MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Electronică și Telecomunicații

Departamentul Telecomunicații și Sisteme Electronice

Admis la susținere
Șefă departament, conf. univ., dr.
Tîrșu Valentina, conf. univ., dr.

_____

„____”_____ 2024

Creșterea securității cibernetice în rețelele TCP/IP

Increasing cyber security in TCP/IP networks

Teză de master

Student: **Șoimu Ion**
gr. SISRC-221M

Conducător: **Ciobanu Mihai**
conf. univ., dr.

Chișinău, 2024

Rezumatul (Adnotarea)

Scopul lucrării este de a defini securitatea cibernetică la nivelș general pentru toate dezvoltările TCP/IP și de arăta performanțele utilzării in detecția intruziunilor a serviciului specializat SNORT

Snort este un sistem de detectare a intruziunilor în rețea, dar vine cu trei moduri de funcționare, toate fiind părți ale NIDS în sine. Primul mod, Sniffer Mode, afișează pachetele care tranzitează prin rețea. Poate fi configurat să afișeze diferite tipuri de pachete (TCP, UDP, ICMP), precum și ce să afișeze pachetele în sine, fie antete, fie pachete de date.

Al doilea mod de operare acordat de snort este Modul Packet Logger. Acesta permite utilizatorului să salveze pachetele detectate din modul Sniffer pentru a fi salvate pe hard disk. Prin acest mod, utilizatorul poate specifica reguli care indică ce pachete să salveze, de exemplu, pentru a salva numai pachetele referitoare la (care merg la sau vin de la) o anumită adresă.

În cele din urmă, ultimul mod este modul NIDS. Acest mod este foarte asemănător cu packet logger-ul, dar permite aplicarea unor reguli mai specifice pachetelor, rafinând pachetele care sunt de fapt înregistrate (sau alertate). Regulile aplicate sunt specificate sau incluse în fișierul de configurare care este transmis ca parametru la lansarea SNORT.

În cele din urmă, activitățile recente sunt introduse în domenii în evoluție, cum ar fi Internetul lucrurilor (IoT), sistemele de transport inteligente (ITS), tehnologiile registrului distribuit (DLT) și comunicațiile bazate pe cuanți pentru viitorul standardizării securității TIC.

Cuvinte-cheie: rețele Home Office, IPCablecom, NGN

Abstract

The aim of the paper is to define cyber security at a general level for all TCP/IP developments and to show the performance of using the specialized SNORT service in intrusion detection

Snort is a network intrusion detection system, but it comes with three modes of operation, all of which are part of NIDS itself. The first mode, Sniffer Mode, displays packets transiting the network. It can be configured to display different types of packets (TCP, UDP, ICMP) as well as what to display in the packets themselves, either headers or data packets.

The second operating mode provided by snort is Packet Logger Mode. It allows the user to save detected packets from Sniffer mode to be saved to the hard disk. In this way, the user can specify rules that indicate which packets to save, for example, to save only packets related to (going to or coming from) a particular address.

Finally, the last mode is the NIDS mode. This mode is very similar to the packet logger, but allows more specific rules to be applied to packets, refining the packets that are actually logged (or alerted). The applied rules are specified or included in the configuration file that is passed as a parameter when launching SNORT.

Finally, recent activities are introduced in evolving areas such as the Internet of Things (IoT), Intelligent Transport Systems (ITS), Distributed Ledger Technologies (DLT) and quantum-based communications for the future of ICT security standardization.

Keywords: Home Office networks, IPCablecom, NGN

CUPRINS

INTRODUCERE

Telecomunicațiile devin o modalitate fundamentală de a face afaceri în lumea extrem de conectată pentru organizațiile publice, private și non-profit, precum și consumatorii individuali și cetățenii. Beneficiile sale neîndoielnice aduc, de asemenea, noi amenințări și riscuri. Acestea pot varia pe cele care decurg din dispozitive, rețele, aplicații și servicii. Pot fi necesare noi măsuri organizaționale și tehnice de securitate pentru a aborda în mod adecvat aceste amenințări și riscuri de securitate.

Orice configurare de rețea trebuie să răspundă provocărilor globale de securitate cibernetică prin recomandări, rapoarte tehnice, documente de orientare și inițiative de informare.

Capitolele introductive oferă o privire de ansamblu asupra domeniilor cheie ale securității ITU-T împreună cu o discuție despre cerințele de bază pentru protecția aplicațiilor, serviciilor și informațiilor TIC. Sunt evidențiate amenințările și vulnerabilitățile care determină cerințele de securitate și este examinat rolul standardelor în îndeplinirea cerințelor. Sunt discutate unele dintre caracteristicile necesare pentru a proteja diferitele entități implicate în furnizarea, sprijinirea și utilizarea tehnologiei și serviciilor informației și comunicațiilor. În plus, este explicată importanța standardelor de securitate TIC și sunt date exemple despre modul în care activitatea de securitate ITU-T evoluează pentru a îndeplini cerințele de securitate.

Arhitecturile de securitate generice pentru sistemele deschise și comunicațiile end-to-end sunt apoi introduse împreună cu câteva exemple de arhitecturi specifice aplicației. Fiecare dintre aceste arhitecturi stabilește un cadru în care multiplele fațete ale securității pot fi aplicate într-o manieră consecventă.

Managementul securității cuprinde multe activități și procese asociate cu controlul și protejarea accesului la resursele de sistem și rețea, monitorizarea și raportarea evenimentelor și auditarea, precum și gestionarea informațiilor legate de aceste funcții și activități conform politicilor. Subiectele legate de managementul securității informațiilor, managementul riscurilor și managementul activelor sunt în centrul unei secțiuni. Operatorii de telecomunicații trebuie să aibă grijă de gestionarea informațiilor de identificare personală (PII), deoarece ar putea fi nevoiți să proceseze PII ale clienților lor.

Tema managementului identității este de o importanță tot mai mare ca răspuns la proliferarea furtului de identitate. Protocoalele de autentificare puternice și utilizarea caracteristicilor biometrice pentru identificarea personală și pentru autentificare devin esențiale în mediile de telecomunicații.

Sunt analizate câteva exemple specifice și abordări ale securității rețelei. Acestea includ cerințele de securitate pentru rețelele de generație următoare și rețelele de comunicații mobile care sunt în tranziție de la o singură tehnologie (cum ar fi CDMA sau GSM) la mobilitate pe platforme eterogene, folosind protocolul Internet. De asemenea, în această secțiune este inclusă o examinare a dispozițiilor de securitate pentru rețelele de acasă, televiziunea prin cablu, rețelele de senzori ubicui și rețelele definite de software.

O secțiune despre securitatea cibernetică și răspunsul la incidente analizează cel mai bun mod de a dezvolta un răspuns eficient la atacurile cibernetice și importanța înțelegerii sursei și naturii atacurilor și a schimbului de informații cu agențiile de monitorizare. Această secțiune discută despre dezvoltarea unui cadru pentru partajarea informațiilor și cerințelor legate de securitatea cibernetică pentru detectarea, protejarea împotriva, atenuarea efectelor și recuperarea atacurilor cibernetice.

Nevoile de securitate ale unui număr de domenii de aplicare sunt examinate cu un accent deosebit pe caracteristicile de securitate care sunt definite în Recomandările ITU-T. Subiectele discutate includ voce prin protocol de Internet (VoIP), televiziune cu protocol de Internet (IPTV) și servicii web.

Sunt prezentate măsuri tehnice pentru contracararea amenințărilor obișnuite ale rețelei, cum ar fi spam-ul, codul rău intenționat și programele spion, și este inclusă o discuție despre importanța notificării și difuzării în timp util a actualizărilor software și necesitatea organizării și consecvenței în gestionarea incidentelor de securitate.

Pe măsură ce adoptarea serviciilor cloud crește rapid, preocupările de securitate cresc și ele. Este prezentat un cadru de securitate bazat pe caracteristicile serviciilor de cloud computing. Controalele de gestionare a securității serviciilor cloud sunt furnizate din perspectiva clienților și furnizorilor. Discuțiile se extind la alte servicii din mediul cloud, cum ar fi sistemele de management virtual bazate pe servicii cloud.

BIBLIOGRAFIE

1. https://www.itu.int/en/publications/pages/notfound.aspx
2. https://www.itu.int/rec/T-REC-X.805/en
3. https://www.itu.int/rec/T-REC-X.810
4. https://www.itu.int/rec/T-REC-X.811
5. https://www.itu.int/rec/T-REC-X.812
6. https://www.itu.int/rec/T-REC-X.813
7. https://www.itu.int/rec/T-REC-X.814
8. https://www.itu.int/rec/T-REC-X.815
9. https://www.itu.int/rec/T-REC-X.1031/en
10. https://www.itu.int/rec/T-REC-Y.2760/en
11. https://www.itu.int/rec/T-REC-M.3016.0
12. https://www.itu.int/rec/T-REC-M.3208.2
13. https://www.itu.int/rec/T-REC-M.3210.1/en
14. https://www.itu.int/rec/T-REC-X.1157/en
15. https://www.itu.int/rec/T-REC-X.790/en
16. https://www.itu.int/rec/T-REC-X.1051/en
17. https://www.itu.int/rec/T-REC-K.87/en
18. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12287
19. https://www.itu.int/rec/T-REC-X.711/en
20. https://www.itu.int/rec/T-REC-X.740/en
21. https://www.itu.int/rec/T-REC-X.741/en
22. https://www.itu.int/rec/T-REC-Y.2001/en
23. https://www.itu.int/rec/T-REC-Y.2701/en
24. https://www.itu.int/rec/T-REC-X.1125/en
25. https://www.itu.int/rec/T-REC-X.1111/en
26. https://www.itu.int/rec/T-REC-X.1112/en
27. https://www.itu.int/rec/T-REC-X.1113/en
28. https://www.itu.int/rec/T-REC-J.160/en
29. https://www.itu.int/rec/T-REC-X.1311/en
30. https://www.itu.int/rec/T-REC-F.744/en
31. https://www.itu.int/rec/T-REC-X.1312/en
32. https://www.itu.int/rec/T-REC-Y.3300/en
33. https://www.itu.int/rec/T-REC-X.1038/en
34. https://www.itu.int/rec/T-REC-X.1042/en
35. https://www.itu.int/rec/T-REC-Y.3302/en
36. https://www.itu.int/rec/T-REC-X.1042/en

37. https://www.itu.int/rec/T-REC-X.1043/en
38. https://www.itu.int/rec/T-REC-X.1038/en
39. https://www.itu.int/rec/T-REC-X.1045/en
40. https://datatracker.ietf.org/doc/html/rfc7665
41. http://opennetworking.wpengine.com/wp-content/uploads/2014/10/openflow-switch-v1.3.4.pdf
42. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM", 2022.
43. Dinu Ţurcanu, Natalia Spinu, Serghei Popovici, Tatiana Țurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.
44. Ludmila Peca, Dinu Țurcanu. Network security: Practical examples solved to be introduced in network security. Chișinău, Publisher „Tehnica-UTM", 2023, pp. 7-232.
45. Mughal, A. A. (2022). Building and Securing the Modern Security Operations Center (SOC). International Journal of Business Intelligence and Big Data Analytics, 5(1), 1–15. Disponibil: https://research.tensorgate.org/index.php/IJBIBDA/article/view/21
46. Bulai Rodica, Ciorbă Dumitru, Țurcanu Dinu, Education in Cybersecurity, Central and Eastern European e|Dem and e|Gov Days 2019 Budapest, Hungary, 2-3 mai 2019.
47. E. Falk, S. Repcek, B. Fiz, S. Hommes, R. State and R. Sasnauskas, "VSOC - A Virtual Security Operating Center," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8254427. Disponibil: https://ieeexplore.ieee.org/abstract/document/8254427
48. Dinu Țurcanu, QUALITY OF SERVICE IN MPLS NETWORKS, Journal of Engineering Science, vol. XXVII, no. 3(2020), pp. 102-110.
49. C. Melo et al., "Availability models for hyper-converged cloud computing infrastructures," 2018 Annual IEEE International Systems Conference (SysCon), Vancouver, BC, Canada, 2018, pp. 1-7, doi: 10.1109/SYSCON.2018.8369580. Disponibil: https://ieeexplore.ieee.org/abstract/document/8369580