Tema3 Securitatea Informatiei
Atac SYN Flooding

Constantinescu George-Gabriel 3E3

31 Decembrie 2021

1 Detalii asupra mediului de lucru Detalii introductive

In cadrul mediului de lucru am 3 masini virtuale ce au instalate versiunea de Ubuntu 32-bit(sursa 1 bibliografie): Un Router si doi clienti, C1 si C2, care primesc conexiune la internet de la Router.

Resursele pentru masinile virtuale:

- Memorie RAM: 768 MB.
- 1 Procesor logic capabil de putere maxima de 4.5 GHz.
- Memorie interna de 8GB.

Configurarea mediului de lucru a fost cea sugerata in fisierul "$config\_retea.pdf$" oferit de catre profesorul de laborator.

Router-ul are acces la internet utilizand conexiunea masinii host si o alimenteaza o retea locala. Cei doi clienti, C1 si C2 au acces la internet prin intermediul Router-ului; astfel, daca Router-ul este oprit, C1 si C2 nu vor avea o conexiune disponibila(acces la internet).

1.1 TCP 3-way handshake

Pentru a exista o conexiune TCP, trebuie realizat un schimb de raspunsuri intre un client si server. Pasii "*intelegerii*"(handshake-ului) sunt urmatorii:

- Clientul trimite catre server un (pachet) SYN Request.
- Serverul primeste raspunsul si ii trimite inapoi un (pachet) SYN-ACK si asteapta un feedback de la client pentru a realiza o conexiune.
- Clientul trimite inapoi la server un (pachet) SYN-ACK si astfel se realizeaza conexiunea. (biblio:sursa2)

2 Atacul SYN Flooding

2.1 Istorie

Atacul a fost descoperit in anul 1994 de catre Bill Cheswick si Steve Bellovin. Ulterior au scris un capitol despre acest tip de atac in cartea "$FirewallsandInternetSecurity$: $RepellingtheWilyHacker$", ulterior nefiind introdus in carte pentru masuri de securitate.(biblio:sursa3)

Incepand cu anul 1996 au inceput sa se manifeste acesti tipuri de atac asupra serverelor de mail.(biblo:sursa4)

2.2 Principiul atacului

Atacul se bazeaza pe supraincarcarea serverului cu cerere de tipul SYN. Astfel, serverul ramane cu foarte multe "half-way connections"(nu mai primesti acel pachet de tipul ACK pentru a stabili conexiunea in cadrul TCP 3-Way Handshake) si rezulta un consum foarte mare de resurse. Ulterior, datorita overloading-ului, serverul nu mai poate raspunde la cereri valide si astfel clientii nu mai au acces la serviciul oferit de server, rezultand bine cunoscutul fenomen de DoS(Denial-of-Service).

3 Metode de protectie impotriva SYN Flooding

3.1 Marirea cozii de cereri ale serverului

- O solutie foarte simpla.
- Din nefericire, duce la efecte negative din cauza implementarii ce foloseste structuri de date ineficiente care au in background backlog-uri de dimensiuni relativ mari.

3.2 Overwrite-ul celor mai vechi conexiuni din coada cu cele noi

- Ideea pe care se bazeaza aceasta preventie ia in calcul ca toate conexiunile valide(generate de utilizatori normali si nu de atacatori) se stabilesc intr-un timp destul de mic relativ la timpul de umplere al cozii de cereri ale serverului.
- Lafel ca la metoda de mai sus, este o metoda neeficienta in cazul in care backlog-ul serverului are un numar relativ mic de cereri de request sau rata de pachete a atacatorului este foarte mare.

3.3 Utilizarea de SYN-Cookies

- Se evita utilizarea clasica, nu se mai creeaza o conexiune in coada la primirea unui pachet de tipul SYN.

- Starea este codificata in SYN-ACK si impreuna cu ACK se realizeaza o noua conexiune stabila.
- Aceasta metoda de preventie este incompatibila cu unele optiuni TCP(biblio:sursa5)

3.4 Reducerea timpului de asteptare al pachetului SYN-RECEIVED

- Conexiunie half-way, care asteapta raspunsul ACK sunt eliminate mai rapid din coada si nu mai sunt folosite resursele sistemului.
- Din nefericire, conexiunile valide care se realizeaza intr-un timp mai lung vor fi eliminate datorita timpul mic de asteptare.
- Metoda este una ineficienta deoarece atacatorul poate trimite cererile mai repede si astfel coada serverului va fi incarcata din nou cu cereri de asteptare.

3.5 Atac similar: UDP Flood Atack

Este similar cu TCP ca functionare. Diferenta consta in faptul ca in acest caz victima isi epuizeaza resursele cand incearca sa raspunda la toate cererile atacatorului datorita arhitecturii din spate a UDP-ului. La TCP resursele sunt consumate asteptand raspunsurile la conexiunile generate.(biblio:sursa6)

4 Rezultatele obtinute in urma experimentului

In realizarea experimentului au fost parcursi pasii din sursa7 din bibliografie.

A fost folosit tool-ul **hping**, o unealta realizata pentru testarea securitatii din libraria/pachetul TCP Penetration Testing Tool.

Exemplu comanda: **hping3 -c 30000 -d 120 -S -w 64 p 80 –flood –randsource <target-ip>**

- -c 30000 reprezinta numarul total de pachete generate
- -d 120 reprezinta dimensiunea pachetelor generate
- -S activeaza SYN-flag
- -w 64 reprezinta dimensiunea unei secvente TCP
- -p 80 reprezinta portul tinta al atacului
- - -flood are rolul de a trimite pachetele la intervale mici de timp
- - -randsource are rolul de a genera adrese random false pentru conexiuni

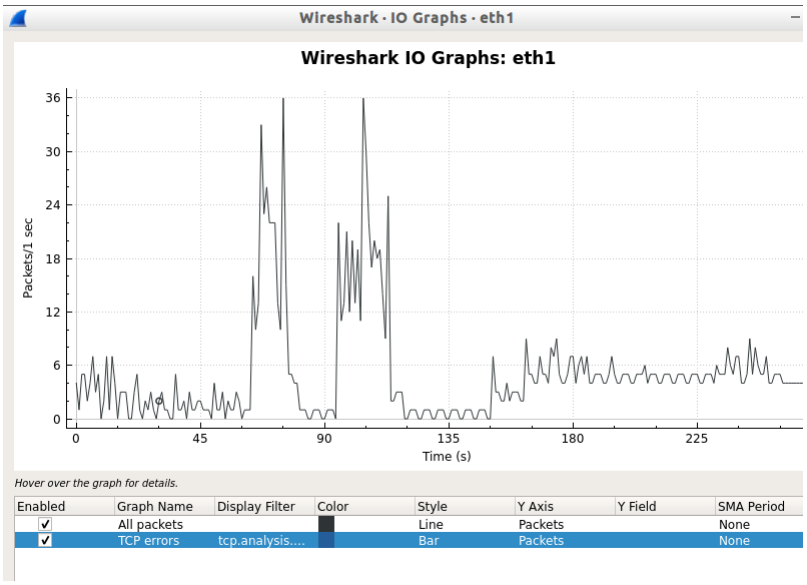

Figure 1: IO Graph generat de wireshark cu 2 ping-uri catre google.com din fiecare client, C1 si C2

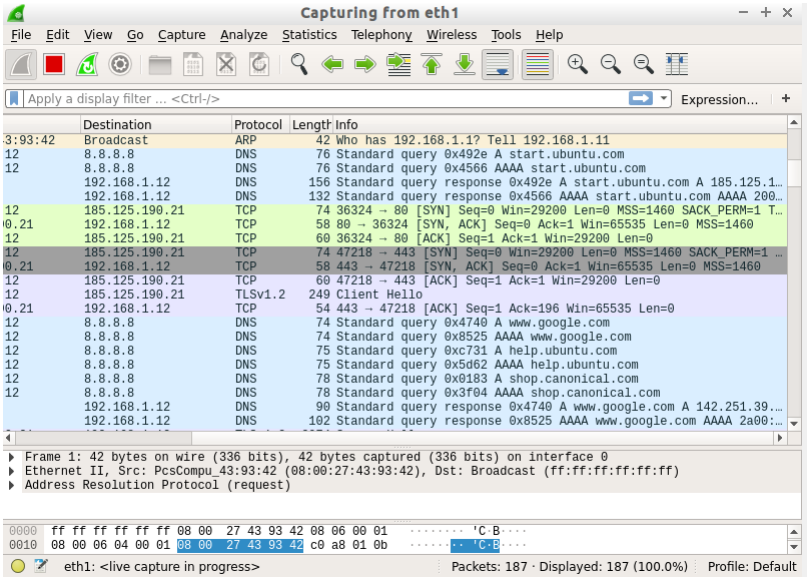

Figure 2: Se poate observa un numar mic de pachete TCP in acest caz, intr-o functionare obisnuita a retelei

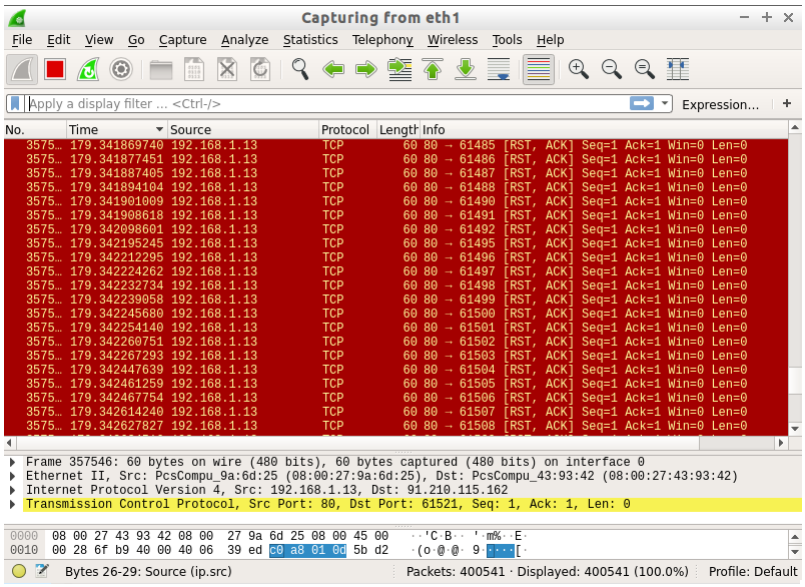

Figure 3: Aici este activitatea generate de wireshark asupra retelei in timpul atacului

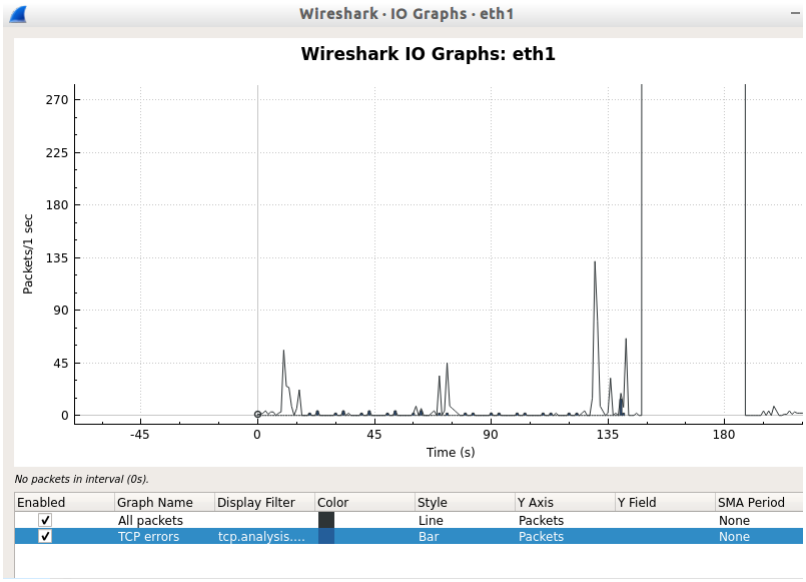

Figure 4: IO Graph attempt1 generat de wireshark in timpul atacului si dupa

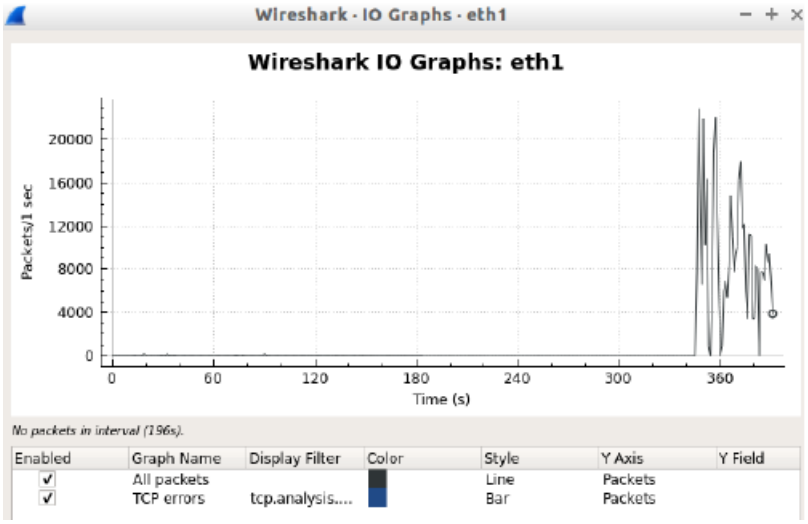

Figure 5: IO Graph attempt2 generat de wireshark in timpul atacului si dupa

4.1 Scenariul atacului

C1 este **atacator** iar C2 este **victima**. Router-ul are rol de **observator** asupra actiunilor prin intermediul aplicatiei wireshark.

Se poate vedea numarul mare de raspunsuri pe care C2 (192.168.1.13) incearca sa le trimita catre router.

Se poate observa ca in timpul atacului, cand C2 este supraincarcat, are performanta scazuta si nu poate utiliza browser-ul (Ramane in connecting si nu reuseste sa acceseze internetul deoarece nu are acces la o conexiune TCP valida si resurse de sistem).

In timpul atacului, puterea de procesare a CPU-ului a fost dusa la 100%. Se mai observa ca atacatorul foloseste mai multe resurse dar apar schimbari minore la victima.

5 Concluzie

Se poate deduce ca acest tip de atac este utilizat impotriva unor servere si nu unor basic users.

Cea mai importanta consecinta este reprezentata de imposibilitatea victimei de a accesa o internetul. In cazul serverelor, efectul se va raspandii la toti clientii conectati la acel server. Daca luam cazul nostru, daca vom ataca(dintr-o sursa externa) router-ul atunci nici C1 si nici C2 nu vor avea acces la internet.

Am pregatit si un video in care se vede o incetinire a masinii atacate.(biblio:sursa8)

6 Bibliografie

1) https://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224-performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html

2) https://www.guru99.com/tcp-3-way-handshake.html

3) https://datatracker.ietf.org/doc/html/rfc4987

4) https://dl.acm.org/doi/book/10.5555/862335

5) https://datatracker.ietf.org/doc/html/rfc4987#ref-cr.yp.to

6) https://en.wikipedia.org/wiki/UDP_flood_attack

7) https://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224-performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html

8) https://www.youtube.com/watch?v=wC31DSAI298