Ministerul Educației și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Electronică și Telecomunicații

Departamentul Telecomunicații și Sisteme Electronice

Admis la susținere
Șefă department TSE:
Valentina Tîrșu, dr., conf. univ.

”___” _____2025

Simularea atacurilor de tip DoS (Denial of Service) și DDoS (Distributed Denial of Service). Analiza, metodele de atac și impactul acestora asupra infrastructurii informatice

Teză de master

Student: Ion MUNTEANU
MMRT-231M

Conducător: Tatiana ȚURCANU
conf.univ., dr.

Chișinău – 2025

REZUMAT

Această lucrare analizează securitatea informațională, metodele de atac cibernetic și impactul acestora asupra infrastructurilor informatice, punând un accent special **pe atacurile DoS (Denial of Service) și DDoS (Distributed Denial of Service).** Studiul oferă o perspectivă detaliată asupra vulnerabilităților rețelelor informatice și strategiilor utilizate pentru a le exploata sau proteja.

Primul capitol definește conceptul de securitate informațională, abordând resursele informaționale și importanța acestora în societatea modernă. Sunt detaliate principiile fundamentale ale securității cibernetice, inclusiv confidențialitatea, integritatea și disponibilitatea, precum și provocările asociate gestionării vulnerabilităților în organizații.

Al doilea capitol este dedicat analizei metodelor de atac cibernetic, în special atacurilor DoS și DDoS. Sunt prezentate tehnicile și vectorii de atac, riscurile asociate acestora și efectele asupra infrastructurilor IT. De asemenea, sunt examinate metodele de securizare a rețelelor informatice și strategiile moderne de reducere a riscurilor cibernetice.

Al treilea capitol descrie procesul de proiectare a unui sistem pentru simularea atacurilor informatice, având ca obiectiv modelarea și testarea scenariilor de atac în medii controlate. Se analizează structura generală a unei platforme care poate fi realizata și dezvoltată, aceasta include metode de atac, examinarea VPN-urilor, obstacolele digitale și utilizarea diagramelor UML pentru modelarea sistemului.

Al patrulea capitol se axează pe implementarea efectivă a simulărilor de atac utilizând **Kali Linux și Python**. Sunt analizate instrumente precum **HPing3, Tcpdump și Wireshark**, iar experimentele practice includ testarea atacurilor **DDoS și analiza impactului acestora asupra infrastructurii**. De asemenea, este descrisă utilizarea scripturilor Python pentru generarea traficului malițios și automatizarea simulărilor de atac.

Al cincilea capitol abordează aspectele economice și strategice ale proiectului. Se realizează o **analiză SWOT** a simulării atacurilor DDoS, evidențiind punctele forte și slabe ale procesului, oportunitățile și amenințările asociate acestui tip de testare. În plus, este estimat costul implementării unui astfel de sistem de testare într-un mediu controlat.

Lucrarea se încheie cu **concluzii și perspective viitoare**, în care se subliniază **importanța simulării atacurilor DDoS pentru îmbunătățirea securității cibernetice**. Sunt propuse direcții de cercetare pentru viitoarea **teză de doctorat**, care va dezvolta un sistem informațional avansat capabil să modeleze și să analizeze atacurile cibernetice, contribuind astfel la consolidarea protecției infrastructurilor IT.

Cuvinte-cheie: securitate cibernetică, atacuri DoS și DDoS, Kali Linux, Python, simulare, infrastructuri IT, vulnerabilități, testare de penetrare, algoritm.

SUMMARY

This thesis analyzes information security, cyberattack methods, and their impact on IT infrastructures, with a particular focus on **Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks**. The study provides a detailed perspective on the vulnerabilities of computer networks and the strategies used to either exploit or protect them.

The **first chapter** defines the concept of **information security**, discussing **informational resources and their importance in modern society**. The fundamental principles of cybersecurity, including **confidentiality, integrity, and availability**, are detailed, as well as the challenges related to managing vulnerabilities within organizations.

The **second chapter** focuses on the analysis of cyberattack methods, especially **DoS and DDoS attacks**. It presents **attack techniques and vectors**, the risks associated with them, and their effects on IT infrastructures. Additionally, methods for securing **computer networks** and **modern strategies to reduce cybersecurity risks** are examined.

The **third chapter** describes the process of **designing a system for simulating cyberattacks**, aiming to model and test attack scenarios in controlled environments. The general structure of a platform that can be developed is analyzed, including **attack methods, VPN analysis, digital obstacles, and the use of UML diagrams for system modeling**.

The **fourth chapter** focuses on the practical **implementation of attack simulations using Kali Linux and Python**. Tools such as **HPing3, Tcpdump, and Wireshark** are analyzed, and practical experiments include **testing DDoS attacks and evaluating their impact on IT infrastructures**. Additionally, **Python scripts** are used to generate **malicious traffic** and automate attack simulations.

The **fifth chapter** addresses the **economic and strategic aspects** of the project. A **SWOT analysis** of **DDoS attack simulations** is conducted, highlighting the strengths and weaknesses of the process, as well as the **opportunities and threats associated with this type of testing**. Moreover, the costs associated with implementing such a **testing system in a controlled environment** are estimated.

The study concludes with **final remarks and future perspectives**, emphasizing the **importance of DDoS attack simulations for improving cybersecurity**. Directions for further **research within the doctoral thesis** are proposed, focusing on the development of an **advanced information system** capable of modeling and analyzing **cyberattacks**, thereby contributing to strengthening the **protection of IT infrastructures**.

Keywords: cybersecurity, DoS and DDoS attacks, Kali Linux, Python, simulation, IT infrastructures, vulnerabilities, penetration testing, algorithm.

CUPRINS

INTRODUCERE

Securitatea informațională reprezintă un domeniu esențial în era digitală, având ca scop protejarea sistemelor informatice și a datelor împotriva accesului neautorizat, utilizării abuzive, divulgării, întreruperii, modificării sau distrugerii acestora. În contextul amenințărilor cibernetice tot mai sofisticate, menținerea unui nivel ridicat de protecție a informațiilor devine o prioritate atât pentru organizații, cât și pentru utilizatorii individuali.

Standardele internaționale, cum ar fi **ISO/IEC 27002:2013**, definesc un set de bune practici pentru securitatea informațiilor, bazate pe trei principii fundamentale:

Confidențialitatea – asigură faptul că informațiile sunt accesibile doar persoanelor autorizate, fiind protejate prin criptare și mecanisme de autentificare.

Integritatea – garantează acuratețea și fiabilitatea datelor prin metode de verificare și control, prevenind modificările neautorizate.

Disponibilitatea – asigură accesul continuu și neîntrerupt la informații, prin implementarea unor măsuri de securitate precum firewall-uri, soluții de protecție împotriva atacurilor cibernetice și realizarea de copii de siguranță periodice.

Securitatea informațională nu se limitează doar la protecția informațiilor digitale, ci vizează toate formele de date, inclusiv cele fizice sau stocate pe suporturi tradiționale. Aceasta integrează diverse aspecte ale siguranței cibernetice, inclusiv protecția infrastructurilor critice, criptarea comunicațiilor, autentificarea utilizatorilor și prevenirea atacurilor cibernetice.

Importanța Simulării Atacurilor Cibernetice

În cadrul acestei teze, un aspect esențial îl reprezintă **simularea atacurilor DDoS utilizând Kali Linux**, un mediu specializat pentru testarea penetrării și securitatea rețelelor. Prin utilizarea acestui sistem de operare, cercetătorii și specialiștii în securitate pot analiza vulnerabilitățile infrastructurilor IT și pot evalua impactul atacurilor distribuite de tip **Denial of Service (DDoS)** asupra acestora.

Kali Linux este recunoscut pentru multitudinea sa de instrumente dedicate securității cibernetice, permițând simularea unor scenarii realiste de atac. În cadrul acestei cercetări, simulările atacurilor DDoS vor fi realizate prin intermediul unor instrumente specifice precum:

- **Slowloris** – un atac care exploatează limitările conexiunilor HTTP ale serverelor web, încetinindu-le până la punctul în care devin inaccesibile.
- **HPing3** – un instrument utilizat pentru generarea și analizarea traficului de rețea, fiind ideal pentru simularea atacurilor de tip **SYN Flood.**
- **T50** – un generator de trafic de mare intensitate, capabil să efectueze atacuri multiple pentru a testa rezistența infrastructurilor IT.
- **DNS Amplification** – o metodă de atac DDoS care utilizează serverele DNS ca reflectoare pentru a genera volume mari de trafic către ținte specifice.

Aceste atacuri sunt testate într-un **mediu virtualizat**, unde a fost configurată o **mașină virtuală Kali Linux** pentru a desfășura experimentele necesare. Această abordare permite analiza impactului atacurilor DDoS asupra performanței sistemelor și identificarea celor mai eficiente metode de apărare.

Obiectivele Generale și Specifice ale Cercetării

Această lucrare își propune să analizeze impactul atacurilor de tip DoS și DDoS asupra infrastructurilor informatice și să dezvolte o metodologie pentru simularea acestora, contribuind astfel la îmbunătățirea măsurilor de protecție.

Obiective specifice:

1. Realizarea unei analize detaliate a tipologiilor de atacuri DoS și DDoS, evidențiind metodele utilizate și vulnerabilitățile exploatate.
2. Realizarea unor scenarii de testare în medii virtualizate, analizând efectele fiecărui atac asupra resurselor sistemului țintă.
3. Examinarea metodelor de protecție împotriva atacurilor DDoS și implementarea unor strategii eficiente de securitate.
4. Evaluarea impactului acestor atacuri asupra performanței rețelelor informatice, prin simulări practice.
5. Propunerea unor soluții tehnice și organizaționale pentru prevenirea și gestionarea atacurilor.

Metodologia Utilizată și Structura Lucrării

Această lucrare îmbină metode teoretice și practice pentru a aborda problema atacurilor de tip DoS și DDoS. Analiza literaturii de specialitate servește ca bază pentru înțelegerea conceptelor fundamentale și a tehnologiilor existente. În partea practică, utilizarea instrumentelor software pentru simularea atacurilor permite testarea diferitelor scenarii și evaluarea soluțiilor de protecție.

Structura lucrării:

1. **Introducerea:** Contextul, obiectivele și metodologia lucrării.
2. **Conceptul teoretic al securității informaționale:** Principii de bază, riscuri și vulnerabilități, standarde internaționale și conceptele fundamentale ale atacurilor cibernetice.
3. **Analiza atacurilor DoS și DDoS:** Clasificare, metode de atac și impact.
4. **Proiectarea și realizarea unor teste de simulare:** Detalierea etapelor de proiectare și implementare a unui mediu practic pentru simulare.

BIBLIOGRAFIE

1. OLD.MTIC.GOV: Piața TIC din R. Moldova. Ministerul tehnologiilor informaţionale şi comunicaţiilor: https://old.mtic.gov.md/ro/mass-media
2. 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
3. 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
4. CISA: An official website of the U.S. Department of Homeland Security. Privacy and Mobile Device Apps Released December 18, 2022 Disponibil: https://www.cisa.gov/
5. LEGIS: Concepţia securităţii informaţionalea a Republicii Moldova. Monitorul Oficial Disponibil: https://www.legis.md/
6. 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
7. Michael E., Whitman, Herbert J. Mattord Principles of Information Security
8. Stuart McClure, Joel Scambray, George Kurtz. Hacking Exposed: Network Security Secrets and Solutions
9. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chişinău, 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. Ferguson, P., Senie, D. (2004). Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827
12. Kampanakis, P., Rescorla, E. (2010). Threat Analysis of the Domain Name System (DNS).
13. Dinu Țurcanu. Regulament privind organizarea şi funcţionarea Direcţiei Tehnologia Informaţiei şi a Comunicaţiilor la Universitatea Tehnică a Moldovei. Chişinău, UTM, 2017.
14. Dinu Țurcanu. Regulament privind organizarea şi administrarea paginii-web oficiale a IP „Universitatea Tehnică a Moldovei" şi a paginilor-web ale subdiviziunilor universitare. Chişinău, UTM, 2016.

15. Dinu Țurcanu. Regulament cu privire la utilizarea sistemelor informaţionale în cadrul Universității Tehnice a Moldovei. Chișinău, UTM, 2017.
16. 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
17. Comunicare comună către Parlamentul European şi consiliu Cadrul comun privind contracararea amenințărilor hibride Un răspuns al Uniunii Europene JOIN/2016/018 final. Disponibil: http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52016JC0018
18. Security Incident Management Maturity Model Manual. Disponibil: https://sim3-check.opencsirt.org/#/;
19. A Security Incident Response Trust Framework for Federated Identity (Sirtfi). Disponibil: https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf;
20. The CREST Cyber Security Incident Response Maturity Assessment Tool. Disponibil: https://www.crest-approved.org/wp-content/uploads/2014/10/CSIR-Maturity-assessment-tool_Info1.pdf;
21. DARPA Celebrates Cyber Grand Challenge Winners, DARPA, Disponibil: https://www.darpa.mil/news-events/2016-08-05a
22. Malicious programs, Kaspersky, © Disponibil: https://encyclopedia.kaspersky.com/knowledge/malicious-programs/
23. HAProxy. The Reliable, High Performance TCP/HTTP Load Balancer Sep, 18th, 2024 Disponibil: https://www.haproxy.org/
24. 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
25. 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
26. 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
27. 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

28. 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
29. 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
30. 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
31. Outbreak Alert- Annual Report 2023 https://www.fortiguard.com/outbreak-alert/2023-annual-report
32. BARCAN, N.-G., ALEXANDRESCU, A., ȚURCANU, T. Gamification of the Learning Process for Acquiring Logical Thinking in Programming. In: 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet). 19-20 September, 2024, Bucharest, Romania. https://doi.org/10.1109/RoEduNet64292.2024.10722314
33. Atacurile Dos și DDoS: diferențele și cum să le preveniți, https://stisc.gov.md/ro/constientizare/atacurile-dos-si-ddos-diferentele-si-cum-sa-le-preveniti
34. 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
35. 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