LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Firewall avansat

Scenariu 1

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)

```
#!/bin/bash

#VARIABLE SECTION
#####################################################################
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"
```

Scenariul 2

Se doreste crearea unui firewall pentru un Router Linux.
Routerul este un host Linux cu 2 interfete Ethernet. Interfata eth0 este de LAN iar interfata eth1 este de WAN. ISP-ul furnizeaza un singur IP public, iar subnetul de LAN este 192.168.0.0/24
Se considera ca Routerul este deja configurat corect pentru NAT.
Cerinte:

- userii din LAN pot accesa pe Internet doar site-uri web, pot sa-ti citeasca e-mailul folosind un client dedicat precum Mozilla Thunderbird sau se pot conecta prin ssh la alte servere. Alte servicii nu trebuie sa fie accesibile
- Routerul nu poate fi verificat cu ping de pe Internet ci doar din LAN

```
#!/bin/bash

#VARIABLE SECTION
#####################################################################
LAN_ACCESS="22 25 80 110 143 443"
#####################################################################
#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 catre 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
```