Universitatea Tehnică a Moldovei

Protecție împotriva atacurilor DDoS

DDoS attack protection

Masterand: **Cucu Dumitru**

Conducător: **Bolun Ion**
prof.univ., dr.hab.

Chișinău, 2020

MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere, Șef departament:

conf. univ., dr. Ion FIODOROV

_____

"__" _____ 2020

PROTECȚIE ÎMPOTRIVA ATACURILOR DDoS

Teza de master în Securitate informațională

Masterand: **Cucu Dumitru**

Conducător: **Bolun Ion**
prof. univ., dr. hab.

Chișinău, 2020

REZUMAT

la teza de master ”**Protecție împotriva atacurilor DDoS**” a masterandului gr. SI-191m,

specialitatea „**Securitatea informațională**”,

CUCU Dumitru

Obiectivul cercetării sunt metodele atacurilor DDoS din exterior care vizează refuzul de serviciu a serverului separat, dar și rețeaua de calculatoare în ansamblu.

Scopul lucrării constă în dezvoltarea unui instrument software inteligent de protecție împotriva atacurilor DDoS. Datorită popularității și vulnerabilității traficului HTTP, protecția ar trebui construită împotriva atacurilor de tip «HTTP-flood».

După analizarea soluțiilor existente pentru protecția împotriva atacurilor DDoS la nivel de software, s-a decis dezvoltarea unui sistem care să clasifice cererile HTTP, separând utilizatorii legitimi de calculatoarele care atacă.

Ca rezultat a fost obținut un sistem configurat astfel ca să fie capabil să protejeze rețeaua de atacuri DDoS de orice magnitudine. Acesta este sistemul Snort, care după o configurare corespunzătoare și stabilirea regulilor necesare și-a îndeplinit sarcina. Costul implementării și întreținerii ulterioare a acestui complex este de zece ori mai mic decât analogii cunoscuți.

Principalele caracteristici ale sistemului dezvoltat:

- cod sursă deschis;
- integrare ușoară la orice platformă;
- inteligența sistemului, datorită analizei anomaliilor de rețea;
- cost de operare redus.

Această dezvoltare este recomandată pentru implementare de către organizații a căror activitate depinde de activitatea serverului web al companiei.

ANNOTATION

to the graduate work **"DDoS attack protection**" of the student of the SI-191m group,

specialty „**Information security**",

CUCU Dumitru

The object of research is the methods of external DDoS attacks that target the denial of service of the separate server, but also the computer network as a whole.

The aim of the paper is to develop an intelligent software tool protection against DDoS attacks. Due to the popularity and vulnerability of HTTP traffic, protection should be built against "HTTP-flood" attacks.

After analyzing the existing solutions to protect against DDoS attacks at the software level, it was decided to develop a system to classify HTTP requests, separating legitimate users from attacking computers.

As a result, it was obtain a system configured to be able to protect the network from DDoS attacks of any magnitude. This system is Snort, which after a proper configuration and setting the appropriate rules has fulfilled its task. The cost of implementation and subsequent maintenance of this complex is ten times lower than foreign analogues.

The main features of the developed system:

- open source code;
- easy integration into any platform;
- system intelligence, due to the analysis of network anomalies;
- low operating cost.

This development is recommended for implementation by organizations whose activity depends on the activity of the company's web server.

CUPRINS

INTRODUCERE

Astăzi este imposibil să ne imaginăm o companie de succes care nu folosește cele mai bune realizări ale științei și tehnologiei în domeniul tehnologiei informației pentru organizarea lucrărilor de birou. Unul dintre domeniile cu cea mai mare prioritate este dezvoltarea infrastructurii cu cheie publică, gestionarea documentelor electronice și semnăturile electronice, corespondența și negocierea prin intermediul tehnologiilor informaționale, utilizarea instrumentelor criptografice de către organismele guvernamentale, companiile mari, instituțiile financiare, întreprinderile etc. Principalele avantaje ale acestor tehnologii sunt accelerarea și micșorarea procesului de lucru la birou, capacitatea de a fi mereu și pretutindeni disponibili pentru comunicare, nu este nevoie de un loc de muncă permanent, deoarece conexiunea și informațiile transmise sunt protejate prin intermediul criptografiei.

Integritatea și fiabilitatea informațiilor primite pot fi garantate printr-o semnătură digitală. Cu toate acestea, toate tehnologiile de mai sus nu garantează disponibilitatea serviciului necesar. Pentru funcționarea cu succes a infrastructurii companiei și a oricărei alte, este necesar să se asigure accesul neîntrerupt la sisteme. În caz contrar, nu are rost să se bazeze pe sistem dacă nu există nicio garanție că acesta va fi disponibil la momentul necesar.

După cum este cunoscut, o întreagă clasă de atacuri care vizează refuzul de serviciu (atacuri Dos și DDoS) s-a dezvoltat din ce în ce mai recent.

Implementarea unor astfel de atacuri de către intruși poate duce la un eșec complet al disponibilității sistemelor companiei, ceea ce duce la pierderi financiare mari, erori de sistem. De regulă, pentru un atac asupra unui server modern puternic, un atac de la o singură mașină nu poate duce la un eșec, iar un astfel de atac, dacă este semnificativ, este ușor de detectat și blocat de server însuși sau de administrator. Pentru atacurile HTTP de astăzi, criminalii cibernetici folosesc de obicei mașinile utilizatorilor pașnici, infectându-i cu software rău intenționat (viruși, viermi, troieni). După infectarea unui număr mare de mașini pașnice, computerul atacant emite o comandă către aceste mașini pentru a începe un atac simultan asupra unei resurse. Acesta este modul în care un atac distribuit de mașini pașnice este implementat pe servere moderne, în timp ce le dezactivează.

Un astfel de atac este foarte greu de detectat. De regulă, serverul în sine nu este capabil să separe o cerere bună de una rea și, având în vedere fluxul uriaș de astfel de cereri, administratorul nu reușește să facă acest lucru. Astfel, este posibil să mențineți serviciul indisponibil pentru o perioadă destul de lungă de timp. Pentru majoritatea companiilor, o

resursă de rețea joacă un rol cheie în afaceri, ceea ce permite concurenților necurați să folosească serviciile hackerilor implicați în atacuri DDoS.

Având în vedere faptul că atacatorul inițiază un atac, controlând de la distanță un număr mare de computere pașnice și, de asemenea, faptul că spoofingul este adesea folosit pentru adresele de rețea (Proxy), uneori este foarte dificil de identificat. În majoritatea țărilor, legislația în legătură cu industria informației este imperfectă, ceea ce nu permite pedepsirea strictă a atacatorului.

În prezent, unele companii de informatică au dezvoltat o serie de soluții care pot acoperi riscurile de eșec al serviciilor cauzate de atacurile DDoS. Astfel de instrumente au dezavantajele și limitările lor. De exemplu, toate produsele prezentate au codul sursă închis, ceea ce nu permite certificarea. De asemenea, datorită complexității, costului dezvoltării, implementării și întreținerii unor astfel de sisteme, multe companii nu și le pot permite.

Dezvoltarea și profitabilitatea atacurilor DDoS, costul ridicat, complexitatea în implementare și disponibilitatea mijloacelor de protecție duce la concluzia că piața necesită ieftin, simplu și soluții eficiente simultan pentru protecție. Teza propune un concept pentru implementarea unei astfel de protecții prin detectarea timpurie a celui mai comun atac TCP SYN. Baza acestui concept este un model matematic care reglementează comunicațiile server-client și ia în considerare configurația serverelor și a infrastructurii de rețea a companiei, ceea ce crește semnificativ eficiența sa în identificarea solicitărilor greșite. Diploma propune, de asemenea, o implementare software a conceptului de mai sus, dezvoltat pe baza instrumentului de detectare a atacurilor Snort Inline.

CONCLUZII GENERALE ȘI RECOMANDĂRI

În stadiul actual de dezvoltare a tehnologiilor moderne, dependența de activitatea productivă a instituțiilor și organizațiilor guvernamentale și private de securitatea și fiabilitatea rețelelor de informații se manifestă cel mai mult. Printre condițiile principale impuse sistemelor prezentate, se poate pune separat importanța asigurării accesului clienților. Probleme cu accesul la informații este extrem de grav în rețea, din cauza atacurilor moderne pe scară largă și în caz de success poate opri complet funcționarea mai multor servere, precum și a rețelelor cee ace poate duce la probleme foarte grave.

Există mai multe soluții pentru protejare împotriva atacurilor DDoS, dar care sunt foarte costisitoare și nu orice companie își poate permite un astfel de produs.

În urma cercetării funcționării sistemului Snort, s-a ajuns la concluzia ca este un instrument care cu o configurare corespunzătoare, poate deveni un instrument foarte puternic care este capabil nu doar sa blocheze un atac DDoS, dar poate sa identifice și să prevină oricare alt atac din rețea. Este un produs foarte flexibil cu un cod open source ce prezintă un foarte mare avantaj.

În lucrare sunt efectuate configurările necesare ale Snort pentru contracararea atacurilor DDoS și au fost efectuate testările corespunzătoare. Rezultatele testărilor au confirmat eficacitatea protecției accesului la rețea contra atacurilor DDoS, folosind configurația efectuată a Snort. Soluția obținută este de circa zece ori mai puțin costisitoare comparativ cu soluțiile cunoscute folosind instrumente comerciale.

BIBLIOGRAFIE

1. Wikipedia, enciclopedie liberă. DoS [accesat 07.09.2020]. Disponibil: https://ro.wikipedia.org/wiki/DoS
2. Bitesize © 2020 BBC. Type of Denial of Service attack [accesat 07:09:2020]. Disponibil: https://www.bbc.co.uk/bitesize/guides/z2c8wmn/revision/3
3. Computer World, The Voice of Business Technology © 2020. Top botnets control 1M hijacked computers [accesat 08.09.2020]. Disponibil: https://www.computerworld.com/article/2536378/top-botnets-control-1m-hijacked-computers.html
4. Cisco. БОРЬБА С АТАКАМИ DDoS [accesat 20.09.2020]. Disponibil: https://www.cisco.com/web/RU/products/ps5887/products_white_paper0900aecd8011e927_.html
5. Cisco DDoS protection. Service Provider Solutions. DDoS Protection Solution Enabling “Clean Pipes” Capabilities [accesat 20.09.2020]. Disponibil: https://www.cisco.com/cdc_content_elements/networking_solutions/service_provider/ddos_protection_sol/ddos_protection.pdf
6. NETSCOUT. Arbor Threat Mitigation System (TMS) [accesat 20.09.2020]. Disponibil: https://www.netscout.com/sites/default/files/2018-10/SECPDS_004_EN-1802-Arbor-Threat-Mitigation-System-%28TMS%29.pdf
7. Kaspersky. Karspersky DDoS protection [accesat: 20.09.2020]. Disponibil: https://www.kaspersky.com/small-to-medium-business-security/ddos-protection
8. E-biblio. Модели теории массового обслуживания [accesat: 05.10.2020]. Disponibil: http://www.e-biblio.ru/book/bib/01_informatika/Modelirovanie_system/158.1.10.html
9. Snort. Documents [accesat 10.10.2020]. Disponibil: https://www.snort.org/
10. Github. Barnyard2 [accesat 11.10.2020]. Disponibil: https://github.com/firnsy/barnyard2
11. Github. PulledPork [accesat 12.10.2020]. Disponibil: https://github.com/shirkdog/pulledpork
12. Github. BASE [accesat 13.10.2020]. Disponibil: https://github.com/NathanGibbs3/BASE
13. Wikipedia. pfSense [accesat: 14.10.2020]. Disponibil: https://ru.wikipedia.org/wiki/PfSense