Detection of Unauthorised Access to Smb using Monoseck Protocol Analyser

Anand M
Assistant Professor
Department of Information Science and Engineering
GSSS Institute of Engineering and Technology for Women,
Karnataka, India.

Bhuvana A N, Chinmayi S, Shriya R
Students
Department of Information Science and Engineering
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 which is a Network Packet Processing and Network Session Analysis system which is based on Network Processor. Also, the traffic generated in this attack produces packets which a recollected in the database and analysed for further use.**

Keywords— SMB, networks, packet analysis, Monosek, network security

I. INTRODUCTION

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

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 an 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 computer.

II. LITRTURE REVIEW

[1] Microsoft will be producing technical documentation for Windows client-server and server-server protocols to enable licensees this in turn will produce interoperable server products. This paper will describe certain aspects of a new quality assurance process for technical documents as it is in place of Microsoft. We will be applying various test methods including, a model-based approach. The paper uses the Server Message Block Protocol Version 2 (SMB2) as an example to illustrate the process.

[2] This paper describes a file sharing traffic analysis methodology for Server Message Block (SMB) which is usually a common protocol in the corporate environment. The design is mainly focused on improvising the traffic analysis rate which can be obtained per CPU core in the analysis machine. SMB is commonly transported through Transmission Control Protocol (TCP) and therefore its analysis will require TCP stream reconstruction. We can evaluate a traffic analysis design which will not require stream reconstruction. We can compare the results obtained to form a reference reconstruction analysis, both will be in accuracy of the measurements and will have maximum rate per CPU core. We can achieve an increment of 30% in the traffic processing rate, this will be at the expense of a small loss in accuracy while computing the probability distribution function for protocol response time.

.[3] Zeng Qi;An Yunjie, describes that the SMB have very important status which plays an important role in our country's economic development. But its development is determined by technological innovation. It is crucial for the SMB must need technological innovation, but their economic and technical strength tends to be weak, the imitating innovation model is the first selection and the cooperation innovation model is the next. Independent technological innovation model does not suit them at the present time.

[4] Penetration testing will help secure networks, and highlight the security issues. In this paper we will be investigating different aspects of penetration testing including tools, attack methodologies, and defense

strategies. We performed different penetration tests using private networks, devices, and virtualized systems. We used tools within the Kali Linux suite. The attacks that we performed includes: 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. Results are then summarized. This paper also outlines the detailed steps and methods for conducting these attacks.

[5] In association with mass introduction of robots in various spheres of activities, and also absence due of attention to such factor as safety, the probability of unauthorized access to their blocks of management increases. Decisions on safety maintenance will be done by introduction of information security systems which are not suitable for the robotized platforms in view of their capacities limitation. Therefore it is a problem for providing protection from various threats of the control unit of robotic platforms. The result of the analysis of approaches to the formation of many types of threats and vulnerabilities of the robotic platform are shown here .

III. METHODOLOGY

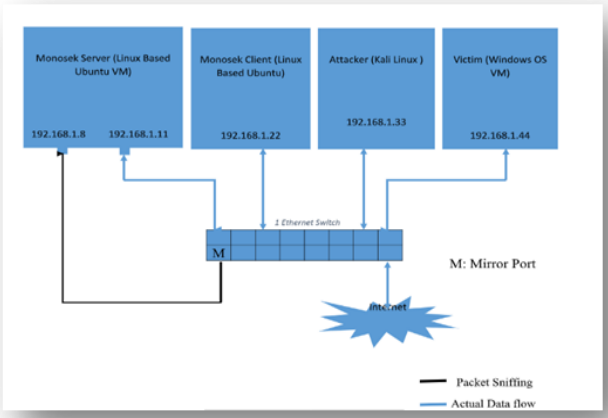

Fig 1: system architecture

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

A. 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.

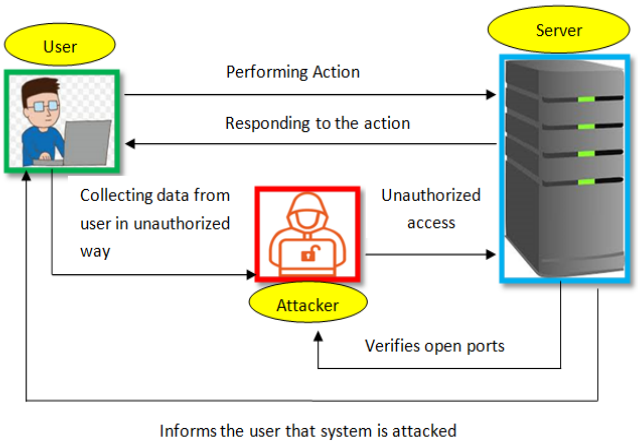

Fig 2: Detection of Unauthorized access

B. 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.

IV 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] Nattwat 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).