Lucrarea 4

1 Modul de construire a regulilor de firewall

O regulă de firewall reprezintă direcţiile la care firewallul se adaptează atunci când blochează sau permite anumite conexiuni şi pachete într-un anumit lanţ. Toate comenzile pe care le scriem şi care sunt inserate într-un lanţ, vor fi considerate reguli de firewall. Cu alte cuvinte, fiecare regula de firewall este o linie de comandă pe care kernelul o analizează, pentru a afla ce trebuie sa facă cu un anume pachet.Dacă un pachet se potriveste unei reguli de firewall, se efectueaza ***destinatia(target-ul)*** regulii respective sau un salt la o instrucţiune definită in regula de firewall respectivă. Sintaxa unei reguli arată astfel:

iptables [-t *table*] command [match] [target/jump]

Observaţie: comanda (command) trebuie să fie tot timpul prima, sau ca alternativă, să fie după tabelă după tabelă(table). ***Potrivirea (match-ul)*** este partea regulii pe care noi o trimitem kernelului, care detaliază caracteristicile specifice ale pachetului, care îl deosebesc de celelalte pachete. Aici putem specifica care este adresa IP de unde vine pachetul, pe ce interfaţă vine acesta, pe ce interfaţă doreşte acesta să meargă, ce port folseste, ce prorocol foloseşte, etc. În final avem ţinta pachetului (target). Daca sunt intâlnite toate potrivirile pentru un anume pachet, se poate specifica kernelului ce sa facă cu el. Putem de exemplu să îi "spunem" kernelului să trimită pachetul către un alt lanţ pe care noi l-am creat, şi care face parte din această tabelă. Putem să îi spunem kernelului să "*arunce" pachetul* ***(drop)*** deci să nu îl mai proceseze, sau putem să îi spunem kernelului să trimită expeditorului un anume mesaj.

1.1 Comenzi

Următoarele comenzi sunt disponibile pentru iptables:

-A, --append inseamna adauga
Exemplu: **iptables –A INPUT INPUT --dport 80 -j DROP**
Această comandă adaugă o regulă la sfarsitul unui lanţ. Această regulă fiind ultima din lanţ, ea va fi verificată ultima, aceasta doar în cazul în care nu se mai adaugă ulterior alte reguli la lanţ.

-D, --delete
Exemplu: **iptables -D INPUT --dport 80 -j DROP**; **iptables -D INPUT 1**
Această comandă, şterge o regulă dintr-un lanţ. Acest lucru poate fi realizat in două moduri; sau specificând intreaga regulă pe care dorim să o stergem (asa ca în primul exemplu), sau specificând doar numărul regulii la care comanda trebuie să se potrivească(ca în al doilea exemplu). Dacă se foloseşte prima variantă, intrarea trebuie să se potrivească exact cu intrarea din lanţ. Dacă se foloseşte a doua metodă, trebuie să se potrivească numărul regulii cu regula pe care dorim să o stergem. Regulile sunt numerotate de la începutul fiecărui lanţ incepând cu numarul 1.

-R, --replace

Exemplu: **iptables -R INPUT 1 -s 192.168.0.1 -j DROP**

Comanda inlocuieste vechea intrare de la linia specificata. Aceasta comanda functioneaza similar cu comanda **–delete**, dar in loc sa stearga complet intrarea, o va inlocui cu noua intrare. Aceasra comanda se utilizeaza atunci cand se experimenteaza implementarea unui firewall.

-I, --insert

Exemlu: **iptables -I INPUT 1 --dport 80 -j ACCEPT**

Cu ajutorul acestei comenzi inseram o regula intr-un lant. Regula este inserata in locul indicat de numarul specificat. In cazul de fata, regula va fi considerate ca fiind prima regula in lantul INPUT.

-L, --list

Exemplu: **iptables -L INPUT**

Aceasta comanda listeaza toate intrarile din lantul specificat. In cazul de fata vom lista toate regulile referitoare la lantul input. Daca nu se specifica lantul, comanda va afisa toate intrarile existente in firewall. Daca comanda se foloseste ci cu optiunea **–v**, se vor afisa si contoarele pentru fiecare regula, adica numarul de pachete care s-au potrivit cu regula respectiva

-F, --flush

Exemplu: **iptables –F INPUT**

Acesta comanda, va elimina toate regulile din lantul specificat. Ea este echivalenta cu stergerea regulilor una cate una. Daca nu se specifica un lant, comanda va sterge toate regulile de firewall.

-Z, --zero

Exemplu: **iptables -Z INPUT**

Comanda de mai sus, spune programului sa aduca la zero toate contoarele din lantul specificat.

-N. –new-chain

Exemplu: **iptables -N allowed**

Aceasta comanda spune kernelului sa creeze un nou lant, care va purta numele specificat. In exemplul nostru, lantul va fi numit **allowed**.

-X, --delete-chain

Exemplu: **iptables -X allowed**

Aceasta comanda sterge din tabela lantul specificat. Pentru ca aceasta comanda sa functioneze correct, trebuie sa nu existe reguli care sa se refere la acest lant care va fi sters. Deci inaintea utilizarii acestei comenzi trebuie sa stergem sau sa inlocuim regulile care se refera la acest lant.

-P, --policy

Exemplu: **iptables -P INPUT DROP**

Comanda de mai sus, spune kernelului sa seteze pentru un anumit lant, o anumita politica implicita. Daca un pachet nu se potriveste cu nici o regula, atunci lui i se va aplica politica implicita; in cazul nostru el va fi "aruncat".

-E, -rename-chain

Exemplu: **iptables -E allowed disallowed**

Comanda –E spune kernelului sa schimbe primul nume cu cel de-al doilea. In cazul nostrum numele allowed va fi schimbat cu disallowed.

1.2 Potrivirea pachetelor la regulile de firewall (Matches)

In continuare, voi prescurta termenul de potrivire a pachetelor la regulile de firewall cu termenul potrivire sau match.

Exista mai multe tipuri de potriviri ale pachetelor de firewall printre acestea se pot enumera: potrivirile generice, care pot fi utilizate in toate regulile, potrivirile TCP, care se pot aplica doar pachetelor TCP, potrivirile UDP, care se pot aplica doar pachetelor UDP, potrivirile ICMP, care pot fi utilizate doar pentru pachetele ICMP. In cele din urma avem potriviri speciale care pot fi legate de: startea conexiunii, de proprietar, de o anumita limita a numarului de pachete, etc.

1.2.1 Match-uri generice

O potrivire generică este o potrivire care este tot timpul disponibilă indiferent de modulele extensiilor de potrivire încarcate în kernel. Nici un parametru special nu este necesar pentru a utiliza acest tip de potrivire. De exemplu daca dorim sa utilizam o potrivire de tip TCP, trebuie sa folosim ca optiune potrivirea de protocol: **--protocol**.

Match: **-p, --protocol**
Exemplu**:** **iptables -A INPUT -p tcp**
Explicație: Aceasta potrivire este folosită pentru a verifica anumite protocoale. Protocoalele pot fi specificate atât prin numele lor (TCP, UDP, ICMP, etc.) cat şi prin numerele corespunzatoare acestor protocoale (de exemplu, protocolului ICMP îi corespunde valoarea 1, protocoluli TCP îi corespunde valoarea 6, iar protocolului UDP îi corespunde valoarea 17). Dacă în loc de numele sau numarul carespunzator protocolului se pune optiunea *ALL,* acest lucru înseamnă că potrivirea se refera doar la protocoalele TCP, UDP, ICMP. Aceasta potrivire poate fi şi inversata cu ajutorul simbolului "!". In acest caz potrivirea **--protocol ! tcp** va fi asociată protocoalelor UDP şi ICMP (mai precis tuturor protocoalelor care nu sunt tcp).

Match: **-s, --src, --source (sursă)**
Exemplu: **iptables -A INPUT -s 192.168.1.1**

Explicațe: Aceasta este o potrivire bazatã pe sursa pachetului (adresa IP a expeditorului). Se poate specifica ca sursã de pachete atât o singurã adresã IP, cât şi o clasã întreagã de adrese IP. În aceastã ultimã situație vom avea sursa de forma: -s 192.168.0.0/24. Aceastã sursã se va potrivi pachetelor care vin de la ip-urile 192.168.0.x, unde x este un numãr cuprins intre 0-255. Dacã se utilizează semnul "!" în fața adresei IP aceasta înseamnã cã regula de firewall se aplica tuturor pachetelor, mai puțin celor de după semnul "!".

Match: **-d, --dst, --destination (destinație)**
Exemplu: **iptables -A INPUT -d 192.168.1.1**
Explicație: Această potrivire este bazată pe destinaþia pachetelor IP. Aceasta înseamnã cã regula de firewall se va aplica pachetelor care au ca adresã IP destinație, adresa IP specificatã după opțiunea -d. La fel ca şi la potrivirea bazatã pe adresa sursã a pachetelor, se poate specifica o clasã întreagã de adrese, şi se poate utiliza simbolul de negare "!".

Match: **-i, --in-interface (interfata pe care intră pachetele)**
Exemplu: **iptables -A INPUT -i eth0**
Explicație: Această potrivire este utilizatã pentru a specifica faptul ca regula de firewall se aplică tuturor pachetelor care intrã în sistem pe o anumită interfață. Această opțiune este valabilã doar pentru lanțurile: INPUT, FORWARD şi PREROUTING. Dacã nu se specificã nici o interfaþã, regula de firewall se va aplica tuturor interfețelor. Şi în acest caz, se poate folosi simbolul de negare "!".

Match: **-o, --out-interface (interfața pe care ies pachetele)**
Exemplu: **iptables -A OUTPUT -o eth0**
Explicație: Această potrivire este utilizatã pentru a specifica fptul ca regula de firewall se aplicã tuturor pachetelor care pleacã de pe o anumitã interfață, spre o anumitã destinație. Opțiunea este valabilã pentru lanțurile OUTPUT, FORARD, şi POSTROUTING. Dacã nu se specificã nici o interfață, regula se va aplica tuturor interfețelor. Şi aici semnul de negare poate fi utilizat, având aceeasi semnificaþie ca mai sus.

Match: **-f, --fragment (fragmente de pachete)**
Exemplu: **iptables -A INPUT -f**
Explicațe: Această regulã este aplicatã fragmentelor de pachete. În cazul în care avem pachete fragmentate, din acestea nu se poate determina portul sursã sau destinație a acestora. Pentru a realiza atacuri în rețelele de calculatoare, se utilizează foarte des fragmente de pachete. Astfel de pachete nu se vor potrivi nici unei reguli de firewall cu excepþia celei de față.

1.2.2 Match-uri implicite

Există trei tipuri de match-uri implicite: match-uri TCP, match-uri UDP, şi match-uri ICMP.

1.2.2.1 Match-uri TCP

Pentru a folosi aceste potriviri, trebuie ca în linia de comndă să specificam mai întai faptul că este vorba de protocolul TCP (acest lucru se realizează folosind match-ul –**-protocol tcp**)

Match: **--sport, --source-port (portul sursă)**
Exemplu**:** **iptables -A INPUT -p tcp --sport 22**
Explicație: Match-ul **–source-port,** este folosit pentru ca regula de firewall să se asocieze pachetelor care au ca port sursă, portul specificat după acest match (in cazul nostru pachetelor care au ca port sursă portul 22).
se poate utiliza în loc de numărul portului, şi numele serviciului corespunzător acestuia (o lista de corespondență între porturi şi servicii poate fi gasită în fisierul /etc/services). Folosind însă numărul portului, regula de firewall se va activa mult mai repede decâ dacă am utiliza numele serviciului. Match-ul –**source-port** se poate utiliza pentru specificare unei clase de porturi; de exemplu porturile de la 22 la 80. Acest lucru poate fi realizat astfel: **--source-port 22:80.** Se poate utiliza şi în acest caz simbolul "!"; de exemplu –**source-port ! 22** va însemna că regula de firewall se va aplica tuturor pachetelor care au ca sursă toate porturile, cu exceptia acelora care au ca sursă portul 22.

Match: **--dport, --destination-port (port destinație)**
Exemplu: **iptables -A INPUT -p tcp --dport 22**
Explicație: Acest match este utilizat pentru ca regula de firewall să se potrivirească pachetelor care au ca destinație un anumit port. La fel ca şi la –**sport**, pot fi specificate clase de porturi la care regula să se potrivirească. Semnul "!" poate fi deasemenea utilizat pentru a specifica căror pachete regula să nu se potrivirească.

Match: **--tcp-flags (flaguri TCP)**
Exemplu: **iptables -p tcp --tcp-flags SYN, FIN, ACK SYN**
Explicație: Acest match este utilizat pentru a specifica căror flaguri dintr-un pachet TCP se poate aplica regula de firewall. Acest match cunoaste următoarele flaguri: SYN, ACK, FIN, RST, URG, PSH. Şi în acest caz se poate folosi simbolul de negare "!".

Match: **--syn**
Exemplu: **iptables -p tcp --syn**
Explicație: Acest match este folosit pentru a se potrivi pachetelor care au biții SYN setați, iar biþii ACK si RST sunt nesetați. Aceste pachete sunt utilizate de obicei pentru a cere unui server permisiunea de realizare a unei

conexiuni TCP. Dacã se blocheazã aceste pachete, putem spune ca am blocat toate posibilitățile de conectare la sererul respectiv. Şi aici se poate folosi simbolul de negare "!".

Match: **--tcp-option (optiuni TCP)**
Exemplu: **iptables -p tcp --tcp-option 16**
Explicaþie: Acest match este utilizat pentru ca regula de firewall sã se potrivieascã pachetelor depinzând de optiunile TCP ale acestora. Optiunile TCP sunt parte specifica a headerului unui pachet. Acesta parte este alcatuitã din trei campuri: primul are o lungile de 8 biti si ne spune ce opțiuni sunt utilizate în acest flux, al doilea camp are si el 8 biti si ne spune cat de lung este câmpul opțiune. Nu trebuie neaparat sã implementãm toate optiunile, putem în schimb sã ne uitam ce fel de optiune este setatã. Daca aceastã optiune este nu este suportatã (implementatã), putem ignora aceast pachet.

1.2.2.2 Match-uri UDP

Aceste match-uri sunt încarcate implicit atunci cand se specifica optiunea – **protocol UDP.** Deoarece protocolul udp nu este orientat pe conexiune,
avem putine match-uri în cazul acestuia.

Match: **--sport, --source-port**
Exemplu: **iptables -A INPUT -p udp --sport 53**
Explicație: Acet match este utilizat pentu a realiza potriviri între regula de firewall şi portul UDP sursă al pachetelor. Pentru a specifica o clasã de porturi, putem utiliza de exemplu notatia 22:80, ceea ce înseamnă că regula se va potrivi tuturor pachetelor UDP care un port sursă cuprins între 22 si 80. Şi aici se poate utiliza simbolul de negare "!"

Match: **--dport, --destination-port**
Exemplu: **iptables -A INPUT -p udp --dport 53**
Explicație: Acest match este are aceleaşi proprietăți ca şi matchul anterior, dar se refera la pachetele care au ca destinatie un anumit port.

1.2.2.3 Match-uri ICMP

Protocolul ICMP este în principiu utilizat pentru a raporta anumite erori şi pentru a controlul conexiunuilor. Header-ul pachetului icmp seamană cu header-ele IP. Tipul headerului ICMP ne spune motuvul pentru care este folosit acest pachet. Un astfel de exemplu ar fi returnarea unui mesaj de eroare primit în cazul unei conexiuni nereusite.

Match: **--icmp-type**
Exemplu: **iptables -A INPUT -p icmp --icmp-type 8**
Explicație: Aceast match este folosit pentru a specifica carui tip de mesaj icmp, i se va aplica regula de firewall.

Intrebari LUCRAREA 4

1. In ce caz se utilizeaza comanda **–A?;** dar –**D?**
2. Cu ce ce comada se seteaza politica implicita a unui lant?
3. Care este diferente intre comenzile **–s** si **--sport** ?
4. Sa se construiasca un firewall care sa realizeze urmatoarele:
    a) sa blocheze accesul ICMP de la orice IP, si de la interfata de loopback.
    b) sa blocheze accesul la portul TCP 21 de la toate ip-urile
    c) sa blocheze accesul la portul TCP 23 catre toate ip-urile
    d) sa clocheze accesul la portul TCP 22 de la un singur ip din reteaua locala
5. Sa se listeze regulile de firewall create si sa se identifice numarul pachetelor care s-au potrivit cu regulile de firewall create.