DEADSEC: System Security made Simple using Web User Interface

J.Jayashree; J.Vijayashree, Vishal Goar* & N.Ch.S.N.Iyengar[#]
School of Computer Science and Engineering, VIT, Vellore, Tamilnadu
*Government Engineering College, Bikaner 334001, India
[#]Department of Information Technology, SNIST, Yamnampet, Ghatkesar, Hyderabad (TS),

Abstract

Till now, there is no such available product in the market which basically provides the service of hacking. This product/service does that. The proposed work provides service of white hat hacking by implementation of four very popular security attacks dictionary attack, man in the middle attacks, malware attack and SQL injection.It aims to reduce the time complexity of dictionary based attacks significantly with the help of Dockers using the concept of parallel programming.This work also aims to increase awareness among people about various system security attacks so that they know the vulnerabilities theirs systems are prone to and be safer.
Keywords: Security, Man in the middle attack, spoofing, password attack.

I. Introduction

People often don't understand the importance of system security until and unless their system is hacked and their data is compromised or the system stops working properly such as gets slow. This is the reason that we need such a product and so the motivation for this product is to make people more aware about security attacks and how black hat hackers achieve success in hacking innocent people's systems. Necessity is the mother of invention. Nations loose battles because of lack of information and resources but if our country has private information about plans of other nations beforehand, we can still win the battle even with fewer resources and make some serious damage in return to other nations. This website-cum-software can also be helpful for nation to hack this valuable data. Also, results are of no use if we don't get them in minimal time. This proposed work reduces the time complexity of dictionary-based network attack with the help of Dockers using parallel programming. The world is today overwhelmed by innovation. As far back as the modern transformation different new advances have been created which have added to the improvement of way of life. The latest advancement in the field of innovation since the 1980's is the utilization of PCs. PCs have refined from massive, complex machines to easy to understand and intelligent machines which could be utilized by any individual. Combined with Internet the PCs have made correspondence less demanding.

Literature Review

There are many types of attacks and this depends on what is the base of our classification. A grouping approach of cyber-attack which utilizes qualities measurements and game theoretic way to deal with arrange the attacks to their nearest classification. The standard loads of the measurements are utilized as the benchmark to order the cyber-attacks in the correct classification. The methodology is straightforward what's more, extendible; as new characters of the recently recognized attacks can be added to the attack trademark measurements and the

comparing one of a kind load to the character are doled out by the proposed equation. Other than this, the proposed methodology obviously speaks to the reason impact relationship for every single imaginable attack which encourages us to locate the proper answer for limits them in the Internet. [1]

Web applications security is a standout amongst the most overwhelming errands today, due to security move from lower dimensions of ISO OSI model to application level, and as a result of current circumstance in IT condition. ASP.NET offers ground-breaking systems to render these assaults vain; however it requires some information of actualizing Web application security. The study by the author centres around attacks against Web applications, either to pick up direct advantage by gathering private data or to handicap target locales. It depicts the two most regular Web application assaults: SQL Injection what's more, Cross Site Scripting, and depends on creator's lasting knowledge in Web application security. It discloses how to utilize ASP.NET to give Web applications security. There are a few standards of solid Web application security which make up the piece of barrier instruments exhibited: executing with least advantaged record, verifying touchy information (association string) and legitimate special case taking care of (where the new approach is exhibited utilizing ASP.NET components for unified special case logging and introduction). These standards help increase present expectations that aggressor needs to cross and therefore add to better security. [2]

ARP Spoofing is a very popular type of cyber-attack and this is the reason it is important to study about it. This study by the author portrays a lot of methods to identify ARP mocking assaults on exchanged Ethernet systems, both by proposing executions to be made straightforwardly to the switches' firmware’s and elective systems that depend just on outside components, such as particular sniffers and induction from SNMP information accumulation. These components are consolidated in an engineering general enough for pragmatic execution underway systems. Results from research facility and certifiable location tests utilizing a few prevalent assault apparatuses are additionally displayed. [3]

The Man-In-The-Middle (MITM) attack is a standout amongst the most basic assaults utilized in the system hacking. MITM aggressors can effectively summon assaults, for example, Denial of Service (DoS) and port taking, and lead to shockingly unsafe ramifications for clients regarding both budgetary misfortune and security issues. The customary guard approaches chiefly think about how to identify and wipe out those assaults or how to keep those assaults from being propelled in any case. This study by the author proposes a diversion theoretic resistance system from an alternate point of view, which goes for limiting the misfortune that the entire framework continues given that the MITM attacks are unavoidable. The author demonstrates the cooperation between the aggressor what's more, the protector as a Stackelberg security amusement and receive the Strong Stackelberg Equilibrium (SSE) as the protector's system. Since the protector's methodology space is unbounded in the show, the author utilizes a novel technique to lessen the looking space of processing the ideal barrier methodology. At long last, we experimentally assess our ideal barrier methodology by looking at it with non-vital barrier methodologies. The outcomes show that our amusement theoretic barrier methodology fundamentally outflanks other non-vital guard systems as far as diminishing the all -out misfortunes against MITM attacks. [4]. Table1 describes the techniques used.

III. Proposed Algorithm

The main aim of proposed work is to design and develop an application that provides the service of hacking. Hacking here includes (for now) some very popular network attacks which are dictionary-based attacks, man in the middle attack (MITM), SQL injection and malware attack.To reduce the time complexity of dictionary-based attacks significantly with the help of 2 or more dockers systems using the concept parallel programming.

My product is a website that allows user to choose between few system security attacks and get the required data. There has been no product like this before because of very less understanding of security attacks and how to implement them among a normal person who does not belong to this domain or profession. Also, this product could be misused also in many ways such as getting credentials of other people (black hat hacking) but because of the way it is build and the restrictions it is built with, no black hat hacking is possible using this product. Only those user requests will be accepted and compiled which does not provide any harm and doesn't comes under black hat hacking. This product is a new and self-contained product which allows user to get the required data. Also, if we understand the running of this proposed work at the backend, then we realize the vulnerabilities which make the hacking possible. So, this product can be used for learning purpose also.

The basic idea of this proposed work is that we have made the execution of different system security attacks easy by writing automated scripts for different attacks and then executing the scripts by interacting with web browser. The series of script execution starts with the selection of user on the web UI. On the basis of the selected attack, corresponding action script will be executed, all the operations and commands will run in the background in a terminal and the output and status of attack will be retrieved from the terminal by use of sub process module in python3 and then it will be displayed on the web UI. In the process all the interaction in between the web server and the web browser will be done by the help of cgi (common gateway interface) standard. For the web UI, we have used webpage templates available on the internet.

3.1 Architecture of Proposed System Design Approach

The proposed system includes different types of system security attacks and executes them on a web GUI as in figure 2. For making the proposed system more portable, a web server has been settled up so that the proposed work can be accessed from different devices on same network. Python-CGI is usedto automate the security hacking process of different attacks. Basically, Common Gateway Interface (CGI) is a standard for writing programs that can interact through a Web server with a client running a Web browser.

Python3 and sub process module is used for executing different shell commands onKali Linux. The basic idea of this proposed work is that we have made the execution of different system security attacks easy by writing automated scripts for different attacks and then executing the scripts by interacting with web browser. The series of script execution starts

with the selection of user on the web UI. On the basis of the selected attack, corresponding action script will be executed, all the operations and commands will run in the background in a terminal and the output and status of attack will be retrieved from the terminal by use of sub-process module in python3 and then it will be displayed on the web UI. In the process all the interaction in between the web server and the web browser will be done by the help of CGI (common gateway interface) standard. For the web UI, webpage templates available on the internet are used.

The basic functioning of the proposed work takes place like this- First of all the apache server setup take place, then CGI module will be enabled. The user enters IP of the server in the browser, then this request is sent to the apache server, the server retrieves the requested data (html and cgi scripts) and sends back the response to the user. After this, the user interacts with the GUI or the website and performs various functions. When the user wants to start the attack it chooses the type of attack and provides with the victims information, and then clicks the start button. On the clicking of the start button, the corresponding python CGI script to the attack will run in the background. This script provides the victim information to the kali OS and then the terminal on the Kali will search for the victim based on the given information. After the victim is found, the Kali OS will attack the victim node with the help of various modules in the terminal. After the success of the attack and the data is retrieved, but in some cases the data need to be decrypted also. In case of MITM attack, the decryption of the data takes place on a module in Kali OS which is wireshark. This decrypted data is sent to the user and displayed on the website using the apache server. The architecture diagram of DEADSEC can be understood more if we understand the architecture of 3 major components of this structure: Man in the middle module, Dockers system and Python-CGI.

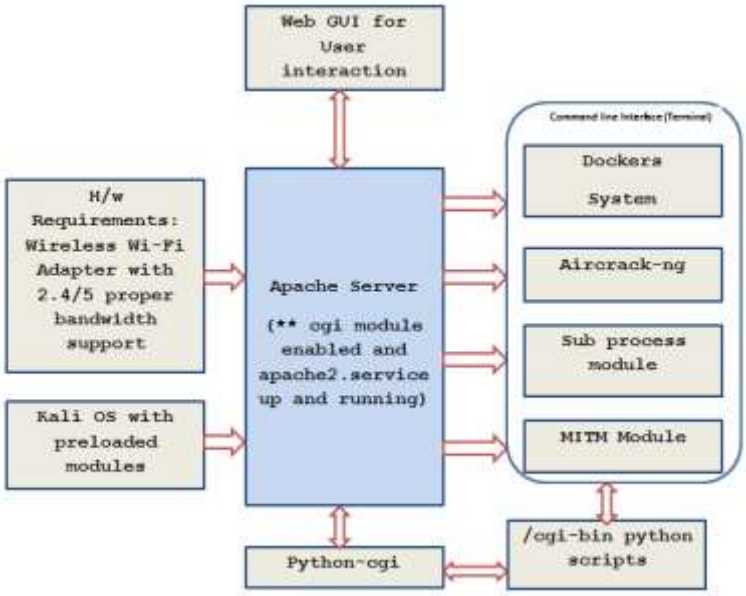

Fig.1. Architecture Diagram of DEADSEC

Activity diagram and Usecase diagram of DEADSEC is given in figure 3 and figure 4.

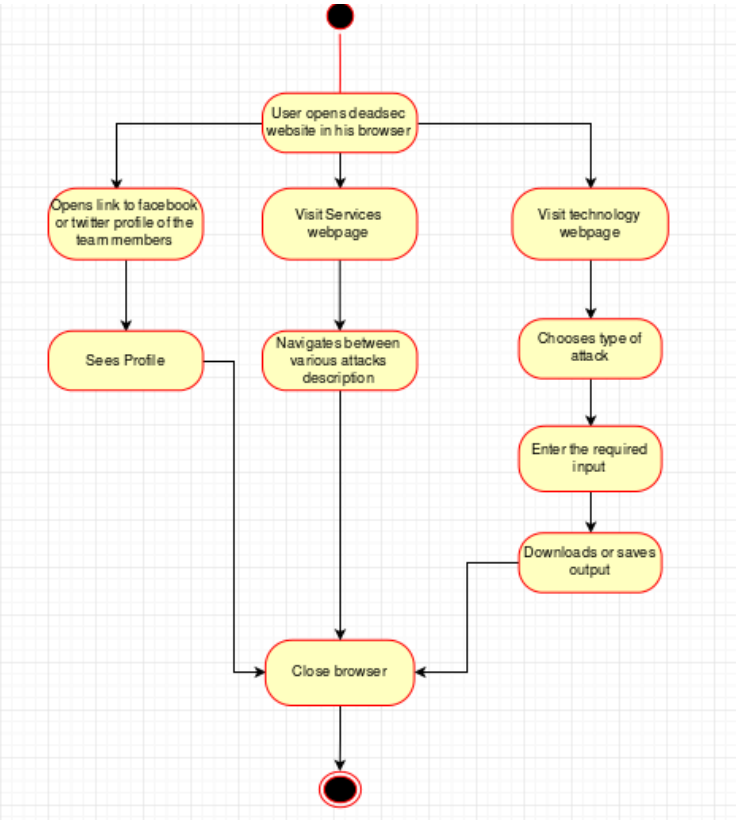

Fig.2. Activity diagram for DEADSEC

3.2 Constraints, Alternatives and Trade-offs

Security is essential for each business property to counteract burglaries and robberies and to guarantee safe business activities. In the event that robberies are not forestalled, it tends to be in all
respects
exorbitant and your business can endure. Security frameworks can help avert burglaries and robberies and guarantee safe activities of your business. Also, understanding of security and realization of how important it is for your system to be secure is like a prerequisite for living safely digitally in today's world. With the advancement in technology, people today understand the devices and systems better but they still lack in understanding the security aspects of their own system. Some of the major gaps that were recognized and solved are as follows:

Till now, there is no available GUI (graphical user interface) for better understanding and implementation of security attacks. With the help of this proposed work, this issue is faced and solved. The interactive and easy to use webpage allows user to choose the type of attack from some implemented attacks and see their implementation.

Dictionary attack usually takes a few minutes or can even take days to find the private key of the client depending on the size of the wordlist and also on the location of the correct keyword in the wordlist. This attack can be performed in a fewer time is parallel systems work together to find the correct keyword by dividing the wordlist in to parts and working on it parallel.

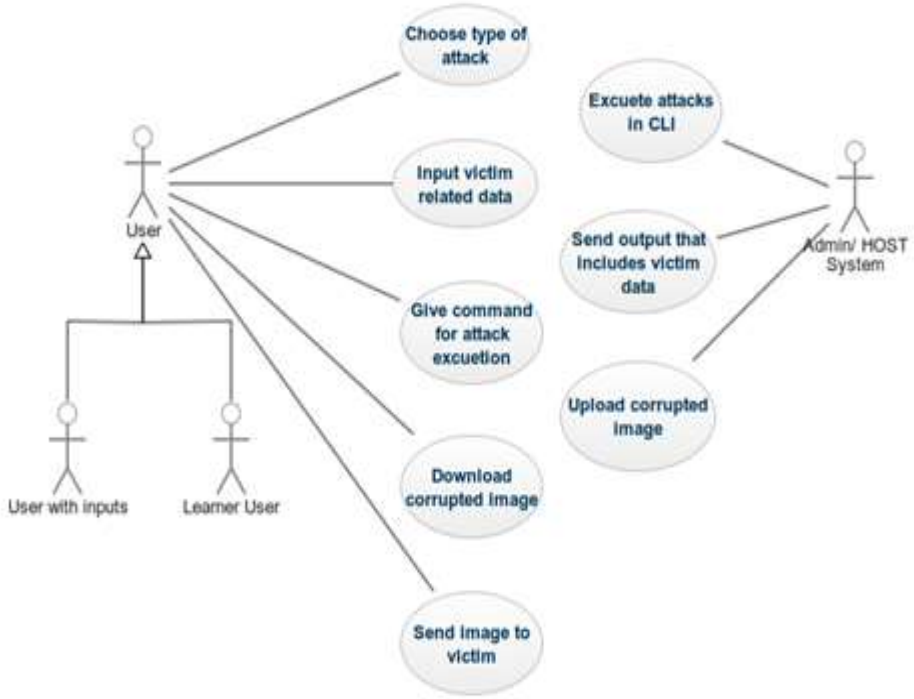

Fig.3. Use-case diagram for DEADSEC

There is no study yet that makes use of Dockers for the implementation of a network attack, and to reduce its time complexity. This paper explains how Dockers are used to reduce time complexity of the dictionary-based attacks significantly.

For the user to implement any security attack they need to either do a complete course or should have complete knowledge and should be working in this domain. But with the help of this proposed work, anyone who has or does not have any knowledge about this field can simply know about security attacks and their implementation using this website. Also, the complete implementation in the backend is done on the CLI (command line interface) without the user having any knowledge about the terminal [12].

There is much vulnerability which isn't mentioned in any of the studies yet and which are really important for everyone to know to get rid of the network breaches. One of them is the disclosement of the IP addresses in an organization network setup. We can take example of my college lab, it has the IP addresses of the system distributed in a bus topology and can

be easily guessed. So, I can access (see/manipulate/delete) data on other systems just by sitting on my system.

IV. Results and Discussion

Home page and acknowledge page is displayed in figure 4 and figure 5.

Fig.4 Welcome to DEADSEC - Homepage

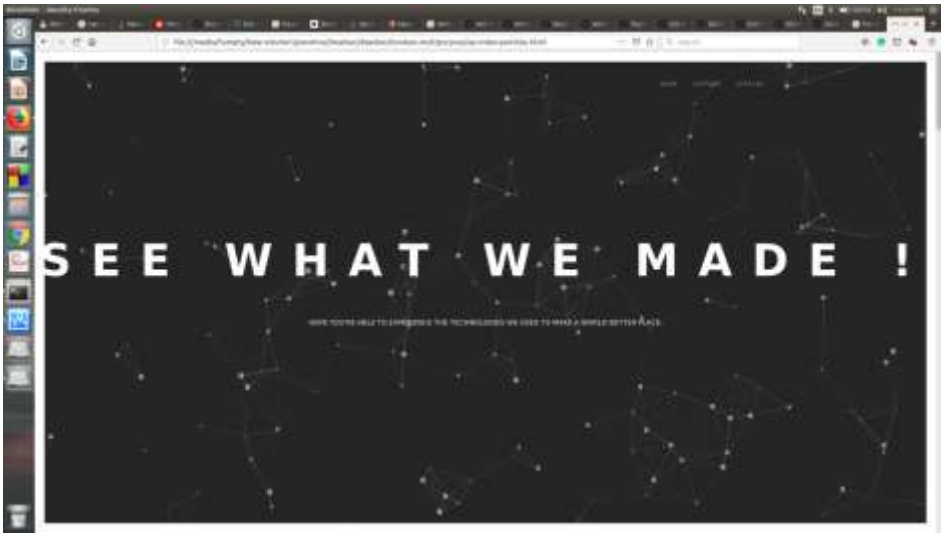

Fig1.5. Acknowledgement Page

Information about various attacks support is given in figure 6 and the password attack input is displayed in figure 7.

Fig..6. Information about different attacks-Support Page

Fig.7. Password Attack Input

The below figure 7 shows password attack successful and the password is displayed.

Fig.8. Password Attack Output

The inputs given to the mam in the middle attack is shown n figure9.

Fig.9. MITM Attack INPUT

The below figure 10 shows ARP spoofing successful. This us the output of man in the middle attack.

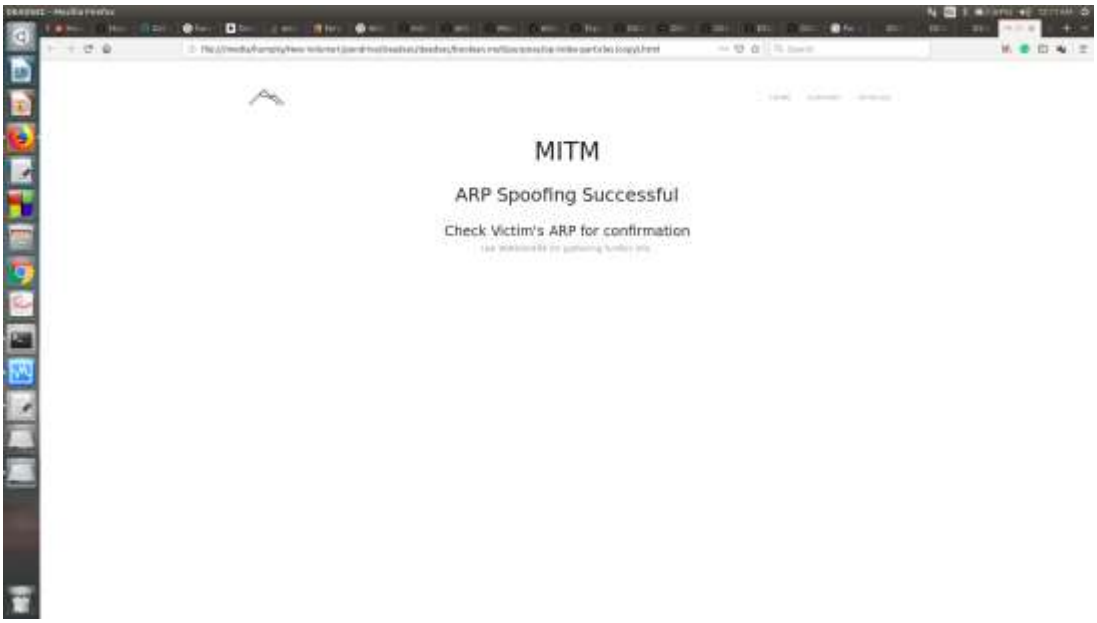

Fig.10. MITM Attack Output

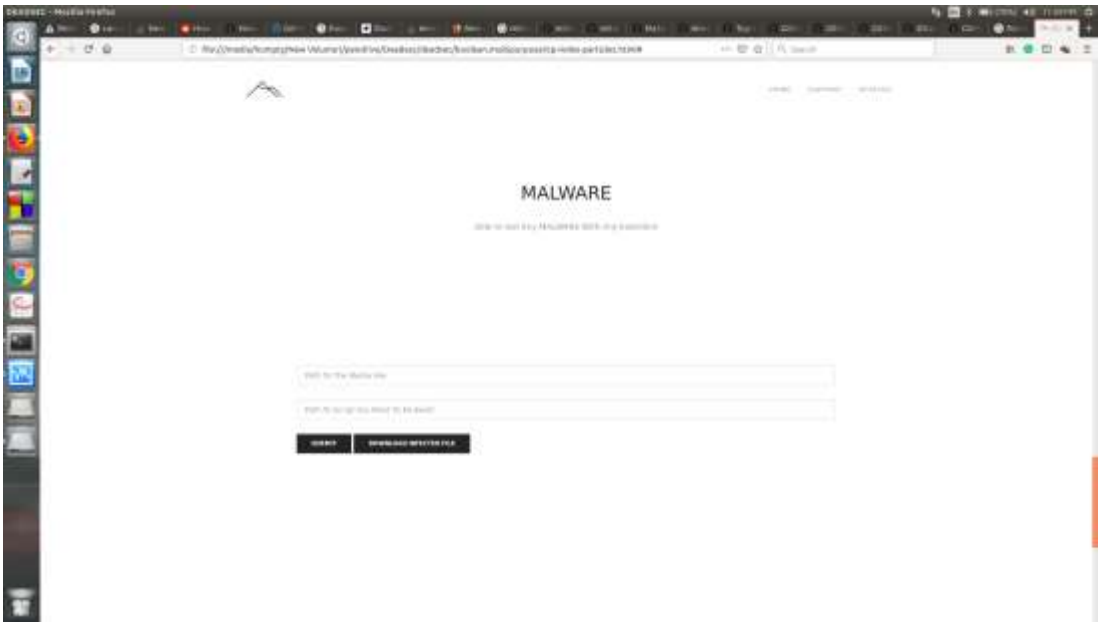

Fig.11. Malware attack input

Figure 12 illustrates the reduction in time complexity of the dictionary attack as the number of dockers increase. This proposed system mainly focused on two things- to implement various security attacks such as WPA/WPA2, MITM, SQL Injection etc. so that there is an increase in awareness among people about how much important it is to secure their

system and to decrease the time complexity of WPA/WPA2 attack using parallel Dockers. The proposed work allowed users to choose between various attacks and get the data which they want but due to lack of knowledge and resources they weren't able to do so. Till now, there wasn't any such website or software which would provide such facility to the users. This is because of the lack of knowledge among people about hacking, data and security breaches and also because such a product would be used for evil purposes also. MITM attack is implemented using various techniques such as IP spoofing, fake authentication or fake pages etc. WPAA/WPA2 security attack is implemented using 'n' number of Dockers working parallel to find the key (MIC) the targeted client. The time complexity of this attack reduces as the number of Dockers increases because the key is matched serially for each docker.

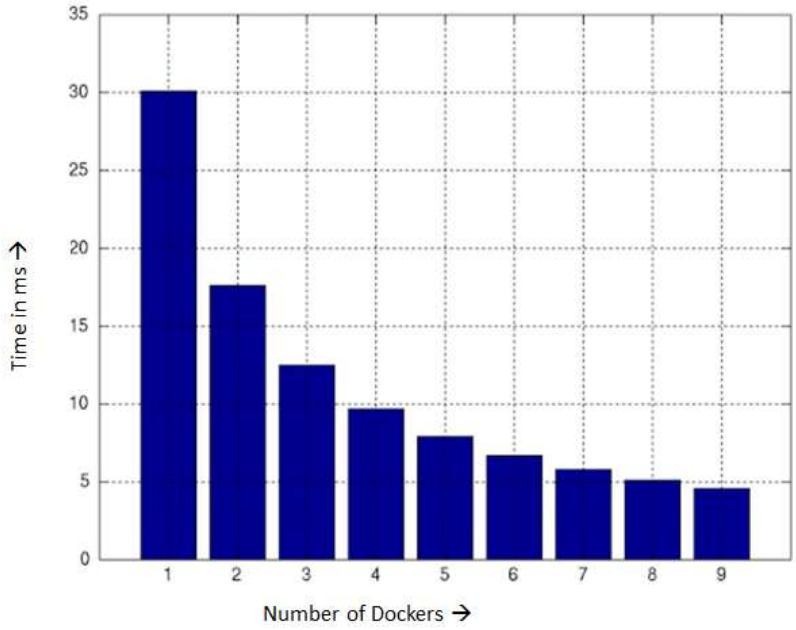

Fig.12. Reduction in time complexity of the dictionary attack as the number of dockers increases.

V. Conclusion

The importance of security can be realized just by looking at the figure of how much loss security breaches do every year financially as well as resourcefully. The proposed work was a beginning step to increase awareness among people about the execution of these attacks, so that they can understand the mindset of the hackers and keep their systems completely secure without using costly software's. However, the website allows user to get hacked data which can be used for evil purpose and this is the reason this is the only limitation of this work. Also, this proposed work discovers a new hybrid algorithm that reduces the time complexity of

WPA/WPA2 security attack drastically with the help of Dockers. In future, we hope to develop such a constraint checking algorithm that would function to accept only those user requests which comes under white hat hacking and reject those which come under black hat hacking.

References

1. B. K. Mishra and H. Saini, “Cyber attack classification using game theoretic weighted metrics,” Approach World Applied Sciences Journal, pp. 206-215, 2009.
2. B. Jovičić and D. Simić, “Common web application attack types and security using ASP.NET,” ComSIS, vol. 3, no. 2, pp. 83-96, Dec. 2006.
3. Marco AntônioCarnut and João J. C. Gondim, "ARP spoofing detection on switched ethernet networks: a feasibility study," 5th Symposium on Security in Informatics held at Brazilian Air Force Technology Institute, November 2003
4. Li, Xiaohong, Shuxin Li, JianyeHao, ZhiyongFeng, and Bo An. "Optimal Personalized Defence Strategy Against Man-In-The-Middle Attack." In AAAI, pp. 593-599. 2017.
5. Kumkar, Vishal, et al. "Vulnerabilities of Wireless Security protocols (WEP and WPA2)." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1.2 (2012): 34-38.
6. Rehman, Rizwan, G. C. Hazarika, and GunadeepChetia. "Malware threats and mitigation strategies: a survey." Journal of Theoretical and Applied Information Technology 29.2 (2011): 69-73.
7. https://www.aquasec.com/wiki/display/containers/Docker+Architecture
8. http://www.scientificamerican.com/article/the-most-vulnerable-ransomware- targets-are-the-institutions-we-rely-on-most/
9. B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, The Economic Impact of Cyber-Attacks, CRS Report for Congress, 2004.
10. Chaudhry, JunaidAhsenali, Shafique Ahmad Chaudhry, and Robert G. Rittenhouse. "Phishing attacks and defenses." International Journal of Security and Its Applications 10, no. 1 (2016): 247-256.
11. FI Software, GFI Targeted Cyber Attacks. http://www.gfi.com.
12. Basha, S. M., Poluru, R. K., Janet, J., Balakrishnan, S., Santhosh, D. D., & Kousalya, A. (2020). A Case Study on Data Vulnerabilities in Software Development Lifecycle Model. In *Impact of Digital Transformation on Security Policies and Standards* (pp. 13-32). IGI Global.