IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DETECTION OF UNAUTHORISED ACCESS TO SMB USING MONOSECK PROTOCOL ANALYSER

[1]Anand M, [2]Bhuvana A N, [3]Chinmayi S [4]Shriya R

[1]Assistant Professor [2,3,4]Student

Department of Information Science and Engineering

[1,2,3,4]GSSS Institute of Engineering and Technology for Women, Karnataka, India.

Abstract: The advent of network in all kinds of business technologies has made every individual more dependent on the internet for all the purposes. So are the threats for the same is increasing and the network security has become a major issue. Our project aims in detecting the unauthorized access to SMB using the Monosek- a Network Processor based Network Packet Processing and Network Session Analysis system. Also, the traffic generated in this attack produces packets which a recollected in the database and analyzed for further use.

Index Terms **- – SMB, networks, packet analysis, Monosek, network security.**

I. INTRODUCTION

An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, and reveal information without authorized access or permission. One of the majors in the cyber-attacks is Cross-site scripting attack. The Server Message Block (SMB) is a network protocol that enables users to communicate with remote computers and servers, to use their resources or share, open and edit files. It is also referred to as the server/client protocol, as the server has a resource that it can share with the client. Like any network file sharing protocol, SMB needs network ports to communicate with other systems. Originally, it used port 139 that allowed computers to communicate on the same network. But since windows 2000, SMB uses port 445 and TCP network protocol to "talk" to other computers over the internet. The SMB protocol creates a connection between the server and the client by sending multiple request-response messages back and forth.

A. INTRUSION DETECTION SYSTEM (IDS)

MONOSEK is intrusion detection software that monitors high speed network traffic by developing own traffic pattern with API calls. This software is embedded software for packet analysis, session analysis and deep packet inspection. MONOSEK plays a major role in order to analyze each packet that is transmitted in the network traffic and to detect the unauthorized access to SMB while transferring files, unauthorized access detection is the major aim of the project where we have an attacker system and victim system along with a MONOSEK server to monitor the packet transmission. As the attacker floods the victim system by enormous packets by forging the victim IP address, attack occurs and victim is denied of the service. In order to detect the attack occurrence, we use MONOSEK server which alerts the user as soon as the unauthorized access occurs.

The main objective of the project is to

- The aim is to analyze the system and detect the attack when the victim visits the web page or application that executes the malicious code using monosek server.
- The objective is to detect unauthorized access to Server Message Block (SMB) and informs the user about system attacked.
- Avoiding malwares to interact and misuse user's

II. LITRTURE REVIEW

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper Do not number text heads—the template will do that for you.Finally, complete content and organizational editing before formatting. Please take note of the following items when proof reading spelling and grammar returns of the shares and estimated betas.[1] Microsoft is producing technical documentation for Windows client-server and server-server protocols to enable licensees to produce interoperable server products. This paper describes certain aspects of a new quality assurance process for technical documents as it is in place at Microsoft. We are applying various test methods including, when appropriate, a model-based approach. The paper uses the Server Message Block Protocol Version 2 (SMB2) as a running example to illustrate the process.[2] This paper presents a file sharing traffic analysis methodology for Server Message Block (SMB), a common protocol in the corporate environment. The design is focused on improving the traffic analysis rate that can be obtained per CPU core in the analysis machine. SMB is most commonly transported over Transmission Control Protocol (TCP) and therefore its analysis requires TCP stream reconstruction. We evaluate a traffic analysis design which does not require stream reconstruction. We compare the results obtained to a reference full reconstruction analysis, both in accuracy of the measurements and maximum rate per CPU core. We achieve an increment of 30% in the traffic processing rate, at the expense of a small loss in accuracy computing the probability distribution function for the protocol response times.[3] Zeng Qi;An Yunjie, describes The SMB have very important status and plays an important role in our country's economic development. But their existence and development are determined by technological innovation. It is urgent for that SMB to need technological innovation, but their economic and technical strength is weak, the imitating innovation model is the first selection, the cooperation innovation model comes next. Independent technological innovation model doesn't suit to them at present time.[4] Penetration testing helps to secure networks, and highlights the security issues. In this paper investigate different aspects of penetration testing including tools, attack methodologies, and defense strategies. More specifically, we performed different penetration tests using a private networks, devices, and virtualized systems and tools. We predominately used tools within the Kali Linux suite. The attacks we performed included: smartphone penetration testing, hacking phones Bluetooth, traffic sniffing, hacking WPA Protected Wifi, Man-in-the-Middle attack, spying (accessing a PC microphone), hacking phones Bluetooth, and hacking remote PC via IP and open ports using advanced port scanner. The results are then summarized and discussed. The paper also outlined the detailed steps and methods while conducting these attacks [5] In connection with mass introduction of robots in various spheres of activity, and also absence of due attention to such factor as safety, the probability of unauthorized access to their blocks of management raises. Typical decisions on safety maintenance by introduction of information security systems are not suitable for the robotized platforms in view of their capacities limitation. Thus, there is a problem of providing protection of the control unit of robotic platforms from various threats. The results of the analysis of possible approaches to the formation of a list of threats and vulnerabilities of the robotic platform are shown.

II METHODOLOGY

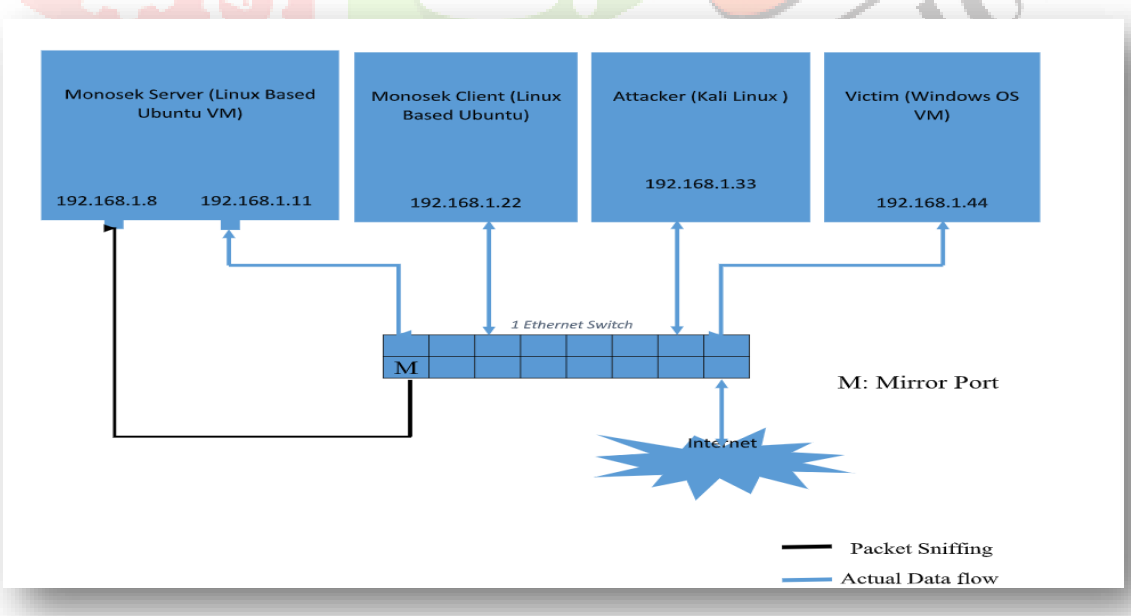

Fig 1: system architecture

As depicted in the fig1 above, internet is connected to a switch, where one port of a switch being mirrored is connected to the Monosek server system to capture all the system's traffic that are connected to the switch.

Monosek is a Network Packet Analyzer System. It offers the most complex packet and flow processing with L2-L4 packet processing, L4-L7 flow processing.

This architecture has three layers of workload - specific packet with deep packet inspection, Detection and Prevention of application services each with increasing levels of granularity. The software modules provide these features are as below.

- Protocol Library Provides the framework to extract the various protocol fields of Layer 2 to Layer 5 of TCP/IP protocol stack from the packet.
- Flow Library Framework to analyze the VoIP traffic, monitoring network bandwidth and depicts TCP Handshake process.
- Deep Packet Inspection Library enables the user to analyze the network traffic at flow level.
- Application Service Detection Library This module identifies more than 100 Services such as HTTP, Facebook and Twitter etc.
- To create snort like rules to identify the particular traffic based on various combinations of source IP, destination IP, source port, destination port, protocol. Reporting the alerts via email.
- Geo IP Library Provides the framework to map the IP address from the analyzed traffic such as SMTP or POP3 to nearest possible latitude and longitude coordinates.
- Virus Signature Detection Library Provides the framework for the following, to identify malware content across packets, to configure the rules to identify the user defined patterns inside packets and it report the alerts to the user through email

Proposed System

The proposed system uses Monosek which is a intrusion detection software that monitors high speed network traffic by developing own traffic pattern with API calls.It detects unauthorized access to SMB and also inform the user about their system attacked Using open ports and SMB network ports. The detection of unauthorized access is illustrated in Fig. 2.

The process consists of the following steps:

1. User performing action to server and server responding to the actions.
2. Attacker collecting information or files from user unknowingly in unauthorized way.
3. Server detects unauthorized access by matching the open ports and informs the user that system being attacked.

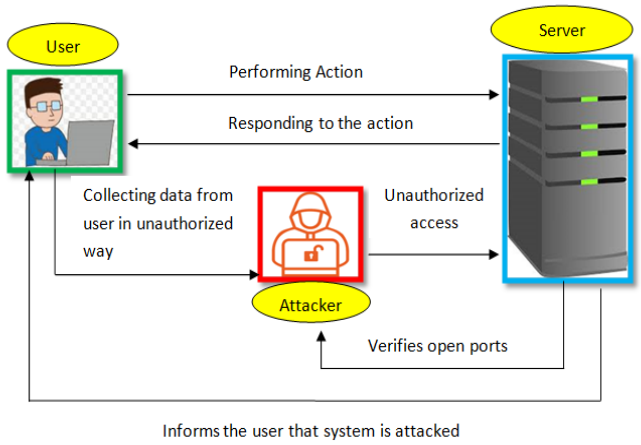

Fig 2: Detection of Unauthorized access

System Modules:

- Attacker: The attacker is the one who will insert the malicious unfiltered code to the server to get the required information for him. Attacker inserts the malicious code to the web page where the victim visits. Whenever the victim visits the web page he will be under attacked by the attacker and will get the information which is needed. And also, attacker get the control over the user data or system via injected exploit.
- Victim: The victim module is the one where he will be affected by the attacker once he get into the malicious page and the malicious data is sent to get required information. Once this has been done by the attacker, the victim will be in the control of the attacker.
- Server: This is the module where the unfiltered code is stored and sent to victim unknowingly.

CONCLUSION AND FUTURE SCOPE

The project helps to detect the unauthorized access to Server Message Block (SMB) using Monosek Protocol, It checks whether SMB is being attacked or not, by matching the port numbers and notify the user if system is being attacked. It helps to reduce cyber-crimes and also aid to improve economy of county.

REFERENCES

[1] Wolfgang Gierskamp, Nicolas kicillof, Dave MacDonald, Alok Nandan, Keith stobie, Fred wurden, Danpo Zhang [Microsoft Corporation, USA], "Model Based Quality Assurance of the SMB2 Protocol Documentation",2008 Institute of Electrical and Electronics Engineers (IEEE).

[2] Eduardo Berrueta, Danieal Morato, Eduardo Magana, Mikel lazal, "High-Speed Analysis of SMB2 File Sharing Traffic without TCP Stream Reconstruction",2019 nstitute of Electrical and Electronics Engineers (IEEE).

[3] Zeng Qi;An Yunjie, "Technological Innovation Model of SMB in International Operation",2009 Institute of Electrical and Electronics Engineers(IEEE).

[4] Matthew Denis, Carlos Zena, Thaier Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies",2016 Institute of Electrical and Electronics Engineers (IEEE).

[5] Marina N. Zhukova;Vyacheslav V. Zolotarev;Vadim G. Zhukov;Anastasya S. Polyakova, "Service Robot Security from Unauthorized Access by Connection Control"2019 Institute of Electrical and Electronics Engineers (IEEE).

[6] Dr. Mahesh Kumar, Rakhi Yadav, "TCP & UDP Packets Analysis Using Wireshark",2019, International Journal of Science, Engineering and Technology Research (IJSETR).

[7] Nattawat Khamphakdee,Nunnapus Benjamas,Saiyan Saiyod, "Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection",2014 2nd International Conference on Information and Communication Technology (ICoICT).

[8] Ang Cui, Salvatore J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan"26th Annual Computer Security Applications Conference, ACSAC 2010, Austin, Texas, USA, 6-10 December 2010.

[9] Jakub Czyz,Matthew Luckie,Mark Allman,Michael Bailey, "Don't Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy" January 2016 DOI:10.14722/ndss.2016.23047 Conference: Network and Distributed System Security Symposium.

[10] Matthew Sargent,Jakub Czyz,Mark Allman,Michael Bailey, "On the Power and Limitations of Detecting Network Filtering via Passive Observation", March 2015 DOI:10.1007/978-3-319-15509-8_13 Conference: International Conference on Passive and Active Network Measurement.

[11] Unal Tatar;Hayretdin Bahsi;Adrian Gheorghe, "Impact assessment of cyber attacks: A quantification study on power generation systems",2016 Institute of Electrical and Electronics Engineers(IEEE).

[12] Elias Bou-Harb,Nataliia Neshenko, "Cyber Threat Intelligence for the Internet of Things" February 2020 DOI:10.1007/978-3-030-45858-4 Publisher: Springer ISBN: 978-3-030-45857-7.

[13] Chih-che sun,Junho Hong, "A coordinated cyber attack detection system (CCADS) for multiple substations",2016 Institute of Electrical and Electronics Engineers(IEEE).

[14] Kensuke Fukuda,John Heidemann, "Who Knocks at the IPv6 Door?: Detecting IPv6 Scanning" October 2018 DOI:10.1145/3278532.3278553 Conference: the Internet Measurement Conference 2018

[15] Sayeed Z.sajal , Israt Jahan , Kendall E.Nygard, "A Survey on Cyber Security Threats and Challenges in Modem Society",2019 Institute of Electrical and Electronics Engineers(IEEE).