat -F
iptables -t mangle -F

logarea pachetelor invalide trimise sau primite de server
iptables -A INPUT -m state –state INVALID -j LOG –log-level info –log-prefix "INPUT INVALID PACKET"
iptables -A OUTPUT -m state –state INVALID -j LOG –log-level info –log-prefix "OUTPUT INVALID PACKET"

dropara pachetelor invalide trimise sau primite de server
iptables -A INPUT -m state –state INVALID -j DROP
iptables -A OUTPUT -m state –state INVALID -j DROP

permitere trafic loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

ciclu for pentru adaugarea unei reguli pentru fiecare port tcp permis (conexiune din LAN catre server)
for tcp_lan in $TCP_IN_LAN
do

permiterea pachetelor din LAN catre server
iptables -A INPUT -s 192.168.0.0/24 -p tcp –dport -j ACCEPT
permitearea raspunsului la pachetele din LAN catre server
iptables -A OUTPUT -d 192.168.0.0/24 -p tcp –sport -j ACCEPT
done

ciclu for pentru adaugarea unei reguli pentru fiecare port tcp permis (conexiune din LAN catre server)
for udp_lan in $UDP_IN_LAN
do
iptables -A INPUT -s 192.168.0.0/24 -p udp –dport -j ACCEPT
iptables -A OUTPUT -d 192.168.0.0/24 -p udp –sport -j ACCEPT
done

ciclu for pentru adaugarea unei reguli pentru fiecare port tcp permis (conexiuni de la server catre Internet)
for tcp_wan in $TCP_OUT_WAN
do
iptables -A OUTPUT -d 0/0 -p tcp –dport -j ACCEPT
iptables -A INPUT -s 0/0 -p tcp –sport -j ACCEPT
done

ciclu for pentru adaugarea unei reguli pentru fiecare port udp permis (conexiune de la server catre Internet)
for udp_wan in $UDP_OUT_WAN
do
iptables -A OUTPUT -d 0/0 -p udp –dport -j ACCEPT
iptables -A INPUT -s 0/0 -p udp –sport -j ACCEPT
done

adaugare reguli pentru pachete ICMP din LAN (userii din LAN pot da ping la server. Acesta nu raspunde la ping de pe Internet)
iptables -A INPUT -s 192.168.0.0/24 -p icmp -j ACCEPT
iptables -A OUTPUT -d 0/0 -p icmp -j ACCEPT

setare policy DROP pentru pachetele care nu au fost permise de regulile de mai sus
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP