MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Informatică și Ingineria Sistemelor

Admis la susținere

Șef Departament:

Sudacevschi Viorica, conf. univ., dr.

_____

„___”_____2022

Studiu asupra atacurilor cibernetice și a remediilor contra lor

Teză de master

Student: **Botnaru Victor, CRI-211M**

Conducător: **Moraru Victor,**

conf. univ., dr.

Chișinău, 2022

ADNOTARE

Structura tezei: introducere, trei capitole, concluzii generale, bibliografie din 33 titluri, 60 pagini, 29 figuri.

Domeniul cercetării: Atacuri și securitate cibernetică,,

Scopul cercetării: studiul și analiza problemelor actuale de transmitere a datelor în rețea, identificarea atacurilor, vulnerabilităților, riscurilor și amenințărilor, precum și aplicarea metodelor de securitate a informațiilor.

***Obiective a lucrării sunt*:** analiza amenințărilor, riscurilor și vulnerabilităților, studiul privind instrumentele și modelele de asigurare a securității informaționale, precum și aplicarea metodei de asigurare a securității informaționale împotriva atacurilor cibernetice

Capitolul: „ Aspecte teoretice ale cercetării ” cuprinde studiul teoretic privind conceptul de atacuri cibernetice și securitate cibernetică, avantaje și dezavantaje ale acestora. În acest capitol sunt evidențiate trăsăturile și caracteristicile diferitor tipuri și metode de atacuri cibernetice.

Capitolul II: „ Instrumente și tehnologii ” cuprinde analiza și descrierea instrumentelor de securitate și hacking. În acest capitol sau fost descride instrumentele folosite pentru securitatea informațională, atât pentru hacking rău intenționat cât si pentru hacking etic.

Capitolul III: „ Realizarea atacurilor cibernetice ” descrie realizarea unor tipuri de atacuri cibernetice prin pași consecutivi, printre ele sunt atacul Man in The Middle Attack folosind Wireshark, DOS/DDOS, Phishing și ARP Spoofing.

Cuvinte cheie: Atacuri cibernetice, Securitate cibernetică, DDOS, MITM, Fhishing, Wireshark, Ettercap, Slowloris, ARP Spoofing,

ANNOTATION

Structure of the thesis: introduction, three chapters, general conclusions, bibliography of 33 titles, 60 pages, 29 figures.

Research Area: Cyber Attacks and Security

The purpose of the research: the study and analysis of current problems of data transmission in the network, the identification of attacks, vulnerabilities, risks and threats, as well as the application of information security methods.

The objectives of the work are: the analysis of threats, risks and vulnerabilities, the study of the tools and models for ensuring information security, as well as the application of the method of ensuring information security against cyber attacks

Chapter I: " Theoretical aspects of the research " covers the theoretical study of the concept of cyberattacks and cyber security, their advantages and disadvantages. This chapter highlights the features and characteristics of different types and methods of cyberattacks.

***Chapter II*:** " Tools and Technologies " covers the analysis and description of security and hacking tools. In this chapter he describes the tools used for information security, both for malicious hacking and for ethical hacking.

Chapter III: " Performing Cyber Attacks " describes performing some types of cyberattacks through consecutive steps, among them are Man in The Middle Attack using Wireshark, DOS/DDOS, Phishing and ARP Spoofing.

Keywords: Cyber Attacks, Cyber Security, DDOS, MITM, Phishing, Wireshark, Ettercap, Slowloris, ARP Spoofing,

CUPRINS

INTRODUCERE

Astăzi trăim și lucrăm într-o lume a conectivității globale. Proliferarea calculatoarelor personale, accesul gratuit la internet și o piață în plină expansiune pentru noi dispozitive de comunicații au schimbat modul în care ne petrecem timpul liber și modul în care facem afaceri. Se schimbă și modul în care sunt comise crimele. Disponibilitatea tehnologiilor digitale globale deschide noi oportunități pentru indivizi fără scrupule. Afacerile și consumatorii deopotrivă au pierdut milioane de dolari „cu ajutorul" criminalilor cunoscători de computere.

Acest subiect este, desigur, relevant în epoca noastră, deoarece volumul cercetărilor în domeniul criminalității cibernetice a crescut exponențial în ultimele decenii, deoarece progresele tehnologice au creat, de asemenea, multe oportunități infractorilor de a comite diverse forme de infracțiune.

Problema criminalității cibernetice se bazează pe faptul că, în multe cazuri, agențiile de aplicare a legii sunt în urmă cu criminalii, lipsind tehnologia și personalul calificat pentru a face față unei noi amenințări care crește rapid.

Scopul cercetării este de a studia sursele și factorii care duc la apariția criminalității informatice, precum și impactul acestora asupra tuturor sferelor vieții publice.

Pe baza obiectivului prezentat, se pot distinge următoarele sarcini ale cercetării:

- să ia în considerare esența conceptului de criminalitate cibernetică,

- să evalueze impactul crimelor din spațiul cibernetic,

- să studieze cauzele care duc la apariția criminalității cibernetice,

- să studieze statisticile privind numărul de infracțiuni cibernetice

- să elaboreze simularea atacurilor cibernetice

- să studieze metodele de remediere a atacurilor

BIBLIOGRAFIE

1.Statistici și informații despite securitatea cibernetică 2022 [on-line] [citat 15.08.2022]. Disponibil: https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/

2. Phishing Attack [on-line] [citat 15.08.2022]. Disponibil: https://www.geeksforgeeks.org/phishing-attack/?ref=gcse

3. Tipuri de atacuri și metode de remedii [on-line] [citat 15.08.2022]. Disponibil: https://www.tadviser.ru

4. Atacurile DOS și DDOS [on-line] [citat 15.08.2022]. Disponibil: https://www.geeksforgeeks.org/difference-between-dos-and-ddos-attack/?ref=gcse

5. Backdoor, caracteristici generale [on-line] [citat 15.08.2022]. Disponibil: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:Backdoor

6. Ce este Backdoor? [on-line] [citat 15.08.2022]. Disponibil: https://nordvpn.com/ru/blog/backdoorattack/#:~:text=Backdoor%20attacks%20involve%20cybercriminals%20using,any%20of%20the%20cybersecurity%20systems

7. Cum de prevenit Man In The Middle Attack [on-line] [citat 15.08.2022]. Disponibil: https://www.geeksforgeeks.org/how-to-prevent-man-in-the-middle-attack/?tab=article

8. Actualitatea criminalității cibernetice [on-line] [citat 15.08.2022]. Disponibil: https://www.hse.ru/edu/vkr/363400280

9. Instrumente de hacking [on-line] [citat 04.09.2022]. Disponibil: https://vasexperts.ru/blog/bezopasnost/oruzhie-hakera-instrumenty-dlya-vzloma/

10. Ce este PuTTY? [on-line] [citat 04.09.2022]. Disponibil: https://www.techopedia.com/definition/4335/putty

11. Hacking etic folosind Linux [on-line] [citat 04.09.2022]. Disponibil: https://medium.com/edureka/ethical-hacking-using-kali-linux-fc140eff3300

12. Hacking etic folosind Python [on-line] [citat 04.09.2022]. Disponibil: https://medium.com/edureka/ethical-hacking-using-python-c489dfe77340

13. Angry IP Scanner, scanner de rețea [on-line] [citat 04.09.2022]. Disponibil: https://angryip.org/about/

14. Ce este Nmap? [on-line] [04.09.2022]. Disponibil: https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

15. ce este Ncrack? [on-line] [citat 06.09.2022]. Disponibil: https://www.kali.org/tools/ncrack/

16. Ce este PingInfoView? [on-line] [citat 06.09.2022]. Disponibil: https://www.nirsoft.net/utils/multiple_ping_tool.html

17. Despre Wireshark [on-line] [citat 06.09.2022]. Disponibil: https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

18. Metasploit Framework [on-line] [citat 06.09.2022]. Disponibil:

https://blog.skillfactory.ru/glossary/metasploit-framework/
19. Ce este Psexec.exe? [on-line] [citat 20.10.2022]. Disponibil:
https://adamtheautomator.com/psexec/
20. Slowloris [on-line] [citat 20.10.2022]. Disponibil:
https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/
21. VMware vSphere Client [on-line] [citat 20.10.2022]. Disponibil:
https://www.techtarget.com/searchvmware/definition/VMware-vSphere-Web-Client
22. Telnet [on-line] [citat 20.10.2022]. Disponibil:
https://www.extrahop.com/resources/protocols/telnet/
23. TeamViewer [on-line] [citat 04.24.2021]. Disponibil:
https://www.teamviewer.com/
24. Radmin VPN [on-line] [citat 20.10.2022]. Disponibil:
https://adamtheautomator.com/radmin-vpn-review/
25. AnyDesk [on-line] [citat 20.10.2022]. Disponibil:
https://www.ibik.ru/ru/what-purpose-anydesk/
26. Волков К. В. "Киберпреступность. Виды и особенности ее влияния." Editura „Уральский государственный юридический университет" 2019
27. Stuart McClure, George Kurtz și Joel Scambray "Hacking Exposed 7: Secrete și soluții de securitate a rețelei". Editura „ McGraw Hill " 2012
28. Thomas A. Johnson "Cyber-security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare". Editura „ Routledge" 2015
29. Mike O'Leary "Cyber Operations: Building, Defending, and Attacking Modern Computer Networks". Editura „Apress" 2019
30. Николюк М. С. " Влияние пандемии на угрозу киберпреступности в России и мире. Editura „СЗИУ РАНХиГС" 2020
31. Комлев Ю.Ю. " Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии". 2020
32. Борисова Е.С., Белоусов А.Л. „Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы". 2019
33. Айков, Д. Компьютерные преступления. „Руководство по борьбе с компьютерными преступлениями". Editura „МИР" 1999