LINUX SERVER ADMINISTRATION

DOCUMENTATIE CURS

Firewall basic

Important

Crearea unui firewall eficient folosind comanda iptables poate avea loc doar dupa intelegerea in profunzime a conceptelor prezentate in sectiunile anterioare. Exersati doar dupa ce notiunile de CHAIN, tabele, reguli, traversarea chainurilor etc va sunt foarte clare !

Nota

Regulile unui firewall se scriu intr-un fisier text, caruia i se seteaza ulterior dreptul de executie si se ruleaza pentru a fi incarcat ir memorie (exceptie acolo unde este precizat ca rularea comenzii iptables are loc direct din consola).

Nota

Prima regula dintr-un firewall este aceea care sterge orice firewall existent (iptables -F). Altfel rulari succesive ale scriptului determina incarcarea aceleiasi reguli de mai multe ori.

Important

In Linux exista o interfata virtuala numita Loopback (prescurtata lo) care poate fi vizualizata folosind ifconfig. Este foarte important ca traficul care paraseste interfata de loopback precum si traficul destinat interfetei de loopback sa fie permis de firewall. Altfel sistemul devine instabil, iar anumite procese nu mai pot functiona corect. Exemplu: serverul grafic X.
Interfata de loopback are ip-ul 127.0.0.1 si numele localhost. Este folosita de catre procesele client-server care ruleaza pe acelasi host.

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

Scenariul 1

Se doreste obtinerea de help pentru comanda iptables pentru diferite optiuni ale acesteia.

Nota

In general se completeaza comanda iptables pana la momentul la care dorim obtinerea helpului apoi se foloseste optiunea -h. Comanda se executa direct in consola

a) ICMP help, specificarea tipurilor ICMP

```
iptables -p icmp -h
```

Output generat:

```
ICMP v1.4.0 options:
 --icmp-type [!] typename       match icmp type
                        (or numeric type or type/code)

Valid ICMP Types:
any
echo-reply (pong)
destination-unreachable
   network-unreachable
   host-unreachable
   protocol-unreachable
   port-unreachable
   fragmentation-needed
   source-route-failed
   network-unknown
   host-unknown
```

```
  network-prohibited
```

b) Obtinerea de informatii despre filtrarea dupa MAC (doar in LAN). Se foloseste optiunea `-m mac`. Se poate filtra doar dupa mac sursa si doar pe INPUT.

```
iptables -m mac -h
```

Output generat:

```
MAC v1.4.0 options:
 --mac-source [!] XX:XX:XX:XX:XX:XX
                        Match source MAC address
```

c) Obtinerea de informatii despre optiunile referitoare la TCP (specificarea porturilor sursa si destinatie dupa care se filtreaza, filtrarea dupa flaguri etc)

```
iptables -p tcp -h
```

Output generat:

```
TCP v1.4.0 options:
 --tcp-flags [!] mask comp      match when TCP flags & mask == comp
                        (Flags: SYN ACK FIN RST URG PSH ALL NONE)
[!] --syn                  match when only SYN flag set
                        (equivalent to --tcp-flags SYN,RST,ACK,FIN SYN)
 --source-port [!] port[:port]
 --sport ...
                        match source port(s)
 --destination-port [!] port[:port]
 --dport ...
                        match destination port(s)
 --tcp-option [!] number       match if TCP option set
```

Scenariul 2

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

- hostul poate genera orice fel de trafic TCP, UDP sau ICMP catre orice IP extern;
- pachetele destinate hostului sunt acceptate doar daca reprezinta raspuns la traficul generat din interior;
- pachetele care reprezinta initializarea unei conexiuni din exterior catre interior sunt filtrate;

```
#!/bin/bash

#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
```

Scenariul 3

Dorim crearea unui firewall statefull pentru Desktop pe care ruleaza si un server SSH care asculta pe portul TCP/22.
Cerinte:

- hostul poate genera orice fel de trafic TCP, UDP sau ICMP catre orice IP extern
- pachetele destinate hostului sunt acceptate doar daca reprezinta raspuns la traficul generat din interior
- userul se conectaza uneori la host prin SSH de la un anumit IP (Exemplu: IP-ul 80.0.0.1 setat in locatia de unde se conecteaza user

- pachetele care reprezinta initializarea unei conexiuni din exterior (exceptand SSH de la IP-ul de mai sus) catre interior sunt filtrate

```
#!/bin/bash

#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

#permiterea pachetelor SSH din exterior catre interior de la IP 80.0.0.1
iptables -A INPUT -p tcp --dport 22 -s 80.0.0.1 -j ACCEPT

#permitea 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 (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
```

Scenariul 4

Se doreste oprirea oricarui firewall care ruleaza pe host cu stergerea oricarei configuratii de SNAT sau DNAT sau de modificare de pachete.

```
#!/bin/bash

#stergerea tuturor regulilor din tabelul filter de pe toate chainurile
iptables -t filter -F

#stergerea tuturor regulilor din tabelul nat de pe toate chainurile
iptables -t nat -F

#stergerea tuturor regulilor din tabelul mangle de pe toate chainurile
iptables -t mangle -F

#setarea policy ACCEPT pe toate chainurile unde se poate realiza filtrare (INPUT,OUTPUT si FORWARD)
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

Scenariul 5

Filtrarea dupa MAC
Cerinte:

- se doreste acceptarea de pachete doar de la un singur MAC
- scenariu poate fi util cand se doreste limitarea hosturilor cu care poate comunica un server in LAN, sau comunicarea doar cu default gateway si deci doar pe Internet

```
#!/bin/bash

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
```

Scenariul 6

Listarea unui firewall sau verificare firewall care ruleaza. Comanda se executa direct in consola.

```
iptables -vnL
```

Outputul acestei comenzi ne indica:

- policy de pe fiecare CHAIN
- regulile din tabelele atasate chain-urilor
- nr de pachete prinse de fiecare regula

Comanda de mai sus listeaza toate regulile din tabelul filter (este default) de pe toate chainurile

Daca se doreste listarea regulilor din tabelul nat sau mangle se foloseste:

```
iptables -t nat -vnL
```

Scenariul 7

Un host Linux a fost transformat in Router pentru conectarea unui LAN la Internet. Acesta este configurat cu 2 placi Ethernet si realizeaza N
Se doreste modificarea TTL-ului inainte procesului de rutare
Cerinte:

- un ISP pentru nu permite unui client sa creeze o retea locala si deci pentru a impune conectarea unui singur calculator la Internet a putea trimite toate pachetele catre client cu TTL=1. In momentul in care se conecteaza un Ruter, acesta va decrementa TTL-ul pachetelor IP si fiindca acesta ajunge la zero, ruterul va arunca pachetele
- se doreste setarea TTL pentru toate pachetele primite de router la 64 (valoarea default pe Linux) inaintea procesului de rutare

```
#!/bin/bash

#orice regula pentru manipularea pachetului se adauga in tabelul mangle. Fiindca se doreste modificarea TTL inaintea procesului de rutare
#foloseste chainul PREROUTING. Se mai poate folosi si OUTPUT pentru modificarea ttl-ului pentru pachetele trimise inaintea procesului de
#rutarea sau POSTROUTING pentru modificare dupa procesul de rutare

iptables -t mangle -A PREROUTING -i eth0 -j TTL --ttl-set 64
```

Scenariul 8

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

```
#!/bin/bash

#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"
```

Nota

Pentru vizualizarea pachetelor poate fi rulata comanda dmesg fiindca se foloseste facilitatea kernel din syslog. Intr-un setup profesional acestea informatii trebuie redirectate catre un fisier special. Pentru aceasta este nevoie de configurarea syslog. Pentru detalii cititi capitolul "Managementul Logurilor" a acestui curs.

Iptables help

Durata: 1.49 min
Marime: 4.7MB

Stateful firewall. Este permis tot traficul outbound si raspunsul la acesta. Ideal pentru Desktop

Durata: 1.46 min
Marime: 336KB

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

Durata: 5.35 min
Marime: 309KB

Logare PING (pachetele ICMP echo-request trimise si echo-response primite).

Durata: 1.55 min
Marime: 435KB