https://doi.org/10.46335/IJIES.2022.7.9.6 **e-ISSN: 2456-3463**
Vol. 7, No. 9, 2022, PP. 28-32

International Journal of Innovations in Engineering and Science, www.ijies.net

Role of Intrusion Detection System in Network Security and Types of Cyber Attacks-A Review

Swati Mirlekar [1], Komal Prasad Kanojia [2]

[1]Assistant Professor, Department of Electronics & Telecommunication Engineering St. Vincent Pallotti College of Engineering & Technology, Nagpur, India,440010
[2]AssistantProfessor, Department of Electronics & Communication
RKDF Institute Of Science And Technology, Bhopal Srk University Bhopal, MPIndia,Pin462026

sonalkharb@gmail.com

***Received on**: 11 June ,2022* ***Revised on**: 06 August ,2022,* ***Published on**: 09 August ,2022*

***Abstract-** As there is rapid advancement in the field of computer network and internet technology network security has become important issue. Many attacks are increasing day by day. An Intrusion Detection System (IDS) detects for any malicious activity in network and keeps alerts when detected. There is insufficiency of awareness of these attacks which are vulnerable to individuals, organization& agencies.[1] It is a need to understand the different types of attacks on network so as to take appropriate actions to mitigate it.[10] study of different types of cyber attacks its strategies and characteristics will help to develop a strong Intrusion detection system using some algorithms.*

Keywords- Intrusion Detection System (IDS) and its types, Network security, Types of Cyber Attacks.

I –INTRODUCTION

In view of sharing data the computer network is created. When computers are connected in network the data and files can be shared.[1] The user can communicate with other devices through networking. A computer network links two or more devices with each other. A computer network consists of some nodes, sub nodes, some hardware and some software. Every node consists of some address. All the host nodes and sub nodes are identified by their addresses.

The networks can be divided on the basis of communication medium such as wired network and wireless network it can be divided on the basic of Division based on area covered as Local Area Network (LAN), Metropolitan Area Network (MAN)and Wide Area Network (WAN), Based on types of communication Point to Point networks, Broadcast networks, Based on type of architecture P2P Networks, Client – Server Networks, Hybrid Networks

Hardware threats are easy to detect. The threat can harm only devices. But the software threat can harm the useful data. Expecting high features from software leads to insecurity in networks which leads to the four goals of software that are Confidentiality, Integrity, Availabilityand Authenticity. [2]

Application software always scan for the network towards any malicious act for violating the standard rules and regulations of the network.

With the new updating in technology cybercrime rate is also increasing which continuously gives rise to new types of cyber-attacks, different techniques that allow attackers to enter into more secure environment. e. M. Uma and G. Padmavathi (2013) [1]

There is less amount of understanding in mitigating the attacks by using some techniques, strategies of attackers, its possible impacts which may not make secure our computer security. The nature, complexity and severity of these attacks are increasing over a period of time.

This paper reviews the insight on Intrusion detection system, techniques. Security background and the

https://doi.org/10.46335/IJIES.2022.7.9.6 e-ISSN: 2456-3463
Vol. 7, No. 9, 2022, PP. 28-32

International Journal of Innovations in Engineering and Science, www.ijies.net

challenges in Network systems. Further we are focusing of Cyber attack & its strategies. Best Practices to Protect from Cyber Threats are discussed. The comparison implementation of cyber attacks detection techniques also discussed.

II- INTRUSION DETECTION SYSTEM

In network security any unauthorized access is called as intrusion. Intruder is a person who gives access to this malicious activity. There needs to be a software that will detect this unauthorized access and it is called as an Intrusion Detection System

It is a software or a system that checks and keeps track of network traffic and detects an intrusion or unwanted activities in the network. There are two types of intruders Inside intruder and outside intruder. Inside intruder is a legitimate user who misuses the privileges given to him whereas outside intruder penetrates the security as a legitimate user. IDS helps to

- Monitor regular function of network traffic.
- Different patterns in the network continuously to compare with normal functioning.
- To make alerts when any unauthorized access is detected.

Different types of Intrusion Detection systems are classified on the basis of different techniques and methods.

Network Based intrusion detection system (NIDS)[3]

NIDS is responsible to monitor the traffic through all the connected devices and generate the alarm to the admin for any intrusion. It can be installed where the firewall is installed.

Host Intrusion Detection System (HIDS)[4]

HIDS is installed the devices which are independly connected to the network. The traffic for incoming and and outgoing packets can be monitored.Fileslog ,misplaced information can be monitored and sends alert for any mismatch.

Distributed Intrusion Detection System (DIDS)

It contains the network sensors that work for both NIDs and HIDS. All the sensors that are connected in network reports to the centralized administrator. If any intrusion happens immediate information is updated. (Fig 1)

IDS can be classified on the basis of detection methods:

Signature Based Intrusion Detection Method

Identification of different signature pattern with matched signatures is noted in this method. Different system has different signature pattern. Examples includes CISCO NIDS, SNORT, BRO, NETPROWLER

Anomaly Based Intrusion Detection Method

Normal traffic s compared against the established traffic for any deviation high false positive rate is shown.

Examples includes OSSEC [5], ALAD AND PHAD.

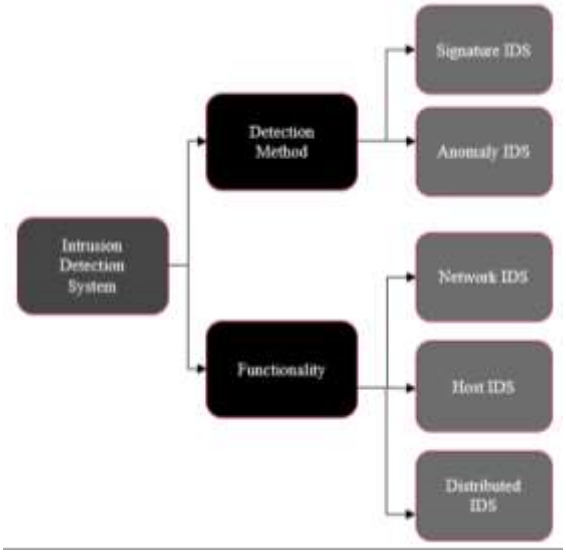

Fig 1: Overall System Diagram for Intrusion Detection system

SECURITY BACKGROUND

Confidentiality, Availability, Authentication, Integrity are four major security goals for network security.[9].

Confidentiality: It is the privacy of the network to avoid any unauthorized access. The right person is authenticated to check and see the data and no other person is allowed from protection point of view. It can be done via Data encryption method Tools for Confidentiality are Encryption, Access Control, Authentication, Authorization and Physical Security.

Availability: To keep the data identity in true sense the integrity is must so that no unauthorized person can modify it. Genuine data is maintained. Tools for Integrity are Backups, Checksums, Data Correcting Codes & Availability.

Availability:

The authenticated person is allowed to access and modify the data on perfect time. Reliability of the data is maintained. Complete access is given to only authorized people Tools for Availability are Physical Protections & Computational Redundancies

Challenges of Intrusion Detection Systems (IDS)

False alarm is the major concern that needs to be focused for IDS [2]Different algorithm and software need to be defined to avoid this false alarm issue. System configuration is needed to identify any

https://doi.org/10.46335/IJIES.2022.7.9.6 e-ISSN: 2456-3463
Vol. 7, No. 9, 2022, PP. 28-32

malicious activity is taking place. If the system behaves in abnormal activity the alarm should be sent to system administrator.

IDS keeps alerts for network They can only raise alerts for any suspicious activity but they incapable of resolving the issues. The good administrator can keep eye on these types of alerts an expert personal will take care of these threats.

Different attacks have different pattern to identify sometimes the new threat have different patens than the normal behavior. In these types of threats also Intrusion Detection Systems IDS. So IDS should be trained with new algorithms so as to analyses and catch the misbehaviors of all the threats and take immediate actions against it.

III- CYBER-ATTACK

As there are advancements in cyberspace and internet more and more people are facing issues of cyber attacks. These attacks are not only affecting on individual person but also on organization also. These attacks are known as targeted attacks and non-targeted attacks. During attacks the threats can steal damage, intellectual property, computer assets or any other important data.

[10][14]Many notations of different types of cyber-attacks and cybercrimes in literatures. They all have the common target to spoil the security goals of network system i.e., confidentiality, integrity and availability of data. Many scientists and researchers are trying to focus on types of attacks, intrusions and remedies to mitigate it.

Man in the middle attack

Is the type of attack when the communication between terminal A and B is hacked by the attacker before it sends to the source Bathe sensitive information is leaked to the attacker because of the unauthorized access. Repeated attempts are given by attacker to steal the information between source A and source B. The sensitive information like passwords and encryption keys are

steal by this man in the middle attack.

*DDoS [13] (Distributed Denial of Service)*The server becomes inoperable since the available data is flooded by the to the victim by the attacker by giving commands.

Malware is a type of attack which will use specific software generated by the attacker to violate the security goals of the network security system. Most common types of malwares are: viruses, worms, Trojans, spyware, ransom ware, adware and shareware/ironware.

Phishing can be termed as a technique which aims at stealing the user's private information considering masquerading as trustful resource. Social engineering is described as a general term which refers gaining information from an unauthorized access by the means of human interaction.[10]

Fig 2-Types of Cyber attacks

SQL Injection

A Structured Query Language (SQL) injection attack happens by use of uploading the malicious SQL scripts. If the attacker is successful for injection of database. It can edit, misuse, update view the database which may be very important information scripts.

Zero-day Exploit

A zero-day attack occurs Cybercriminals exploits the system even though the software or hardware vulnerability is announced the network administrator even don't get a time to take action on the specific threat.

Ransom ware

This type of attack is a malware attack where the attacker steals the personal information of the person and make changes in it by encryption and unless and until some ransom is paid. the information will not be given back till that time he or she will be threatened.

Here are some of the common sources of cyber threats*: Nation [16]States, Criminalgroups, Hackers, Terrorist Groups, Hacktivists, Malicious Insiders and Corporate Spies*

Table I: Implementation techniques of different cyber security attacks.

https://doi.org/10.46335/IJIES.2022.7.9.6 **e-ISSN: 2456-3463**
Vol. 7, No. 9, 2022, PP. 28-32

International Journal of Innovations in Engineering and Science, www.ijies.net

Ref no	***Dataset***	***Algorithm***	***Implementation field***	***Description & Performance***
17	KDD cup99	hybrid K means and KNN	Network traffic action	99.99% rate of detection, time 0.18
15,18	UNS WNB15	CNN, WDLSTM	IDS in big data set	accuracy 97.1%
19	ISCX 2012	K Means, decision Tree, Random Forest	K Apache Spark for anomaly detection	RF acc 99.5%, DT acc 93.5%
20	NSL-KDD	DNN	IoT Apps.	DNN type- anomaly 98% and for other attack types 97%
21	UNS W-NB15	Hybride method	Anomaly IDS model	Hybrid method acc of 87.74% over performance of 10 classes
22	MOD BUS	NB, DT J48, OneR, ANN DBSCAN	Application to detect cyber-attacks	DT J48 algorithm performs 0.995 better performance
23	CSIC HTTP 2010	J48, DT, NB One R	E-web application	DT J48 good result detection rate of 94.5%.
24	Hacked reath Network attack	WOA	Cloud computing	WOA accuracy 80%

Characteristics of Cyber Attacks

Attacker steals important data from government agencies and organization. In order to hack the data Attacker, follow some characteristics [1] Harmonized, Organized, Enormous, Regimented, scrupulously designed, not spontaneous or ad hoc Demanding Time and Resource

Best Practices to Protect from Cyber Threats [11]

- Seft induced threat programs can be developed
- Working staff can be trained for anynetwork misbehavior activity
- Maintain rules and regulations.
- To make a plan of responses on cyber attacks
- Updating in software on regular basis.
- To take backup of system data.
- To initiate simulations on attacks like phishing.
- To maintain security of website with https

IV-CONCLUSION

Intrusion detection system reduces the no of intrusions on network security by giving alerts. Human life is engrossed with computers and internet nearly in all activities of day-to-day life. In recent years, Cyber security has gained much implicit importance. Cyber threats try to steal data from government agencies. These attacks make impact on confidentiality, integrity, availability and security of the networks.

The only solution for this kind of issues to understand the type of attack [26] and to take necessary actions to prevent our data and network. Various deep learning and machine learning algorithms are adopted in order to reduce network attacks. [12] It is a need to develop the perfect cyber security model based on these concepts. With the advancements in Intrusion detection systems different approaches to improve the network security in suitable way.

REFERENCES

[1] *M. Uma and G. Padmavathi," A Survey on Various Cyber Attacks and Their Classification", International Journal of Network Security, Vol.15, No.5, PP.390-396, Sept. 2013*

[2] *Venkata Ramesh Bontupalli Tarek M. Taha," Comprehensive Survey on Intrusion Detection on various Hardware and Software.*

[3] *Sourdis, loannis and Dionisios Pnevmatikatos," Pre-Decoded CAM's for efficient and High speed NIDs pattern matching." Field Programmable Custom Computing Machines,2004. FCCM2004.12th Annual IEEE National ,2014*

[4] *Ying, Lin, Zhang Yan & Ou Yang-jia." The design and Implementation of host-based intrusion detection system." Intelligent Information Technologyand Security Informatics (IITSI),2010Third International Symposium on IEEE,2010.*

[5] *Bray, Rory, Daniel Cid and Andrew Hay.OSSEC host-based intrusion detection guide. Syngress,2008.*

[6] *Jibi Mariam Biju1, Neethu Gopal2, Anju J*

Prakash,"CYBER ATTACKS AND ITS DIFFERENT TYPES",International Research Journal of Engineering and Technology (IRJET)Volume: 06 Issue: 03 | Mar 2019.

[7] *Azar Salih,Subhi T. Zeebaree,Sadeeq Ameen,"A Survey on the Role of Artificial Intelligence, Machine Learning and Deep Learning for Cybersecurity Attack Detection",7th International Engineering Conference Research &Innovation amid Global Pandemic (IEC2021) Erbil, Iraq*

[8] *Venkata Ramesh Bontupalli Tarek M. Taha Department of ECE University of Dayton, Dayton, OH 45469, USA,"Comprehensive Survey on Intrusion Detection on various hardware and software"*

[9] *Mini Sharma,Aditya Tandon,Subhashini Narayan,Bharat Bhushan,"Classification and Analysis of Security Attacks in WSNs and IEEE 802.15.4 Standards: A Survey",2017 IEEE*

[10] *Types Of Cyber-Attacks, And How To Prevent Them-E-Book, Les, Olson It Company*

[11] *S. Latha,Dr. Sinthu Janita Prakash,"A Survey on Network Attacks and Intrusion Detection Systems",2017 International Conference on Advanced Computing and Communication Systems (ICACCS -2017), Jan. 06 – 07, 2017, Coimbatore, INDIA*

[12] *L.Haripriya,M.A. Jabbar,"Role of Machine Learning in Intrusion Detection System: Review",Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018) IEEE Conference Record # 42487; IEEE Xplore ISBN:978-1-5386-0965-1*

[13] *L. Meyer; W.T. Penzhorn "Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks", IEEE AFRICON 2004*

[14] *Wang, P., Liu, J., 2014. Threat analysis of cyber-attacks with Attack, Journal of Information Hiding and Multimedia Signal Processing, 5, 4, 778:787*

[15] *Thudumu, S.; Branch, P.; Jin, J.; Singh, J.J. A comprehensive survey of anomaly detection techniques for high dimensional big data. J. Big Data 2020, 7, 1–30.*

[16] *S. Cheung, "Modeling multistep cyber-attacks for scenario recognition," in Proceedings of the Third DARPA Information Survivability Conference and Exposition, vol. I, pp. 284-292, Washington, D. C., Apr. 22-24, 2003.*

[17] *Y. Y. Aung and M. Myat Min, "Hybrid Intrusion Detection System using K-means and K-Nearest Neighbors Algorithms," Proc. - 17th IEEE/ACIS Int. Conf. Comput. Inf. Sci. ICIS 2018, pp. 34–38, 2018.*

[18] *[34] M. M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, "A hybrid deep learning model for efficient intrusion detection in big data environment," Inf. Sci. (Ny)., vol. 513, pp. 386–396, 2020.*

[19] *M. Jain and G. Kaur, "A novel distributed semi-supervised approach for detection of network-based attacks," Proc. 9th Int. Conf. Cloud Comput. Data Sci. Eng. Conflu. 2019, pp. 120–125, 2019.*

[20] *C. Liang, B. Shanmugam, S. Azam, M. Jonkman, F. De Boer, and G. Narayansamy, "Intrusion Detection System for Internet of Things based on a Machine Learning approach," Proc. - Int. Conf. Vis. Towar. Emerg. Trends Commun. Networking, ViTECoN 2019, pp. 1–6, 2019.*

[21] *Z. Chkirbene, S. Eltanbouly, M. Bashendy, N. Alnaimi, and A. Erbad, "Hybrid Machine Learning for Network Anomaly Intrusion Detection," 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020, pp. 163–170, 2020.*

[22] *R. Das and T. H. Morris, "Machine learning and cyber security," 2017 Int. Conf. Comput. Electr. Commun. ICCECE2017, 2018.*

[23] *S. Sharma, P. Zavarsky, & S. Butakov, "Machine Learning based Intrusion Detection Web-Based Attacks," Proc. - 2020 IEEE 6th Intl Conf.*

[24] *V. Ravindranath, S. Ramasamy, R. Somula, K. S. Sahoo, and A. H. Gandomi, "Swarm Intelligence Based Feature Selection for Intrusion and Detection System in Cloud Infrastructure," 2020 IEEE Congr. Evol. Comput. CEC 2020 - Conf. Proc., pp. 1–6, 2020.*

[25] *AndreeaBendovschi,"Cyber-Attacks – Trends, Patterns and Security Countermeasures",7th INTERNATIONAL CONFERENCE ON FINANCIAL CRIMINOLOGY 201513-14 April 2015,Wadham College, Oxford, United Kingdom,ScienceDirect,Procedia Economics and Finance 28 (2015) 24 – 31.*

[26] *N. Goderdzishvili, Legal Assessment of Cyber Attacks on Georgia, Data Exchange AgencyMinistry of Justice of Georgia, Nov. 2010.*