PROACTIVE NETWORK SECURITYAPPROACH FOR MULTILAYERED ARCHITECURE

Lalitha Kumari R[#1], Priyanka M[#2], Lizyflorance C[#3]
School of Information Technology and Engineering,
VIT University, Vellore-632014, India.
[1]lalithakumari.r2011@vit.ac.in
[2]priyanka.m2011@vit.ac.in
[3]lizyflorance.c2011@vit.ac.in
Prof. John Singh K*[4], Assistant Professor –Selection Grade
School of Information Technology and Engineering,
VIT University, Vellore-632014, India.
[4]johnsingh.k@vit.ac.in

***Abstract*-In order to fulfill the organization goals and objectives, multilayered network architecture and various heterogeneous server environments are used. As the network architectures are complex, there is an increased demand in information security. So each organization needs to provide sufficient network security for the known and the unknown attacks according to its goals, requirements and objectives. Highly skilled hacker's everyday discovers the new threats in order to break the security bridge in each organization. Hence the organizations are forced to revise their security policies in order to handle the network vulnerabilities that are increasing day by day. So to handle this issue a proactive network strategy is proposed against network vulnerabilities such as fraud, information leakage, denial of service attack and so on. By this approach the network is scanned periodically and the threats are prioritized and evaluated accordingly.**

Keyword-Penetration testing, Ethical hacking, Proactive security approach

I. INTRODUCTION

To challenge the growth in today's technology, multilayered architecture is implemented under various heterogeneous server environments in the organization. To secure the multilayered architecture against the vulnerability issues and the exposures an effective approach for security is needed. As organizations now acquire multilayered network architecture and heterogeneous server environments to achieve its goal it is very essential to achieve the information security. As the network threats are new and are increasing day by day it is very essential to develop the security policy for the network which is highly sensitive to the network threats and the vulnerabilities. A proactive approach should be used which will sort all types of vulnerabilities by using an appropriate method as that of the hackers. One such proactive approach is the penetration testing which is used in the organization for validating the network security. Penetration testing is used to monitor the network inside the organization against network threats. This assists the organizations to assess the security implemented and to ensure that the devices that are to be added are free from the network vulnerabilities. In this paper the existing systems are analyzed and a new algorithm is proposed to achieve the security and to safeguard the information of the organization.

II. RELATED WORK

Y. Hamisi et al. [1] have proposed that the continuous effort of an organization is to maintain the highly expanded user information. However the organization LAN must ensure the entire user content to be safe at all times and it must be prevented from all possible risk and attacks. Hence the information is systematically monitored and the security policies are evaluated in an infinite loop. To aggressively seek out all the practical vulnerabilities and risks a relevant intrusion detection test called penetration test should be suggested to scan and exploit the better prevention implication for the network security. As a result of generating the minimal percentage of the information leakage and the selective information cumulated from the penetration test one can make a deployed network safe from practical risks and attacks and make several users to share the network resources.

Zheng wu,et al. [2] have proposed a paper to build a relationship between the responses and the attacks in the Automated Intrusion Response (AIR). Based on the factors like the source attack actually initiated the techniques the hacker used and the effect of the attack caused, they proposed three dimension attack taxonomy which consists of the source dimension, technique dimension and the result dimension. In source dimension the

source of the attack can be identified into local and remote. Local attacks are from the target itself and the remote attacks are those that are initiated outside the target. In technique dimension the techniques are based on the technique that hacker adopts. In this paper the attacks are classified into seven main categories like infection, exploding, probing, cheating, traversing, concurrency and others. In result dimension the effect of the attack has four categories such as no category, rights escalation, harm implementation and information revealing. By the above taxonomy the relationship between the attacks and its response can be easily built.

Hayato Ishibashi et al. [3] have proposed a paper that deals with the protection against the network threats that are based on the IP and the MAC addresses. In this paper a protection method is used to solve the hacker from unauthorized access even if they forge the IP or MAC address. A technique in which the LAN switches are utilized in such a way to support VLAN tagging feature (The MAC frame format is included with VLAN ID so that the VLAN of each frame can be recognized). A unique VLAN ID is assigned to every switch port except the port that connects the frame filter. The frame filter is configured in such a way that the user's PC are allowed to access only the IP address assigning servers. Then the user's PC can be connected to a port of LAN switches and authenticated. This access control mechanism allows only the authorized person to send or receive the data and prevent the address spoofing.

Igor and Vitaly [4] alleges that each and every organization has to design security policies to implement it during the exploitation stage of the computer network. Security administrator has to monitor the performance of security policies on a deployed network. In this paper the authors proposed a common approach on proactive monitoring of security policy. When this approach is used, the administrator must act as an observer to reveal the serious violation of security policy taken by the user. If there is any serious violation in the result the action is taken in to an account of changing the security policies. To avoid this they suggest a model of criminal act and try to sniff the network traffic, hack the password and tries out all the possible parameter which might affect the secured data. If the security expert figures out the right parameter and access the secured data then the network is not secure and therefore the policy has to be disapproved by the organization. Such representation of criminal act controls the system from the security violation and produce better analyzed result.

GopiNath Nayak et al. [5] have proposed MITM technique which is the primary technique engaged for hacking in computers. MITM (Man-In-The-Middle attack) cite the attacks effectively. The attacks are invoked using the ARP poisoning. ARP performs the process of converting the IP address to MAC address and vice versa during LAN communication and data transformation. During this process there are many chances for hacking the system by the intruders. This paper proposes different reasons for performing attacks and the solutions to overcome it. ARP poisoning is the important issue which has to be viewed to avoid many consequences. The user-friendly solutions are proposed which are not based on the aid of the third party tool.

Nik Zulkarnaen Khidzir, et al. [6] have proposed that the Information and Communication Technology (ICT) projects were outsourced to vendors due to lack of resources. Due to this outsourcing there are chances of risk for the information security. To avoid this, a proper information security management system (ISRM) is proposed in order to manage the risks for the information disclosure during outsourcing. Research is made on this issue and the risk treatment planning is tricky during outsourcing implementation while comparing to the identification and the monitoring, due to the practices followed to execute it. The result says that the practices in the outsourcing will not affect the government and the private sectors. Other factors of risks will influence the outsourcing. The improvements in the perspective of adaptability can be achieved by bettering the process usability as per the environment. As an outcome the outsourcing in the ICT will be efficient.

Even though there are many security policies are in use, they does not result in achieving an effective security. The issue in the existing proactive approach is that they cannot predict where they are vulnerable in the multilayered architecture. The up-to-date security approach is also not sufficient to detect the modified configurations in the system. We must also keep track the system to know where they are vulnerable and also it should prevent the IP address spoofing (creation of IP packets with the forged source IP address), ARP poisoning, phishing, denial of service attack and the information disclosure etc.

III. ITERATIVE PENETRATION TESTING FOR MULTILAYERED ARCHITECTURE

The multilayered penetration testing aims at achieving security using penetration testing for the multilayered architecture. A penetration test helps to identify the threats and the vulnerabilities that exist in the organization and to ensure that the current security methods implemented are effective. It also allows finding the new vulnerabilities within the organization by keep on penetrating into the various levels of the multilayered architecture. For better security, the model in the levels of the architecture should run in an indefinite loop to identify the malicious threats and the vulnerabilities that are likely to occur at any level in the multilayered architecture. The penetration test should keep on track the activities of the organization.

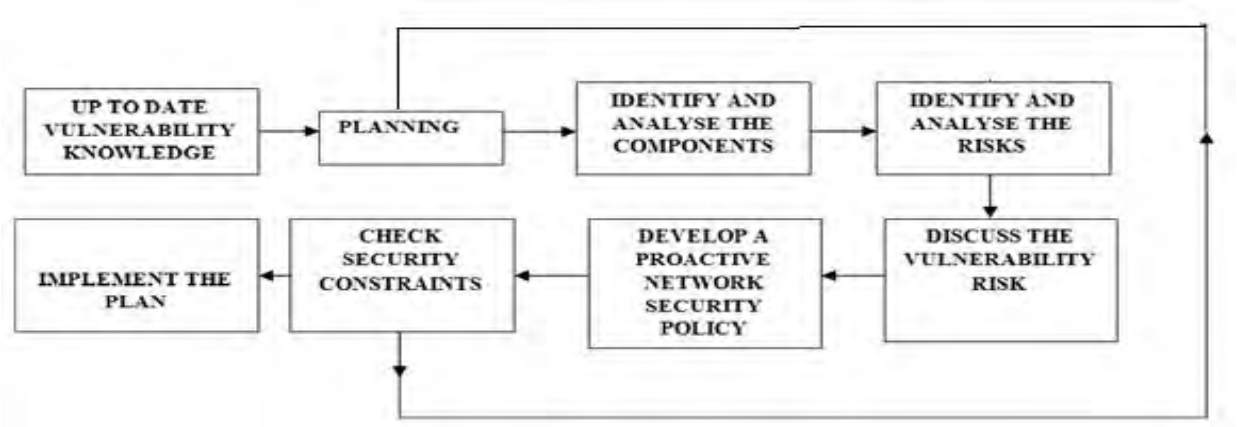

Fig 1.1 Architecture diagram for iterative penetration testing

A. Up-To-Date Vulnerability Knowledge

This is the initial phase in the penetration testing. Before we start the penetration testing we should have a thorough up-to-date knowledge about the vulnerabilities. Vulnerabilities can be classified into logical and physical vulnerabilities. The logical vulnerabilities are associated with the nodes in the network, software's, applications etc. They can be discovered manually or using automated tools or even through by browsing the internet. The detection of logical vulnerabilities can also be called as security scanning or vulnerability scanning. Physical vulnerabilities are for those that are physically connected to the network. This vulnerability analysis helps to identify logical and physical weakness in the network related to the organization.

B. Planning

The planning is the next phase in the penetration testing. It involves assembling a team for the penetration testing, gathering the information about the organization network like, the nodes involved in the network, protocols used, network architecture, access rights etc.

C. Identify and analyze the components

This phase involves in identifying the physical and logical components of the network. Physical component involves the nodes, server and the node hardware configurations, routers and all physical components that are involved in the network. Wherein the logical component involves the protocols used, the network architecture and the security methods used in the organization network.

D. Identify and analyze the risks

As the monitoring the network for security runs in an indefinite loop, the penetration testing should be able to exploit the internal and external risks that are hidden in the network. The external risk could be physical like physical damage and also logical risk like the vulnerability from the internet. In this phase the possible risks in the organization networks are identified and analyzed.

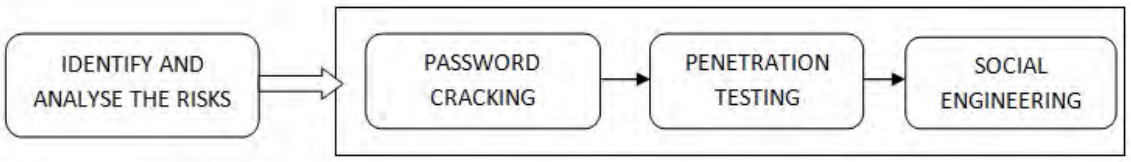

Fig.1.2 Components for Identification and Analysis of Risks

This section involves the techniques used to validate the target vulnerabilities. The objective of this section is to assume that there exists vulnerability and to demonstrate the security exposures when it is manipulated. These techniques are used to estimate the amount of risks and its impact in the target system or in the network than in any other technique.

I) *Cracking passwords:* Password cracking is the process of retrieving the password from the password hashes stored in the computer system. A hash is generated for the entered password and it is matched with the hash of the actual password of the user. If the hash values generated and the hash values of the actual password are same then the user is authenticated and is authorized. It is used to identify the user accounts with weak passwords. Password cracking involves various methods like dictionary attack, hybrid attack or brute force method etc. Using any of these methods the passwords can be cracked. If the passwords are easy to crack,

we must change the password encryption policy. Still various methods can be used to authenticate the user like password change after regular intervals of time, answering various questions after entering password etc.

II) *Penetration testing:* In penetration testing we can detect the intrusion using two analyzing approaches namely the signature based and the behavior based. In signature based penetration testing the source can communicate with the other nodes in the network only when it matches the signature of the other nodes in the network. In behavior based the penetration test is engaged to identify the new attacks without the signature. The behavior based testing is based on the previous behavior of the attacks and the behaviors that are prone to change. Throughout this phase the expected threats are to be managed. The data transfer is between the server and the client or between the source and the destination. This phase should be handled meticulously as if there is any break down in the middle of the information transfer the penetration testing will be blamed. During this phase it is important to have a constant communication with the source to manage the expected threats. When it is discovered that the potential vulnerabilities have undertaken the data, then it should inform and acknowledge the source about unauthorized access of data in middle by capturing and sending the flag value and the source has to stop the information transfer and corresponding actions are to be taken for the attack that has happened. The goal of achieving the security is that the response should be proportional to the threats. The penetration testing should be able to block, modify or redirect any malicious threats and the vulnerabilities.

III) *Social Engineering:* It is the most important method in the field of network security. It plays a main role in improving the security of the organization. Social engineering is a trick of revealing privacy information of the specific target such as high value individual or a group in the organization. It tests the awareness of user security and makes use of their weakness behavior of not following the standard procedure. These targets have to be identified by the organization or the individual only by the known existing threats or by the information loss. Some of the methods followed are phishing, fraudulent emails or analog engineering which may be tracked by their conversation conducted through phone (Eaves dropping). Penetration tester should produce a complete report of successful and unsuccessful policy used which helps the organization to modify their security policy and to have a clear awareness about the tactics.

E. Discuss the vulnerability risk

Here the impacts of the risks are discussed. How far the risk could damage the network falls under this phase. The degree of the information exposure and the risk vulnerabilities are discussed for developing an appropriate security strategy.

F. Develop a proactive network security policy:

This is the most important phase in the proposed system. The proactive network security policy includes the penetration testing. As the organizations uses multilayered architecture it is vital to provide security at each layer as they are more prone to security threats. The developed proactive security policy should be highly sensitive in identifying the network vulnerabilities such as spoofing, denial of service attack, information fabrication, privilege escalation, viruses and malwares etc. The security approach should be proactive. On identifying an intrusion it should give the intruder a warning and also it should prevent the intrusion from occurring.

G. Check security constraints:

This can be achieved by ethical hacking. If so the system is not secure enough it should report and record why they are vulnerable and also it should iterate from identifying the risk until an effective security plan which is highly sensitive to network risks end vulnerabilities are developed for the organization. On successful development the plan should be implemented.

IV. RESULTS AND DISCUSSIONS

A. Statistical attacks

Statistical attacks are based on prediction. Predicting the relationship between the source and the destination may allow the hacker to determine the possibilities of attack to damage the network system. But in the proposed penetration testing architecture it keeps track the network and safeguards the network with a proactive network approach which is highly sensitive to the network threats. So the attacker can hardly predict the relationship.

B. System use attack

System use attack is based on the security approach used in the system. The security system should increase the security and it should be able to handle the attacks effectively. The penetration testing approach thus proposed runs in an indefinite loop. It keeps on monitoring the system and identifies the network vulnerabilities and also the threats that are prone to happen. It prevents the system from attack that causes damage to the system by proactively implementing the security policies that are sensitive to the network attacks.

C. Perceptual attack

*P*erceptual attack is based on the perception. This attack is handled in the proposed system by ethical hacking. The trusted persons in the organization by perception are allowed to hack the system. If the system can be attacked then build a better security approach to safeguard the system from attacks.

The vulnerabilities are handled intelligently by monitoring the attacks in an indefinite loop. The proactive way of identifying the critical vulnerabilities allows the organization to intelligently manage the vulnerabilities. Immediate actions and remedial measures have to be performed on the attacks and the necessary security patches are applied. As no company wants to lose its clients due to data breeches, penetration testing is used to preserve the customers and to maintain a good image in the corporate world. This testing ensures how well an organization defensive policy and mechanisms are functioning through iterative testing and monitoring to protect the valuable assets. To achieve this penetration testing effectively one should have a clear up-to-date knowledge about the emerging threats and should know to handle it immediately and effectively.

VI. CONCLUSION

The proposed penetration testing approach helps to proactively monitor the network security policies and uses various methodologies to track the attackers. It checks for the vulnerabilities and explain how the vulnerabilities can be demoralized iteratively to achieve the better access of the network with the reduced risk of security attacks. Risks are coupled with all methodologies, to ensure the security of each technique a penetration tester should follow the basic skill set. The suggested approach in this paper is based on the imitation of different users and attackers action in the network which provides us the clear idea of approving or not approving the security policy and to redesign the organization security policy effectively.

REFERENCES

[1] N. Y. Hamisi, N. H. Mvungi, D. A. Mfinanga, B. M. M. Mwinyiwiwa, “Intrussion detection by penetration test in an organization network”. Proceedings on the 2nd International Conference on Adaptive Science & Technology, 2009, Pp: 226-231.

[2] Zheng Wu, Yang Ou, Yujun Liu, “Taxonomy of Network and Computer Attacks Based on Responses”, Proceedings on the International Conference of Information Technology, Computer Engineering and Management Sciences.2011-IEEE, Pp: 26-29.

[3] Hayato Ishibashi , Nariyoshi Yarn,Kota Abe,Toshio Matsuura, “A Protection Method against Unauthorized Access and Address Spoofing for Open Network Access Systems”. Proceedings on the IEEE-2011, Pp: 10-13.

[4] Igor Kotenko, Vitaly Bogdanov,” Proactive monitoring of security policy accomplishment in computer networks”.Proceedings on the IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. 2009. Pp: 364-369.

[5] Gopi Nath Nayak and Shefalika Ghosh Samaddar,” Different Flavors of Man-In-The-Middle Attack Consequences and Feasible Solutions”.Proceedings on the IEEE. 2010. Pp: 491-495.

[6] Nik Zulkarnaen Khidzir, Azlinah Mohamed, Noor Habibah Hj Arshad ,“Information Security Risk Management-An Empirical Study on the Difficulties and Practices in ICT Outsourcing” Proceedings on the 2nd International Conference on Network Applications, Protocols and Services 2010. Pp: 234-239.