Universitatea Tehnică a Moldovei

Tehnici de identificare a penetrarilor în rețele informaționale

Masterand:

Dumitru GANCEARUC

Conducător:

conf.univ., dr. Victor ABABII

Chişinău - 2020

Adnotare

La teza de master ”Tehnici de identificare a penetrarilor în rețele informaționale” a studentului grupa CRI-191M, GANCEARUC Dumitru.

Lucrarea dată constă într-o analiză a sistemului de depistare a intruziunilor deoarece securitatea sistemelor informatice şi de comunicaţii a devenit, în prezent, o problemă extrem de importantă, de care trebuie să ţină cont atât producătorii de echipamente, cât şi dezvoltatorii de aplicaţii şi integratorii de sistem, precum şi administratorii de reţea. Securitatea sistemului informațional trebuie să fie o responsabilitate asumată de către structurile de conducere ale oricărei organizații din mediul privat sau public. Structurile de conducere trebuie să asigure o direcţie clară şi gestionată corespunzător pentru indeplinirea obiectivelor stabilite prin politica de securitate.

Desigur, integritatea sistemelor informatice şi de comunicaţii, precum şi cerinţele de protejare a confidenţialităţii datelor, pot fi abordate printr-o multitudine de tehnici şi metode. În prezent, metodele de autentificare bazate pe semnătură electronică avansată, devin din ce în ce mai folosite. Pe de altă parte, soluţiile actuale de securitate se bazează pe utilizarea de componente hardware şi pe dezvoltarea de soluţii software capabile să detecteze elemente suspecte de a fi considerate intruziuni, acţiuni nepermise şi consecinţe ale acestora. Securitatea informaţiei este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei.

Teza de master este elaborată pe 82 de pagini și include: introducere, trei capitole de bază, concluzii finale și lista de surse bibliografice.

Annotation

At the master's thesis "Techniques for identifying penetrators in information networks" of the student group CRI-191M, GANCEARUC Dumitru.

This paper is an analysis of the intrusion detection system because the security of information and communication systems has become an extremely important issue, which must be taken into account by both equipment manufacturers, application developers and integrators system administrators, as well as network administrators. The security of the information system must be a responsibility assumed by the governing bodies of any organization in the private or public sphere.

The governing structures must ensure a clear and properly managed direction to meet the objectives set by the security policy.

Of course, the integrity of information and communication systems, as well as data protection requirements, can be addressed through a multitude of techniques and methods. Today, authentication methods based on advanced electronic signature are becoming more and more used.

On the other hand, current security solutions are based on the use of hardware and on the development of software solutions capable of detecting suspicious items to be considered intrusions, unauthorized actions and their consequences. Information security is a broader concept that refers to ensuring the integrity, confidentiality and availability of information.

The master's thesis is elaborated on 82 pages and includes: introduction, three basic chapters, final conclusions and the list of bibliographic sources.

Cuprins

Introducere

Dinamica tehnologiei informaţiei induce noi riscuri pentru care instituțiile trebuie să implementeze noi măsuri de control. Lucrul în reţea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar fraudă. Dezvoltarea tehnologică a fost acompaniată şi de soluţii de securitate, producătorii de echipamente şi aplicaţii incluzând metode tehnice de protecţie din ce în ce mai performante. Totuşi, în timp ce în domeniul tehnologiilor informaţionale schimbarea este exponenţială, componenta umană rămâne neschimbată.

Dorința de a aprofunda aspectele temei de cercetare legate de domeniul sistemului informatic am constatat că este important de înțeles că securitatea rețelelor este necesară instituției pentru ași proteja datele și resursele informatice. Această soluție trebuie să includă autentificare și autorizare, confidențialitatea datelor și securitatea perimetrului. Sistemele informaţionale niciodată nu pot fi în siguranţă totală, şi uneori preţul informaţiei este mult mai mare decât preţul acelor sisteme pe care se află, dacă se iau în consideraţie datele confidenţiale, secrete.

Tema cercetării în sine o considerăm de actualitate, deoarece securitatea informațională, la fel ca și protecția datelor, este o sarcină complexă, care are scopul furnizării securității, realizabilă prin implementarea unui sistem de securitate. Protecția datelor este o problemă multilaterală și complexă, care cuprinde o serie de sarcini importante. Problema securității informaționale se agraveaza permanent din cauza pătrunderii mijloacelor tehnice de prelucrare și transfer de date, dar mai ales a sistemelor de calcul, în toate domeniile societății. Astfel, penetrarea sistemelor informaţionale sau de comunicaţii electronice ale autorităţilor administraţiei publice şi ale altor instituţii şi întreprinderi de stat sau private, în cadrul cărora se gestionează informaţie sensibilă, poate duce la compromiterea confidenţialităţii, integrităţii sau disponibilităţii acestei informaţii, şi, prin urmare, la cauzarea prejudiciilor financiare sau de altă natură, inclusiv la afectarea securităţii statului.

Metodologia specifică domeniului sisteme informaționale s–a constituit dintr–un ansamblu de metode teoretice – documentarea ştiinţifică (informarea, studierea documentelor, observarea), analiza şi sinteza teoretică, generalizarea şi sistematizarea, abstractizarea şi modelarea teoretică; interpretarea surselor bibliografice teoretice; metode practic–aplicative – observarea, chestionarea, analiza, sinteza, comparaţia şi interpretarea rezultatelor. Toate acestea au permis efectuarea unei analize care aduce în atenţie şi deschide noi oportunităţi de abordare a unor idei şi perspective a sistemelor informatice, care propune soluţii realiste şi viabile în măsură să asigure identificarea intruziunilor în sisteme și rețele informaționale.

Teza de master este organizată în trei părţi, prima parte o constituie analiza amenințărilor și a riscurilor la care sunt supuse rețelele informaționale, a doua parte reprezintă componentele și

capabilitatea sistemelor de detecție a intruziunilor, iar a treia parte o constituie aplicarea propriu-zisă a metodelor şi tehnicilor elaborate pe baza părţilor teoretice şi metodologice studiate.

În partea practic–aplicativă a cercetării se propun următoarele obiective specifice:

- studierea legislaţiei Republicii Moldova privind securitatea informaţională în Republica Moldova, şi a modului de aplicare a legislației în cadrul instituțiilor;
- stabilirea, analiza şi verificarea vulnerabilităţii securităţii informaţiei;
- menținerea securitatii a infrastructurii de rețea WAN si LAN;
- analiza incidentelor de securitate și soluționarea lor, în scopul îmbunătățirii nivelului de securitate a centrelor de comunicaţii a punctelor de comandă a unităţilor şi subunităţilor Armatei Naţionale;
- menținerea documentației aferente infrastructurii actuale și elaborarea documentației noi;
- elaborarea unui plan de tratare a riscurilor pentru eficientizarea securităţii informaţiei în cadrul Sistemului de Comunicații și Informatică.

BIBLIOGRAFIE

1. STĂNESCU Mihaela, Articol: Internetul sub amenințare: virușii informatici, 9 mai 2012.
2. APETRII. Maria, Lucrare științifică, ,, Securitatea rețelelor, metode de atac și protecție" pag.5
3. PATRICIU Victor, Editura ALL Educational, Bucureşti 1994,,Securitatea reţelelor" pag.87.
4. STĂNESCU Mihaela, Articol: Internetul sub amenințare: virușii informatici, 9 mai 2012. pag 227-235
5. SULARI Victor, Curs de lecții ,, Sisteme informaționale- 1 "pag 226-227
6. APETRII Maria, Lucrare științifică ,, Securitatea rețelelor, metode de atac și protecție" pag.13-18
7. OPREA Dumitru, Suport de curs ,,Protecția și securitatea sistemelor informaționale " pag. 50-52
8. MANDY Andress, Editura SAMS 2001, Surviving Security, p.97.
9. LEGEA Nr. 299 din 21.12.2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova Publicat : 16.02.2018 în Monitorul Oficial Nr. 48-57 art Nr.122
10. MOJZI Mihai, Material de învăţare – partea II ,, Securitatea sistemelor de calcul şi a reţelelor de calculatoare" pag.40-42
11. APETRII Maria, Lucrare științifică ,, Securitatea rețelelor, metode de atac și protecție" (Accesat:22.08.20).
12. IOANA Iulia, Editura București 2013, Manual Cyberterorismul ,,O Noua Forma de Terorism" pag.15-18
13. MOJZI Mihai, Material de învăţare – partea I ,, Securitatea sistemelor de calcul şi a reţelelor de calculatoare" pag.46-47
14. ILIESCU Florin-Mihai Editura CISA, CISSP, Manual,, Politica de Securitate a Informației" pag.7-9
15. http://cisco.ctcnvk.ro/itessentials/start.html, accesat la data de 21.08.2020, ora 13.32.
16. ILIESCU Florin-Mihai Editura CISA, CISSP, Manual,, Politica de Securitate a Informației" pag.15-18.
17. Regulamentul privind asigurarea securităţii informaţionale şi utilizare a resurselor sistemului de comunicaţii şi informatică ale armatei naţionale CI-101 pag 3-4.
18. Regulamentul privind asigurarea securităţii informaţionale şi utilizare a resurselor sistemului de comunicaţii şi informatică ale armatei naţionale CI-101 pag 4-5.
19. OPREA Dumitru, Editura Polirom, Iaşi, 2003, "Protecţia şi securitatea informaţiilor" pag.79.

20. MIHAI Ioan-Cosmin, Editura Dunărea de Jos Galați, 2007 „Securitatea sistemului informatic”, pag .23-28.
21. https://cloudmania2013.com/2018/03/22/avem-iso-27001-ce-ne-mai-trebuie-pentru-alinierea-gdpr/ (Accesat:12.09.20).
22. VLADIMIRESCU Ion Manual „Sisteme de management al securității informației” Standartul ISO/IEC 27000:2014, pag 25-30
23. https://cloudmania2013.com/2018/03/22/avem-iso-27001-ce-ne-mai-trebuie-pentru-alinierea-gdpr/ (Accesat:12.10.20).
24. NECULCEA Vladislav Manual „Codul de practică al managementului securităţii informaţiilor” pag 19-25
25. VERYARD Robert, Editura Prentice Hall, New York „Informaţion modelling - practical guidance” p.83.
26. www.techopedia.com/definition/12826/host-based-intrusion-detection-system-hids (Accesat: 13.08.20).
27. https://ids.q8.com/ (Accesat:12.09.20).
28. Andrei ȘESTACOV, Articol Științific „Dezvoltarea durabilă a agenților adaptivi pentru identificarea intruziunilor în sisteme și rețele informaționale” pag.10-15.
29. GREGG M., Kim D. Inside Network Security Assessment. Guarding Your IT Infrastructure, TechRepublic pag 16.
30. ВАККА Джон Издательство Диалектика Киев, 1997 „ Секреты безопасности в Internet” pag.108
31. https://www.academia.edu/201223/SECURITATEA RC LSCRIPCARIU(Accesat:12.10.20)
32. http://datasystemssolutions.ro/consultanta securitatea datelor si sistemelor/ (Accesat:15.10.20).
33. https://cloudmania2013.com/2018/03/22/avem-iso-27001-ce-ne-mai-trebuie-pentru-alinierea-gdpr/ (Accesat:18.09.20).
34. KLANDER Lars, Editura ALL Educational, Bucureşti, 1998, Anti-hacker „ Ghidul securităţii reţelelor de calculatoare” pag.142.
35. DABIJA George „Securitatea Sistemelor de Calcul Si a Retelelor de Calculatoare - Partea I” pag 16-19.
36. Alin-Florentin OPREA, Proiect de diplomă „Sistem de detecţie şi prevenire a intruziunilor într-o reţea” pag 15-16.
37. VERYARD Robert, Editura Prentice Hall, New York „Informaţion modelling - practical guidance” pag.83.

38. APETRII Maria, Lucrare științifică ,, Securitatea rețelelor, metode de atac și protecție” pag.101-103.
39. SCRIPCARIU Luminiţa, Editura Venus, Iaşi, 2008 ,,Securitatea reţelelor de comunicaţii” pag.194.
40. DOHERTY, Jim. Cisco networking simplified / Jim Doherty, Neil Anderson, Paul Della Maggiora. - 2nd ed. ISBN: 978-1-58720-199-8 pag 225.
41. TANENBAUM Andrew, Editura Computer Press Agora ,,Reţele de calculatoare” pag.124.
42. IONESCU Dan, Alba Iulia, Editura All, 2007 ,,Reţele de calculatoare” pag.98.
43. https://despretot.info/firewall-definitie/ (Accesat:22.10.20).
44. https://despretot.info/firewall-definitie/ (Accesat:22.10.20).
45. https://www.cisco.com/ (Accesat:02.10.20).
46. https://www.cisco.com/ (Accesat:02.09.20).
47. https://support.microsoft.com/ro-ro/help/129972/how-to-prevent-and-remove-viruses-and-other-malware (Accesat:09.09.20).
48. https://suricata-ids.org/ (Accesat:11.09.20).
49. https://web.ceiti.md/lesson.php?id=7 Accesat:11.09.20.
50. Проектирование компонент управления конфигурациями и обработки событий системы обнаружения вторжений. Posibil de accesat pe https://sibac.info/studconf/science/xx/75319, pag 15-18, (Accesat:12.10.2020).
51. ȘESTACOV Andrei, ,,Teză de master în calculatoare și rețele informaționale” pag.65
52. https://stisc.gov.md/ (Accesat:15.09.2020).
53. ВАККА Джон , Секреты безопасности в Internet, 1997, pag. 108.
54. TANENBAUM Andrew, Editura Computer Press Agora ,,Reţele de calculatoare” pag.129.
55. SCRIPCARIU Luminiţa, Iaşi, Editura Venus, 2008 ,,Securitatea reţelelor de comunicaţii” pag.204.
56. https://github.com/Security-Onion-Solutions/security-onion/wiki/Snorby (Accesat:28.09.20)
57. https://bammv.github.io/sguil/index.html (Accesat:15.10.20).
58. KRON Emanuel ,,Manualul Tao of Network Security Monitoring” pag. 16-19
59. https://xakep.ru/2018/11/14/snort-rules/ (Accesat:18.08.20).
60. https://www.ionos.com/digitalguide/online-marketing/web-analytics/kibana-tutorial/ (Accesat:29.08.2020).