IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 2, February 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102030 |

Securing Website against Vulnerabilities Using Intrusion Detection System and Firewall

Prof.R.M.Bhutada[1], Yash Bakal[2], Shyam Wasankar[3], Tejas Tayade[4], Abhijeet Pawar[5], Kunal Namdas[6]

Department of Computer Science and Engineering, Mauli Group of Institutions and College of Engineering, Shegaon, India

ABSTRACT: In this project we are securing a website having vulnerabilities using Intrusion Detection System and Firewall. We will have one website hosted on our Linux machine. The following are some common vulnerabilities. 1. SQL injection 2. Bruit Force 3. XSS (Reflected and Stored) 4. File upload, and we are securing the website from these vulnerabilities by using some validation technics while developing websites which act as a first level of defence and if the attacker cracks the validation layer, as the data is stored on the server, the next attack will be on the server. Now, the attacker will try to get access to the server i.e. Linux Machine. Here, the Intrusion Detection System is used for detecting the attack and the attacker's ip address and acknowledgement is given to the administrator. Administrator have the privilege to block the attacker's ip address using Linux ip-table's firewall.

I. INTRODUCTION

Preventing websites from various vulnerabilities is very important because nowadays websites are used for many purposes. As websites are hosted on servers, if websites are not developed with proper validation and techniques, then there are chances of getting hacked using some attacks and also a chance of the server also getting hacked and we losing our personal data stored on the server. So, preventing these types of losses, we need to be more careful about the websites and servers also, for that we are presenting solution using IDS and Firewall. An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaches. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms. A Firewall is a necessary part of any security architecture and takes the guesswork out of host level protection and entrusts it to your network security device. Firewalls, and especially Next Generation Firewalls, focus on blocking malware and application-layer attacks, along with an integrated intrusion prevention system (IPS). These Next Generation Firewalls can react quickly and seamlessly to detect and react to outside attacks across the whole network. They can set up policies to better defend your network and carry out quick assessments to detect invasive or suspicious activity, like malware, and shut it down. The following are some common vulnerabilities. 1. SQL injection 2. Bruit Force 3. XSS (Reflected and Stored) 4. File upload, and we are securing the website from these vulnerabilities by using some validation technics while developing websites which act as a first level of defence and if the attacker cracks the validation layer, as the data is stored on the server, the next attack will be on the server. Now, the attacker will try to get access to the server i.e. Linux Machine. Here, the Intrusion Detection System is used for detecting the attack and the attacker's ip address and acknowledgement is given to the administrator. Administrator have the privilege to block the attacker's ip address using Linux ip-table's firewall.

II. LITERATURE SURVEY

In this project we are securing a website having vulnerabilities using Intrusion Detection System and Firewall. We will have one website hosted on our Linux machine. The following are some common vulnerabilities.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102030 |

The growth of computer networks has made it essential to develop network and system security. The development of IDS for detecting attacks in several network environments and Firewalls has been done. This paper gives a comparative study on Intrusion detection system and Firewall. To overcome the security related issues, intrusion detection systems is used which provides confidentiality, integrity and security. Similarly, there are firewalls that protect the systems from hazards.[1]

The capacity to distinguish interlopers in PC frameworks increments in significance as PCs are progressively incorporated into the frameworks that we depend on for the right working of society. This paper surveys the historical backdrop of research in interruption identification as performed in programming in the setting of working frameworks for a solitary PC, an appropriated framework, or a system of PCs. There are two essential methodologies: inconsistency location and abuse recognition. Both have been polished since the 1980s. Both have normally scaled to use in appropriated frameworks and systems.[2]

This survey is intended to be a comprehensive compilation and categorization of currently available intrusion detection system (IDS) commercial products. It was undertaken at the instigation and with the support of the Global Security Analysis Laboratory at IBM's Zurich Research Laboratory in Rueschlikon, Switzerland. It is based almost entirely on published reports, published product evaluations, and vendorsupplied product information. Prior to publication, considerable effort was expended attempting to contact every referenced vendor, so that they might point out and suggest corrections. The comments by those who responded were reviewed carefully and incorporated where appropriate. This survey does not recommend or endorse any specific product or service; it is intended wholly as a resource for those interested in the current state and the ongoing evolution of IDS products and what that implies for IDS research and development.[3]

Computer and network security are challenging topics among executives and managers of computer corporations. Internet security is the practice of protecting and preserving private resources and information on the Internet. Even discussing security policies may seem to create a potential liability. As a result, enterprise management teams are often not aware of the many advances and innovations in Internet and intranet security technology.[4]

FLOWCHART

1)Attacker scanning for vulnerabilities.

2)Getting all the information of the website.

3)Cracking the validation layer.

4) Attacker can try to hack the website or server but,website is hosted on Linux Machine then attacker will try to hack Linux Machine.

5) Attacker will try to attack on server i.e. Linux Machine.

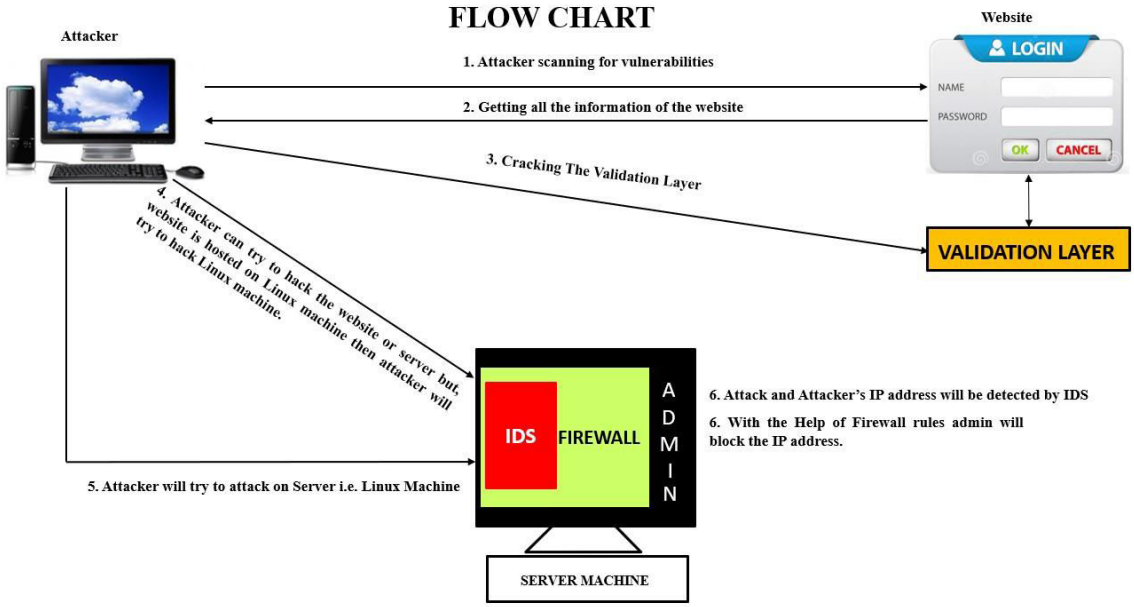
6) Attack and Attacker's IP address will detected by IDS.

7) With the help of Firewall rues admin will Block the IP address.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102030 |



III. CONCLUSIONS

We conclude that by using the correct validation techniques along with Intrusion Detection System to detect suspicious activities and provide acknowledgement to administrator and preventing invader's ip address to enter our system by using Firewall, therefore we could secure the websites effectively.

REFERENCES

1.Shardul Sharad Vichare Comparative Study on Firewall and Intrusion Detection System, volume 7, issue 6 Posted: 2017-06
2.Vijay Ramalingam, Dr. R. Saminathan, Dr. K.M Baalamurugan A Novel Survey on Intrusion Detection System and Intrusion Prevention System, volume 8, Posted: 2019-12
3.Kathleen A. Jackson INTRUSION DETECTION SYSTEM (IDS) PRODUCT SURVEY, Posted: 1999
4. Mohit Rathi, Manish Lohia RESEARCH PAPER ON FIREWALLS SYSTEM, volume 1, issue 5 Posted: 2014

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details