Ministerul Educației și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Electronică și Telecomunicații

Departamentul Telecomunicații și Sisteme Electronice

Admisă la susținere

Șefă department TSE:

Valentina Tîrșu, dr., conf. univ.

”___” _____2025

Protecția împotriva atacurilor DDoS (Distributed Denial of Service). Îmbunătățirea managementului, detecției și răspunsului la incidentele cibernetice

Teză de master

Studenta: Natalia MUNTEANU

MMRT-231M

Conducător: Dinu ȚURCANU

conf.univ., dr.

Chișinău - 2025

ADNOTARE

Titlul: Protecția împotriva atacurilor DDoS (Distributed Denial of Service). Îmbunătățirea managementului, detecției și răspunsului la incidentele cibernetice

Masterandă: Munteanu Natalia, MMRT-231M

Structura tezei: introducere, trei capitole, concluzii generale, bibliografie, 3 anexe, 65 de pagini text de bază, cuvinte-cheie 14.

Cuvinte-cheie: DDoS, atacuri, cibernetice, trafic, securitate, critic, retea, analiza, protectie, incidente, solutii, detectarea, management, pachete

Lucrarea abordează una dintre cele mai critice probleme ale securității cibernetice contemporane: atacurile de tip Distributed Denial of Service (DDoS). Aceste atacuri, care urmăresc blocarea accesului utilizatorilor legitimi la resursele informatice, reprezintă o amenințare majoră pentru organizațiile din diverse sectoare, afectând disponibilitatea, performanța și reputația acestora. Lucrarea analizează în detaliu mecanismele utilizate în atacurile DDoS, precum și soluțiile tehnologice actuale pentru protecția împotriva acestora. De asemenea, sunt investigate metode de îmbunătățire a managementului incidentelor cibernetice, punând accent pe:

1. **Detecția avansată a atacurilor** – utilizarea tehnologiilor moderne, cum ar fi inteligența artificială și machine learning, pentru identificarea rapidă și precisă a traficului malițios.
2. **Managementul eficient al incidentelor** – implementarea unor politici de securitate bine definite și utilizarea soluțiilor automatizate pentru răspuns la incidente.
3. **Răspunsul prompt și adaptativ** – dezvoltarea unor strategii proactive și reactive care să minimizeze impactul atacurilor asupra infrastructurilor critice.

Lucrarea include studii de caz practice și exemple de configurare a soluțiilor de securitate, cum ar fi Fortinet FortiGate, pentru protecția rețelelor împotriva atacurilor DDoS. Sunt prezentate și strategii pentru optimizarea proceselor operaționale, inclusiv monitorizarea, analiza logurilor și raportarea incidentelor de securitate.

Prin contribuția sa, această lucrare oferă o bază teoretică și practică pentru specialiștii în securitate cibernetică, precum și recomandări pentru organizații care doresc să își îmbunătățească reziliența la atacuri DDoS.

ANNOTATION

Title: Protection against DDoS attacks. (Distributed Denial of Service). Improving the management, detection and response to cyber incidents

Magister: Munteanu Natalia, MMRT-231M

Thesis structure: introduction, three chapters, general conclusions, bibliography, 3 annexes, 65 pages of basic text, 14 keywords.

Keywords: DDoS, attacks, cyber, traffic, security, critical, network, analysis, protection, incidents, solutions, detection, management, packets

This master's thesis addresses one of the most critical issues in modern cybersecurity: Distributed Denial of Service (DDoS) attacks. These attacks, aimed at disrupting access to IT resources for legitimate users, pose a significant threat to organizations across various sectors, impacting their availability, performance, and reputation.

The thesis provides an in-depth analysis of the mechanisms behind DDoS attacks and explores current technological solutions for defending against them. It also investigates methods for enhancing the management of cyber incidents, with a focus on:

1. **Advanced attack detection** – leveraging modern technologies such as artificial intelligence and machine learning to quickly and accurately identify malicious traffic.
2. **Efficient incident management** – implementing well-defined security policies and using automated solutions for incident response.
3. **Adaptive and prompt response** – developing proactive and reactive strategies to minimize the impact of attacks on critical infrastructures.

The thesis includes practical case studies and examples of configuring security solutions, such as Fortinet FortiGate, to protect networks from DDoS attacks. It also presents strategies for optimizing operational processes, including monitoring, log analysis, and incident reporting.

By contributing to the field of cybersecurity, this thesis provides both a theoretical and practical foundation for cybersecurity professionals and offers recommendations to organizations seeking to enhance their resilience to DDoS attacks.

CUPRINS

INTRODUCERE

Într-o eră digitală în continuă expansiune, în care tehnologia și internetul sunt esențiale pentru buna funcționare a organizațiilor și economiilor, securitatea cibernetică devine o prioritate absolută. Amenințările cibernetice sunt tot mai sofisticate și mai frecvente, iar organizațiile se confruntă cu o diversitate de atacuri ce pot avea consecințe devastatoare asupra infrastructurilor IT, datelor sensibile și reputației acestora. Printre cele mai periculoase și răspândite forme de atac se numără atacurile de tip **DDoS** (*Distributed Denial of Service*), care au ca scop perturbarea accesului la servicii online, generând pierderi financiare semnificative și afectând operabilitatea organizațiilor vizate.

Atacurile *Distributed Denial of Service* (DDoS) constituie o amenințare semnificativă în domeniul securității cibernetice, având un impact major asupra infrastructurilor internetului. Diverse mecanisme de apărare au fost dezvoltate pentru a mitiga acest tip de atac, însă atacatorii ajustează continuu uneltele și tehnicile utilizate, pentru a ocoli măsurile de securitate implementate. În același timp, cercetătorii din domeniu își revizuiesc constant abordările pentru a răspunde eficient noilor strategii de atac. Domeniul DDoS a devenit tot mai sofisticat, atingând un nivel de complexitate care face dificilă identificarea esenței problemei printre multiplele variabile. Această diversitate a metodelor de atac creează impresia unui spectru larg de vulnerabilități, ce sunt dificile de explorat și de adresat în mod eficient. În paralel, mecanismele de apărare existente sunt caracterizate printr-o gamă variată de strategii tehnice, fiecare având propriile puncte forte și limitări, iar analiza comparativă a acestora în ceea ce privește eficiența, costurile și implementabilitatea devine un proces extrem de complex. [2]

Protecția împotriva atacurilor DDoS necesită nu doar implementarea unor soluții tehnice eficiente, dar și o abordare integrată care implică planuri clare de management al incidentelor cibernetice, strategii avansate de detecție și răspuns rapid. În acest context, managementul incidentelor cibernetice devine un element cheie, având rolul de a asigura o reacție promptă și coordonată în fața unor atacuri sau breșe de securitate. Cu toate acestea, nu este suficient doar să se răspundă la incidentele deja produse; este necesară o pregătire continuă, un sistem de monitorizare eficient și o evaluare constantă a vulnerabilităților pentru a preveni astfel de atacuri.

Actualitatea temei. Studierea atacurilor de tip *Distributed Denial of Service* (DDoS) are o importanță majoră în contextul actual al securității cibernetice, deoarece acestea reprezintă una dintre cele mai frecvente și disruptive amenințări la adresa sistemelor informatice. Prin natura lor, aceste atacuri au capacitatea de a bloca accesul la servicii critice, afectând organizații de toate dimensiunile, de la companii mici până la infrastructuri naționale vitale. În acest context, este esențial să înțelegem cum pot fi gestionate mai bine astfel de incidente, cum pot fi detectate cu

promptitudine și cum se poate răspunde eficient pentru a minimiza impactul. Atacurile DDoS pun în evidență necesitatea unor politici solide de management al incidentelor cibernetice, detecție avansată bazată pe inteligență artificială și răspuns eficient prin măsuri tehnice adaptate. Studierea acestora contribuie la îmbunătățirea securității, protejarea infrastructurilor critice și menținerea încrederii în tehnologiile digitale, fiind esențială într-un context global marcat de creșterea dependenței de tehnologie. Securitatea cibernetică, fiind la pragul actual din ce în ce mai solicitată și abordată, este deosebit de importanta la oricare nvel de organizare instituțională, respectiv și managementul atacurilor de securitate cibernetică necesită un studiu amplu, aplicând diverse metode de studiu.

Scopul tezei constă în analiza și cercetarea metodelor de management și protecție a datelor împotriva atacurilor DDos, analiza metodelor de eficientizare a managementului împotriva atacurilor de securitate cibernetică a atacurilor DDos, metodele de detecție și răspuns la incidentele de securitate cibernetică.

Obiectivele de studiu. La implementarea tezei s-au propus spre cercetare următoarele obiectve de studiu:

- Analiza mecanismelor de acțiune ale atcurilor Ddos, clasificarea lor, caracteristicile tehnice, impacturile economice și provocările actuale în protecția împotriva atacurilor Ddos;
- Cercetarea managementului incidentelor de securitate cibernetică;
- Analiza metodelor și strategiilor pentru implementarea unui management eficient ale incedentelor Ddos;
- Cercetarea metodologiilor și a modelelor existente de evaluare a tehnologiilor pentru detecția și metodele existente de răspuns la atacurile Ddos, precum și măsurile de recuperare;
- Studierea strategiilor și direcțiilor de dezvoltare în domeniul protecției și managementului incidentelor cibernetice împotriva atacurilor Ddos;
- Evidențierea direcțiilor prioritare în viitor de cercetare a atacurilor Ddos;
- Analiza importanței colaborării internaționale în domeniul combaterii atacurilor Ddos și a managementului acestuia.

BIBLIOGRAFIE

1. DOULIGERIS, Christos, MITROKOTSA, Aikaterini, DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION, Department of Informatics University of Piraeus, Piraeus, Greece, Disponibil: https://www.cse.chalmers.se/~aikmitr/papers/ISSPIT03.pdf , pag. 190-193;
2. MIRKOVIC, Jelena, et REIHER, Peter, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, Publicat în: ACM SIGCOMM Computer Communications Review Volume 34, Number 2: April 2004, Disponibil: https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/DDoSmirkovic.pdf, pag. 39-54
3. TIMCO, C., ȚURCANU, T., ȚURCANU, D. Dezvoltarea societăţii informaţionale în Republica Moldova în contextul globalizării. In: Conferința "Particularităţile dezvoltării economiei mondiale în condiţiile globalizării". Chişinău, Moldova, 15 aprilie 2016. pp. 387-398. https://ibn.idsi.md/sites/default/files/imag_file/387-398.pd
4. ȚURCANU, T. Sectorul TIC – între producere şi servicii. In: Meridian Ingineresc, Numărul 1 / 2018 / ISSN 1683-853X, pp.72-75. https://ibn.idsi.md/sites/default/files/imag_file/72-75_1.pdf
5. Țurcan Rina, Țurcanu Dinu, Ciubuc Alexandru. The impact of Internet access on economic development. The 5th Economic International Conference „COMPETITIVENESS AND SUSTAINABLE DEVELOPMENT", 2-3.11.2023, pp 160-165, https://doi.org/10.52326/csd2023.24
6. NICOLĂESCU, Nicu-Sebastian, CONTRIBUŢII PRIVIND MONITORIZAREA SECURITĂŢII REŢELELOR DE CALCULATOARE, Bucureşti, 2011, pag. 26, 46-47;
7. Atacurile Dos și DDoS: diferențele și cum să le preveniți!, Disponibil: https://stisc.gov.md/ro/constientizare/atacurile-dos-si-ddos-diferentele-si-cum-sa-le-preveniti;
8. Bitesize © *2020 BBC*. Type of Denial of Service attack https://www.bbc.co.uk/bitesize/guides/z2c8wmn/revision/3
9. Ludmila Peca, Dinu Țurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „TehnicaUTM", 2022. Disponibil: http://repository.utm.md/bitstream/handle/5014/20549/Computernetworks-Practical-examples-DS.pdf?sequence=1&isAllowed=

10. Dinu Țurcanu, Natalia Spinu, Serghei Popovici, Tatiana Țurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences. Vol. IV, no. 1 (2021), pp. 74 – 83, https://doi.org/10.52326/jss.utm.2021.4(1).10
11. BOYD, Sam, Ce Este un Atac DDoS și Cum să Previi Unul în 2024, Disponibil: https://ro.safetydetectives.com/blog/ce-este-un-atac-ddos/#type;
12. Canadian Centre for Cyber Security, Defending against distributed denial of service (DDoS) attacks, ITSM.80.110,
Disponibil: https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110
13. What is an Attack Vector?, Disponibil: https://www.akamai.com/glossary/what-is-attack-vector
14. Ludmila Peca, Dinu Țurcanu. Network security: Practical examples solved to be introduced in network security. SBN 978-9975-45-941-9. Chișinău, Publisher ,,Tehnica-UTM", 2023.
Disponibil:http://repository.utm.md/bitstream/handle/5014/22819/Network-securityPractical-examples-Guide.pdf?sequence=1&isAllowed=y
15. DISTRIBUTED DENIAL-OF-SERVICE (DDoS) ATTACKS: AN ECONOMIC PERSPECTIVE, pag. 6-8, Disponibil: https://nsfocusglobal.com/wp-content/uploads/2017/01/Distributed_Denial_of_Service_Attacks__An_Economic_Perspective__Whitepaper.pdf;
16. Ghid de conștientizare a atacurilor de tip Distributed Denial of Service, pag. 17-19, https://certmil.ro/wp-content/uploads/2022/06/20220629_N_Ghid-DDoS.pdf;
17. Azure Network Security Team, 2022 în revizuire: tendințe și perspective asupra atacurilor DDoS, Disponibil: https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/;
18. SPYRIDOPOULUS, T., KARANIKAS, G., et. All, A game theoretic defence framework against DoS/DDoS cyber attacks, Disponibil: https://www.sciencedirect.com/science/article/abs/pii/S016740481300059X;
19. KAZEEM, A., B., ADNAN, M., A-M., et. All., „DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges", publicat în Journal of Sensor Actuator Networks, 2023, Disponibil: https://www.mdpi.com/2224-2708/12/4/51;
20. CĂCIULESCU, A.R., RUGHINIȘ, R., ȚURCANU, D., RADOVICI, A. Mapping Cyber-Financial Risk Profiles: Implications for European Cybersecurity and Financial Literacy. In: Risks. 2024, 12(12), 200. https://doi.org/10.3390/risks12120200

21. VULPE, S.-N., RUGHINIȘ, R., ȚURCANU, D., ROSNER, D. AI and cybersecurity: a risk society perspective. In: Frontiers in Computer Science. Volume 6-2024. https://doi.org/10.3389/fcomp.2024.1462250
22. BRAN, E., RUGHINIȘ, R., ȚURCANU, D., RADOVICI, A. AI Leads, Cybersecurity Follows: Unveiling Research Priorities in SDG-Relevant Technologies Across Nations. In: Sustainability. 2024, 16(20), 8886. https://doi.org/10.3390/su16208886
23. BRAN, E., RUGHINIȘ, R., ȚURCANU, D., NADOLEANU, G. Technical Innovations and Social Implications: Mapping Global Research Focus in AI, Blockchain, Cybersecurity, and Privacy. In: Computers. 2024, 13(10), 254. https://doi.org/10.3390/computers13100254
24. BRAN, E., RUGHINIȘ, R., ȚURCANU, D., STĂICULESCU, A. Decoding National Innovation Capacities: A Comparative Analysis of Publication Patterns in Cybersecurity, Privacy, and Blockchain. In: Applied Sciences. 2024, 2024, 14(16), 7086. https://doi.org/10.3390/app14167086
25. GRIGORESCU, O., BOTEZATU, L., MUTU, A., ȚURCANU, D. Contextual Remediations Prioritization System Designed to Implement Theoretical Principles of CVSS V4. In: University Politehnica of Bucharest scientific bulletin series C-Electrical Engineering and Computer Science. 2024, Volume 86, Issue 3, Page 121-138. https://www.scientificbulletin.upb.ro/rev_docs_arhiva/rez833_656075.pdf
26. BĂLUȚĂ, A., SOARE, R. M., RUGHINIȘ, R., ȚURCANU, D. GeckoNet - Self-Healing SDN Framework. In: 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet). 19-20 September, 2024, Bucharest, Romania. https://doi.org/10.1109/RoEduNet64292.2024.10722172
27. ZWINGINA, K., AMB. ENIKANOLAIYE, S., et. All. Impact of DDoS attacks on critical national information infrastructure and human security, publicat în International Journal of Social Science, Management, Peace and Conflict Research, Disponibil: https://ijsmpcr.com/;
28. Chouraik C., El-founir R., Taibi K., The Impact of AI on Cybersecurity: A New Paradigm for Threat Management, publicat în African Journal of Management Engineering and Technology African Journal of Management Engineering and Technology, Morocco, 2024, pag. 92-99;
29. Saeed, M., M., Saeed, R., et. all. Machine Learning Techniques for Detecting DDOS Attacks, ISBN 979-8-3503-0533-3, pag. 3-7;
30. Baciu, Cristian, E-learning. Concepte, strategii,aplicații, ISBN:978-606-49-1051-6, Editura Eikon, București, 2024;

31. OUHSSINI, M., AFDEL, K., et. All., Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches, publicat în Egyptian Informatics Journal Vol. 27;
32. PECA, L., ȚURCANU, D. Reducing cyber risk through a human-centered approach. In: The 13th International Conference on Electronics, Communications and Computing. IC ECCO-2024, 17-18 October, 2024, Chisinau, Republic of Moldova. http://repository.utm.md/bitstream/handle/5014/28769/Int-Conf-ECCO-2024-Abstract-Book-p111-112.pdf?sequence=1&isAllowed=y
33. ȚURCANU, D., PRISĂCARU, A., PECA, L., ȚURCANU, T. Cyber security professional development within CYBERCOR. In: The 13th International Conference on Electronics, Communications and Computing. IC ECCO-2024, 17-18 October, 2024, Chisinau, Republic of Moldova. http://repository.utm.md/bitstream/handle/5014/28823/Int-Conf-ECCO-2024-Abstract-Book-p212-213.pdf?sequence=1&isAllowed=y
34. Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM), Ghid de implementarea a măsurilor de securitate în domeniul managementului incidentelor, aprilie, 2006.
Disponibil:
https://www.ancom.ro/uploads/links_files/Ghid_de_implementare_a_masurilor_de_securitate.pdf;