Universitatea Tehnică a Moldovei

Tehnici pentru securitatea cibernetică a rețelelor informaționale.

Techniques for cyber security of information networks.

Student:
Nirca Anton

Conducător:
Conf.univ.,dr. Ciobanu Oleg

Chişinău – 2019

ADNOTARE

La proiectul de master: „Tehnici pentru securitatea cibernetică a rețelelor informaționale”elaborat Nirca Anton, Chișinău, 2019.

Teza de master este realizată pe 70 pagini formatul A4 şi cuprinde 35 figuri, 30 surse bibliografice şi 4 pagini de anexe.

Cuvinte cheie: “securitate”, “rețea informațională”, “Dos”, “DDos”, “android”, “atac cibernetic”, “sistem de operare”,“utilizator”, “aplicație” și “hacker”.

Domeniul de studiu îl constituie securitatea rețelelor informatice și vulnerabilități lor, care dacă nu sunt depistate, pot aduce prejudicii considerabile.

Scopul lucrării este de elabora o combinație între analiză/sinteză a atacurilor informatice și a modalităților de contracarare sau prevenire care de cele mai multe ori sunt ignorate de către administratori sau dezvoltatorii de softuri. Se va analiza atacurile de tip DoS, DDoS, MITM, CAM OVERFLOW și a metodelor de bază de securizare a rețelelor informaționale ca exemplu VPN sau configurarea iBarierelor.

Scopul lucrării este accentuarea necesității securizării rețelelor cu soluții noi care blochează sau ameliorează, un potențial atac.

Cota personală se regăsește în creearea unei aplicații de tip android care generează un atac de tip DDoS, apoi s-a implementat metode de protecție precum CloudFlare sau Kaspersky.

Metodologia cercetării este la baza literaturii de specialitate cu diferită proviniență și diferită abordarea a informației reflectând diverse unghiuri și puncte de vedere.

Elementele de cercetare și inovație științifică reprezintă aplicarea instrumentelor de securizare a rețelelor informatice.

Teza constituie introducerea, trei capitole, concluzia, bibliografiile şi anexele.

În concluzie această teză de master reprezintă un studiu complex al securității rețelelor informatice și a soluțiilor de prevenire și curmare a atacurilor parvenite atît din interiorul sistemului cât și din exteriorul lui.

ANNOTATION

At the master project: "Techniques for cyber security of information networks" elaborated by Nirca Anton, Chisinau, 2019.

This master thesis is written on 70 pages A4 format and includes 35 figures, 30 bibliographical sources and 4 pages with annexes.

The keywords are: "security", "hacker", "informational network", "user", "computer network", "attack", "Dos", "Ddos", "system", "application" and "android platform",.

The domain of the study was replaced by the security if their informed networks and their vulnerabilities, if not detected and with considerable prejudice.

The power of actions is the combination between analysis/synthesis and informed illness and the moderation of counteractment, and the truth of which I am thankful for you. You will also be informed of the Dos, Ddos, MITM, CAM OVERFLOW and the basic methods of securing information and informational networks such as VPN, which may have been implemented.

The purpose of the work is to find the need for the securing of networks with new solutions that could block or to kill the attack.

The part to be found in creating an android-like group generates an amount of typ DDoS, then methods of protection were implemented like CloudFlare and Kaspersky.

The methodology of research is at the heart of the literacy of different soursces with different origins and degrees of information reflecting different angles and points of view.

The elements of scientific innovation and scientific innovations require the application of tools to security informants. Thesis contains the introduction, three chapters, conclusion, bibliography and the Annexe.

In this study, this thesis of the Master is degree is a complex study of the security of the informed network and the solution of the meeting and closure of the system both inside and outside.

Cuprins:

INTRODUCERE

Furturile online și crimile cibernetice au provocat prejudicii de miliarde de dolari doar în anul 2019, toate firmele de securitate cibernetică au devenit o ținta majoră a hackerilor, la fel se evedințiază o sursă a atacurilor virtuale care sunt țările autoritare. Anual sunt înregistrate aproape 6 milioane de tentative de atac cibernetic în Republica Moldova. Malware-ul pentru furtul de informații, phishingul, exploituri zero-day, cripto-jacking-ul etc.

Conţinutul tezei de licenţă include toate compartimentele necesare, structurate logic şi coerent, se descrie metodologia cercetării care a fost bazată pe literatura de specialitate prin abordarea informației din diferite puncte de vedere. În primul capitol se descriu aspectele generale a resurselor informaționale și a securizării acestor rețele, se menționează unele tehnici și este dusă tangenta dintre societate modernă și influența atacurilor asupra ei.

În capitolul 2 este descrisă o sinteză a atacurilor informatice și a modalităților de înlăturare sau prevenire ale lor, s-a efectuat analiza și descrierea de nivel înalt tehnicilor de securizare a rețelelor informaționale. Sunt menționate elementele de inovație și cercetare științifică ce reprezintă utilizarea instrumentelor de securizare a rețelelor informatice. În urma cercetărilor efectuate am luat cunoștință cu diverse tipurile de atacuri informaționale cum ar fi Dos, DDos, MITM, SYN FLOOD și respectiv metode de prevenire, depistare și contracarare a acestor atacuri. Modul fiecăruia de funcționare și estimarea prejudiciului ce poate fi pricinuit din partea lor.

Conform informației obținute printr-un studiu profond a domeniului, în capitolul 3 a tezei de master s-a elaborat o aplicație care ar putea genera un atac cibernetic simplu, precum și exemplu detaliat de atac Dos (CAM OVERFLOW) de suprapopularea tabelei CAM a switch-lui.

BIBLIOGRAFIE:

1. Drăgănescu, M. De la Societatea informaţională la Societatea cunoaşterii. Bucureşti: Editura Tehnică, 2003. 244 p;

2. Mihai Drãgãnescu, Societatea Informaţională şi a Cunoaşterii. Vectorii Societăţii Cunoaşterii, studiu pentru Proiectul SI-SC (Societatea Informaţională - Societatea Cunosşterii) al Academiei Române, Bucureşti, 9 iulie 2001. Publicat, p.43 - 112, în vol. coord. Florin Gh. Filip, Societatea informaţională-Societatea cunoaşterii. Concepte, soluţii şi strategii pentru România, Academia Română, 2002;

3. Борис Бейзер Тестирование черного ящика, 2014, pag. 232;

4. Алексей Петровский Эффективный хакинг для начанающих и не только, Kiev 2014, pag. 320-322;

5. Петренко С.А., Курбатов В.А. Политики безопасности компании при работе в интернет, Moscova 2013, pag. 112;

6. http://old.mtic.gov.md/;

7. Monica Ene Pietroșanu,Victor Valeriu Patriciu, Justin Priescu , Ion Bica, Semnături electronice și securitate informatică, 2006 pag. 211-222;

8. Kent HUNDLEY, Gil HELD, Arhitecturi de securitate, Editura Teora, 2003, pag. 33-40;

9. https://en.wikipedia.org/wiki/Ping_of_death;

10. https://www.geeksforgeeks.org/network-address-translation-nat/;

11. Richard Bejtlich Practice of Network Security: Understanding Incident Detection and Response, pag. 320;

12. Tony Bevis Java Design Pattern Essentials, Second Edition Paperback, October 11, 2012, pag. 126;

13. http://www.consultanta-certificare.ro/stiri/colectie-iso-9000.htmlș

14. https://www.sciencedirect.com/topics/computer-science/dumpster-diving;

15. Robert C. MARTIN Clean Code: A Handbook of Agile Software Craftsmanship, 1st Edition 2013, pag.102;

16. John Strand and Paul Asadoorian Offensive Countermeasures: The Art of Active Defense, pag. 100;

17. Gene Kim, Jez Humble, Patrick Debois, and John Willis The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations, pag 40;

18. Paul DUVALL, Andrew GLOVER, Steve MATYAS Continuous Integration: Improving Software Quality and Reducing Risk, 1st Edition, pag. 396-398;

19. Armstrong A. TAKANG, Penny GRUBB, Software Maintenance: Concepts and Practice, Edition Praga 2012, pag 189-192;
20. https://developer.android.com/reference/android/util/Config;
21. George Spafford, Paul Love, and Gene Kim Visible Ops Security: Achieving Common Security And IT Operations Objectives, pag 65;
22. Jeremiah Doriam The Social Engineer's Playbook 2014,pag 33-35;
23. Cosmin MIHAI Securitatea sistemului informatic, Editura Dunărea de Jos, 2007, pag. 14-18;
24. Ramón J. Hontanon Securitatea în Linux, 2005, pag. 16-19;
25. By Kim Zetter Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, pag. 90-92;
26. Savas PARASTATIDIS, Jim WEBBER, VPN in Practice - Hypermedia and Systems Architecture, Third Edition NY – December 2014, pag 21-26;
27.http://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224 performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html;
28. https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/;
29. https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/;
30. https://www.kaspersky.ru/small-business-security.