

# **STUDIAREA SECURITĂȚII REȚELELOR PRIN INTERMEDIUL EMULĂRII cu GNS3**

**Masterand:  
Mihail GRAUR**

**Conducător:  
conf. univ. Victor MORARU**

## ADNOTARE

La teza de master cu tema „Studierea securității rețelelor prin intermediul emulării cu GNS3” al st. gr. CRI 191-M Mihail Graur.

Teza este constituită din introducere, 3 capitole, 12 surse bibliografice, 14 figuri, concluzie.

Managementul securității sistemelor IT constituie un factor hotărâtor în buna desfășurare a activității unei companii, pentru asigurarea protecției datelor și a efectuării de tranzacții electronice.

În prezent rețelele de calculatoare s-au răspândit în toate domeniile: economic, administrativ, financiar, etc., din această cauză schimbul de date între calculatoare prin rețea trebuie securizat la cel mai înalt nivel. Așadar, securitatea unui calculator sau a unei întregi rețele este foarte importantă, întrucât nimeni nu este total securizat de atacurile din rețea, orice calculator este vulnerabil într-o oarecare măsură și într-o rețea cu securitate ridicată, un calculator fără aceste măsuri de securitate poate fi veriga slabă ce poate duce la pierderea datelor sau chiar la defecte în rețea.

Abordarea acestei situații are ca obiectiv diminuarea efectelor negative asupra sistemului informațional, precum și la crearea unui mediu favorabil de dezvoltare atât a sistemului cât și a specialiștilor din domeniu, desigur dacă sunt gata să se implice.

Securitatea unei rețele depinde nu numai de software-ul instalat în interiorul rețelei (antivirus, firewall, OS, etc.), ci, în egală măsură, de componentele hardware, cunoștințele în domeniul securității a personalului, etc. Cheia succesului unei lupte reprezintă cunoașterea atacurilor folosite de dușman, deci dacă considerăm acțiunile hackerilor ca o luptă, este crucială cunoașterea atacurilor pe care le va utiliza.

Astfel printre principalele mijloace tehnice implementate de întreprinderile societății moderne se pot enumera: programe antivirus, soluții de detectare și prevenire a intruziunilor, salvare a datelor, instruire referitoare la importanța implementării și urmării măsurilor de Securitate.

Pentru organizarea unei protecții fiabile, este necesară identificarea clară a tipurilor de atacuri de informații care ar trebui protejate. Iar pentru a putea contracara aceste atacuri este necesar crearea unui laborator de cercetare ca cel propus în continuare.

Studierea securității va fi mereu un factor important deoarece neajustarea politicilor și instrumentelor de securitate vor fi supuse mai multor amenințări.

## ANNOTATION

Annotation to the master's thesis with the topic "Studying network security through emulation with GNS3" of st. g. CRI 191-M Mihail Graur.

The thesis consists of introduction, 3 chapters, 12 bibliographic sources, 14 figures, conclusion.

IT systems security management is a decisive factor in the smooth running of a company's activity, to ensure data protection and electronic transactions.

At present, computer networks have spread in all fields: economic, administrative, financial, etc., because of this the exchange of data between computers through the network must be secured at the highest level. Therefore, the security of a computer or an entire network is very important, because no one is completely secure from network attacks, any computer is to some extent vulnerable and in a high security network, a computer without these security measures it can be a weak link that can lead to data loss or even network failures.

The approach to this situation aims to reduce the negative effect on the information system, as well as to create a favorable environment for the development of both the system and the specialists in the field.

The security of a network depends not only on the software installed inside the network (antivirus, firewall, OS, etc.), but also on the hardware components, knowledge in the field of personnel security, etc. The key to the success of a fight is to know the attacks used by the enemy, so if we consider the actions of hackers as a fight, it is crucial to know the attacks he will use.

Thus, among the main technical means implemented by the enterprises of modern society can be listed: antivirus programs, intrusion detection and prevention solutions, data saving, training on the importance of implementing and monitoring Security measures.

In order to organize reliable protection, it is necessary to clearly identify the types of information attacks that should be protected. And in order to counteract these attacks, it is necessary to create a research laboratory like the one proposed below.

The study of security will always be an important factor because non-adjustment of security policies and instruments will be subject to several threats.

## CUPRINS

INTRODUCERE .....	11
1. SECURITATEA REȚELELOR INFORMAȚIONALE ȘI TEHNICILE DE EMULARE.....	12
1.1 Concepte privind securitatea informațională .....	12
1.2 Politici, standarde, norme și proceduri de securitate .....	22
1.3 Tehnologia de emulare.....	37
2. ANALIZA METODELOR DE CERCETARE ȘI INSTRUMENTELOR UTILIZATE .....	40
2.1 Tehnici de proiectare și cercetare.....	40
2.2 Analiza instrumentelor utilizate .....	47
3. STUDIAREA INTRUZIUNILOR PRIN EMULARE CU GNS3 .....	57
3.1 Instalarea și configurarea softului și a instrumentelor utilizate .....	57
3.1.1 Instalarea Wmware Workstation Pro 16 .....	57
3.1.2 Instalarea GNS3 .....	58
3.1.3 Instalarea VM Windows 10 și Kali Linux în VMware Workstation Pro 16.....	59
3.2 Implementarea practică a intruziunilor cu GNS3. ....	63
3.3 Metode de respingere a intruziunilor în rețele informaționale.....	67
CONCLUZIE .....	71
BIBLIOGRAFIE.....	72

## INTRODUCERE

Studiul a fost bazat pe studierea securității rețelelor informaționale într-un mediu virtual și emulat.

Actualitatea temei de studiu este reprezentată de potențialul societății informaționale care este în continuă creștere datorită dezvoltării tehnologice și a căilor de acces multiple.

În acest context, desfășurarea în bune condiții a activității securității sistemelor informatice impune existența unui sistem IT funcțional. Astfel se propune crearea și utilizarea unui laborator informațional pentru pregătirea specialiștilor în domeniu.

Capitolul 1 “ Securitatea rețelelor informaționale și tehnicile de emulare” cuprinde studiul teoretic și analiza politicilor, standardelor, normelor și procedurilor de securitate, impactul negativ al acestora asupra sistemului informațional. Se reflectă propria înțelegere a temei și se formulează scopul și sarcina de cercetare/proiectare.

În Capitolul 2 „Analiza metodelor de cercetare și instrumentelor utilizate” sunt descrise metodele de cercetare și instrumentele utilizate pentru crearea unui laborator de securitate informațională cu scopul de bază al activității fiind atât suportul studenților, doctoranzilor, tinerilor specialiști cât și specialiștilor avansați în activitatea științifică de cercetare în domeniul IT, suportând cheltuieli minime și obținând rezultat maxim dorit.

Capitolul 3 “Studierea intruziunilor prin emulare cu GNS3” este consacrat prezentării rezultatelor practice/experimentale în domeniul de cercetare/proiectare obținute pe parcursul elaborării tezei de master. Sunt prezentate metode de atac și protecție contra acestora utilizând softul de emulare GNS3 și softul de virtualizare Wmware Workstation 16 ca exemplu de utilizare a capacităților laboratorului.

Concluziile prezintă succint principalele rezultate obținute în teză.

Această teză nu prezintă un produs finit ci un model de laborator bazat pe produse soft care pot fi utilizate în concluzare unele cu altele în scopul realizării unei analize asupra problemelor unei rețele reale. La următoarea etapă era planificată implementarea în cadrul unui laborator cu capacități mai mari pentru a putea analiza mai multe tipuri de probleme de securitate în rețele și realizarea unei rezolvări ale acestora pentru un lucru mai eficient a sistemului informațional cât și a unei practici de lucru pentru specialiștii în domeniu.

## **BIBLIOGRAFIE**

[1] Ce este securitatea sistemelor informatice? <https://www.quora.com/What-is-computer-system-security> [Resursă electronică, accesat 07.10.2020].

- [2] Legea privind aprobarea Concepției securității informaționale a R.Moldova Nr. 299 Chișinău, 21 decembrie 2017. Publicat: 16-02-2018 în Monitorul Oficial Nr. 48-57 art. 122
- [3] ALONSO S. book: Computer network defense operations, disrupting the enemy's attack. Publicată 2016, December 30.
- [4] DABIJA GEORGE informatician, profesor grad definitiv. Proiect cofinanțat din Fondul Social European în cadrul POS DRU 2007-2013 *Securitatea sistemelor de calcul și a rețelelor de calculatoare*.
- [5] ASHLEY CHONKA,. book: System security defence to protect against HTTPDoS and XML-DoS attacks. Publicat 2011.
- [6] MoldData Harta uimitoare a atacurilor cibernetice <https://www.molddata.md> [Resursă electronică, accesat 05.11.2020].
- [7] Sisteme de control al accesului la Intranet. <https://www.kp.ru/guide/sistemy-kontrolja-i-upravlenija-dostupom.html>. [Resursă electronică, accesat 05.11.2020].
- [8] ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management <https://www.iso.org/standard/39612.html> [Resursă electronică accesat 15.11.2020]
- [9] Standardul ISO/IEC 27000 actualizat. <https://www.iso.org/ru/standard/73906.html> [Resursă electronică, accesat 05.11.2020].
- [10] PĂDURARU M. book:Vulnerabilități ale sistemelor informatice 2015 European Conferences. Publicată 27 Mai 2015.
- [11] Factorul uman-element crucial în asigurarea securității cibernetice <http://moldova.md/ro/content/factorul-uman-element-crucial-asigurarea-securitatii-cibernetice>. [Resursă electronică, accesat 05.11.2020].
- [12] MARK STAMP, course support: Information security. Principles and Practice, Second Edition, SanJose State University. Publicat 2011 de John Wiley & Sons, Inc.