Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 6, June-2016

Enhancement of network security: An ethical hacking approach

B. S. Malapur, Soumya I. Patil

Department of Computer science and engineering, Basaveshwar engineering college Bagalkot

Abstract — In any organization most important issue is in maintaining information security. Nowadays cracking into security systems is very common issue. Even though all precautions are taken still data may be compromised. One among this is data theft using web sites. There are thousands of web sites those fool user by wearing a mask of real web sites. So in order to avoid security leakage it is important to use web sites safely because hacking is growing like a bamboo tree. Hackers are those whose intention is to break into the system and they may compromise the data or my not. So it is essential to avoid such situations. There are many ways by which user can safely use web sites and can go for online transaction. One way is through logging into safe website. This is done by safely logging into registered URLs. And second is keeping webpage safe by developing it using strong design tools. First one is achieved by developing a tool that identifies real and fake websites. And second is demonstrated by taking an example of admin panel. Main aim of the work is to achieve data security as well as trust.

Keywords- Ethical hacking; network security; information security; fake website; SQL injection

I. INTRODUCTION

Ethical hacking refers to penetration testing that ensures security of an organization's information system. First time this technique was used in security evaluation that is conducted by the United States Air Force of the Multics operating systems. And now this hacking is big billion business. Every big organization is in need of hackers to check their network tightness and weaknesses. There are many ways to do this hacking say fake websites, viruses, worms, malware attacks, Trojan horse etc. This work speaks about enhancing network security by using hacking as a tool. As it is already discussed, there are many types and categories in hacking. Using any of these types one can enhance network security. Such as by means of spoofing one can check how network behaves for unknown entity and how it reacts for unregistered entity. This work consists of two modules first is generation of tool so that fake websites can be identified by taking 100 samples. Second is SQL injection. In which Java code is written to solve the problem of SQL injections to web admin panels. First module involves generation of fake website of facebook and pretending as a real website by sending suspicious mail to real facebook user. By this means user enters username and password of their account. This information is being stored into database of third party as it is not real website. This is one way of hacking username and password of social network account holders. This may leads to data theft, compromising sensitive information, un-authorized accessing or even harm to individual user. So in order to overcome this problem in our work we have produced solution by means of a tool. This tool will prevent one to access malicious or fake websites. In module 2 we are going to demonstrate about SQL injections and how to get rid of SQL injections. SQL injection is very old and powerful hacking technique. It involves breaking into database hence modify database structure. It may involve update of tables, deleting tables, modifying tables etc. Our work involves hacking into admin panel by means of SQL injection and adding Java script to get rid of it. Usually SQL injections are carried on admin panels of websites to gain access. Once the access is gained anything can be done on database.

II. RELATED WORK

There are many issues identified by literature survey such as accountability, security of data, distributed systems, configuration of tasks etc. Among these data security and configuration of tasks are the main issues that are appearing in almost all the papers. And it is also identified that hacking is a big challenge in growing network systems. It is also proved by survey that hacking is best possible way to pull out the flaws provided hacker should follow the professional ethics. There are many ways of hacking as given in few papers, one may use cryptography, one may use ASCII key code, one may use WEP or may go for already developed hacking tools. In order to cope up with these challenges new hacking techniques are needed to identify the vulnerabilities in the system. Even though there are lots of security given by providers, website developers, organizations etc. there may be a possibility by which they may be cheated. There are many issues in network such as synchronization, connection, hardware-software etc. These issues are simple can be solved easily. But there are complex issues to be solved. These complex issues are discussed below:

- *Network growth*: as the number vehicles increases traffic increases, space required to seat occupancy increases, burden over maintenance increases. Like this as the number of machines increases in computer network traffic of packets increases, space required to place machines increases, burden over maintenance increases. It is big challenge in computer networks.
- *Network security*: Most of the times computer anal0yst speak about none other than computer security. It is very important in terms of computer science and engineering. So security is one more important issue.

- *Configuration task*: Most of the money and time of industrialist is consumed on configuration of systems. Configuring computers, configuring tasks among computers is more time consuming. So it is also an important issue.
- *Centralized management*: As the technology is growing we are moving towards distributed management where there is no centralized control. Even though distributed is far better than centralized there are issues can only be solved by centralized system.
- *Lack of accountability*: in networks accountability is very important. As network grows machine also grows and it becomes important to keep track of every device.

Among above discussed issues our work mainly concentrates on *Network security*. As we have already discussed as the usage grows, system also grows. So it becomes important to keep system secure. In last few decades security became most important issues in every field. Take hospital management, railway reservation, cloud computing etc. security is a main issue. There is a different module to manage surety issue. So keeping this in mind our work mainly concentrates on security that too in websites. Websites are easiest and dangerous ways to leak or to compromise sensitive information. Through fake websites they may acquire username passwords of social networks, credit card details, ATM pin numbers etc. fake websites look like real but if we cleanly observe it we can identify. One more method of data theft is SQL injections. SQL injection is very old yet developing technique. Data theft by means of this is 65% -75%.

III. IMPLEMENTATION AND RESULTS

There are many ways to do ethical hacking. This work is making use of two categories among 18 modules of hacking. There are two modules first one deals with hacking username and password through fake website and developing a tool that identifies fake websites. And second module deals with code injection and getting rid of SQL injection by Java and PHP script.

3.1. First module

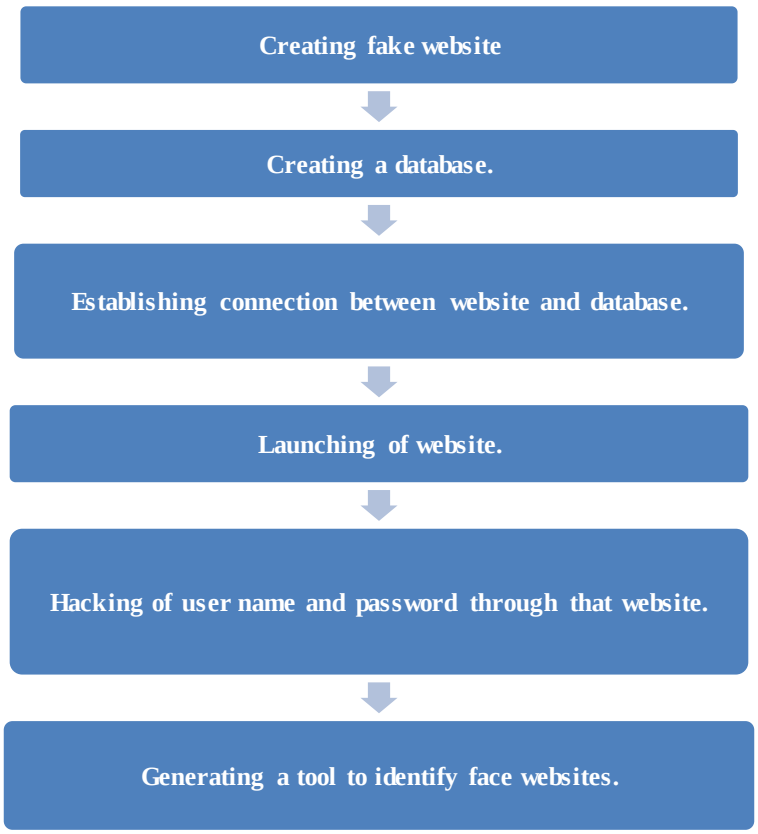

Figure 1. Work flow of first module

For demonstration purpose fake website of facebook is created using HTML and PHP in the backend. For storing username and password mySQL of WAMP server is used in backend. And tool is developed using mySQL. Brief working of first module is as follows: Facebook user is mailed with suspicious e-mail saying facebook is providing free software. On clicking the link fake facebook website appears user enters username and password without knowing it is fake website. Once the data is entered it comes and hits database. This is nothing but hacking by fake website. There are many steps to indentify real website. First comes always domain name of a website, if website is registered in domain

name server it will be having domain name such as “facebook.com” or “gmail.com”. If it is not registered domain name will be some IP address such as “192.168.91.12/facebook.html” or http://198.165.241.22/gmail.php”. If website address is like this then it is fake. Second is spelling of website say spelling of facebook website is facebook all are English letters. If it is like faceb0k where second ‘o’ is actually a zero(0) not character ‘o’. In such cases website is fake. Third is domain name server information of a website. If website is registered we can get domain name server information of website otherwise no. Fourth is about more secure websites such as online banking websites, shopping websites some government website where there is sensitive information. All websites of this type are running under SSL that is secu re socket layer. That we can identify by looking at URL bar which consists of green lock symbol. If a website is running under SSL it is more secure. If all the above conditions are satisfied then the website is real and safe to use. In our work we are considering all the above conditions to identify real and fake websites. The tool will display whether the website is safe or fake by copying protocol and domain name of the website. Such as “http://www.onlinesbi.com”. This tool is developed keeping online frauds such as online banking, online shopping and some social networks such as gmail, facebook, radiffmail etc. Operating this tool is simple user has to just copy part of URL (Protocol part+ Domain name of website) and paste in the search bar of tool before entering sensitive information such as usernames and passwords, press enter.

3.2. Second module

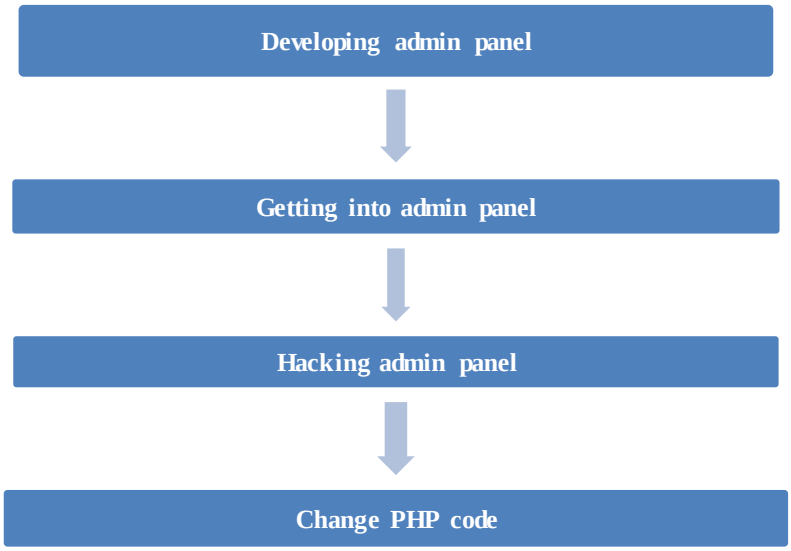

Figure 2. Work flow of second module

In second module we have developed admin panel to illustrate how admin panels are being hacked. Using again HTML and PHP designing tools. Admin panel contains two text boxes one for username and one more for password. Username is “root” and password is “admin”. If user enters root and admin inthere respctive positions a window opens which contains table “user” information (This user table in in first module where contents of table are all the user information i.e username and password entered through fake website of facebook.). If user enters different username and password other than root and admin webpage will display SQL error. This is normal operation of any admin panel. But one can hack or gain access to admin pacel by means of suspicious queries. Such as instead of entering simply root in the text box we can write 1’ or ‘1’=’1 or 1.1’ or ‘1.1’=’1.1. This is nothing but “select * from user where username= ‘1’ or ‘1’= ‘1’;” where second condition always holds true. Even in the palce of password we can place the same code. If it is enterded we can get access to admin panel. In order to stop it we have to add one extra line of code in PHP or in Java.

By changing small code in PHP script we can avoid injections. Usually admin panels are written in PHP or HTML using of Java script is less. We can enhance security by means of using Java script. SQL injection plays with queries such as select. By changing a query or by confusing it we may do our work. Such as usually select query contains comparison part as “select * from user where username=’admin’;” in this case * means complete table content and user is table name. Instead we can write “select * from user where username= ‘admin’ or 1=1;” where second statement always holds true. This is called as SQL injection. Not only getting access to admin panel we can drop entire table by using Drop command. Our work is doing the same thing. First it is shown that how admin panels are hacked and next how to get rid of it. Totally there are 18 modules in hacking we are considering two among them one is fake website and second is SQL injections. By using each of the technique we are showing how it is working and how to overcome that by using our own developed tools not using any tools that are already available.

IV. CONCLUSION AND FUTURE WORK

The main aim of the work is to improve network security by using hacking as a tool. Result of the work is the tools developed those will provide efficient solution for the problem defined and emerge as one of the strongest tool in the future. The tool is needed because now a day every transaction in through online and there are more chances of online fraudulent. So in order to avoid miscommunication as well as keeping safety of data which is sensitive it is more important to provide safety. Data security and trust are main key concepts in this work and are achieved as well. This project is made by keeping 100 samples of real web site URLs and admin panel developed in PHP and HTML. This can be carried away by taking all real website URLs and admin panels developed using ASP.net and Java. Yet it is difficult to check all the websites as there are thousands of websites are being developed per day but this can be worked over very frequently used website that needs secure transaction.

REFERENCES

[1] Bryan Smith, William Yurcik and David Doss, "Ethical Hacking: The Security Justification Redux, 2002" 0-7803-7824-0/02 62002.

[2] Tzer-Shyong Chen, Fuh-GwoJeng and Yu-Chia Liu, "Hacking tricks toward security on network environments, 2004" 0-7695-2736-1/06.

[3] Matt Bishop and Deborah A. Frincke, "About Penetration testing, 2007" 1540-7993/07.

[4] Aakash Trivedi, "A Comprehensive Online Tool that Detects Security Flaws in Networks, 2008", 978-1-4244-5540-9/10.

[5] Thomas G. Zimmerman, "Hacking in Industrial Research and Development, 2008", 1536-1268/08.

[6] David Alan Grier, "Harry and Georgie, 2008" publication.

[7] Mamatha G and Ashoka B M, "Unofficial Hacking Algarithms, 2009", 4th-6th June 2009.

[8] S Vinjosh Reddy, K Rijutha, K SaiRamani, Sk Mohammad Ali and CR Pradeep Reddy, "Wireless Hacking - A WiFi Hack By Cracking WEP, 2010", 978-1-4244-6370-1.

[9] Esha Datta, and Neeraj Goyal, "Security Attack Mitigation Framework for the Cloud, 2012", 978-1-4799-2848-4/14.

[10] Gabriel Avramescu, Mihai Bucicoiu, Daniel Rosner, Nicolae Tapus, "Guidelines for Discovering and Improving Application Security, 2013", 978-0-7695-4980-4/13.

[11] Gatta Sambasiva Rao, P.Naveen Kumar, P.Swetha and G.BhanuKiran, "Security Assessment of Computer Networks –an Ethical Hacker's Perspective, 2013".

[12] Zouheir Trabelsi and Walid Ibrahim, "Teaching Ethical Hacking in Information Security Curriculum: A Case Study, 2013", b978-1-4673-6110-1/13.

[13] Mr. Prashant Rewagad and Ms.Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing, 2013", 978-0-7695-4958-3/13.

[14] Nandita Sengupta and Jeffrey Holmes, "Designing of Cryptography Based Security System for Cloud Computing, 2013", 978-0-4799-2235-2/13.

[15] Nedaa Baker Al Barghuthi and Huwida Said, "Ethics behind Cyber Warfare: A study of Arab Citizens Awareness, 2013", 978-1-4799-4992-2/14.

[16] Mr. Prashant Rewagad and Ms.Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing, 2013" , 978-0-7695-4958-3/13.

[17] Victor Chang and Muthu Ramachandran, "Towards achieving Data Security with the Cloud Computing Adoption Framework ,2015",DOI 10.1109/TSC.2015.2491281 .

[18] Text book of Manthan Desai "Hacking for beginners, 2010".

[19] Text book of Patrick Engebretson "The basics of hacking and penetration testing".

[20] Text book of Dan Boneh "SQL injection: attacks and defences".