Facultatea de Electronica, Telecomunicatii şi Tehnologia Informatiei

UNIVERSITATEA POLITEHNICA BUCURESTI

Securitate pe INTERNET

RCI
Masterand **Ing. Badea Mihai Bogdan**
SIVA Anul 2

Cuprins

1. Nivele de securitate

1.1. Securitatea la nivel de retea Layer 3

1.2. Protocolul Ipsec

1.3. Securitatea e-mailului (postei electronice)

2. Software malitios si antivirus

2.1. Malware

2.2. Antivirus

3. Firewall-uri

3.1. Rolurile firewall-urilor pentru securitatea web

3.2. Tipuri de firewall-uri

4. Atacuri prin respingerea serviciului

5. Atacuri cu overflow de buffer

6. Referinte

1. Nivele de securitate

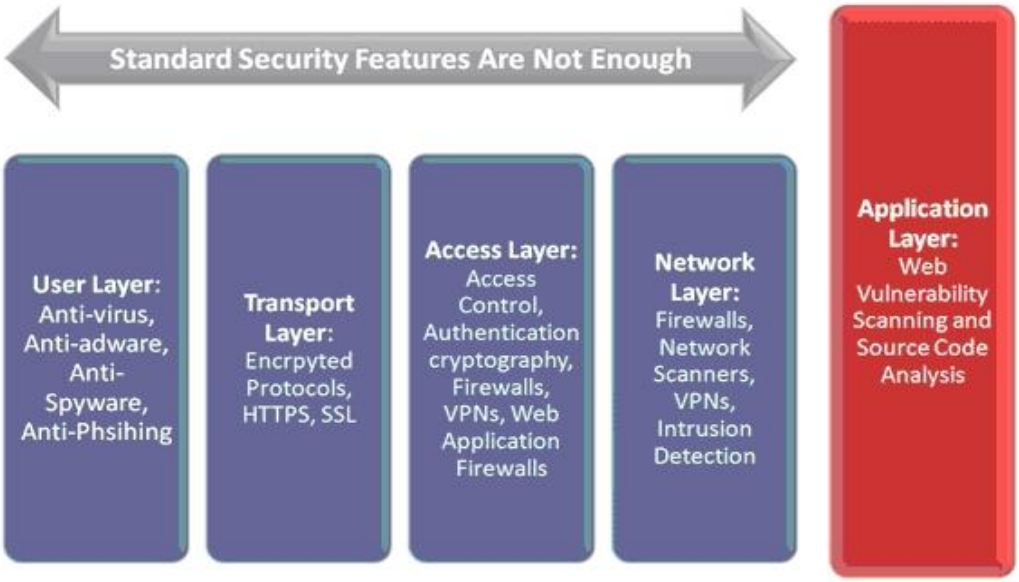

Figura 1. Nivelele de securitate in internet

Securitatea in Internet poate fi descompusa pe mai multe nivele, acestea fiind prezentate in figura 1.

In continuare voi prezenta securitatea la nivel de retea Layer 3 in TCP/IP.

1.1. Securitatea la nivel de reţea - Layer 3

Securitatea la nivelul retelei - nivelul 3 este asigurata de IPSec, care este un protocol de comunicatii utilizat la securizarea pachetelor Internet Protocol (IP) prin autentificarea si criptarea fiecarui pachet IP al unei sesiuni de comunicatii. El este un ansamblu de protocoale care includ protocoale pentru stabilirea autentificarii intre agenti la inceputul sesiunii si negocierea cheilor criptografice utilizate in desfasurarea sesiunii. Acest protocol poate fi utilizat pentru protejarea informatiilor intre o pereche de gazde (host-to-host), intre o pereche de porti (retea-retea), sau intre o poarta si o gazda (network-to -host). IPSec reprezintă singura solutie open-source pentru securizarea conexiunilor pe Internet. IPSec poate fi configurat pentru două moduri distincte: modul **tunel** şi modul **transport**.

În modul **tunel**, IPSec impacheteaza pachetele IPv4 in cadre IP securizate, care ajuta la transferul privat al informației.

In modul **transport**, informația este impachetata altfel încât poate fi securizată intre punctele terminale ale conexiunii, deci pachetul nu ascunde informatia de rutare end to end. Modul tunel este cea mai sigură metodă de securizare, însă creşte gradul de încărcare a sesiunii de comunicație, prin mărirea dimensiunilor pachetelor.

Functionarea Internet Protocol Security

Arhitectura IPSec presupune:

- IPSec driver or core engine - este nucleul protocolului ajutand la realizarea criptarii, autentificarii, decriptarii şi la verificarea semnaturii; de asemenea este ajuta la coordonarea efortului celorlalte componente IPSec pentru a asigura o buna indeplinire a sarcinilor.
- IPSec Policy Agent - este functia protocolului care examinează setarile IPSec ale ansamblului precizand ce trafic ar trebui protejat; nu protejeajă datele ci doar avertizeată ca un anumit trafic ar trebui protejat.
- Internet Security Association Key Management Protocol - este managerul setarilor care asigura securitatea Internetului; ISAKMP stabileste grupul de setări folosite pentru criptare şi autentificare atunci cand doua statii vor sa

transfere informatii.

- Internet Key Exchange - datorita faptului ca IPSec-ul foloseşte chei secrete, trebuie să fie prezent un mecanism care să asigure conexiunea echipamentelor si sa stabileasca existenta unei chei; aceasta cheie depinde de setarile date de ISAKMP.

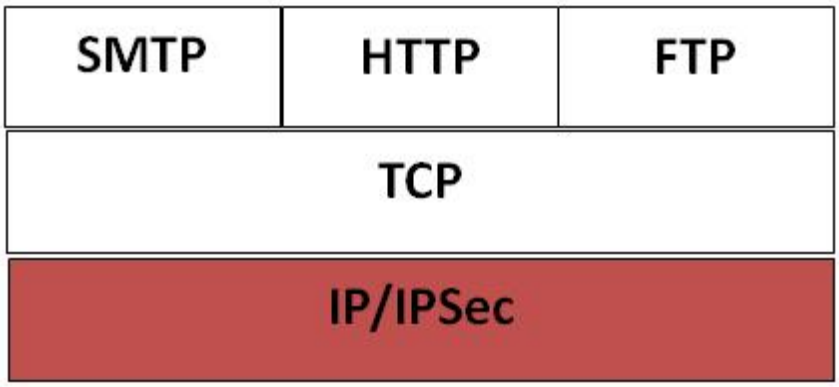

Figura 2. IPSec

Asigurarea securitatii retelei (denumita criptare la nivel de retea) este un procedeu de securitate pe retea care include servicii criptografice la nivelul de transport al retelei – peste nivelul de legatura, dar sub nivelul de aplicatie. Nivelele de transfer in retea sunt layerele 3 si 4 ale modelului de referinta OSI (Open Systems Interconnection), nivelele fiind responsabile pentru conexiune si rutare intre 2 puncte. Utilizand serviciile existente de retea si aplicatie software, criptarea la nivel de retea este transparenta utilizatorului final si functioneaza independent de orice alt proces de criptare utilizat. Datele sunt criptate doar in tranzit, ele fiind in plain-text la cele 2 capete.

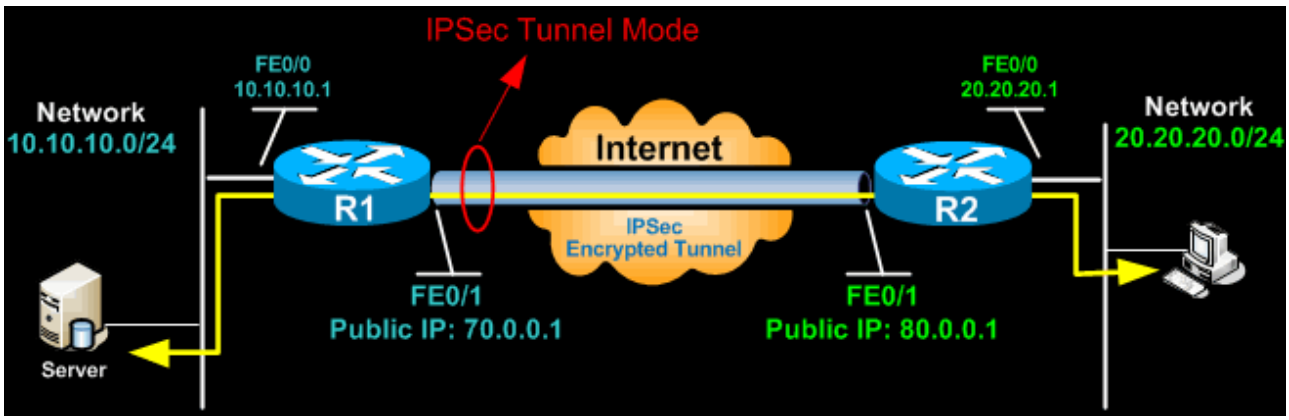

Figura 3 Tunelul securizat IPSec.

IPSec reprezinta criptarea la nivel de retea care este implementata printr-un ansamblu de standarde IETF (Internet Engineering Task Force) care creaza o platforma pentru comunicatia securizata intre retele IP. Pachetele criptate apar identice celor necriptate si sunt rutate usor prin orice retea IP. IPSec functioneaza cu ajutorul arhitecturi retelei, ceea ce inseamna ca utilizatorul final si aplicatiile nu trebuiesc modificate in niciun fel.

1.2. Protocolul Ipsec

Protocolul Ipsec este un ansamblu de securitate end-to-end la nivelul Internet al stivei de protocoale Internet, in timp ce alte sisteme de securitate Internet utilizate majoritar, ca Secure Sockets Layer (SSL), Transport Layer Security (TLS) si Secure Shell (SSH), functioneaza in nivelele superioare ale stivei TCP/IP. In consecinta, IPSec protejeaza orice trafic de aplicatie pe o retea IP. Aplicatiile nu trebuiesc implementate special pentru a utiliza IPSec. Fara IPSec, utilizarea TLS/SSL trebuie implementata in aplicatie pentru a proteja protocoalele de aplicatie.

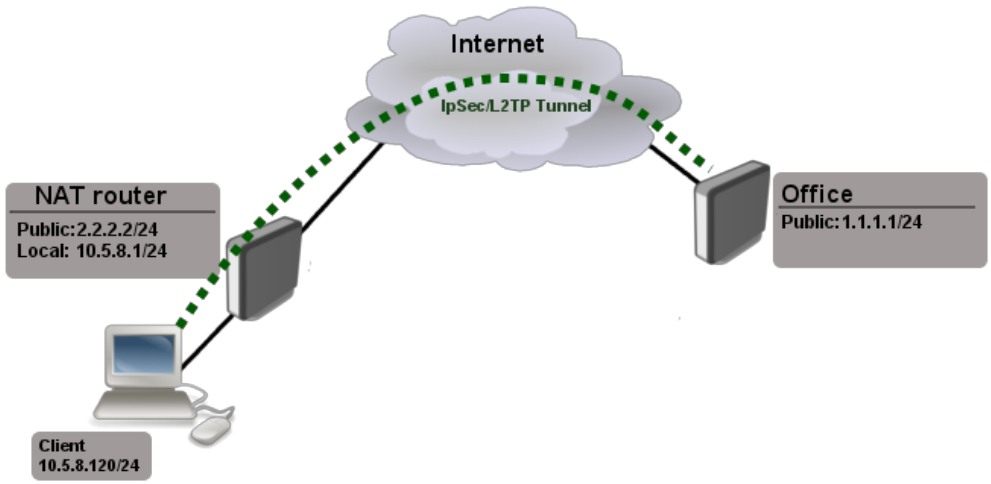

Figura 4. IPSec.

1.3. Securitatea e-mailului (postei electronice)

Emailul este vulnerabil la atacurile pasive si active. Amenintarile pasive includ Release of message contents, si analiza traficului in timp ce amenintarile active includ Modification of message contents, Masquerade, Replay, si atacul de respingere a serviciului. Defapt, toate amenintarile mentionate sunt aplicabile protocoalelor traditionale de email.

Protejarea emailului de catre un acces neautorizat si analizarea lui este cunoscuta ca securitate electronica.

Figura 5. Email security.

Brese de securitate:

- **Dezvaluirea informatiei:** Majoritatea email-urilor sunt transmise in clar (necriptate). Utilizand unelte adecvate, persoane altele decat cele destinate pot citi continutul emailului.
- **Analiza traficului:** Se crede ca unele tari monitorizeaza constant email-urile ca metoda de supraveghere. Aceasta este nu doar pentru anti-terorism ci si pentru a combate spionajul industrial.
- **Modificarea mesajului:** Continutul emailului poate fi modificat in timpul transportului sau stocarii. Aici, atacul man-in-the-middle nu necesita in mod necesar controlul retelei deoarece atacatorul care poate fi in aceeasi retea

locala, poate utiliza o unealta de ascultare ARP pentru a intercepta si modifica toate pachetele email care vin din si inspre serverul de mail.

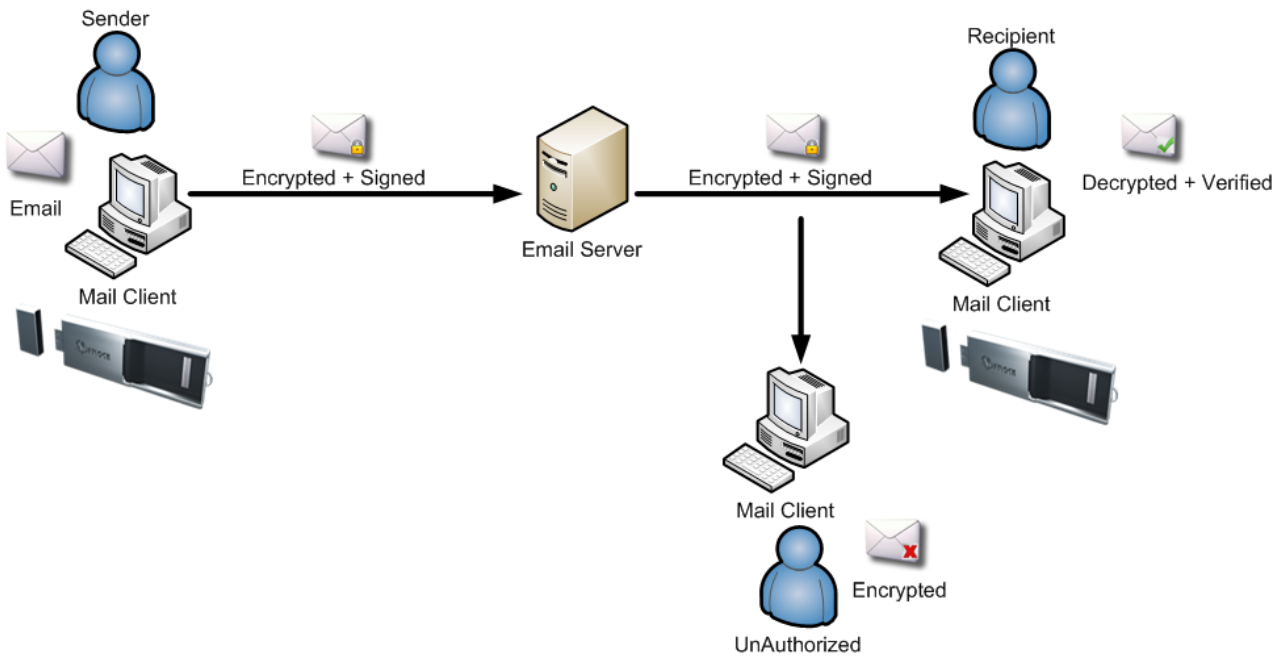

Figura 6. Securitatea email-ului

2. Software maliţios şi antivirus

Malware-ul sau software-ul malitios, este un soft utilizat la intreruperea operatiilor unui computer care colecteaza informatii sau capata acces la sisteme private de calculatoare. El poate aparea sub forma de cod, script, continut activ sau alte tipuri de software. 'Malware' este un termen general utilizat la o varietate de forme ostile sau software ostil.

Malware include virusi de computer, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware sau alte programe malitioase; majoritate malware-urilor active sunt mai mult worms sau troiani decat virusi.

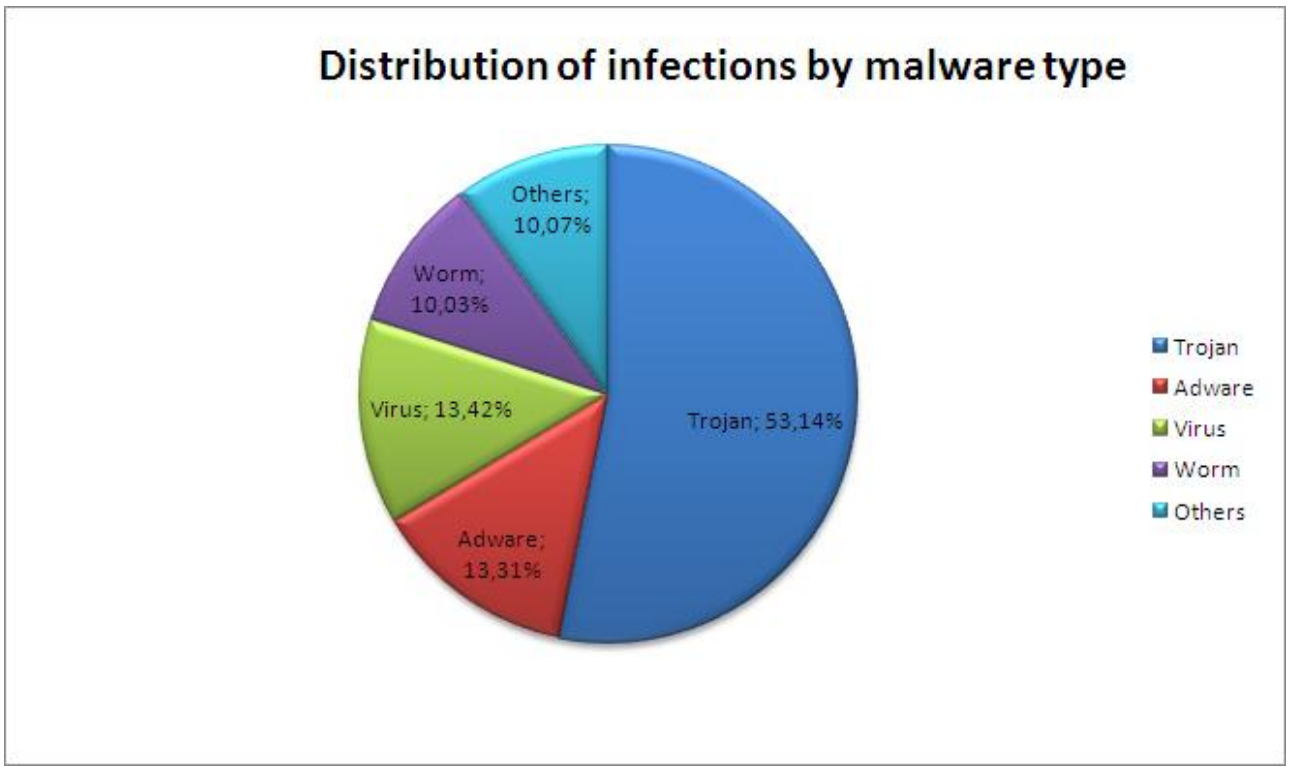

Figura 9. Distributia malware-ului specific in procente.

2.2. Antivirus

Antivirusul este un program de computer utilizat la blocarea, detectia si eliminarea programelor malitioase. Majoritatea soft-urilor impotriva altor tipuri de malware, cum ar fi Browser Helper Objects, browser hijackers, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, adware and spyware. Securitatea computerelor, incluzand tehnicilor protectiei ingineriei sociale este furnizata in mod comun in serviciile companiilor de antivirusi.

Detectia pe baza de semnatura este una dintre strategiile folosite, si implica cautarea tiparelor cunoscute de informatii in codul executabil. Desi este posibil pentru un computer a fi infectat cu un malware nou pentru care nu este cunoscuta nicio semnatura; malware-ul este adesea modificat in a-si schimba semnatura fara a afecta functionalitatea. Pentru a preveni aceste amenintari sunt utilizati algoritmi heuristici.

Figura 10. Principalii furnizori de solutii anti-virus.

3. Firewall-uri

Un firewall este un program de computer sau un dispozitiv hardware care filtreaza informatia care vine din Internet intr-o retea privata sau sistem de computere. Daca un pachet corespunde filtrelor, acesta este respins.

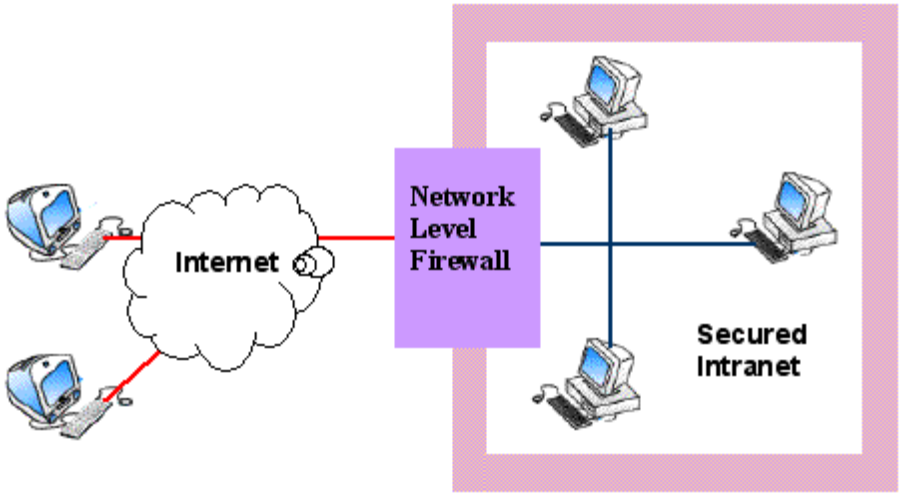

Figura 7. Exemplu de firewall pentru o retea locala

Firewall-ul este un ansamblu care separa o retea externa (internetul) de catre o retea interna (locala), ea putand fi reprezentata de catre un Local Area Network al unei cladiri de birouri sau de calculatoarele unei familii. Cel mai simplu firewall permite celor din reteaua locala sa acceseze pe cea externa (Internetul), dar opreste traficul astfel incat niciun ultilizator din reteaua externa sa nu poata accesa reteaua locala.

3.1. Rolul firewall-urilor pentru securitatea web

Firewall-urile au rolul de a bloca accesul neautorizat la fisierele sau sistemele confidentiale.

3.2. Tipuri de firewall-uri

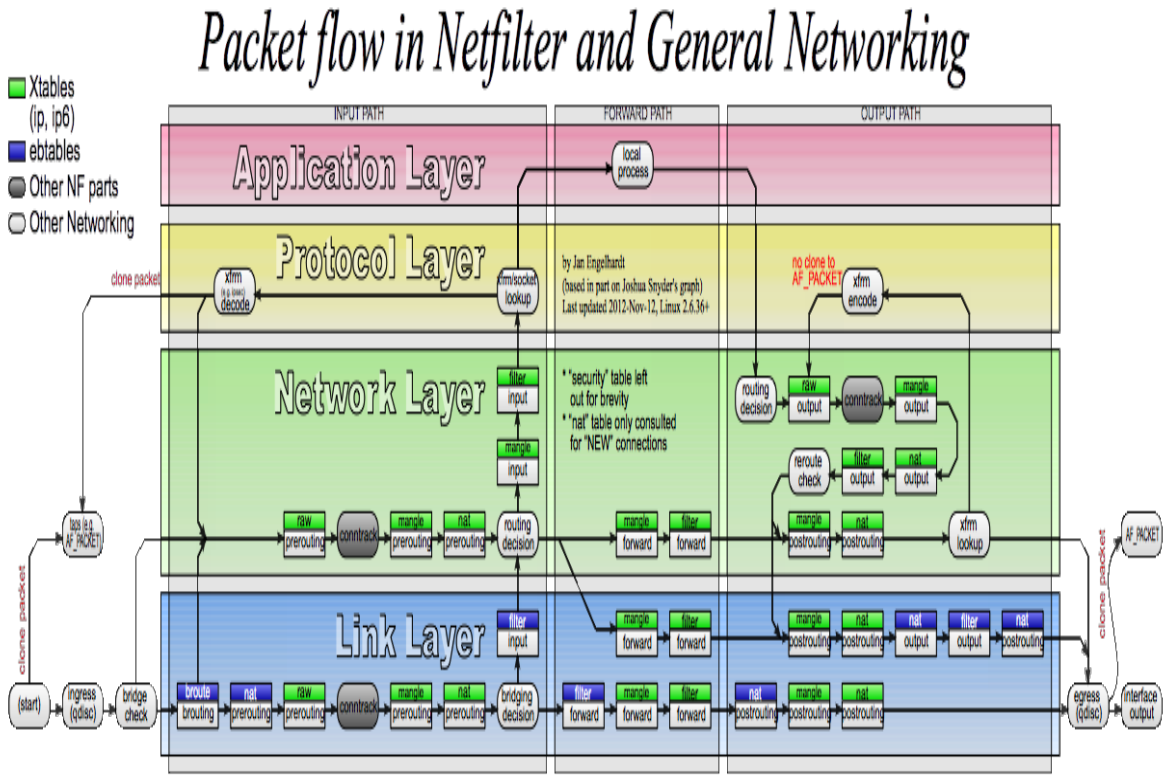

Figura 8. Filtrarea pachetelor.

Nivele de filtrare la firewall:

- Stratul 2 (MAC) şi 3 (diagrama informatii): filtrare de pachete (packet filtering).
- Stratul 4 (transport): tot filtrare de pachete, dar se poate diferentia intre protocoalele de transport si există optiunea unui firewall cu mentinere de stare, in care sistemul stie in orice moment care sunt principalele

caracteristici ale urmatorului pachet asteptat, evitand astfel o intreaga clasa de atacuri.

- Stratul 5 (aplicaţie): firewallul la nivel de aplicatie. In general se comporta ca un server proxy pentru diferite protocoale, analizand si luand decizii pe baza cunostintelor despre aplicatii si a continutului conexiunilor. De exemplu, un server SMTP cu antivirus poate fi considerat drept un firewall la nivel de aplicatie pentru e-mail.

4. Atacuri prin respingerea serviciului

Un atac distribuit prin respingerea serviciului (DDoS) sau Distributed Denial of Service reprezinta particularitatea in care o grupare de sisteme compromise ataca o singura tinta, astfel cauzand blocarea serviciului pentru utilizatorii sistemului atacat. Multimea mesajelor catre sistemul tinta forteaza oprirea acestuia, astfel respingand serviciul pentru utilizatorii legitimi.

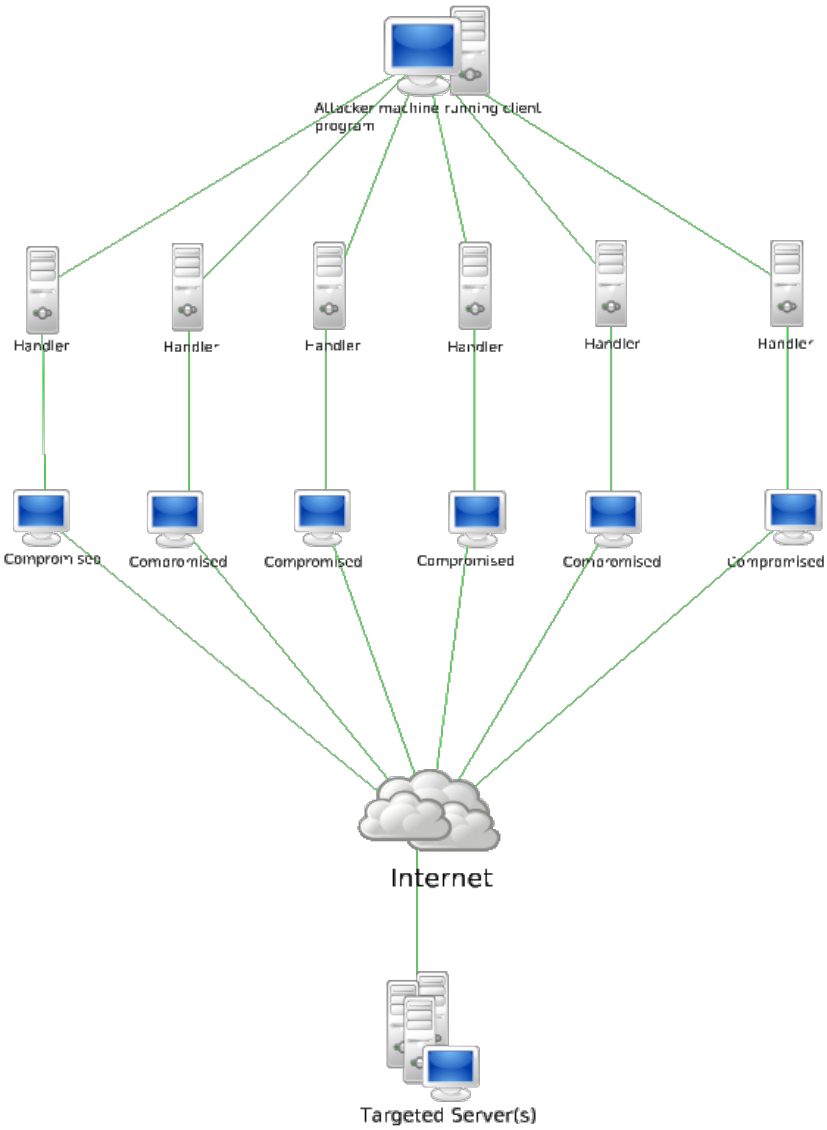

Figura 11.Schema unui atac DDOS

5. Atacuri cu overflow de buffer

In domeniul securitatii computerelor si a programarii software, un buffer overflow este o anomalie in care un program, in timpul scrierii datelor catre un buffer, depaseste limita acestuia si suprascrie memoria adiacenta.

Buffer overflows pot fi incepute de intrari care sunt desemnate de a executa cod, sau modifica modul in care acel program executa. Acesta poate rezulta intr-un comportament haotic al programului.

Verificarea limitelor poate preveni buffer overflows.

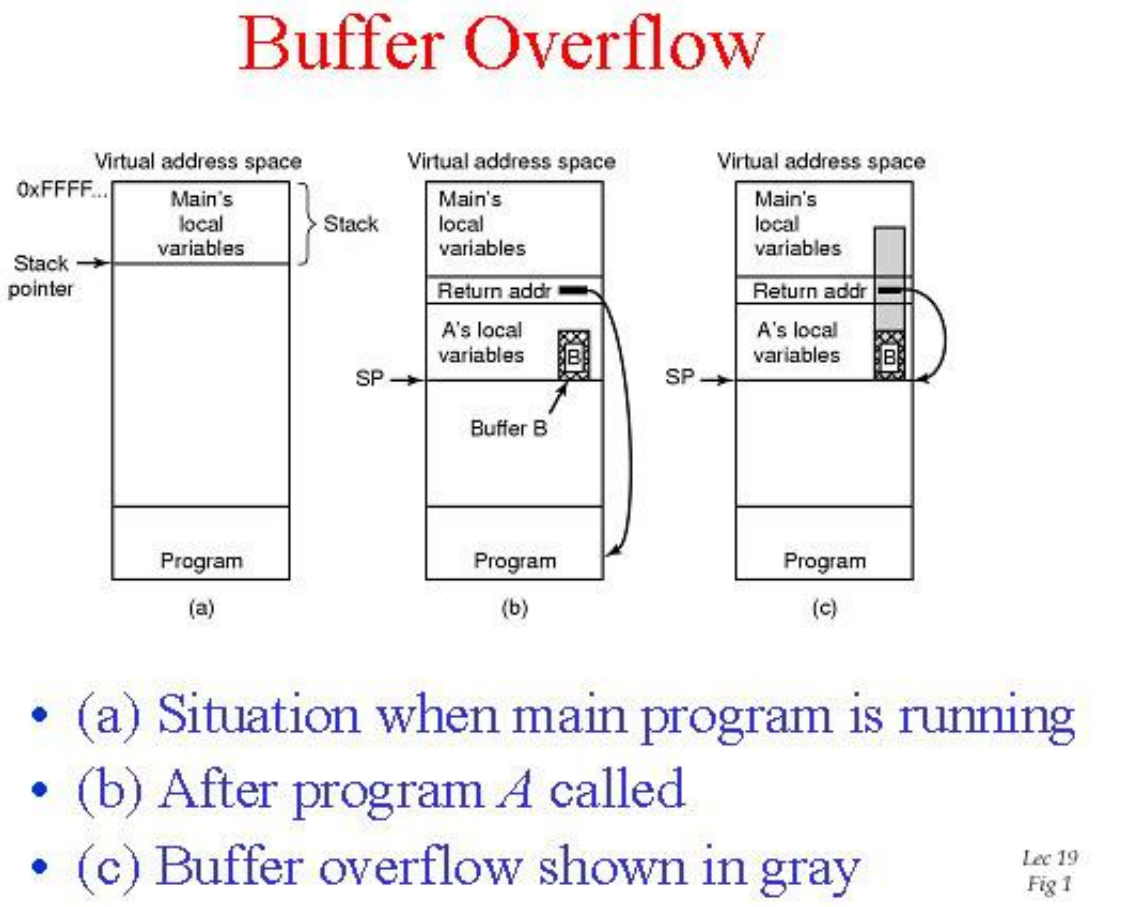

Figura 12. Buffer Overflow

6. Referinte

1. Securitate multi-nivel http://en.wikipedia.org/wiki/Multilevel_security

2. Securitate la nivel de retea
http://technet.microsoft.com/en-us/library/cc261825(v=office.12).aspx
http://searchmidmarketsecurity.techtarget.com/definition/IPsec

3. Securitatea pentru email
http://www.zdnet.com/10-security-best-practice-guidelines-for-businesses-7000012088/

4. Firewall http://www.webopedia.com/TERM/F/firewall.html

5. Malware
https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work

6. Tanenbaum – Computer networks