LUCRAREA 1

Firewall-uri. Notiuni introductive

1. Introducere

Orice legatură între sistemele unei corporaţii şi Internet comportă un risc major din punct de vedere al securităţii. Odată realizată această legătură, orice navigator pe internet poate teoretic să comunice cu orice calculator din intranet care rulează ***TCP/IP***(Transmition Control Protocol/Internet Protocol). Acest lucru impune deci existenta unui sistem de securitate între intranet si internet, care să stabilească ce pachete de date pot circula între cele două retele. Un asemenea sistem este cunoscut sub denumirea de „***firewall***" Un „firewall" este implementat pe un calculator de mare putere (uzual bazat pe UNIX) care rulează un software relativ special şi care este plasat între reteaua corporaţiei şi Internet. El examinează fiecare pachet de date ce trece din intranet către Internet şi invers.

Calculatorul de firewall este configurat cu un set de reguli care determină ce fel de traffic de reţea va fi admis să circule între cele două reţele, şi ce fel de traffic va fi refuzat. În multe cazuri firewalurile sunt intalnite şi în interiorul organizaţiilor mari pentru a separa anumite zone ale reţelei de angajaţii firmei, acest lucru datorându-se faptului ca multe atacuri care sunt orientate spre anumite calculatoare vin chiar din interiorul organizaţiei şi nu doar din afara acesteia.

Firewallurile pot fi construite în mai multe feluri. Cea mai sofisticată implement-tare implică existenţa mai multor calculatoare pentru firewall, această structură purtând numele de reţea perimetru. Putem avea doua calculatoare care acţionează ca filtre de traffic cunoscute sub numele de "sufocante", care permit trecerea doar pentru anumite tipuri de trafic, şi între aceste doua calculatoare se gasesc serverele reţelei ca de exemplu serverul de e-mail, proxy-ul de World Wide Web(***WWW***). Configuraţia poate fi foarte sigură, şi permite un control foarte mare asupra celor care se pot conecta atât din interior cât şi din exterior la serverele reţelei. Acest tip de configuraţie este folosit de organizaţiile mari.

Calculatoarele pe care se construiesc firewall-uri trebuie sa fie foarte securizate deoarece daca firewallul este vulnerabil, acest lucru poate permite anumitor persoane să aibă acces la calculatorul pe care acesta este constuit şi astfel securitatea întregii reţele este compromisă . În figura 1.1 sunt prezentate cele mai utilizate configurări de firewall.

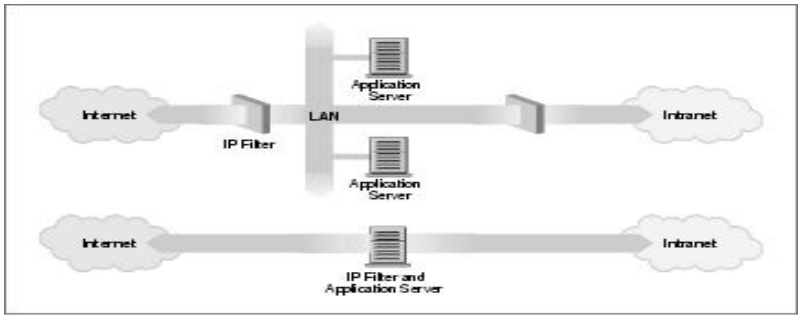

Figura 1.1

Kernelul Linux prezintă un set de servicii care îi permit acestuia sa funcționeze ca şi firewall. Firewallul Linux este flexibil si usor de utilizat pentru a implementa configurațiile prezentate în figura de mai sus.

1.1 Filtrul de pachete

Filtrtul de pachete este o parte a unui program care se "uită" la antetul (headerul) pachetelor pe care acesta le interceptează, şi care decide soarta acestora. Acesta poate decide să "arunce" pachetul (ca si cum acesta nici nu ar fi fost recepționat), poate sa il accepte (pachetul este lăsat să treacă mai departe), sau poate să facă alte lucruri mai complicate cu acesa, lucruri care urmează să fie discutate pe parcursul acestei lucrări.

1.2 Cauzele pentru care se filtrează pachetele

Control:

Dacă avem un calculator pe care este instalat LINUX şi acesta conectează o anumită rețea internă de altă rețea (de exemplu Internet), există posibilitatea de a permite accesul pentru anumite tipuri de trafic, şi de a interzice altele. Un exemplu simplu ar fi blocarea paginilor de reclame care se suprapun peste paginile pe care dorim să leaccesăm.

Securitate:

Când calculatorul LINUX este singurul lucru care stă între haosul Internetului şi rețeaua noastră, este bine să stim cum putem restricționa accesul în reteaua noastră. De exemplu putem permite ca toate pachetele care provin din interiorul retelei noastre să ajungă pe internet, şi putem în acelaşi timp sa blocăm anumite pachete care provin din exterior. Un alt exemplu ar fi să blocam accesul telnet pe server pentru toți utilizatorii din exteriorul rețelei noastre, dar să permitem accesul telnet utilizatorilor din interiorul rețelei.

Verificare volum de trafic:

Uneori, un calculator care nu este bine configurat, şi care face parte din rețeaua locală, să trimită foarte multe pachete catre exterior (de exemplu poate face inundare/*flood*). Este foarte util să specificăm în acest caz filtrului de pachete că dorim să fim anunțați când apar astfel de situații.

1.3. Termeni utilizați :

-DNAT (Destination Network Address Translation). DNAT se referă la tehnica de modificare a adresei IP destinatie a unui pachet.. Aceasta este folosită impreună SNAT pentru a permite mai multor hosturi dintr-o retea locală să împartă între ele o adresa IP oferită de un firnizor de servicii internet (adresă IP rutabilă), astfel încât toate aceste

hosturi să poată naviga pe internet.Acest lucru se face, asignând diferite porturi cu o adresă internet IP rutabilă, şi apoi specificând ruterului locul unde să trimită pachetele.

-Flux de date(Stream) – Acest termen se refera în general la o conexiune între două calculatoare pe care trimit şi primesc pachete. Îm lucrarea de faţa, acest termen se refera la orice conexiune prin care se trimit si se primesc doua sau mai multe pachete. În TCP aceasta ar putea însemna o conexiune care trimite un pachet de sincronizare(***SYN***) şi apoi se răspunde cu un pachet de sincronizare/confirmare (***SYN/ACK***), dar ar putea însemna de asemenea o conexiune care trimite un SYN şi apoi răspunde cu un pachet control a conexiunii ***ICMP***(Internet Control Message Protocol) Host unreachable(host de neatins).

-SNAT (Source Network Address Translation). Acest termen se referă la o tehnica utilizată pentru a modifica adresă sursă a unui pachet. Această tehnică este utilizată pentru a permite mai multor hosturi să împartă o singură adresă internet IP rutabilă.

Pentru a putea utiliza un firewall bazat pe pachetul de programe iptables trebuie recompilat kernelul sistemului de operare LINUX astfel incât acesta să ofere suport pentru utilizarea acestui pachet (vezi Anexa 1)

2. Tabele si lanturi:

2.1 Tabela de modificare a pachetelor *(Mangle)*

Această tabela este folosită pentru a modifica pachetele. Cu ajutorul acesteia se pot modifica campurile: tip de serviciu, TOS (Type of Service), timpul de viaţa al pachetului TTL(Time to Live), marcarea pachetelor MARK.

TOS - este folosit pentru a schimaba în pachet campul Type of Service. Este folositor la setarea politicii unei reţele în cazul rutarii unui pachet. În funcţie de protocoalele utilizate putem avea nevoie de legaturi: rapide dar cu transfer mic de date, mai lente dar cu o incarcare mai mare a liniilor de date, etc. Prin setarea corespunzătoare a acestui câmp, putem alege ruta optima pentru protocolul pe care îl folosim.

TTL - este folosit la schimbarea campului TTL al unui pachet. Valoarea acestui câmp este decrementă cu o unitate de fiecare router pe care pachetul îl străbate pâna la destinatie.

MARK - este folosit pentru a marca diferite valori specifice pachetelor. Aceste valori pot fi recunoscute de iproute2 ptentrua lua diverse decizii de routare pe baza lor.

2.2 Tabela Nat

Această tabelă este folosită în principiu pentru modificarea adreselor IP (***NAT*** - Network Address Translation) Cu alte cuvinte, se va folosi petru a modifica adresa IP sursă a pachetului sau adresa IP destinaţie a pachetului. Doar primul pachet va intra în acest lanţ dintr-un stream; restul vor suferi automat aceeaşi modificare ca si primul.

Target-uri valide în această tabelă sunt DNAT, SNAT si ***MASQUARADE***. Prin target se înțelege actiunea ce urmează se ia atunci când un anume pachet este primit într-o tabelă.

DNAT - este utilizat încazul în care avem o adresa IP publica şi dorim sa redirectam accesul la firewall unei alte stații de lucru. Cu alte cuvinte schimbam adresa destinație a pachetului

SNAT – este de obicei utilizat atunci când se doreste schimbarea adresei sură a pachetelor. Se poate folosi pentru a ascunde o retea locala. Un exemplu de astfel de utilizare ar fi acela al unui firewall a carui adresă de ieşire o cunoaştem, dar dorim să substituim adresa noastră IP locală cu cea a firewall-ului. Folosind ținta SNAT, firewallul va permite crearea conexiunilor intre LAN si Internet.

MASQUERADE – această țintă este folosită ca si SNAT, dar operația MASQUARADE se face într-un timp mai lung. Utilizarea acestei operatii face posibil lucrul cu adrese IP dinamice furnizate de un server DHCP, adresă obtinuta printr-o conexiune ce foloseste protocolul punct la punct (Point to Point Protocol) PPP.

2.3 Tabela de filtrare

Tabela de filtrare este utilizată pentru filtrarea pachetelor. Se face o analiză a pachetului pentru a vedea dacă acesta se potriveste cu ceea ce vrem sa filtram, iar daca aceasta potrivire există, pachetului i se aplică regulile de filtrare (vezi tabelul 4.1).

2.4 Lantul Prerouting

Acest lanț este de obicei folosit pentru a schimba pachetele (de exemplu schimbarea de tipului de serviciu TOS/Type of Service) înainte ca ascestea să fie rutate către calculatorul local.

2.5. Lantul INPUT

Folosim acest lanț pentru a modifica pachetele, după ce ele au fost rutate, dar înainte ca ele să fie trimise către procesul care le va intercepta. In acest lant se fac filtrari pentu pachetele care au ca destinatie calculatorul nostru

2.6 Lantul OUTPUT

Folosim acest lant pentru a face filtrari asupra pachetelor care au ca sursa calculatorul nostrum.

2.7 Lantul POSTROUTING

Lanțul POSTROUTING folosit in tablea mangle este în general utilizat atunci cand dorim să modificam pachetul înainte ca acesta să părăsească hostul, dar dupa decizia de rutare.

2.8 Lantul FORWARD

Acesta poate fi folosit pentru nevoi foarte specifice, în care dorim să modificăm pachetele după deciza inițiala de rutare, dar înainte de ultima decizie de rutare. Aici se pot face filtrari asupra pachetelor care au ca destinatie alte hosturi

3. Traversarea lanturilor si tablelor

Pachetele care sunt interceptate de firewall traverseaza lanturile si tabelele intr-o anumita ordine. Se poate alcatui o organigrama pentru a simplifica modul in care pachetele trec prin firewall:

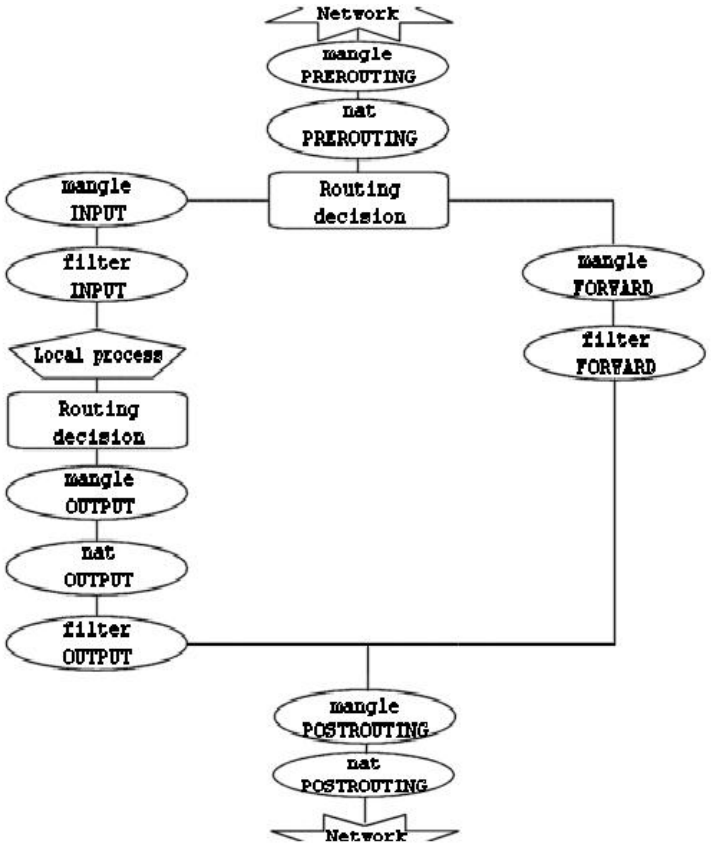

Fig 3.1 Traversarea tabelelor si lanturilor

Intrebari Laborator 1:

1. Pentru ce se foloseste lantul FORWARD .Dati un exemplu theoretic de folosire.

2. Explicati la nivel de principiu folosirea SNAT-ului.
3. Reprezentati ordinea de traversarea lanturilor si tabelelor pentru urmatoarele situatii:
    a) Pachetele sunt transmise de pe hostul local catre o alta retea
    b) Pachetele se transmit intre doua hosturi din reteaua noastra locala

    Se presupune ca hosturile din reteaua locala si serverul sunt conectate intr-un switch, iar intre retele nu este nevoie sa se faca NAT.