MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice

Admis la susținere
Șef departament:
Sava Lilia, conf. univ., dr.

„____" _____ 2020

SOLUȚII HARDWARE ȘI SOFTWARE PENTRU PREVENIREA ATACURILOR ASUPRA REȚELELOR DE CALCULATOARE

Teză de master

Student: **Brunchi Ion, MMRT-191**

Conducător: **Nicolaev Pavel, conf. univ., dr.**

Chișinău, 2020

ADNOTARE

Teza de master, a studentului Brunchi Ion, cu tema “Soluții Hardware și Software pentru prevenirea atacurilor asupra rețelelor de calculatoare” este structurată în: introducere, 4 capitole având câte 4-6 paragrafe, concluzii și bibliografie. Teza este dedicată abordarării securității rețelelor informaționale, care are ca scop identificarea și alertarea timpurie a potențialelor amenințări, sau a atacurilor aflate în fazele inițiale, iar cu ajutorul soluțiilor propuse să fie stopate și protejate rețelele informaționale.

Cuvinte-cheie ale lucrării sunt: securitate, atac, software, date, filtrarea traficului, internet.

Scopul acestei lucrări este propunerea unor soluții care v-or sta la baza securizării rețelelor de calculatoare împotriva atacurilor nesancționate de către răufacători. Obiectivele generale sunt expuse în capitolele lucrării, și anume: primul capitol este dedicat obiectivului studierii importanței informației, clasificării metodelor de atac asupra tehnologielor informaționale. În următoarele capitole sunt propuse soluțiile (firewall, proxy server squid, criptarea datelor), ca metode de securizare a rețelelor. Principalele metode aplicate la elaborarea tezei de master sunt: cercetarea, simularea soluțiilor propuse pe calculator.

În lucrare sunt prezentate 29 de figuri, 5 tabele și 31 surse de bibliografie.

Rezultatul obținut în urma elaborării tezei de master este cunoașterea utilizării echipamentelor și aplicațiilor pentru securizarea rețelelor infomaționale, activări și configurări a firewall-ului, proxy server-ului squid, astfel încât se poate de monitorizat securitatea rețelei.

ANNOTATION

The master's thesis, of the student Brunchi Ion, with the topic "Hardware and Software solutions for preventing attacks on computer networks" is structured in: introduction, 4 chapters with 4-6 paragraphs, conclusions and bibliography. The thesis is dedicated to addressing the security of information networks, which aims to identify and alert both early and potential threats or of the attacks in the initial phases, and with the help of the proposed solutions to stop and protect the data networks.

The key words of the project are security, attack, software, data, traffic filtering, internet.

The purpose of this science work is to propose solutions that will be based on securing computer networks against unauthorized hacker attacks. The general objectives are set out in the chapters of the paper, namely: the first chapter is dedicated to the objective of studying the importance of information, the classification of attack methods on information technologies. In the following chapters proposes solutions (firewall, squid proxy server, data encryption), such as network security methods. The main methods applied to the elaboration of the master's thesis are: research, simulation of the proposed solutions on the computer.

The project presents 29 figures, 5 tables and 31 bibliographic sources.

The result obtained after the elaboration of the master’s thesis is the knowledge of the use of equipment and applications for security of data networks, activations and configurations of the firewall, proxy server squid, so, in this way, the networks can be monitored.

CUPRINS

INTRODUCERE

Datorită complexității și dinamicii schimbărilor pe planul tehnologiilor informaționale, precum și a creșterii diversității și complexității amenințărilor la adresa oricărei structure conectate la Internet, strategiile de securitate construite exclusiv pe mecanisme de protecție sunt sortite eșecului. Abordarea securității ca proces, și dintr-o perspectivă proactivă, orientată spre identificarea și alertarea timpurie asupra potențialelor amenințări, sau atacurilor aflate în faze inițiale, poate oferi timpul necesar elaborării unui răspuns eficace înainte ca o structura să fie afectată.

Asigurarea eficacității oricărui gen de proces, inclusiv procesul de securitate, presupune adesea definirea si implementarea unei componente care să urmărească constant evoluția procesului, astfel încât să se poată efectua în timp util corecții și actualizări ca răspuns la schimbările ce au loc în mediul de operare.

O abordare procesuală care să asigure o vizibilitate asupră componentelor cu relevanța în procesul de securitate, este monitorizarea securității cu ajutorul unor softuri speciale. Aceasta se definește ca fiind abilitatea de a colecta, și analiza în timp util evenimentele și informațiile de securitate disponibile la nivelul unei structure de rețea, atât din surse interne și externe, în scopul elaborării unui răspuns eficace la amenințări și atacuri. Ca și în cazul altor componente ale procesului de securitate, pentru o implementare și utilizare adecvată și eficientă a securității, trebuie să se elaboreze în prealabil o politică de securitate, și un program de monitorizare care va gestiona elementele de ordin tehnologic, procesual și organizațional implicate în procesul de securitate.

Pentru elaborarea tezei s-a folosit următoarea metodologie de lucru: s-au studiat numeroase articole, documentații, standarde, cărți etc. cu factor de impact ridicat și de actualitate, care analizează și descriu multiple aspecte din sfera securității rețelelor informaționale.

BIBLIOGRAFIE

1. Bajenescu, T. Internetul, societatea informaţională şi societatea cunoaşterii. Aspecte tehnice, economice, politice şi sociale. Bucureşti: Ed. Matrixrom, 2006.
2. Drăgănescu, M. De la Societatea informaţională la Societatea cunoaşterii. Bucureşti: Editura Tehnică, 2003
3. Dumitru, O. Protecția și securitatea sistemelor informaționale. Suport de curs. Iași., 2017.
4. Ce este securitatea rețelelor de calculatoare.
   Disponibil: https://ro.wikipedia.org/wiki/Securitatea_re%C8%9Belelor_de_calculatoare
5. Apetrii M. Introducerea în securitatea rețelelor. Centru de formare și analiză în ingineria riscurilor. 2018
6. Cum funcționează un atac backdoor.
   Disponibil: https://www.trendmicro.com/vinfo/us/security/definition/backdoor
7. Ce este o rețea virtuală privată.
   Disponibil: https://ro.wizcase.com/blog/ghid-complet-despre-vpn-uri-pentru-incepatori/
8. Cum lucrează o rețea privată virtuală. Cum de conectat la un VPN?
   Disponibil: https://www.digitalcitizen.ro/intrebari-simple-ce-este-un-vpn-si-cum-functioneaza/
9. Identificarea fundamentală și principiile securității sistemelor de calcul și a rețelelor de calculatoare
   Disponibil:https://www.referatele.com/informatica/Nivele-minime-de-securitate555.php
10. Articol: Human Factors Attacks: Social Engineering
    Disponibil: https://veracomp.ro/blog/securitate/4131-social-engineering.html
11. Atacurile de tipul Distributed Denial of Service.
    Disponibil: http://www.veracomp.ro/stiri/considerente-in-privinta-atacurilor-ddos
12. Scurta descriere a diverselor tipuri de atacuri DoS și DDoS.
    Disponibil: https://profs.info.uaic.ro/~eonica/netsec/lab08.html
13. What is a ping flood attack.
    Disponibil: https://www.imperva.com/learn/ddos/ping-icmp-flood/
14. Spoofing defined, explanained, and explored.
    Disponibil: https://www.forcepoint.com/cyber-edu/spoofing
15. Popa S. Securitatea Sistemelor Informatice . Note de curs. Bacău. 2007

16. Securitatea și Vulnerabilitatea Sistemelor Informatice
Disponibil:http://www.banatnet.ro/download/Securitatea%20si%20vulnerabilitatea%20sistemelor%20informatice.pdf
17. Securitatea Sistemelor Informatice - note de curs şi aplicaţii pentru studenţii Facultăţii de Inginerie.
Disponibil: http://cadredidactice.ub.ro/sorinpopa/files/2011/10/Curs_Securit_Sist_Inf.pdf
18. Florin Ogîgău-Neamțiu. Cercetări privind Securizarea informației în Sistemul Cloud Computing. Brașov 2018.
19. Armbrust M., F. A. (2010). A view of cloud computing. Communications of the ACM, Vol. 53
20. Care, J., & Litan, A. (2016). Hype Cycle for Application Security,. Gartner
21. Securizarea informației cu ajutorul listelor de control a accesului.
Disponibil: http://andrei.clubcisco.ro › cursuri › aac-msi › misc
22. Ce este un Firewall şi care este rolul acestuia.
Disponibil: https://www.thc.ro/blog/ce-este-un-firewall-si-ce-rol-are/
23. Securizarea rețelei cu firewall.
Disponibil: https://ramonnastase.ro/blog/ce-este-un-firewall-si-cum-securizeaza-reteaua/
24. Clasificarea firewall, cum se configurează un firewall.
Disponibil: https://newtravelers.ru/ro/asus/chto-takoe-faervol-chto-takoe-firewall-i-dlya-chego-on-nuzhen-faervol-dlya-setevoi.html
25. Setările pentru firewall pentru utilizatorii de reţea.
Disponibil:
https://support.brother.com/g/s/id/htmldoc/mfc/dcp195c/ro/html/sug/chapter7.html
26. Server proxy-ul Squid.
Disponibil: https://en.wikipedia.org/wiki/Squid_(software)
27. Instalarea și configurarea proxy server-ului Squid.
Disponibil: https://ubuntu.com/server/docs/proxy-servers-squid
28. Configurarea server proxy Squid pe Ubuntu.
Disponibil: https://www.liquidweb.com/kb/install-squid-proxy-server-ubuntu-16-04/
29. Configure the cache type.
Disponibil: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/networking_guide/configuring-the-squid-caching-proxy-server