International Research Journal of Mathematics, Engineering and IT

ISSN: (2348-9766)
Association of Academic Researchers and Faculties (AARF)
Impact Factor- 5.489 Volume 6, Issue 5, May 2019
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

NETWORK MONITORING MODELS FOR SECURITY PERSPECTIVE AND ITS IMPACT: A STUDY

Aarti[1], Prof. Om Prakash[2]

Department of Computer Science

[1,2]OPJS University, Churu (Rajasthan)

Abstract

This article discusses the network monitoring models for security perspective and its impact.Networking, which is one of the most significant aspects of information technology revolution, is developing increasingly day after day. This is because it offers a huge amount of knowledge, resources and human experiences. It contains a considerable amount of harmful content, because of misusing. On the other hand, sitting for a long time in front of PC's or other network-based devices can affect body badly. As enterprise computing environments become more network-oriented, the importance of network traffic monitoring and analysis intensifies. Most existing traffic monitoring and analysis tools focus on measuring the traffic loads of individual network segments. Further, they typically have complicated user interfaces.A Network Node Manager (NNM) will inform an external, remote database about the network status by sending real time data containing alerts and events. The whole tool is called Network Management Analysis Tool (NMAT).

1. OVERVIEW

The network consists of a collection of systems connected through any communication channel. The communication channel may include any physical “wired” or logical “wireless” medium and any electronic device known as a node. Computers and printers are some of the examples of nodes in a computer network.

If we talk about the telecommunication network, these may be mobile phones, connecting towers equipment, and main control units. The main function of any network is to divide resources among the nodes. The system under specific rules finds resources and then shares it between the nodes in such a way that authenticity and security issues are guaranteed. The rules for communication among network nodes are network protocols. A protocol is the complete set of regulations governing the interaction between two systems. It varies for varying different working assignments between nodes communication[1-8].

The Open System Interconnected Model (OSI)

The International Standard Organization (ISO) designed a standard communication framework for heterogeneous systems in a network. As per the usefulness of the communication system in the open-world, this system is called Open System Interconnection Model (OSI). The OSI reference model provides a framework to break down complex between networks into such components that can all the more effectively be understood and used.

The reason for OSI is to permit any computer anyplace on the planet to speak with some other, as long as both keep the OSI standards. The OSI reference model is misused into seven levels. Each level in the OSI Model has its own working usefulness; these levels are secluded yet then again cascaded to one another and have communication usefulness in a proper stream between them. Concerning the above standard communication framework, this arrangement of layers known as OSI layers. The usefulness of each layer is not the same as each, and each layer has a diverse level and labels.

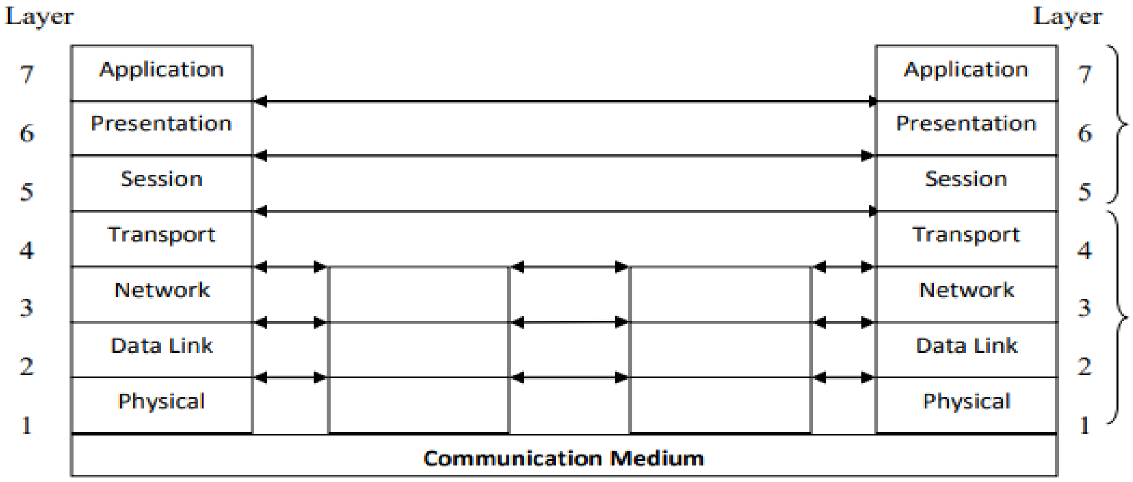

Figure 1: OSI Reference Model Layer Architecture

Three-level of abstraction is expressly recognized, the architecture, and the service specifications, and the protocols specifications. The OSI service specifications are responsible for specific services among clients and the system in a specific layer. Equal OSI protocol specifications are responsible that, which sort of protocol is running against the specific communication service. So obviously, the combination of these two parts becomes OSI system architecture.

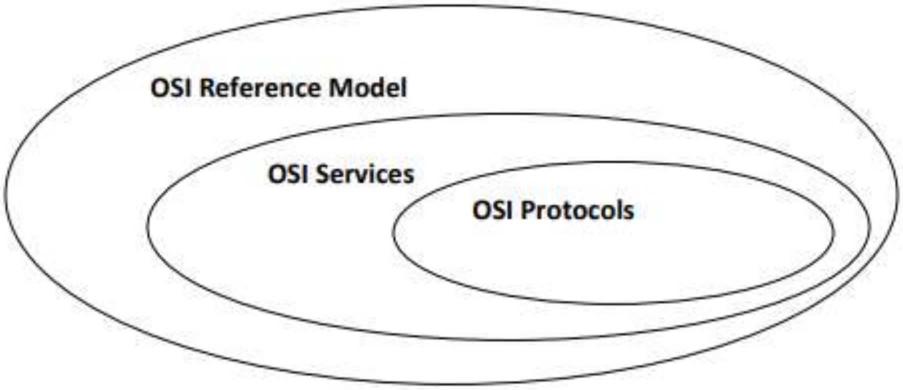

Figure 2: OSI System Architecture

It is patent that the OSI reference model consists of seven layers and each layer offers different functionalities, different services with different protocols. Whereas each layer, with the exception of the lowest, covers a lower layer, effectively isolating them from higher layers functions.

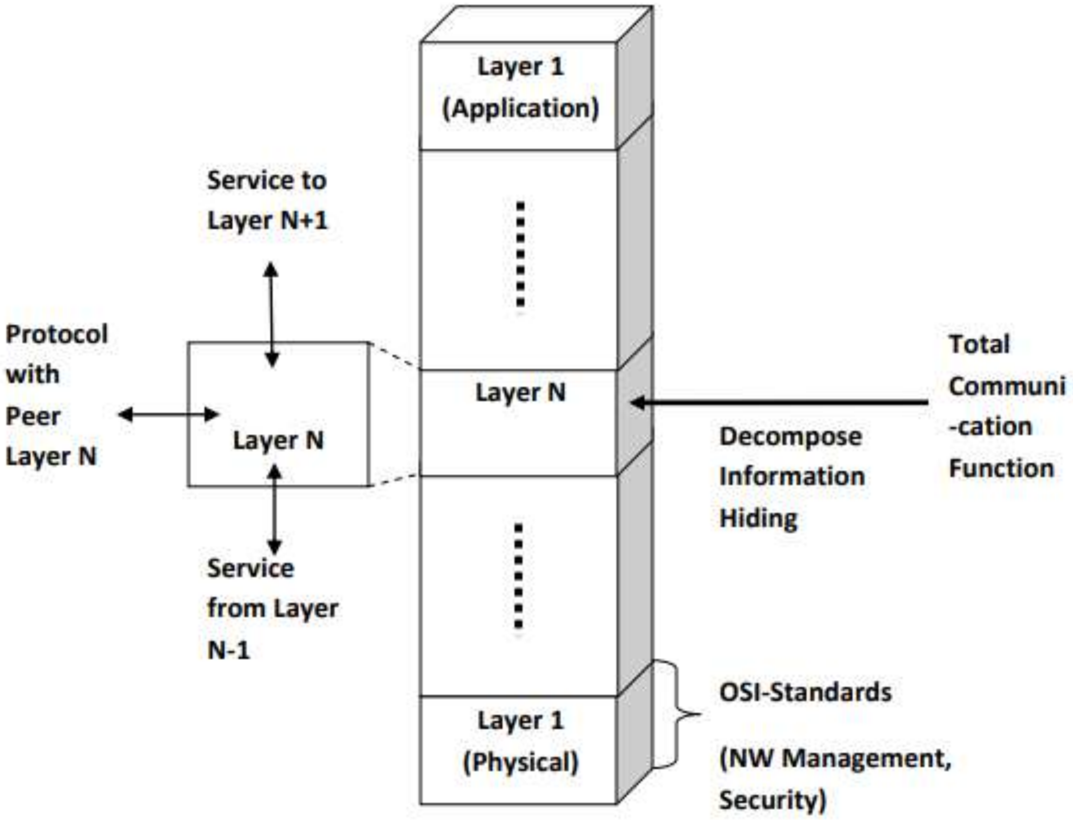

Figure 3: OSI framework structure

Physical layer

The lowest layer in OSI model is Physical Layer; it facilitates the connectivity between system interface cards and physical mediums. This layer understands and transforms electrical/electronic signals in the form of bits. So that it administrates physical “wire” and/or logical “wireless” connection establishment between the hardware interface cards and communication medium; example of physical layer standard includes RS-232, V.24 and V.35 interfaces.

Data link Layer

In the OSI Reference Model, the Data Link Layer is the subsequent layer. Data Link layer is responsible for control methods that provide the proper format of data, and it can access data stream blunders in the physical layer.

Network layer

The third layer in the OSI Reference Model is the Network Layer. This layer is responsible for making a logical connection between source and destination. The data at this layer is as packets. The network layer protocols provide the accompanying services. The network layer has two sorts of connections among source and destination; initial one is known as connectionless communication, which doesn't provide connection affirmation. The case of connectionless communication is the Internet Protocol (IP).

Transport Layer

The fourth layer in OSI reference model is Transport Layer. It contains two types of protocols, first is Transport Control Protocol (TCP) which is connection oriented protocol and supports some upper layer protocols like HTTP and SMTP. The second is User Datagram Protocol (UDP) which is a connection less protocol. Like TCP it also supports some upper layer protocols such as DNS, SNMP and FTP. The main thing in transport layer protocols is that they have port addresses in their header fields.

Session layer

The fifth layer in OSI Reference Model is Session Layer. The Session Layer is responsible for session management i.e. start and end of sessions between end-user applications. It is used in applications like live TV, video conferencing, VoIP etc, in which sender establishes multiple sessions with receiver before sending the data. Session Initiation protocols (SIP) is an example.

Presentation layer

The sixth layer in OSI Reference Model is Presentation Layer. This layer is responsible for presentation of transmitted/received data in graphical mode. Data compression and decompression is the main functionality of this layer. The data encryption is done before transmission in presentation layer.

2. NETWORK TRAFFIC ANALYSIS FOR IR: DATA COLLECTION AND MONITORING

Data collection and analysis for use by network engineers, security professionals, and occurrence reaction has just detonated throughout the years with the development of cloud-based services, mobile devices and tablets, remote workforces, interconnected applications, and global enterprises. Research has discovered that 41 percent of organizations claim that they were collecting significantly more network data for security analysis than they realized how to process.

The same research discovered 49 percent of organizations experienced difficulty connecting security issues with network performance. At the same time, cyber-attacks are turning out to be increasingly complex, modern, and customized. In any case, regardless of these complexities, the basic job of data collection, processing, and analysis in episode reaction and security monitoring is unaltered, assuming a crucial job in recognizing and dealing with network intrusion.

Rather, organizations have started to use additional categories or types of network data that could be collected. This permits security professionals to increase deeper knowledge into their network's movement, measure its security, and make feeling off, in any case, overpowering levels of data to detect cyber-attacks.

3. NETWORK MONITORING APPROACHES AND ITS IMAPCT

The network has become an infrastructure for many applications that influence our daily lives. Significantly, the computer network should be managed properly. Management of networking requires monitoring. Network monitoring is a lot of mechanisms that permits network administrators to know the quick state and long haul trends of a complex computer network. Network monitoring and measurement have become increasingly more significant in an advanced entangled network. Before, administrators may monitor a couple of network devices or less than a hundred computers[2].

The network bandwidth maybe only 10 or 100 Mbps; be that as it may, presently, administrators need to manage not just a higher speed wired network (more than 10 Gbps and ATM (Asynchronous Transfer Mode) network) yet in addition wireless networks. They need progressively modern network traffic monitoring and analysis tools so as to maintain the network system soundness and accessibility, for example, to fix network problems on time or to avoid network failure, to ensure the network security quality, and to make good decisions for network planning[3-5].

Network Monitoring includes multiple methods that are sent intentionally to maintain the security and integrity of an internal network. The internal network is otherwise called a Local Area Network (LAN), and monitoring encompasses hardware, software, viruses, spyware, vulnerabilities, for example, backdoors and security holes, and different aspects that can compromise the integrity of a network[6-8].

4. CONCLUSION

In this research we are trying to study these different kinds of attacks that penetrate our system. As the threats are increasing, so for secure use of our systems and internet there are various different security policies are also developing. In the research we have mention some of the security policies that can be used mostly by number of users and some new advance qualities that fits to the todays more penetrating environments like Trend micro security mechanism, use of big data qualities in providing security, etc. Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, will it be achievable.

In this research of the network management system, the proposed approach is implementing a set of well-known networking protocols to find everything about them and monitor the full state of the network. It is an efficient method that provides all the needed knowledge about a system suitable way that optimizes the needed owner interactions that are necessary to configure things as desired..

REFERENCES

[1]. One Approach to Enterprise Security Architecture-SANS Institute InfoSec Reading Room-2002-Prepared by: Nicholas Arconati.

[2]. David Bailey, “A Philosophy of Security Management”, P-98- 110, 2010

[3]. V. P. Gulati and V. Radha, “IDRBT’s Working Paper No. 8 Enterprise Network Security”, 2012

[4]. Victor-Valeriu PATRICIU, Iustin PRIESCU and Sebastian NICOLAESCU, “Interdisciplinarity New Approaches and Perspectives in the Use of Quantitative Methods”,

[5]. Scott A. Bernard, “An Introduction to Enterprise Architecture: Third Edition”,-https://books.google.co.in/books?hl=en&lr=&id=OkNMFI3_L_YC&oi=fnd&pg=PA7&dq=Enterprise+Network+Security+Architecture+Strategy+Evaluation&ots=wAkyWxxzLV&sig=BTy0JEIVRa8QrFbHW-gNHL_s1X4#v=onepage&q&f=false

[6]. Peter E.D Love, ZahirIranib& David J Edwardsc, “Industry-centric benchmarking of information technology benefits, costs and risks for small-to-medium sized enterprises in construction”, Volume 13, Issue 4, July 2004, Pages 507–524 - http://www.sciencedirect.com/science/article/pii/S0926580504000202

[7]. Enterprise Architecting: Critical Problems by Kaisler, S.H. ; U.S. Senate ; Armour, F. ; Valivullah, M.- Published in: System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on ate of Conference:03-06 Jan. 2005, Page(s): 224b & ISSN: 1530-1605, Print ISBN:0-7695-2268-8

[8]. A Novel Architecture for Enterprise Network Security by Chao Chen, Beijing, China, Ke Wang &Yiqi Dai. -Published in: Computational Intelligence and Security, 2009. CIS '09. International Conference on (Volume:1)Date of Conference:11-14 Dec. 2009 (s): 537 – 541.