MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică şi Telecomunicaţii
Departamentul Telecomunicaţii şi Sisteme Electronice

Admis la susţinere
Şefă departament:
Tîrşu Valentina, conf. univ., dr.

_____

„____”_____ 2024

Cercetarea completă a securității rețelelor wi-fi pentru vulnerabilități, atacuri și contramăsuri

Teză de master

Student: **Vizitiv Egor,**
gr. SISRC-221M

Conducător: **Jdanov Vladimir**
conf. univ., dr.

Chişinău, 2024

ADNOTAREA

Autor: Studentul Vizitiv Egor, SISRC-221M

Titlul tezei de master: "Cercetarea completă a securității rețelelor Wi-Fi pentru vulnerabilități, atacuri și contramăsuri**"**

Structura proiectului: Conține 50 de pagini, Introducere, 3 secțiuni, Concluzie, Bibliografie.

Cuvinte cheie: Rețele fără fir, aircrack-ng, WI-FI, WPA, 802.1, vulnerabilități

Problematica studiului: -Provocarea pentru cercetarea în domeniul securității rețelelor Wi-Fi constă în natura în continuă schimbare a amenințărilor cibernetice, ceea ce implică faptul că apărarea trebuie să fie actualizată în mod constant. Vulnerabilitățile din protocoalele de criptare și autentificare, precum și posibilele atacuri asupra dispozitivelor Wi-Fi, prezintă riscuri pentru confidențialitatea și integritatea datelor. Apărarea eficientă a rețelelor fără fir necesită cercetare și dezvoltare continuă de metode inovatoare pentru a contracara amenințările cibernetice moderne.

Scopul lucrării: Cercetarea completă a securității rețelelor Wi-Fi pentru vulnerabilități, atacuri și de a lua în considerare strategii și tehnici eficiente pentru a le aborda

Obiectivile:

1. Cercetare în domeniul rețelelor fără fir;
2. Analiza configurației și a setărilor rețelei Wi-Fi pentru a identifica vulnerabilitățile;
3. Efectuarea de pentesting pentru a determina nivelul de vulnerabilitate și răspunsul rețelei la potențiale atacuri;
4. Spargerea securității WPA/WPA2 utilizând hashcat;
5. Propunerea de contramăsuri împotriva atacurilor asupra protocoalelor WEP și WPA2;
6. Elaborarea de recomandări practice pentru protejarea rețelelor wireless;
7. Scrierea unui script Python pentru scanarea Wi-FI;

Metode aplicate: Scanarea completă a securității rețelelor Wi-Fi utilizează metode de scanare activă și pasivă pentru a identifica rețelele disponibile și a analiza parametrii acestora. În plus, se efectuează o scanare a vulnerabilităților, inclusiv auditul porturilor deschise, al serviciilor și al parolelor, pentru a identifica amenințările potențiale și a aplica contramăsuri adecvate**.**

Rezultatele obținute: Rezultatele acestui studiu au scos la iveală amenințări serioase la adresa protocoalelor de criptare WEP și WPA2, evidențiind vulnerabilitățile acestora și potențialele riscuri de securitate pentru rețelele fără fir. Un pentest al acestor protocoale a confirmat securitatea lor insuficientă, ceea ce subliniază necesitatea de a trece la metode de criptare mai avansate. În plus, scriptul Python dezvoltat pentru scanarea rețelelor Wi-Fi subliniază importanța vigilenței și a adoptării unor măsuri de securitate adecvate pentru a preveni astfel de amenințări.

SUMMARY

Author: student Vizitiv Egor, SISRC-221M

Title: "Comprehensive security research of Wi-Fi networks for vulnerabilities, attacks and countermeasures**"**

Thesis structure: contains 50 pages, Introduction, 3 sections, Conclusion, Bibliography.

Keywords: wireless networks, aircrack-ng, WI-FI, WPA, 802.1, vulnerabilities.

Research problem: The challenge for Wi-Fi network security research is the ever-changing nature of cyber threats, which means that defenses must be constantly updated. Vulnerabilities in encryption and authentication protocols, as well as possible attacks on Wi-Fi devices, pose risks to data privacy and integrity. Effective defence of wireless networks requires continuous research and development of innovative methods to counter modern cyber threats.

Thesis purpose: is to analyse in depth the vulnerabilities of wireless computer networks and consider effective strategies and techniques to address them.

Objectives:

1. Research in wireless networks;
2. Analysis of Wi-Fi network configuration and settings to identify vulnerabilities.
3. Perform pentesting to determine the level of vulnerability and network response to potential attacks
4. Breaking WPA/WPA2 security using hashcat;
5.Proposed countermeasures against attacks on WEP and WPA2 protocols
6.Develop practical recommendations for protecting wireless networks.
7. Writing a Python script for Wi-FI scanning; ;

Applied methods: Full Wi-Fi network security scanning uses active and passive scanning methods to identify available networks and analyse their parameters. In addition, vulnerability scanning, including auditing of open ports, services and passwords, is performed to identify potential threats and apply appropriate countermeasures.

The obtained results: The results of this study revealed serious threats to the WEP and WPA2 encryption protocols, highlighting their vulnerabilities and potential security risks for wireless networks. A pentest of these protocols confirmed their insufficient security, highlighting the need to move to more advanced encryption methods. In addition, the Python script developed for scanning Wi-Fi networks underlines the importance of vigilance and adopting appropriate security measures to prevent such threats.

CUPRINS

INTODUCERE

În zilele noastre, rețelele Wi-Fi fără fir au devenit o parte integrantă a vieții noastre de zi cu zi, oferindu-ne confort și libertate de acces la Internet. Cu toate acestea, împreună cu această libertate fără precedent, rețelele Wi-Fi sunt, de asemenea, expuse la diverse amenințări la adresa securității care pot avea consecințe grave pentru persoane fizice, companii și societate în ansamblu.

În acest studiu, ne vom concentra pe un studiu cuprinzător al securității rețelelor Wi-Fi, explorând vulnerabilitățile acestora, potențialele atacuri și măsurile de prevenire a acestora. Scopul nostru este de a oferi cititorului o înțelegere aprofundată a stării actuale a securității rețelei fără fir și de a oferi sfaturi și strategii practice pentru a asigura o protecție fiabilă a mediului Wi-Fi.

Studierea vulnerabilităților rețelelor Wi-Fi este extrem de importantă, având în vedere că tot mai multe dispozitive se conectează la rețele fără fir, iar amenințările cibernetice devin din ce în ce mai complexe și mai diverse. Pe parcursul acestui studiu, vom lua în considerare diferite tipuri de atacuri, începând cu cele mai frecvente, cum ar fi atacurile cu parole și terminând cu metode mai complexe, cum ar fi atacurile asupra protocoalelor de criptare și phishing.

Pe lângă identificarea vulnerabilităților și a potențialelor atacuri, vom prezenta cititorilor și un set de contramăsuri care pot contribui la consolidarea securității rețelelor Wi-Fi și la prevenirea posibilelor amenințări. Aceste măsuri includ atât aspecte tehnice, cât și cele mai bune practici pentru utilizarea rețelelor Wi-Fi, precum și recomandări pentru instruirea utilizatorilor.

Securitatea rețelelor Wi-Fi a devenit o problemă urgentă și numai printr-o înțelegere profundă a amenințărilor și utilizarea eficientă a contramăsurilor, vom putea asigura protecția datelor, informațiilor personale și infrastructurii noastre. Acest studiu este destinat să devină o resursă valoroasă pentru cei care încearcă să asigure securitatea mediului lor Wi-Fi și să obțină controlul asupra resurselor lor de rețea

Relevanța subiectului securității rețelei Wi-Fi în timpul nostru este dificil de supraestimat. Rețelele Wi-Fi fără fir sunt o parte integrantă a vieții noastre de zi cu zi și acoperă aproape fiecare aspect al societății și al afacerilor.

Scopul lucrării: Cercetarea completă a securității rețelelor Wi-Fi pentru vulnerabilități, atacuri și de a lua în considerare strategii și tehnici eficiente pentru a le aborda

Obiective:

1. Cercetare în domeniul rețelelor fără fir;
2. Analiza configurației și a setărilor rețelei Wi-Fi pentru a identifica vulnerabilitățile.
3. Efectuarea de pentesting pentru a determina nivelul de vulnerabilitate și răspunsul rețelei la potențiale atacuri

4. Spargerea securității WPA/WPA2 utilizând hashcat;

5.Propunerea de contramăsuri împotriva atacurilor asupra protocoalelor WEP și WPA2

6.Elaborarea de recomandări practice pentru protejarea rețelelor wireless.

7. Scrierea unui script Python pentru scanarea Wi-FI;

BIBLIOGRAFIA

1. Kali Linux. Penetrare și testare de securitate[Text]: sat.sci.TR / S. Parasram [și colab.]. - SPb.: Petru, 2019. - 448 p .
2. Roshan P., " fundamentele construirii rețelelor locale fără fir standardul 802.11. Ghid practic pentru studiu, dezvoltare și utilizarea standardului LAN fără fir 802.11 " / P. Roshan, D. Lieri.
3. 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.
4. Gordeychik S. V., Dubrovin V. V. securitatea rețelelor fără fir. -Moscova: Intuit, 2007. – 177c
5. Flenov, M. E. Linux prin ochii unui hacker. Ediția a 4-A / M. E. Flonov. –Sankt Petersburg.: BHV-Petersburg, 2016. - 432 p .
6. Sergeev A. N. fundamentele rețelelor locale de calculatoare. Educație manual / A. N. Sergeev. - SPb.: Lan, 2016. - 184 p .
7. Tipuri de securitate și criptare a unei rețele fără fir [resursă electronică]. Mod de acces:https://help-wifi.com/nastrojka-zashhity-wi-fi-setej/tip-bezopasnosti-i-shifrovaniya-besprovodnoj-seti-kakoj-vybrat/?ysclid=lnm4mocx1u518833828
8. Tehnologiile WEP, WPA, WPA2 și WPA 3: care sunt acestea și care sunt diferențele lor? [resursă electronică]. Mod de acces: https://www.kaspersky.ru/resource-center/definitions/wep-vs-wpa?ysclid=lnm4uhqr54920057486
9. Tot ce nu știați despre securitatea WI-Fi [resursă electronică]. Mod de acces: https://club.dns-shop.ru/blog/t-280-marshrutizatoryi/72409-vse-chego-vyi-ne-znali-o-bezopasnosti-wi-fi/?ysclid=lnm4xs9r5z318418676
10. Instrumente Kali Linux [resursă electronică]. Mod de acces: https://www.kali.org/tools/.
11. 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.
12. Ludmila Peca, Dinu Țurcanu. Network security: Practical examples solved to be introduced in network security. Chișinău, Publisher „Tehnica-UTM”, 2023, pp. 7-232.
13. Instrumente populare în Kali linux [resursă electronică]. Mod de acces:https://habr.com/ru/articles/762988/
14. Proletarsky, Smirnova, Romashkina. Tehnologia rețelelor WI-Fi fără fir moderne –Moscova, 2017. - 448 p.