International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 11 (2020), pp. 3596-3600
 https://dx.doi.org/10.37624/IJERT/13.11.2020.3596-3600

Neural Network Model for Detecting Network Scanning Attacks

Oleg Yuryevich Panischev[1], Artur Tagirovich Makridin[2], Alexey Sergeevich Katasev[3], Amir Muratovich Akhmetvaleev[4], Dina Vladimirovna Kataseva[5]

[1]Researcher, Scientific Laboratory for Near Space Research, Kazan Federal University; Russia.

Scopus ID: 8355604900; ORCID: 0000-0001-5490-912X, Kazan Federal University, Russia.

[2]Research Laboratory Assistant of the Scientific Laboratory for Microwave Design and Radio Telecommunications, Kazan Federal University; tel: +7 999 155-27-54; Scopus ID: no; ORCID: 0000-0001-8192-1917, Kazan Federal University, Russia.

[3]Doctor of Engineering Sciences, Professor, Department of Information Security Systems, Institute of Computer Technologies and Information Protection, Kazan National Research Technical University named after A.N. Tupolev "KAI", Russia. Scopus ID: 57193408902; ORCID: 0000-0002-9446-0491, Kazan National Research Technical University named after A.N. Tupolev,

[4]Candidate of Engineering Sciences, Associate Professor, Department of Information Security Systems, Institute of Computer Technologies and Information Security, Kazan National Research Technical University named after A.N. Tupolev "KAI"; Russia. Scopus ID: 57202913457; ORCID: 0000-0003-0384-9539, Kazan National Research Technical University named after A.N. Tupolev,

[5]Senior Lecturer, Department of Information Security Systems, Institute of Computer Technologies and Information Security, Kazan National Research Technical University named after A.N. Tupolev "KAI"; Russia. Scopus ID: 57193401954; ORCID: 0000-0001-6141-8329, Kazan National Research Technical University named after A.N. Tupolev,

Abstract

This paper discusses the concept and problem of detecting network scanning attacks and describes the targets of network scanning attacks. The main attack methods and approaches to scanning network ports are considered. Intrusion detection systems (IDS) are used to detect network scanning attacks. Based on the method of detecting attacks, such systems are divided into IDS, which detects attacks based on signatures, and IDS, which detects attacks based on anomalies. In practice, it is recommended that these IDS detection methods be used together. It is proposed to use a trained neural network as a tool for detecting network scanning attacks. The implementation of the neural network required to prepare the initial data for training, to determine the parameters of the network, to conduct training, and to evaluate the results of its testing. When developing a neural network model, data from the publicly available set "NSL-KDD" were used. During data processing, entries that were not related to network scanning attacks were removed from the original NSL-KDD set. After processing the initial data, the sample contained 5108 records, 3379 of which characterized normal connections, and 1729 connections were related to network scanning attacks. The Deductor modeling environment was used to build a neural network model. The structure of the constructed neural network was as follows: 11 input neurons, 1 output neuron, and one hidden layer consisting of 23 neurons. The neural network was trained using an error backpropagation algorithm. The quality of the neural network model was assessed using contingency tables with the calculation of the classification accuracy, as well as errors of the first and second kind. The values of these errors turned out to be insignificant. The constructed neural network model revealed most of the connections characterizing network scanning attacks. The neural network assessment confirmed its adequacy and the possibility of effective practical use for detecting network scanning attacks.

Keywords- network scanning attack, information security, data mining, neural network, neural network model.

I. INTRODUCTION

Currently, the issues of protecting information systems from malicious attacks, as well as improving information security policies are becoming important [1, 2]. Information flow is increasing every day. In this flow, it is more and more difficult to ensure the security of information systems and the information processed. The mechanisms for detecting cyberattacks are constantly being improved [3-5]. However, the development of mechanisms for the implementation of threats also does not stand still. Data transmission networks are the most vulnerable to attacks. In this regard, the problem of detecting network attacks is urgent.

Network attacks are malicious actions of cybercriminals, which are performed both by the attackers themselves and by the malware installed on the attacked computer [6]. The main type of network attacks is network scanning [7, 8]. The further success of other network attacks directly depends on the network scanning stage. Therefore, the identification of this particular type of network attacks is especially important. The purpose of these attacks is to identify hosts connected to the network and network services open on them (open TCP / UDP ports) [9].

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 11 (2020), pp. 3596-3600
 https://dx.doi.org/10.37624/IJERT/13.11.2020.3596-3600

II. METHODS

There are 4 main methods of scanning network ports depending on the attacker's strategy [10, 11].

1. Horizontal scanning. With this approach, an attacker checks the same port at different IP addresses. This approach is the most common.
2. Vertical scanning. This is an approach in which an attacker scans multiple ports on the same IP address.
3. Distributed vertical scanning. If multiple sources sequentially scan multiple ports at the same IP address, then this approach is called distributed vertical scanning.
4. Distributed horizontal scanning. If multiple sources sequentially scan a specific port at multiple IP addresses, then this approach is called distributed horizontal scanning.

Various utilities can be used to detect network scanning attacks, such as TCP dump, firewalls, or intrusion detection systems (IDSs) [12]. The most advanced of this list are intrusion detection systems. They help solve problems such as intrusion or network attack detection, attack prediction, vulnerability identification, attack source identification, and others.

According to the method of detecting an attack, intrusion detection systems are usually divided into the following categories [13]:

1) Signature-based attack detection;

2) Anomaly-based attack detection.

Thus, a network scanning attack can show certain signs. When an attack occurs, the intrusion detection system will identify it by signature. Also, the intrusion detection system, which knows the normal behaviour of the system, will determine the network scanning attack based on the deviation from this normal state, i.e. recognizes it as an anomaly. In practice, it is recommended to use them together based on the advantages and disadvantages of these attack detection methods.

An efficient way to detect network scanning attacks is the data mining of network traffic based on a neural network approach [14-17]. This approach is based on the creation of a neural network trained with the use of data that include the signs of a network scanning attack. As a result of training, the neural network is able to detect the presence of a network scanning attack. The complexity of this approach lies in finding a sufficient number of network traffic examples which are both normal and defining a network scanning attack to build an adequate neural network model. However, the neural network method attracts the attention of developers of intrusion detection systems with its ability to effectively solve the intrusion detection task by flexible responding to signs of network attacks, and adapt to the current conditions of their implementation.

The construction of a neural network model is preceded by the stage of selection and preparation of data for subsequent mining. In this work, the NSL-KDD dataset was selected to train the neural network to detect network scanning attacks. The data in this set is determined by 41 input parameters of network traffic and 1 output parameter, which determines the availability or unavailability of a network attack. In total, the dataset describes the patterns of 4 categories of network scanning attacks: DoS, U2R, R2L, and Probe.

When processing data from the original set of "NSL-KDD", records that are not related to network scanning attacks were removed. Also, for processing the initial data, the method of calculating Pearson's correlation was used [18], which allows one's to reduce the dimension of the input feature space. As a result of preprocessing the data, the most significant input attributes that are involved in training the neural network were selected. The final training sample contained 11 input attributes and one output (attack), as well as 5108 records, 3379 of which described normal connections, and 1729 - connections related to network scanning attacks.

III. RESULTS AND DISCUSSION

The analytical platform Deductor Studio Academic was chosen as a modelling environment for training and testing a neural network [19]. Deductor software is a user-friendly analytical platform. The analyst's work with it comes down to visual scripting. A script is a sequence of actions that allows a user to obtain useful knowledge from the source data and identify patterns through such operations as data import, data processing, data visualization, and others.

When training a neural network in the Deductor modeling environment, the results of data classification were obtained; they are presented in Table 1 [20].

Table 1. Model Results on Training Data

Actually	Classified		
	False	True	Total
False	3351	28	3379
True	82	1647	1729
Total	3433	1675	5108

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 11 (2020), pp. 3596-3600
 https://dx.doi.org/10.37624/IJERT/13.11.2020.3596-3600

Based on the data presented in Table 1, we can conclude that the classification accuracy of data from a training sample of 5108 records was 97.85%. At the same time, 3379 records in the training set accounted for normal network connections, and 1729 records corresponded to network attacks.

When testing the neural network in the Deductor modeling environment, the data classification results presented in Table 2 were obtained.

Table 2. Model Results on Testing Data

Actually	Classified		
	False	True	Total
False	1184	16	1200
True	48	818	866
Total	1232	834	2066

Based on the data presented in Table 2, we can conclude that the classification accuracy of data from the test sample with a volume of 2066 records was 96.9%. At the same time, 1200 records in the test sample accounted for normal network connections and 866 records corresponded to network attacks.

Based on the results of the neural network model operation on test data, errors of the first and second kind were calculated using the following formulas [21]:

- Error of the first kind $E_1 = \frac{n_1}{N_1} * 100\%$, where n_1 – the number of attacks in the sample mistakenly classified as normal connections, N_1 – total number of attacks in the sample;

- Error of the second kind $E_2 = \frac{n_2}{N_2} * 100\%$, where n_2 is the number of normal connections in the sample mistakenly classified as attacks, N_2 – total number of normal connections.

As a result of calculations, the error of the 1st kind was $E_1 = \frac{n_1}{N_1} * 100\% = \frac{48}{866} * 100\% = 5{,}54\%$, and the error of the 2nd kind was $E_2 = \frac{n_2}{N_2} * 100\% = \frac{16}{1200} * 100\% = 1{,}33\%$.

The constructed neural network model correctly identified most of the connections characterizing the network scanning attack. The obtained values of errors of the first and second kind are also not critical, and, therefore, the results of neural network modelling are adequate.

IV. SUMMARY

Although network scanning attacks are not very harmful by themselves, their main danger is the further implementation by an attacker of other types of attacks on vulnerabilities identified during the network scan. Identifying network scanning attacks is challenging because of the challenge of identifying malicious connections from general network traffic. In this work, a neural network approach was used to detect network scanning attacks. The constructed neural network model successfully coped with the task of identifying and classifying malicious connections. Thus, the model is adequate and suitable for use in intelligent detection systems for network scanning attacks [22]. As a direction for further research, it is proposed to develop other models and evaluate the results obtained on the basis of other methods of data mining [23-28]. In addition, the actual construction and practical use of intelligent decision support systems [29-34] to identify and prevent network attacks on computer systems.

V. CONCLUSIONS

Thus, the research has been used to solve the problem of detecting network scanning attacks based on the construction of a neural network model, as well as assessing its effectiveness. The results of the studies have shown the effectiveness of the proposed approach to solving the problem. The constructed neural network showed high accuracy in terms of minimizing errors of the first and second kind. This indicates its effectiveness and practical use for detecting and preventing network scanning attacks.

ACKNOWLEDGEMENTS

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

REFERENCES

[1] Diesch R, Pfaff M, Krcmar H. A comprehensive model of information security factors for decision-makers. Computers & Security. 2020 May 1;92:101747.

[2] Hina S, Dominic PD. Information security policies' compliance: a perspective for higher education institutions. Journal of Computer Information Systems. 2018 Mar 30.

[3] Misra S, Singh R, Mohan SV. Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. Sensors. 2010 Apr;10(4):3444-79.

[4] Katasev AS, Kataseva DV. Neural network diagnosis of anomalous network activity in telecommunication systems. In2016 Dynamics of Systems, Mechanisms and Machines (Dynamics) 2016 Nov 15 (pp. 1-4). IEEE.

[5] Zhi T, Liu Y, Wu J. A Reputation Value-Based Early Detection Mechanism Against the Consumer-Provider Collusive Attack in Information-Centric IoT. IEEE Access. 2020 Feb 24;8:38262-75.

[6] Saied A, Overill RE, Radzik T. Artificial Neural Networks in the detection of known and unknown DDoS attacks: Proof-of-Concept. InInternational Conference on Practical Applications of Agents and Multi-Agent Systems 2014 Jun 4 (pp. 309-320). Springer, Cham.

[7] Rajeswari PVN, Rasagna B, Sireesha K, Shahina Begum SK. Network intrusion detection techniques and network attack types. International Journal of Recent Technology and Engineering. 2019;8(8):934-940.

[8] Bhowmik J, Daryanani PL, Mazumdar SN, Krishnan SR. Implementing different types of attacks in network and their mitigation. International Journal of Pharmacy and Technology. 2016;8(4):26101-26116.

[9] Pawar MV, Anuradha J. Network security and types of attacks in network. Procedia Computer Science. 2015 Jan 1;48:503-6.

[10] Makwana RRS, Tomar DS. A network forensic framework for port scanning attack based on efficient packet capturing. International Journal of Innovative Technology and Exploring Engineering. 2019;8(12):4632-4641.

[11] Han X, Ma Y. A new method about port scan of network hosts. Key Engineering Materials. 2011; 480: 190-194.

[12] Ngo DM, Pham-Quoc C, Thinh TN. Heterogeneous hardware-based network intrusion detection system with multiple approaches for sdn. Mobile Networks and Applications. 2019 Nov 20:1-5.

[13] Rajendra PP, Shivashankar. Energy secured intrusion detection system and analysis of attacks for mobile ad-hoc networks. Journal of Communications. 2020;15(5):406-414.

[14] Farhana K, Rahman M, Ahmed MT. An intrusion detection system for packet and flow based networks using deep neural network approach. International Journal of Electrical and Computer Engineering. 2020 Oct 1;10(5):5514.

[15] Katasev AS, Emaletdinova LY, Kataseva DV. Neural Network Model for Information Security Incident Forecasting. In2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) 2018 May 15 (pp. 1-5). IEEE.

[16] Aleesa AM, Zaidan BB, Zaidan AA, Sahar NM. Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions. Neural Computing and Applications. 2020 Jul;32(14):9827-58.

[17] Pacheco J, Benitez VH, Félix-Herrán LC, Satam P. Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes. IEEE Access. 2020 Apr 15;8:73907-18.

[18] Jebarathinam C, Home D, Sinha U. Pearson correlation coefficient as a measure for certifying and quantifying high-dimensional entanglement. Physical Review A. 2020 Feb 24;101(2):022112.

[19] Lomakin N, Shokhnekh A, Sazonov S, Polianskaia A, Lukyanov G, Gorbunova A. Hadoop and Deductor Based Digital Ai System for Predicting Cost of Innovative Products in Conditions of Digitalization of Economy. InProceedings of the 2019 International SPBPU Scientific Conference on Innovations in Digital Economy 2019 Oct 24 (pp. 1-8).

[20] Sulewski P. Some contributions to practice of 2× 2 contingency tables. Journal of Applied Statistics. 2019 Jun 11;46(8):1438-55.

[21] Zhang Q, Xia D, Wang G. Three-way decision model with two types of classification errors. Information Sciences. 2017 Dec 1;420:431-53.

[22] Ernawati T, Fachrozi MF, Syaputri DD. Analysis of Intrusion Detection System Performance for the Port Scan Attack Detector, Portsentry, and Suricata. InIOP Conference Series: Materials Science and Engineering 2019 Nov (Vol. 662, No. 5, p. 052013). IOP Publishing.

[23] Katasev AS. Neuro-fuzzy model of fuzzy rules formation for objects state evaluation in conditions of uncertainty. Computer research and modeling. 2019;11(3):477-92.

[24] Chupin MM, Katasev AS, Akhmetvaleev AM, Kataseva DV. Neuro-Fuzzy Model in Supply Chain Management for Objects State Assessing. Int. J Sup. Chain. Mgt Vol. 2019 Oct;8(5):201.

[25] Perfilieva IG, Yarushkina NG, Afanasieva TV, Romanov AA. Web-based system for enterprise performance analysis on the basis of time series data mining. InProceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry"(IITI'16) 2016 (pp. 75-86). Springer, Cham.

[26] Dagaeva M, Garaeva A, Anikin I, Makhmutova A, Minnikhanov R. Big spatio-temporal data mining for emergency management information systems. IET

Intelligent Transport Systems. 2019 Sep 5;13(11):1649-57.

[27] Anikin IV, Makhmutova AZ, Gadelshin OE. Symmetric encryption with key distribution based on neural networks. In2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) 2016 May 19 (pp. 1-4). IEEE.

[28] Emaletdinova LY, Kabirova AN. Methods of Constructing the Neural Network Models of Regulators for Controlling a Dynamic Object with Smooth Monotonous Behavior. Russian Aeronautics. 2019 Apr 1;62(2):213-21.

[29] Radhi AM. Risk assessment optimization for decision support using intelligent model based on fuzzy inference renewable rules. Indonesian Journal of Electrical Engineering and Computer Science. 2020;19(2):1028-1035.

[30] Mukhametzyanov F, Katasev AS, Akhmetvaleev AM, Kataseva DV. The neural network model of DDoS attacks identification for information management fail. International Journal of Supply Chain Management. 2019;8(5):214-218.

[31] Kizim AV, Kravets AG. On systemological approach to intelligent decision-making support in industrial cyber-physical systems. Studies in Systems, Decision and Control. 2020;260:167-183.

[32] Alekseev A, Katasev A, Kirillov A, Khassianov A, Zuev D. Prototype of classifier for the decision support system of legal documents. CEUR Workshop Proceedings. 2020; 2543:328-335.

[33] Alekseev AA, Katasev AS, Khassianov AF, Tutubalina EV, Zuev DS. Intellectual information decision support system in the field of economic justice. CEUR Workshop Proceedings. 2018; 2260: 17-27.

[34] Bolshakov AA, Kulik A, Sergushov I, Scripal E. Decision support algorithm for parrying the threat of an accident. Studies in Systems, Decision and Control. 2020; 260: 237-247.

Oleg Yurievich Panishchev is a researcher at the Research Laboratory of Near Space Research, Kazan (Volga Region) Federal University. He graduated from Yelabuga State Pedagogical University with a degree in Physics, Informatics and Computer Science in 2003. Research interests: Time Series Analysis, methods of analysis of non-equilibrium distributed systems.

Artur Tagirovich Makridin is a Research Laboratory Assistant for Microwave Design and Radio Telecommunications, Kazan (Volga Region) Federal University. He graduated from Kazan (Volga Region) Federal University with a degree in radio physics in 2018. Research interests: methods of mathematical modelling of physical processes, automation of scientific experiments.

Aleksey Sergeevich Katasev - Doctor of Engineering Sciences, Professor of the Department of Information Security Systems in the Institute of Computer Technologies and Information Security, Kazan National Research Technical University named after V.I. A.N. Tupolev “KAI” (KNRTU-KAI). He graduated from the Yelabuga State Pedagogical Institute with a degree in Physics, Informatics and Computer Engineering in 2002, as well as with a master's degree from KNRTU “KAI” in the direction of Informatics and Computer Engineering in 2018. He defended his doctoral thesis in KNRTU “KAI” in 2019. His research interests: data mining technologies, formation of knowledge bases of expert systems, neural network, fuzzy and neuro-fuzzy modelling.

Amir Muratovich Akhmetvaleev - Candidate of Engineering Sciences, Associate Professor of the Department of Information Security Systems in the Institute of Computer Technologies and Information Security, Kazan National Research Technical University named after A.N. Tupolev “KAI” (KNRTU KAI). He graduated from Kazan State Technical University named after A.N. Tupolev in the specialty "Information security of telecommunication systems" in 2008, as well as with a master's degree from KNRTU “KAI” in the direction of "Informatics and computer technology" in 2012. He defended his candidate thesis in KNRTU “KAI” in 2018. Research interests: data mining, neural network modelling, assessment of human functional states by pupillary responses to changes in illumination.

Dina Vladimirovna Kataseva - postgraduate student, senior lecturer in the Department of Information Security Systems in the Institute of Computer Technologies and Information Security, Kazan National Research Technical University named after A.N. Tupolev “KAI” (KNITU “KAI”). She graduated from the Kazan State Financial and Economic Institute with a degree in Accounting, Analysis and Audit in 2008, and with a master's degree from KNRTU “KAI” in the direction of Informatics and Computer Engineering in 2018. Research interests: intellectual analysis of time series, fuzzy logic, neural networks, decision support systems.