Universitatea Tehnică a Moldovei

Analiza procedurilor și tehnicilor pentru securizarea rețelei wireless în Radisson Blu Leogrand Hotel

Student: Bulban D.

Conducător:

Conf. Univ. dr., Nazaroi I.

Chișinău 2018

Ministerul Educației, Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Programul de masterat „Mentenanța și Managementul Rețelelor de Telecomunicații”

Admis la susținere

Șef departament:

conf. univ. dr. Bejan Nicolae

„ ” 2018

Analiza procedurilor și tehnicilor pentru securizarea rețelei wireless în Radisson Blu Leogrand Hotel

Teză de master

Masterand: Bulban D.

Conducător: Nazaroi I.

Chișinău 2018

REZUMA

În cadrul prezentei teze au fost cercetate și propuse proceduri și tehnici folosite pentru asigurarea securității rețelei wireless în hotelul Radisson Blu Leogrand. Teza este compusă din 3 capitole.

În cadrul capitolului 1 se prezintă rezultatul cercetării standardului de comunicație wireless IEEE 802.11. Sunt analizate particularitățile unei rețele bazate pe standardul IEEE 802.11, topologiile utilizare, procedeele de comunicare și protocoalele de securitate.

Capitolul 2 prezintă principalele vulnerabilități existente în cadrul rețelei wireless. În cadrul acestui capitol sunt realizate și teste de ”penetrare” a rețelei wireless, folosindu-se diferite instrumentarii software.

În capitolul 3 sunt descrise principalele proceduri și tehnici pentru asigurarea securității comunicațiilor wireless. În acest capitol este utilizat scenariul direct de securitate în cadrul hotelului Radisson Blu din Chișinău. Sunt analizate punctele de acces existente, metode de segmentare a traficului, politici de securitate, etc.

Teza conține 61 de pagini, 29 de figuri și 10 resurse bibliografice.

SYMMAR

In the present paper has been researched and proposed the wireless network security procedures and techniques used in the Radisson Blu Leogrand Hote. The thesis consists of 3 chapters.

Chapter 1 presents the result of wireless communication research under the IEEE 802.11 standard. The features of a IEEE802.11-based network, different topologies, communication procedures, and security protocols are analyzed.

Chapter 2 describes the main vulnerabilities within the wireless network. Within this chapter, various wireless penetration tests are conducted using different software tools.

Chapter 3 describes the main procedures and techniques for wireless communications security. This chapter uses the direct security scenario within the Radisson Blu Hotel in Chisinau. Existing access points, traffic segmentation methods, security policies are analyzed.

The thesis contains 61 pages, 29 figures and 10 bibliographic resources.

CUPRINS

INTRODUCERE

Sintagma de comunicație wireless, tradus direct din engleză ar fi comunicație fără fir și prezintă comunicarea la distanță prin unde electromagnetice. Istoric vorbind, această tehnologie a fost utilizată încă din secolul XIX (în 1896 fiind testat primul telegraf de către Marconi), iar dezvoltările drastice ulterioare au adus această tehnologie la nivelul pe care îl cunoaștem azi.

Din punct de vedere fizic, tehnologia wireless folosește undele electromagnetice pentru transmi- terea informației. Cele mai cunoscute tehnologii pentru comunicații wireless fiind GSM, Wi-Fi, Blu- etooth și altele.

Cu implementarea globală a tehnologiilor numite mai sus, a crescut și îngrijorarea pentru asigu- rarea securității necesare pentru fiecare tehnologie. Ca rezultat, au fost elaborate mai multe tehnici și proceduri de criptare, autentificare pentru asigurarea transmiterii securizate a informației în cadrul rețelelor.

În cadrul tezei curente ne vom referi anume la tehnologia wireless care a primit denumirea co- mercială de Wi-Fi (de la Wireless Fidelity). Și anume vom prezenta proceduri și tehnici pentru asi- gurarea securității în astfel de rețea. Rețeaua o vom considera în cadrul hotelului Radisson Blu Leo- grand din orașul Chișinău, ținând cont de faptul că autorul prezentei teze a activat în departamentul IT al acestui hotel.

Problematica curentei teze este de a stabili și a cerceta diferite tehnici și proceduri pentru asi- gurarea securității rețelei Wi-Fi în cadrul hotelului Radisson Blu.

Obiectivele tezei curente sunt următoarele:

- Cercetarea tehnologii Wi-Fi existente și a topologiilor de rețea
- Analiza și cercetarea vulnerabilităților cunoscute a rețelei Wi-Fi
- Cercetarea protocoalelor existente de securitate în cadrul rețelei Wi-Fi

- Realizare unor teste de ”penetrare” pentru evidențierea problemelor existente
- Analiza datelor în urma testelor
- Propunerea unor proceduri și tehnici pentru crearea unei rețele fiabile pentru rețeaua wi- reless din carul hotelului Radisson Blu,
- Stabilirea concluziilor referitor la tehnicile și proceduri de securitate

Întreaga teză va fi divizată în 3 capitole, în cadrul capitolului 1 se va realiza studiul bibliografic și se va prezenta nivelul actual al tehnologii wireless și a metodelor de securitate, în capitolul 2 se vor cerceta vulnerabilitățile și se vor prezenta câteva teste de ”penetrare” a rețelei, iar în capitolul 3 se vor realiza rezultatele și se vor prezenta tehnicile și procedurile necesare pentru asigurarea securității rețelei wireless.

BIBLIOGRAFIE

[1] M.Gast, „802.11® Wireless Networks: The Definitive Guide" O'Reilly, 2002, O'Reilly & Associates, Inc. 1005 Gravenstein Highway North Sebastopol, CA 95472

[2] 802.11-2016 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks, accesat: 11 noiembrie, 2017

[3] Andreas Molisch „Wireless Communications 2nd Edition ", 884 pagini, Wiley-IEEE Press; 2 edition (December 1, 2010)

[4] David D. Coleman, David A. Westcott „CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-106" , Sybex, 2014

[5] Shree Krishna Lamichhane, „Penetration Testing In Wireless Networks" Helsinki Me tropolia University of Applied Sciences Bachelor's Degree in Information Technology Thesis, 28.11.2016

[6] https://docs.kali.org/ - Documentația oficială a distributivului Linux Kali, accesat pe data de: 10.10.2017

[7] http://www.aircrack-ng.org/doku.php?id=Main#documentation – documentația oficială a pachetului software aicrack-ng, accesat pe data de 9.10.2017

[8] Mallikarjun Hangargi " Denial of Service Attacks in Wireless Networks" Northeastern University

[9] Banerji S. & Chowdhury R.S RCC - Institute of Information Technology, India, On IEEE 802.11; Wireless LAN Technology. 2013