



Universitatea Tehnică a Moldovei

**Analiza procedurilor și tehnicilor pentru
securizarea rețelei wireless în Radisson Blu
Leograd 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 Leograd. 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 Leograd 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.....	14
1. ANALIZA COMUNICAȚIEI WIRELESS SUB STANDARDUL 802.11	15
1.1 Rețele wireless	15
1.2 Standardul IEEE 802.11	16
1.3 Particularitățile unei rețele IEEE 802.11	18
1.3.1 Punct de acces (Acces Point)	18
1.3.2 Serviciul de integrare	19
1.3.3 Serviciul de distribuție.....	19
1.3.4 Identificatorul setului de servicii (Service Set Identifier).....	20
1.3.5 Setul de servicii de bază (Basic Service Set)	21
1.3.6 Identificatorul setului de servicii de bază (Basic Service Set Identifier -SSID)...	21
1.3.7 Aria serviciului de bază (Basic Service Area)	22
1.3.8 Set de servicii extins (Extended Service Set).....	23
1.3.9 Setul de bază de servicii independent (Independent Basic Service Set)	24
1.3.10 Setul de bază de servicii de tip mesh (Mesh Basic Service Set).....	25
1.4 Protocoale de securitate IEEE 802.11	26
1.4.1 Wired Equivalent Privacy (WEP).....	26
1.4.2 WPA (Wi-Fi Protected Acces).....	27
1.4.3 WPA-2 (Wi-Fi Protected Acces-2).....	28
1.4.4 Protocolul 802.1X.....	29

1.5	Concluzii	30
2.	CERCETAREA VULNERABILITĂȚILOR IEEE 802.11	31
2.1	Kali Linux	31
2.2	Punct de acces răufăcător (Rogue AP)	32
2.3	Testarea practică a vulnerabilității unui punct de acces răufăcător.....	33

2.4	”Spargerea” criptării.....	33
2.5	Testarea practică a spargerii criptării	34
2.6	Clonare MAC	37
2.7	Realizarea practică a clonării MAC	38
2.8	Evil Twin	41
2.9	Realizarea practică a atacului Evil Twin.....	42
2.10	Denial of Service (DoS).....	44
2.11	Realizarea practică a testului pentru refuzul de serviciu.....	45
3.	PROCEDURI ȘI TEHNICI PENTRU ASIGURAREA SECURITĂȚII REȚELEI WIRELESS ÎN HOTELUL RADISSON BLU LEOGRAND.....	46
3.1	Metode generale de securizare.....	47
3.2	Punctele de acces în cadrul hotelului.....	49
3.3	Securitatea pentru oaspeții hotelului	52
3.4	Segmentarea traficului.....	53
3.4.1	VLAN-urile.....	54
3.4.2	Accesul pe bază de rol (RBAC)	55
3.4.3	Securitate wireless VPN.....	56
3.5	WIPS și WIDS.....	57
3.6	Server RADIUS	58
	CONCLUZII	59
	BIBLIOGRAFIE	60

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 unele electromagnetice pentru transmiterea informației. Cele mai cunoscute tehnologii pentru comunicații wireless fiind GSM, Wi-Fi, Bluetooth și altele.

Cu implementarea globală a tehnologiilor numite mai sus, a crescut și îngrijorarea pentru asigurarea 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 comercială de Wi-Fi (de la Wireless Fidelity). Și anume vom prezenta proceduri și tehnici pentru asigurarea securității în astfel de rețea. Rețeaua o vom considera în cadrul hotelului Radisson Blu Leograd din orașul Chișinău, ținând cont de faptul că autorul prezentei teze a activat în departamentul IT al acestui hotel.

Problematika curente teze este de a stabili și a cerceta diferite tehnici și proceduri pentru asigurarea securității rețelei Wi-Fi în cadrul hotelului Radisson Blu.

Obiectivele tezei curente sunt următoarele:

- Cercetarea tehnologiei 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 tehnologiei 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 Metropolia 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 aircrack-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

