MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Electronică și Telecomunicații

Departamentul Telecomunicații şi Sisteme Electronice

Admis la susţinere
Şefă departament TSE:
Valentina Tîrșu dr., conf.univ.

„___” _____ 2025

SISTEME OPTIMIZATE DE MONITORIZARE ŞI DETECŢIE A INTRUZIUNILOR (IDS)

Teză de master

Student: _____ **MERIACRI Ion,** SISRC-231M

Conducător: _____ **DOROGAN Andrei,** lec.univ., dr.

Chişinău, 2025

REZUMAT

Meriacri Ion

Tema: Sisteme optimizate de monitorizare şi detecţie a intruziunilor (IDS).

Structura lucrării: Introducere, Capitolul 1. Practica de documentare: 1.1. Contextul actual și tendințele modern în securitatea cibernetică, 1.2. Analiza soluțiilor tehnice și metodele de simulare pentru implementarea unui sistem IDS, 1.3. Scop, obiective, și evaluarea eficienței rezultatelor. Capitolul 2. Elaborarea sistemului de monitorizare și detecție a intruziunilor (IDS): 2.1. Sistemele de monitorizare și detecție a intruziunilor. Generalități, 2.2. Arhitectura sistemului IDS elaborat, 2.3. Evaluarea performanței sistemului**.** Capitolul 3. Analiza economică: 3.1. Introducere, 3.2. Stabilirea priorității criteriilor globale, 3.3. Determinarea priorităților globale, 3.4. Concluzii economice.

Cuvintele cheie: Java, Wireshark, Linux, IDS, Securitate.

Scopul lucrării: De a proiecta și elabora un sistem de monitorizare și detecție a intruziunilor (IDS) utilizând metode optimizate.

Obiectivele:

1. Analiza contextului actual și a tendințelor moderne în domeniul securității cibernetice, cu accent pe necesitatea utilizării sistemelor IDS.
2. Studierea și evaluarea diferitelor arhitecturi și metode de implementare a sistemelor IDS, inclusiv analiza soluțiilor tehnice existente.
3. Testarea sistemului implementat utilizând instrumente specifice precum Wireshark, nmap, și hping pentru analiza traficului de rețea și identificarea potențialelor atacuri.
4. Evaluarea performanței sistemului IDS implementat, incluzând ratele de detecție și frecvența alarmelor false.
5. Analiza impactului economic al implementării unui sistem IDS, evidențiind costurile de dezvoltare, mentenanță și eficiența economică.
6. Formularea de recomandări pentru îmbunătățirea performanței sistemului IDS și aplicabilitatea acestuia în alte organizații sau industrii.

Metodele aplicate: Java pentru dezvoltarea sistemului, Wireshark pentru analiza traficului, hping pentru simulări și teste, nmap pentru scanarea sistemului.

Rezultatele obținute: Proiectarea și implementarea unui sistem eficient de monitorizare și detecție a intruziunilor folosind metode optimizate, capabil să identifice activitățile suspecte în traficul de rețea.

SUMMARY

Meriacri Ion

Theme: Optimized systems for intrusion detection and monitoring (IDS).

Structure: Introduction, Chapter 1. Documentation practice: 1.1. Current context and modern trends in cybersecurity, 1.2. Analysis of technical solutions and simulation methods for implementing an IDS system, 1.3. Purpose, objectives, and evaluation of the effectiveness of the results. Chapter 2. Development of intrusion detection and monitoring system (IDS): 2.1. Intrusion detection and monitoring systems. General, 2.2. Architecture of the developed IDS system, 2.3. Chapter 3. Economic analysis: 3.1. Introduction, 3.2. Prioritization of overall criteria, 3.3. Determination of overall priorities, 3.4.

Keywords: Java, Wireshark, Linux, IDS, Security.

Target: To design and develop an intrusion detection and monitoring system (IDS) using optimized methods.

Objectives:

1. To analyze the current context and modern trends in the field of cybersecurity, focusing on the necessity of IDS systems.
2. To study and evaluate various architectures and implementation methods for IDS systems, including the analysis of existing technical solutions.
3. To test the implemented system using specific tools such as Wireshark, nmap, and hping to analyze network traffic and identify potential attacks.
4. To evaluate the performance of the implemented IDS system, including detection rates and the frequency of false alarms.
5. To analyze the economic impact of implementing an IDS system, highlighting development, maintenance costs, and economic efficiency.
6. To develop recommendations for improving the performance of the IDS system and its applicability in other organizations or industries.

Methods applied: Java for system development, Wireshark for traffic analysis, hping for simulation and testing, nmap for system scanning.

Results: Design and implementation of an efficient intrusion monitoring and detection system using optimized methods, capable of identifying suspicious activities in network traffic.

CUPRINS

INTRODUCERE

Într-o lume tot mai conectată și digitalizată, amenințările cibernetice au devenit o provocare majoră pentru securitatea informațiilor și integritatea rețelelor. Atacurile de tip zero-day, DDoS și amenințările persistente avansate (APT) prezintă riscuri semnificative atât pentru organizații, cât și pentru persoane, având potențialul de a compromite confidențialitatea, integritatea și disponibilitatea datelor esențiale. În fața acestor amenințări din ce în ce mai sofisticate, protejarea infrastructurilor IT a devenit o prioritate absolută.

Sistemele de detectare și monitorizare a intruziunilor (IDS) joacă un rol esențial în securitatea rețelelor prin monitorizarea traficului și identificarea comportamentelor suspecte care pot semnala prezența unui atac. Cu toate acestea, metodele tradiționale de detectare bazate pe semnături și reguli predefinite au dificultăți în detectarea atacurilor noi sau necunoscute, precum și a atacurilor complexe care nu urmează un model predefinit. În acest context, apariția unor noi metode de analiză, cum ar fi analiza comportamentală și tehnicile de detectare bazate pe anomalii, oferă o alternativă mai eficientă pentru identificarea activităților neobișnuite și a atacurilor neașteptate.

Această teză de masterat se concentrează pe dezvoltarea unui sistem de monitorizare și detectare a intruziunilor care utilizează atât tehnici de analiză a pachetelor de rețea, cât și tehnici de analiză comportamentală pentru a detecta în mod eficient comportamentele suspecte și potențialele atacuri cibernetice. Teza va explora soluțiile tehnice disponibile, metodele de simulare a atacurilor și a traficului de rețea și va evalua performanța sistemului propus printr-o serie de teste. Scopul acestei teze este de a contribui la îmbunătățirea securității rețelelor informatice și de a propune o soluție pentru detectarea avansată a intruziunilor.

Această teză este structurată astfel încât să ofere o bază teoretică solidă, o analiză detaliată a soluțiilor moderne și o descriere a metodelor de evaluare utilizate, cu scopul de a dezvolta un sistem IDS eficient și aplicabil în contextul provocărilor actuale de securitate cibernetică.

BIBLIOGRAFIA

1. Roesch, M. (1999). *Snort: Lightweight Intrusion Detection for Networks.* Disponibil la: https://www.usenix.org/legacy/event/lisa99/full_papers/roesch/roesch.pdf [citat 09.10.2024]
2. Paxson, V. (1998). *Bro: A System for Detecting Network Intruders in Real-Time.* Disponibil la: https://www.usenix.org/legacy/publications/library/proceedings/sec98/full_papers/paxson/paxson.pdf [citat 09.10.2024]
3. Statista. *Cyber Crime & Security.* Disponibil la: https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#insights. [citat 15.10.2024]
4. Kali Linux. *Kali Linux Documentation.* Disponibil la: https://www.kali.org/tools/ [citat 09.10.2024]
5. Cybersecurity SpringerOpen. *Survey of intrusion detection systems: techniques, datasets and challenges.* Disponibil la: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7. [citat 12.10.2024]
6. Wireshark. *Wireshark User Guide*. Disponibil la: https://www.wireshark.org/docs/ [citat 05.10.2024]
7. Verizon. *Data Breach Investigations Report* Disponibil la: https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf [citat 15.04.2024]
8. Hping. *Hping3 User Manual*. Disponibil la http://www.hping.org/manpage.html [citat 23.11.2024]
9. Fyodor. (2008). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Disponibil la: https://nmap.org/book/ [citat 23.11.2024]
10. Tcpreplay. *Tcpreplay Documentation*. Disponibil la: https://tcpreplay.appneta.com/ [citat 23.11.2024]
11. GitHub. *Java IDS Implementation Repository*. Disponibil la: https://github.com/mrtea9/java_ids [citat 23.11.2024]
12. Statista. *Distribution of detected cyberattacks worldwide in 2023, by type.* Disponibil la: https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/#:~:text=Global%20cyberattack%20distribution%202023%2C%20by%20type&text=In

%202023%2C%20ransomware%20was%20the,19%20percent%20of%20the%20detections. [citat 15.10.2024].

13. Țurcanu, D., Spinu, N., Popovici, S., Țurcanu, T. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. In: Journal of Social Sciences. 2021, IV (1), pp. 74–83. https://doi.org/10.52326/jss.utm.2021.4(1).10 [citat 23.11.2024]

14. Tîrșu V., Cerbu O. *Interactive visualization of geographical data using proxmox and modern technologies.* In: The scientific heritage. Economic Sciences., Vol.1 № 142 (142), 2024, p.21-26. Budapest, Hungary. ISSN 9215 — 0365, Cosmos Impact Factor - 3.336 SJIF Impact Factor - 5.78 DOI: , Categoria B+. Disponibil: http://www.scientific-heritage.com/ru/arhiv/

15. Peca, L., Țurcanu, D. Network security: Practical examples solved to be introduced in network security. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chişinău: Tehnica-UTM, 2023. – 243 p. ISBN 978-9975-45-941-9. http://repository.utm.md/handle/5014/22819 [citat 27.11.2024]

16. Peca, L., Țurcanu, D. Computer networks: Practical examples solved to be introduced in computer networks. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chişinău: Tehnica-UTM, 2022. – 188 p. ISBN 978-9975-45-812-2. http://repository.utm.md/handle/5014/20549 [citat 29.11.2024]

17. Tîrșu, V. Programare : Ghid metodic pentru lucrări de laborator. Chișinău: Ed. "Tehnica-UTM", 2022, pag.130, ISBN 978-9975-45-861-0. Disponibil: https://library.utm.md/items/?biblionumber=2619626

18. Sava, L., Vortolomei, D. Organizarea şi analiza activităţii economice în domeniul telecomunicaţiilor. Note de curs, Chişinău, Editura UTM, 2022, ISBN: 978-9975-45-805-4.