International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

IDS FOR WIFI SECURITY

Nikhil Inamdar[1], Siddharth Jadhav[2], Ravina Kamble[3], Roshan Bauskar[4]

[1,2,3]*Student, Department of Computer Engineering, L.E.S. G.V. Acharya Institute of Engineering and Technology, Shelu, Maharashtra*

[4]*Asst. Professor, Department of Computer Engineering, L.E.S. G.V. Acharya Institute of Engineering and Technology, Shelu, Maharashtra*

Abstract - *Nowadays, there are several cyberattacks on the computer system, networks, websites, and several applications. Use of wireless network has been increased these days, and these wireless networks are more vulnerable. As the number of devices connected to the wireless network is increasing, so it creates more vulnerabilities for wireless security Attackers have available a lot of tools for attacking and disrupt the network. That's why it's essential to provide more security to wireless network. In this paper, the implementation of IDS (Intrusion Detection System) for WIFI (Wireless Fidelity) security. This will detect the vulnerable activities of connected devices in network and alert the system and provide the information of intruders. This will help to provide security in the network.*

***Key Words*: Wireless Network, IDS, IEEE 802.11, WiFi, WEP**

1. INTRODUCTION

Violation of the security of wireless networks in small offices, homes, cyber cafes, etc. Many times small offices are not able to keep a separate IT network specialist, also at home, everyone is not able to handle wireless network security. Even unskilled people may be able to find open source utilities over the internet to crack, attack Wi-Fi passwords, WEP or WPA encryption and subsequently gain access to the network in an unauthorized way. The principal goal of this paper is to design and verify (evaluate) the system that would utilize passive monitoring of wireless network traffic in the small office, home network. In case of attack, the detection system will give a warning about devices that could be attacked on the system and protect the system from attack. The paradigm of communication has changed because of wireless local area network WLAN security vulnerabilities exposed in real-time. The security mechanism which already exists is vulnerable. WLAN exposes vulnerability on a large scale, it needs security which opens a new world to the wireless networking field and gives new challenges. Various kinds of attacks are targeted by the WLAN network. WLAN has various types of security for encryption such as WEP, WPA, and WPA2. These types of security protected only internal intruders.

Wireless intrusion detection is described in, as the process of monitoring the network for the activity that may compromise the security of the area that is under surveillance, and analyzing events that may indicate possible incidents. Intrusion Detection System (IDS) also executes automated responses to the detected malicious behavior.

Intrusion detection, Intrusion Detection Systems (IDS) generally are available 2 forms:

Host-based IDS (HIDS): A host-based IDS solution is one that runs on a specific pc or device. A HIDS monitors log files on your server and compare events within the log files against a database. The HIDS can then use the comparison to spot patterns of behavior that reflect commonly well-known hacker attacks.

Network-based IDS (NIDS): A network-based IDS, whereas making an attempt to supply constant function, operates during a very totally different manner. Network-based IDS scan network packets at the router level. they will generate log files to reflect any suspicious packets that will be occurring on your network.

2. RELATED WORK

A practical demonstration of exposing vulnerabilities in MAC filtering, Hidden SSID with MAC filtering and WPA2-PSK with hidden SSID and MAC filtering security mechanisms of AP was carried out in real-time. It was observed that the existing security mechanisms were vulnerable. Researchers have exploited many security mechanisms of WLAN focusing upon a single parameter of WLAN security at a time. However, in this work, the three available security mechanisms were cascaded to produce three layers of security mechanism i.e. WPA2 with hidden SSID and MAC filtering. This cascaded model was exploited in real-time. [1]

Upon probing to the weakness of current enterprise Wi-Fi security, a security defense system is designed to monitor WiFi security on Physical Layer, Data-link Layer and Internet Layer of the enterprise WiFi network, and provide attack defense mechanism to minimize the damage to enterprises when their WiFi network is under attack.[2]

A deadlock vulnerability is that the most severe form of DoS vulnerabilities, so checking for deadlock vulnerabilities is a necessary a part of robust protocol design. we tend to demonstrate the usefulness of the planned methodology through the discovery and experimental validation of deadlock vulnerabilities within the published IEEE 802.11w amendment to the 802.11 standards. [3]

The management frames on 802.11a/b/g/n were sent an unencrypted plain text, thus it should be spoofed and forged by an intruder. The 802.11w was introduced to protect frames but still contains a legacy in wireless devices been used that is not supported with 802.11w. This analysis planned a tool that may be used as a personal WIDS (Wireless intruder Detection System). This analysis also introduced the mechanism to get de-authentication and disassociation attacks on 802.11a/b/g/n nearby area.[4][5]

3. EXISTING SYSTEM

The WEP, WPA and IEEE 802.11i security amendments concentrate their protection to the data frames. The management and control frames present no protection, being vulnerable to DOS attacks. The newer amendments (IEEE 802.11k and 802.11v), have relevant information in the management frames. To preserve this information, the IEEE ratified the 802.11w amendment. This amendment presents robust management (RM) that is composed of the de-authentication, dissociation, and action frames that use the management frame protection (MFP).

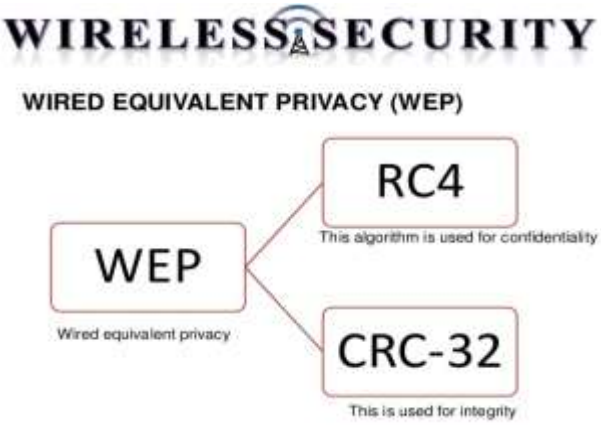

Figure 3.1 Existing System

4. METHDOLOGY

Intrusion detection refers to the method of observance of the events happening during a computing system or network, examining them for signs of security issues. intrusion detection is outlined as a method of detection and responding to malicious activity directed at computing and networking resources. Intrusion detection is outlined as the method of observant of the events occurring during a computing system or network and analyzing the violations or imminent threats of security policies or customary security practices violation. These violations are also caused by malware like worms, spyware, virus, unauthorized access to the systems by some attacker, and licensed users misusing their privileges or flaws leading to granting the attacker elevated access to the network. An Intrusion Detection System (IDS) may be a computer code used for the automation of intrusion detection methods. IDS monitors network or system events for malicious activities that tend to compromise the confidentiality, integrity, and convenience of network and send a report back to sixty-nine the management station. an IDS gathers and analyses the information inside a network or a pc to understand possible security fissures, which has each attack from outside the organization and inside the organization. It uses a technology, known as a vulnerability assessment or scanning, for assessing the protection of a computer or Accuracy: It deals with the right discovery of attacks and therefore the absence of false alarms.

- Performance: it's the speed at that audit events are processed.
- Completeness: it's the property of an intrusion detection system to spot all attacks. Fault Tolerance: An intrusion detection system must be resilient to attacks, particularly denial-of-service attacks.
- Timeliness: An intrusion detection system needs to accomplish and thrive its analysis as quickly as potential to empower the safety administrator to reply before a lot of damage has been done, and also to inhibit the attacker from subverting the audit source or the IDS itself.

The intrusion detection system procures data regarding the information system to perform the analysis of the protection status of that system. The foremost goal of IDS is to discover the protection breaches, as well as each attempted breaches and potential breaches. In order to ensure the right to make sure of the IDS, sensors are wont to notice data, analyzers to evaluate to monitor, panels functionality activities, and user-interfaces to manipulate configuration settings. The IDS items may be in the type of packets, audit records of system, computed hash values or alternative data formats. Analyzers receive input from sensors then determine the intrusive activity.

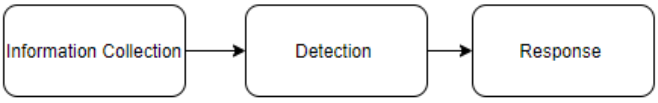

Figure 3.2 Components of IDS

An intrusion detection system depends on the subsequent parameters:

A. Information Collection
B. Detection
C. Response

4.1 INFORMATION COLLECTION

Wireshark is that the world's foremost network protocol analyzer.it's the actual (and typically de jure) normal across several industries and academic institutions. Wireshark development thrives due to the contributions of networking specialists across the world.

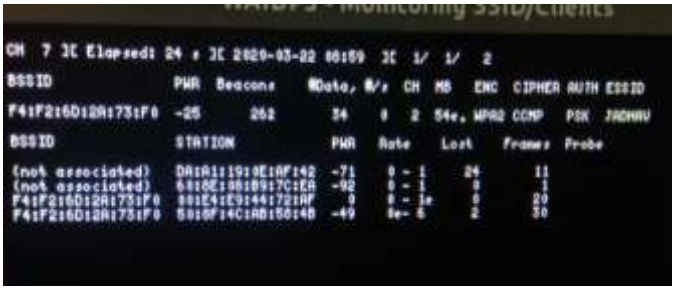

Figure 4.1.1 Collection of Information

Figure 4.1.2 Packet Capturing

4.2 Detection

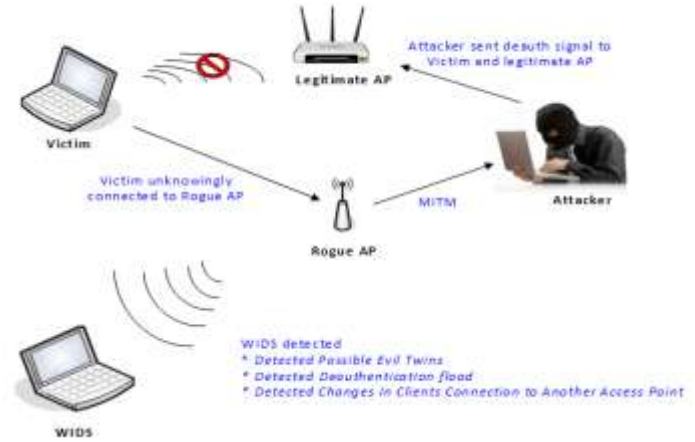

Figure 4.2 Hacking and Detection Process

Wireless IDS is an open supply tool written in Python and work on Linux atmosphere. This tool can sniff your close nearby air traffic for suspicious activities like WEP/WPA/WPS offensive packets. It do the subsequent

I. Detect mass de-authentication sent to consumer / access point that unreasonable quantity indicate potential WPA attack for handshakes.
II. Continual sending data to access point exploitation broadcast Mac address that indicate a prospect of WEP attacks
III. Unreasonable quantity of communication between wireless consumer and access point exploitation EAP authentication that indicate the chance of WPS brute force attack by Reaver / WPS Crack.
IV. Detection of changes in connection to anther access point which can have the chance of connection to rogue AP (User must assess the case whether or not similar AP name).
V. Detects potential rogue Access point responding to probe by wireless devices within the near by area.

4.3 RESPONSE

1. Display similar Access Point's name (SSID) that might have the chance of WLAN 'Evil Twins'.
2. Display of searching SSID by wireless devices.
3. Detection of Korek Chopchop packets sent by Aircrack-NG (WEP attacks). Detection of Fragmentation PRGA packets sent by Aircrack-NG (WEP attacks).
4. Detection of attainable WPA Downgrade attack by MDK3. Detection of doable Michael termination exploitation (TKIP) by MDK3. Detection of Beacon flooding by MDK3. Detection of attainable Authentication DoS by MDK3.
5. Detection of attainable association flooding. Detection of WPA Migration Attack by Aircrack-NG (WPA Attack).
6. Allow logging of events to file. Permit disabling of displaying of searching devices.
7. The setting of scanning count

5. CONCLUSION

The detection of intruders by capturing the packets of clients in a network and monitoring the network clients. This will provide suspicious activities performed by clients on network using Wireshark and T-shark along with some important factors like xterm. The output will provide in every certain refreshment of time. It is the live detection of intruders based on packet capturing and monitoring network traffic. It uses capturing information like BSSID, STA ENC, cipher, auth, CH, PWR, Range, ESSID, packets, channel, rate, lost frames, probe, data, beacons, stations connected, etc terms and factors used from the interface of xterm with capturing data, monitoring and accessing the channel It detects the Evil twin's attacks, beacon flood attacks, Dos attacks, etc.

6. FUTURE SCOPE

Future works intend to investigate attribute selection or optimization techniques in order to improve the IDS overall accuracy. Moreover, the continuous training to the proposed neural network will be able to run real time detecting, even when new attacks happen.

7. REFERENCES

[1] Hongye Zhong, Jitian Xiao " Design for integrated WiFi defence strategy in mordern enterprise context ", 2014 IEEE 5th International Conference on Software Engineering and Service Science , DOI:10.1109/ICSESS.2014.6933675

[2] Zeeshan Akramv, Muhammad Anwaar Saeed, Marriam Daud "Real time exploitation of mechanism of residential Wlan access point ", 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) , DOI:10.1109/ICOMET.2018.8346378

[3] Martin Eian, Stig F. Mj□lsnes "A Formal Analysis of IEEE 802.11w Deadlock Vulnerabilities", 2012 Proceedings IEEE INFOCOM, DOI: 10.1109/INFCOM.2012.6195841

[4] Norzaidi Baharudin, Fakariah Hani Mohd Ali, Mohamad Yusof Darus, Norkhushaini Awang, "Wireless Intruder Detection system (WIDS) in Detecting De-Authentication Attacks in IEEE 802.11", 2015 5th International Conference on IT Convergence and Security (ICITCS), DOI: 10.1109/ICITCS.2015.7293037

[5] Haihang Wang, "Weakness in 802.11w and an improved mechanism on protection of management frame", 2011 International Conference on Wireless Communications and Signal Processing (WCSP), DOI: 10.1109/WCSP.2011.6096780

BIOGRAPHIES

Mr. Nikhil S. Inamdar, Final Year Student of B.E. (computer Engineering), at G.V. Acharya Institute of Engineering And Technology, Shelu , Maharashtra
Domain of Interest : Data Science, MySql Database

Mr. Siddharth G. Jadhav, Final Year Student of B.E. (computer Engineering), at G.V. Acharya Institute of Engineering And Technology, Shelu , Maharashtra
Domain of Interest : Data Science, Machine Learning ,Artificial Intelligence

Ms. Ravina R. Kamble , Final Year Student of B.E. (computer Engineering), at G.V. Acharya Institute of Engineering And Technology, Shelu , Maharashtra
Domain of Interest : Web technologies, Database

Mr. Roshankumar Ashok Bauskar (ME IT Information and Cyber warfare), Asst. Professor and Head Of Department (HOD) Computer Engineering, G.V. Acharya Institute Of Engineering And Technology, Shelu, Maharashtra. Domain Of Interest : Big Data Analytics , Data Mining, Machine Learning, Advance Algorithm and Data Structure