MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departament Telecomunicații și Sisteme Electronice

Admis la susținerea
șef departament
conf. univ., dr. Sava Lilia

_____

"_____" _____ 2023

Analiza securității pe nivele în administrarea rețelelor de comunicații

Teză de master

Student: Iovu Nicolae., gr. SISRC-211M

Coordonator: Cerbu Olga, conf. univ., dr

Chișinău, 2023

Rezumat

Autorul tezei: Iovu Nicolae, gr.SISRC-211M.

Titlul tezei de master: "Analiza securității pe nivele în administrarea rețelelor de comunicații."

Structura lucrăririi: pagina de titlu, avizul, declarația, rezumatul, introducere, 3 capitole, concluzii bibliografie.

Cuvinte-cheie: analiza securității pe nivele, analiza amenințărilor, atacuri, metode de securizare.

Problematica studiului: Analiza amenințărilor de scuritate în administrarea rețelelor de comunicații și metodele de securizare ale rețelei de comunicații pe nivele.

Scopul lucrării: Analiza securității pe nivele în administrarea rețelelor de comunicații.

Obiective:

1. Analiza noțiunilor teoretice privind proiectarea rețelelor de comunicații.
2. Analiza modelelor de bază utilizate în rețele de comunicații.
3. Analiza amenințărilor actuale în administrarea securității rețelei de comunicații.
4. Analiza metodelor de securizarea a rețelei de comunicații pe nivele.
5. Proiectarea rețelei de comunicații.
6. Implementarea și prezentarea metodei de securitzare în cadrul RC proiectat.

Metode aplicate: Pentru proiectarea rețelei de comunicații în baza căreia au fost testate metodele de securizare aplicate a fost folosit echipament de la Cisco. Pentru setarea echipamentului a fost utilizat softul Putty iar pentru testarea metodelor de securitate a fost utilizat sistemul de operare Kali Linux și instrumentul de imitare a atacurilor yersenia.

Rezultatele obținute: În urma cercetărior efectuate au fost enumărate și descrise amenințările de securitate și metodele de securizare contra acestora. S-a efectuat proiectarea unei rețele de comunicații cu echipament de la Cisco și s-au efectuat setările necesare pentru implementarea măsurilor de securitate. În cadrul rețelei proiectate au fost implementate 2 măsuri de securitate: DHCP snooping și setarea securității porturilor. În urma testării setării securității portului prin atac de umplere a tabelului de adrese MAC atacul a fost respins prin deconectarea portului cand asupra acestuia a fost trimis un număr mare de adrese MAC care depășește numărul maxim de adrese MAC setat. De menționat că atacul dat a fost efectuat asupracomutatorului din rețea.

SUMMARY

Author: Iovu Nicolae, gr.SISRC-211M.

Title: "Level security analysis in communications network administration."

The structure: title page, notice, statement, summary, introduction, 3 chapters, conclusions bibliography.

Keywords: security analysis by levels, threat analysis, attacks, security methods.

Research problem: Analysis of security threats in communication network administration and layered communication network security methods.

Thesis purpose: Level security analysis in communications network administration.

Objectives:

1. Analysis of theoretical notions regarding the design of communication networks.
2. Analysis of the basic models used in communication networks.
3. Analysis of current threats in communication network security management.
4. Analysis of the methods of securing the communication network by levels.
5. Communication network design.
6. Implementation and presentation of the securitization method within the designed RC.

Applied methods: For the design on the basis of which the communication network was designed, equipment from Cisco was used. The Putty software was used to set up the equipment and the Kali Linux operating system and the yersenia attack simulation tool wereused to test the security methods.

The obtained results: Following the research carried out, the security threats and the security methods against them were listed and described. The design of a network with equipment from Cisco was carried out and the settings necessary for the implementation of security measures were carried out. Within the designed network, 2 security measures were implemented: DHCP snooping and port security setting. After testing the port security setting by filling the MAC address table attack, the attack was rejected by disconnecting the port when a large number of MAC addresses were sent to it that exceeded the maximum number of MAC addresses set. It should be noted that the given attack was carried out on the switch in the network.

CUPRINS

INTRODUCERE

Omenirea progresează continuu, au loc noi descoperiri în domeniul tehnico-științific, excepție nu este și domeniul tehnologiilor informaționale. Se elaborează noi aplicații și dispozitive. Toate acestea se fac pentru a ne simplifica viața și a oferi utilizatorilor mari posibilități în gestionarea bussinesului. De asemenea progresul tehnologiilor informaționale permite gestionarea efecientă a informației, comunicarea între doi sau mai mulți utilizatori oriunde și oricând, partajarea fișierelor de orice tip (video, foto, document). Fiind conectați la rețea utilizatorii au posibilitatea de a gestiona careva date, de a dirija cu diferite despozitive care recepționează careva date precum senzori de temperatură, de gaz, sisteme de alarmă, dispozitive de tipul smart, însă toate aceste funcționează doar fiind conectați la o rețea fie cu fir, fie la o rețeawireless.

Desigur conectarea calculatoarelor în rețea ne oferă mari oportunități însă pe lângă avantaje sunt și mari riscuri precum cele de securitate. Odată cu evoluția tehnologiilor informaționale apar și noi amenințări la adresa utilizatorilor acestor tehnologii. Persoane răuvoitoare sau așa zișii hackeri mereu tind să obțină informații fie cu scop de spionare, fie cu scopul de extorcare a mijloacelor bănești. Cu acest scop hackerii utilizează metode precum atacuri asupra rețelei locale ale întreprinderii, virusarea calculatorului, criptarea informației, și alte mijloace de obținere a informației cu scopuri rele. Odată cu creșterea pericolelor crește și măsuri de contracararea atacurilor asupra rețelelor și protejarea datelor utilizatorilor în rețea. În prezent sunt utilizate diferite mijloace de protecție a informației și securizarea rețelei mai puțin sau mai mult efective, despre care va fi relatat în continuare.

În cadrul lucrării vor fi descrise noțiunile generale despre rețele, modelele de bazăutilizate în cadrul gestionării unei rețele de comunicații cît și nivelele din care sunt create aceste modele. Ne vom aprofunda în noțiunile de bază privind asigurarea securității în rețele pe fiecare nivel ale modelelor pe care se bazează rețelele de comunicații.

Scopul lucrării: Analiza securității pe nivele în administrarea rețelelor de comunicații.

Obiective:

1. Analiza noțiunilor teoretice privind proiectarea rețelelor de comunicații.
2. Analiza modelelor de bază utilizate în rețele de comunicații.
3. Analiza amenințărilor actuale în administrarea securității rețelei de comunicații.
4. Analiza metodelor de securizarea a rețelei de comunicații pe nivele.
5. Proiectarea rețelei de comunicații.
6. Implementarea și prezentarea metodei de securitzare în cadrul RC proiectat.

CONCLUZII

În urma elaborării acestei lucrări au fost studiate o varietate de resurse bibliografice, aceasta a fost pentru atinge scopul lucrării și anume, analiza securității pe nivele în administrareaarețelelor de comunicații. A fost proiectată rețeaua în baza căreia au fost implementate 2 metode de securizarea a nivelului 2 acestea fiind testate pe 2 tipuri de atacuri.

În urma realizării acestei lucrări au fost atinse următoarele obiective:

1. Analiza noțiunilor teoretice privind proiectarea rețelelor de comunicații.

Pentru realizarea acestui obiectiv au fostdate mai multe definiții noțiunii de rețea de comunicații astfel definind rețeau ca un sistem sau ansamblu de dispozitive finale de genul PC- uri sau dispozitive mobile(samrtphone, laptopurii interconectate între ele prin dispozitive intermediare cum ar fi router, switch pentru ca dispozitivele finale ca să poată comunica între ele. La fel a fost definită o noțiune importantă în rețele de comunicații care este protocolul de rețea care se definește ca un set de reguli care definește cum comunică entitățile în rețea. Au fost clasificate rețelele după mai mai multe prprietăți cum ar fi topologie, arhitectură, mărime. De asemenea a fost caracterizat echipamentul care este utilizat în proiectarea rețelelei de comunicații de orice mărime.

2. Analiza modelelor de bază utilizate în rețele de comunicații.

Se cunoște că în rețele de comunicație sunt utilizate două modele de bază, modelul OSI și modelul TCP/IP. Modelul OSI servește ca un model de referință pentru producătorii de chipamente de rețea iar modelul TCP/IP este un model aplicat în practică de programatorii de softuri de rețea precum browsere. Deasemenea s-a descris fiecare model în parte și a fost arătatcă modelul OSI are 7 nivele iar TCP/IP are patru, efectuând-use o anliză detaliată a fiecărui nivelale ambelor modele. La fel au fost prezentate protocoalele care sunt cunoscute pe fiecare nivel spre exemplu pe nivelul 7 al modelului OSI sunt cunoscute următoarele protocoale: HTTP, FTP, SMTP, DNS, DHCP. La fel s-a efectuat o analiză comparative a ambelor modele prezentând-use avantajele și dezavantajele ale ambelor modele.

3. Analiza amenințărilor actuale în administrarea securității rețelei de comunicații.

În urma realizării acestui obiectiv a fost stabilit că amenințările în rețele de comunicații se împart în 3 tipuri: de ordin tehnic, natural și de tip uman. Axarea în timpul studierii amenințărilor a fost făcută pe cele de tip uman. Au fost analizate amenințările pe fiecarea nivel al modelului OSI. Spre exemplu pe nivelul 3 ne putem confrunta cu asemena amenințări precum atacul DOS,

IP spoofing, sau atacul Smurf care ar pute cauza pagube material mari iar pe nivelul 2 sunt asemenea amenințări ca inundarea tabelui de adrese MAC sau DHCP spoofing care presupune atcul serverului DHCP.

4. Analiza metodelor de securizare a rețelei de comunicații pe nivele.

Pe fiecare nivel sunt mai multe sau mai puține metode de securizare a rețelei de comunicații. Spre exemplu un simplu asimplu firewall ar putea asigura securitatea rețelei de comunicații pe mai multe nivele iar controlul accesului ar asigura o bună securitate la primul nivel al modelului OSI. Dar spre exemplu efectuând careva setări am putea securiza nivelul 2 cel puțin de 2 de atacuri

5. Proiectarea rețelei de comunicații.

Pentru implementare măsurilor de securitate a fost proiectată o rețea de comunicații care constituie dintr-un switch de la Cisco 2690 și un router Cisco 4321. Ambele dispozitive au fost setate cu ajutorul softului Putty.

6. Implementarea și prezentarea metodei de securitzare în cadrul RC proiectat.

Pe rețeaua proiectată au fost implemntate și testate 2 metode de securizare:

1.Setarea porturilor ca deconectate în cazul afectării securității.
2.Activarea DHCP Spoofing.

Pentru testarea acestor metode de securitatea fost folosit sistemul de operare Kali Linux care a fost descris în cadrul acestei lucrări. Eficiența metodelor de securizare a fost prezentată în lucrare prin imagini, spre exemplu în urma testării pe atacul MAC acesta nu avut loc deoarece portul care a fost atacat s-a deconectat în urma transmiterii pe port a unui numă mare de adrese MAC ce adepășit numărul de adrese MAC maxim setat. Metoda dată la fel a fost analizată din punct de vedere financiar și a fost demonstrat că în cazul implementării proiectului nostru s-ar putea recupera în mai puțin de 4 ani.

BIBLIOGRAFIE

1. De ce este importantă securitatea cibernetică? Cât costă atacurile cibernetice? [Citat la 01.10.2022] Disponibil: https://www.europarl.europa.eu/news/ro/headlines/society/20211008STO14521/de-ce-este-importanta-securitatea-cibernetica
2. Statisticile atacurilor cibernetice pentru anul 2021, la nivel mondial. [citat la 01.11.202]Disponibi:https://xontech.md/ru/news/statisticile-atacurilor-cibernetice-pentru-anul-2021-la-nivel-mondial/
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. [citat la 01.10.2022] Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/JSS-1-2021_74-83_0.pdf
4. What Is Cybersecurity?[citat la01.10.2022] Disponibil: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works
5. Rețea de calculatoare. [citat la 04.10.2022].Disponibil:https://ro.wikipedia.org/wiki/Re%C8%9Bea_de_calculatoare
6. Network.[citat la data 04.11.202]. Disponibil:https://www.computerhope.com/jargon/n/network.htm
7. 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. [citat la data 06.11.2022]. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/JSS-1-2021_74-83_0.pdf
8. Rodica Bulai, Dinu Ţurcanu, Dumitru Ciorbă. Education in Cybersecurity. Central and Eastern European eDem and eGov Days 2019 - Conferința "Central and Eastern European eDem and eGov Days ", Budapesta, Hungary, 2-3 mai 2019. [citat la data 06.11.202]. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/33_9.pdf
9. 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. [citat la data 05.11.202]. Disponibil: http://repository.utm.md/bitstream/handle/5014/20549/Computer-networks-Practical-examples-DS.pdf?sequence=1&isAllowed=y
10. PROIECTAREA UNEI RETELE DE CALCULATOARE. [citat la 04.10.2022]. Disponibil:https://www.academia.edu/29979280/PROIECTAREA_UNEI_RETELE_DE_CALCULATOARE
11. Rețea de arie largă. [citat la 05.10.2022]. Disponibil:

https://ro.wikipedia.org/wiki/Re%C8%9Bea_de_arie_larg%C4%83

12. Global Area Network (GAN). [citat la 06.10.2022]. Disponibil: https://www.techopedia.com/definition/7368/global-area-network-gan
13. Clasificarea retelelor de calculatoare. [citat la 06.10.2022]. Disponibil: https://www.scritub.com/stiinta/informatica/retele/Clasificarea-retelelor-de-calc42385.php
14. Switch de rețea. [citat la 07.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Switch_de_re%C8%9Bea
15. Ruter. [citat la 07.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Ruter
16. Note de curs – Introducere în reţelele de calculator. [citat la 07.10.2022]. Disponibil: https://www.afahc.ro/ro/facultate/cursuri/retele_note_curs.pdf
17. Modelul OSI. [citat la 08.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Modelul_OSI
18. OSI Model. [citata la 08.10.2022]. Disponibil: https://www.imperva.com/learn/application-security/osi-model/#:~:text=The%20application%20layer%20is%20used,present%20meaningful%20data%20to%20users.
19. Definition TCP/IP. [citat la 09.10.2022]. Disponibil: https://www.techtarget.com/searchnetworking/definition/TCP-IP
20. TCP/IP. [citat la 10.10.2022]. Disponibil: https://ru.wikipedia.org/wiki/TCP/IP
21. Advantages and disadvantages of TCP/IP. [Citat la 10.10.2022]. Disponibil: https://www.ecstuff4u.com/2020/05/advantage-disadvantages-tcpip.html
22. What is Network Administration? [Citat la 10.101.2022]. Disponibil: https://www.solarwinds.com/resources/it-glossary/network-administration
23. Network administrator. [citat la 10.10.202]. Disponibil: https://en.wikipedia.org/wiki/Network_administrator
24. Planificarea Rețelei de Calculatoare la o mini-întreprindere de Design Interior. [citat la 11.10.2022]. Disponibil: https://biblioteca.regielive.ro/laboratoare/retele/planificarea-retelei-de-calculatoare-la-o-mini-intreprindere-de-design-interior-241124.html
25. Forme de manifestare a pericolelor în spațiul cibernetic. Infracțiuni informatice. [citat la 11.10.2022]. Disponibil: https://moodle.usm.md/pluginfile.php/234540/mod_resource/content/1/Forme%20de%20manifestare%20a%20pericolelor%20in%20sistemele%20informatice.pdf
26. How Computer Virus works. [citat la 14.10.2022]. Disponibil: https://www.engineersgarage.com/how-computer-virus-works/
27. What Is A Backdoor Attack?[citat la 15.10.2022]. Disponibil: https://www.wallarm.com/what/what-is-a-backdoor-attack
28. 6 types password attacks. [citat la 16.10.2022]. Disponibil:

https://www.onelogin.com/learn/6-types-password-attacks

29. Structured Query Language Injection (SQLi) - Part 1. [citat la 17.10.2022]. Disponibil: https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1
30. Network Vulnerabilities and the OSI Model. [citat la 17.10.2022]. Disponibil: https://ipwithease.com/network-vulnerabilities-and-the-osi-model/
31. What kind of attacks does SSL prevent? [citat la 17.10.2022]. Disponibil: https://www.encryptionconsulting.com/education-center/ssl-attacks/#:~:text=SSL%20Hijacking%20attacks,the%20session%20key%2FID%20information.
32. Logjam (computer security). [citat la 18.10.2022]. Disponibil: https://en.wikipedia.org/wiki/Logjam_(computer_security)
33. What Is the ROBOT Attack and How To Prevent It. [citat la 19.10.2022]. Disponibil: https://crashtest-security.com/prevent-robot-attack/
34. What is a session hijacking attack? [citat la 20.10.2022]. Disponibil: https://powerdmarc.com/what-is-a-session-hijacking-attack/
35. Man in the middle (MITM) attack. [citat la 21.10.2022]. Disponibil: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
36. What is a SYN Flood Attack? [citat la 22.10.2022]. Disponibil: https://www.f5.com/glossary/syn-flood-attack
37. Ping of Death (POD). [citat la 22.10.2022]. Disponibil: https://www.imperva.com/learn/ddos/ping-of-death/
38. Dos-атака. [citat la 25.10.2023]. Disponibil: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0#%D0%9A%D0%BB%D0%B0%D1%81%D1%81%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_DoS-%D0%B0%D1%82%D0%B0%D0%BA
39. What is a DDOS Attack? [citat la 23.10.2022]. Disponibil: https://www.onelogin.com/learn/ddos-attack
40. De ce este importantă securitatea cibernetică? Cât costă atacurile cibernetice? [Citat la 01.10.2022] Disponibil: https://www.europarl.europa.eu/news/ro/headlines/society/20211008STO14521/de-ce-este-importanta-securitatea-cibernetica
41. Statisticile atacurilor cibernetice pentru anul 2021, la nivel mondial. [citat la 01.11.202]Disponibi:https://xontech.md/ru/news/statisticile-atacurilor-cibernetice-pentru-anul-2021-la-nivel-mondial/
42. What Is Cybersecurity?[citat la01.10.2022] Disponibil: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works

43. Rețea de calculatoare. [citat la 04.10.2022].Disponibil:https://ro.wikipedia.org/wiki/Re%C8%9Bea_de_calculatoare
44. Network.[citat la data 04.11.202]. Disponibil:https://www.computerhope.com/jargon/n/network.htm

45. PROIECTAREA UNEI RETELE DE CALCULATOARE. [citat la 04.10.2022]. Disponibil:https://www.academia.edu/29979280/PROIECTAREA_UNEI_RETELE_DE_CALCULATOARE
46. Rețea de arie largă. [citat la 05.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Re%C8%9Bea_de_arie_larg%C4%83
47. Global Area Network (GAN). [citat la 06.10.2022]. Disponibil: https://www.techopedia.com/definition/7368/global-area-network-gan
48. Clasificarea retelelor de calculatoare. [citat la 06.10.2022]. Disponibil: https://www.scritub.com/stiinta/informatica/retele/Clasificarea-retelelor-de-calc42385.php
49. Switch de rețea. [citat la 07.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Switch_de_re%C8%9Bea
50. Ruter. [citat la 07.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Ruter
51. Note de curs – Introducere în rețelele de calculator. [citat la 07.10.2022]. Disponibil: https://www.afahc.ro/ro/facultate/cursuri/retele_note_curs.pdf
52. Modelul OSI. [citat la 08.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Modelul_OSI
53. OSI Model. [citata la 08.10.2022]. Disponibil: https://www.imperva.com/learn/application-security/osi-model/#:~:text=The%20application%20layer%20is%20used,present%20meaningful%20data%20to%20users.
54. Definition TCP/IP. [citat la 09.10.2022]. Disponibil: https://www.techtarget.com/searchnetworking/definition/TCP-IP
55. TCP/IP. [citat la 10.10.2022]. Disponibil: https://ru.wikipedia.org/wiki/TCP/IP
56. Advantages and disadvantages of TCP/IP. [Citat la 10.10.2022]. Disponibil: https://www.ecstuff4u.com/2020/05/advantage-disadvantages-tcpip.html
57. What is Network Administration? [Citat la 10.101.2022]. Disponibil: https://www.solarwinds.com/resources/it-glossary/network-administration
58. Network administrator. [citat la 10.10.202]. Disponibil: https://en.wikipedia.org/wiki/Network_administrator
59. Planificarea Rețelei de Calculatoare la o mini-întreprindere de Design Interior. [citat la 11.10.2022]. Disponibil: https://biblioteca.regielive.ro/laboratoare/retele/planificarea-retelei-de-calculatoare-la-o-mini-intreprindere-de-design-interior-241124.html

60. Forme de manifestare a pericolelor în spațiul cibernetic. Infracțiuni informatice. [citat la 11.10.2022]. Disponibil: https://moodle.usm.md/pluginfile.php/234540/mod_resource/content/1/Forme%20de%20manifestare%20a%20pericolelor%20in%20sistemele%20informatice.pdf

61. How Computer Virus works. [citat la 14.10.2022]. Disponibil: https://www.engineersgarage.com/how-computer-virus-works/

62. What Is A Backdoor Attack?[citat la 15.10.2022]. Disponibil: https://www.wallarm.com/what/what-is-a-backdoor-attack

63. 6 types password attacks. [citat la 16.10.2022]. Disponibil: https://www.onelogin.com/learn/6-types-password-attacks

64. Structured Query Language Injection (SQLi) - Part 1. [citat la 17.10.2022]. Disponibil: https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1

65. Network Vulnerabilities and the OSI Model. [citat la 17.10.2022]. Disponibil: https://ipwithease.com/network-vulnerabilities-and-the-osi-model/

66. What kind of attacks does SSL prevent? [citat la 17.10.2022]. Disponibil: https://www.encryptionconsulting.com/education-center/ssl-attacks/#:~:text=SSL%20Hijacking%20attacks,the%20session%20key%2FID%20information.

67. Logjam (computer security). [citat la 18.10.2022]. Disponibil: https://en.wikipedia.org/wiki/Logjam_(computer_security)

68. What Is the ROBOT Attack and How To Prevent It. [citat la 19.10.2022]. Disponibil: https://crashtest-security.com/prevent-robot-attack/

69. What is a session hijacking attack? [citat la 20.10.2022]. Disponibil: https://powerdmarc.com/what-is-a-session-hijacking-attack/

70. Man in the middle (MITM) attack. [citat la 21.10.2022]. Disponibil: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

71. What is a SYN Flood Attack? [citat la 22.10.2022]. Disponibil: https://www.f5.com/glossary/syn-flood-attack

72. Ping of Death (POD). [citat la 22.10.2022]. Disponibil: https://www.imperva.com/learn/ddos/ping-of-death/
73. Dos-атака. [citat la 25.10.2023]. Disponibil: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0#%D0%9A%D0%BB%D0%B0%D1%81%D1%81%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_DoS-%D0%B0%D1%82%D0%B0%D0%BA
74. What is a DDOS Attack? [citat la 23.10.2022]. Disponibil: https://www.onelogin.com/learn/ddos-attack

75. De ce este importantă securitatea cibernetică? Cât costă atacurile cibernetice? [Citat la 01.10.2022] Disponibil: https://www.europarl.europa.eu/news/ro/headlines/society/20211008STO14521/de-ce-este-importanta-securitatea-cibernetica
76. Statisticile atacurilor cibernetice pentru anul 2021, la nivel mondial. [citat la 01.11.202]Disponibi:https://xontech.md/ru/news/statisticile-atacurilor-cibernetice-pentru-anul-2021-la-nivel-mondial/
77. What Is Cybersecurity?[citat la01.10.2022] Disponibil: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works
78. Rețea de calculatoare. [citat la 04.10.2022].Disponibil:https://ro.wikipedia.org/wiki/Re%C8%9Bea_de_calculatoare
79. Network.[citat la data 04.11.202]. Disponibil:https://www.computerhope.com/jargon/n/network.htm

80. PROIECTAREA UNEI RETELE DE CALCULATOARE. [citat la 04.10.2022]. Disponibil:https://www.academia.edu/29979280/PROIECTAREA_UNEI_RETELE_DE_CALCULATOARE
81. Rețea de arie largă. [citat la 05.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Re%C8%9Bea_de_arie_larg%C4%83
82. Global Area Network (GAN). [citat la 06.10.2022]. Disponibil: https://www.techopedia.com/definition/7368/global-area-network-gan
83. Clasificarea retelelor de calculatoare. [citat la 06.10.2022]. Disponibil: https://www.scritub.com/stiinta/informatica/retele/Clasificarea-retelelor-de-calc42385.php
84. Switch de rețea. [citat la 07.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Switch_de_re%C8%9Bea
85. Ruter. [citat la 07.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Ruter
86. Note de curs – Introducere în rețelele de calculator. [citat la 07.10.2022]. Disponibil: https://www.afahc.ro/ro/facultate/cursuri/retele_note_curs.pdf
87. Modelul OSI. [citat la 08.10.2022]. Disponibil: https://ro.wikipedia.org/wiki/Modelul_OSI
88. OSI Model. [citata la 08.10.2022]. Disponibil: https://www.imperva.com/learn/application-security/osi-model/#:~:text=The%20application%20layer%20is%20used,present%20meaningful%20data%20to%20users.
89. Definition TCP/IP. [citat la 09.10.2022]. Disponibil: https://www.techtarget.com/searchnetworking/definition/TCP-IP
90. TCP/IP. [citat la 10.10.2022]. Disponibil: https://ru.wikipedia.org/wiki/TCP/IP
91. Advantages and disadvantages of TCP/IP. [Citat la 10.10.2022]. Disponibil: https://www.ecstuff4u.com/2020/05/advantage-disadvantages-tcpip.html
92. What is Network Administration? [Citat la 10.101.2022]. Disponibil: https://www.solarwinds.com/resources/it-glossary/network-administration
93. Network administrator. [citat la 10.10.202]. Disponibil: https://en.wikipedia.org/wiki/Network_administrator
94. Planificarea Rețelei de Calculatoare la o mini-întreprindere de Design Interior. [citat la 11.10.2022]. Disponibil: https://biblioteca.regielive.ro/laboratoare/retele/planificarea-retelei-de-calculatoare-la-o-mini-intreprindere-de-design-interior-241124.html

95. Forme de manifestare a pericolelor în spațiul cibernetic. Infracțiuni informatice. [citat la 11.10.2022]. Disponibil: https://moodle.usm.md/pluginfile.php/234540/mod_resource/content/1/Forme%20de%20manifestare%20a%20pericolelor%20in%20sistemele%20informatice.pdf

96. How Computer Virus works. [citat la 14.10.2022]. Disponibil: https://www.engineersgarage.com/how-computer-virus-works/

97. What Is A Backdoor Attack?[citat la 15.10.2022]. Disponibil: https://www.wallarm.com/what/what-is-a-backdoor-attack

98. 6 types password attacks. [citat la 16.10.2022]. Disponibil: https://www.onelogin.com/learn/6-types-password-attacks

99. Structured Query Language Injection (SQLi) - Part 1. [citat la 17.10.2022]. Disponibil: https://www.wallarm.com/what/structured-query-language-injection-sqli-part-1

100. Network Vulnerabilities and the OSI Model. [citat la 17.10.2022]. Disponibil: https://ipwithease.com/network-vulnerabilities-and-the-osi-model/

101. What kind of attacks does SSL prevent? [citat la 17.10.2022]. Disponibil: https://www.encryptionconsulting.com/education-center/ssl-attacks/#:~:text=SSL%20Hijacking%20attacks,the%20session%20key%2FID%20information.

102. Logjam (computer security). [citat la 18.10.2022]. Disponibil: https://en.wikipedia.org/wiki/Logjam_(computer_security)

103. What Is the ROBOT Attack and How To Prevent It. [citat la 19.10.2022]. Disponibil: https://crashtest-security.com/prevent-robot-attack/

104. What is a session hijacking attack? [citat la 20.10.2022]. Disponibil: https://powerdmarc.com/what-is-a-session-hijacking-attack/

105. Man in the middle (MITM) attack. [citat la 21.10.2022]. Disponibil: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

106. What is a SYN Flood Attack? [citat la 22.10.2022]. Disponibil: https://www.f5.com/glossary/syn-flood-attack

107. Ping of Death (POD). [citat la 22.10.2022]. Disponibil: https://www.imperva.com/learn/ddos/ping-of-death/

108. Dos-атака. [citat la 25.10.2023]. Disponibil: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0#%D0%9A%D0%BB%D0%B0%D1%81%D1%81%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_DoS-%D0%B0%D1%82%D0%B0%D0%BA

109. What is a DDOS Attack? [citat la 23.10.2022]. Disponibil: https://www.onelogin.com/learn/ddos-attack