International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 2 –NOVEMBER 2014.

Ethical Hacking and its Advantages

Ramesh Babu Palepu

Associate Professor, Department of CSE, Amrita Sai Institute of Science & Technology

Abstract— Today more and more software are developing and people are getting more and more options in their present software. But many are not aware that they are being hacked without their knowledge. A good ethical hacker should know the methodology chosen by the hacker like reconnaissance, host or target scanning, gaining access, maintaining access and clearing tracks. From the point of view of the user one should know at least some of these because some hackers make use of those who are not aware of the various hacking methods to hack into a system. Also when thinking from the point of view of the developer, he also should be aware of these since he should be able to close holes in his software even with the usage of the various tools. With the advent of new tools the hackers may make new tactics. But at least the software will be resistant to some of the tools. Here in this paper described various advantages of ethical hacking.

I. INTRODUCTION

Ethical hacking-also known as penetration testing or intrusion testing or red teaming has become a major concern for businesses and governments. Companies are worried about the possibility of being “hacked” and potential customers are worried about maintaining control of personal information. The expression "computer hacking" carries images of unscrupulous techies who use their skills to However, some companies have employed so-called "ethical hackers" to explore their own computer systems and find potential weaknesses. These "white hat" hackers can demonstrate how their "black hat" counterparts can damage vulnerable systems, while offering advice on how to protect their clients from such dangers. Ethical hacking can also ensure that vendor’s claims about the security of their products are legitimate.

Security

Security is the condition being protected against danger or loss. In the general sense, security is a concept similar to safety those persons who is a passive person should not see those data. For example in the case of a credit card transaction, the authorized person should see the credit card numbers and he should see that data.

Integrity

Integrity means that data cannot be modified without authorization. This means that the data seen by the authorized persons should be correct or the data should maintain the property of integrity. Without that integrity the data is of no use. Integrity is violated when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. In such cases the data is modified and then we can say that there is a breach in the security.

Availability

Information system to serve its purpose, the information must be available when it is needed. Consider the case in which the data should have integrity and confidentiality achieving both these goals easily we can make those data off line. But then the data is not available for the user or it is not available. Hence the data is of no use even if it have This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it functioning correctly.

Security

Computer security is required because most organizations can be damaged by hostile software or intruders. Moreover security is directly related to business. This is because if a company losses a series of credit card numbers of its customers then many customers would be hesitant to go back to the same company and that particular company will lose many customer and hence the business. There may be several forms of damage which are obviously interrelated which are produced by the intruders. These include: lose of confidential data damage or destruction of data damage or destruction of computer system loss of reputation of a company .There may be many more in the list due to security breaches.Ethical hacking is also known as penetration testing, intrusion testing or red teaming. With the growth of the Internet, computer security has become a major concern At the same time, the potential customers of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses. In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems. This scheme is called Ethical Hacking. This similar to auditors come into an organization to verify its bookkeeping records. This method of evaluating the security of a system has been in use from the early days of

computers. In one early ethical hack, the United States Air Force conducted a security evaluation of the Multics operating systems for potential use as two-level (secret/top secret) system Successful ethical hackers possess a variety of skills. First and foremost, they must be completely trustworthy. While testing the security of a client's systems, the ethical hacker may discover information about the client that should remain secret. In many cases, this information, if publicized, could lead to real intruders breaking into the systems, possibly leading to financial losses. During an evaluation, the ethical hacker often holds the keys to the company, and therefore must be trusted limited-access labs with connections, a safe to hold paper documentation from clients, strong cryptography to protect electronic results, and isolated networks for testing. Ethical hackers also should possess very strong programming and computer networking skills and have been in the computer and networking business for several years. Another quality needed for ethical hacker is to have more drive and patience than most people since a typical evaluation may require several days of tedious work that is When they encounter a system with which they are unfamiliar, ethical hackers will spend the time to learn about the system and try to find its weaknesses. Finally, keeping up with the ever.

II. WHAT DO AN ETHICAL HACKER DO?

An ethical hacker is a person doing ethical hacking that is he is a security personal who tries to penetrate in to a network to find if there is some vulnerability in the system. An ethical hacker will always have the permission to enter into the target network. An ethical hacker will first think with a mind-set of a hacker who tries to get in to the system. He will first find out what an intruder can see or what others can see. Finding these an ethical hacker will try to get into the system with those information in whatever method he can. If he succeeds in penetrating into the system then he will report to the company with a detailed report about the particular vulnerability exploiting which he got in to the system.

Advantages of Ethical Hacking

Testing Security Measures The primary advantage of having ethical hackers on a company's payroll is that the hackers are allowed to test a can help companies determine which of their computer security measures are effective, which measures need updating, and which ones pose little to no deterrent to dangerous intruders. The data from these tests allows management to make informed decisions on where and how to improve their information security.

Finding Vulnerable Areas When the white-hat hacker's finish exploring the company's system, they turn in a report on the system's vulnerable areas. These areas can be related to the technology, based systems, such as administrators who give out passwords to unauthorized personnel. The exposure of these vulnerabilities allows management to install more secure procedures to prevent attackers from exploiting either the computer Understanding Hacker Techniques White hat hackers can also demonstrate the techniques used by unethical invaders. These demonstrations serve to show management how thieves, terrorists and vandals can attack their systems and handle sensitive data must understand that they serve as potential targets of a hacker attack. Smaller companies that lack the resources for adequate network security present black-hat hackers with tempting targets of opportunity. These attacks can cripple or destroy small businesses as much as a fire or a natural disaster. The use of white-hat hackers can show these companies.

Transcription

What are the benefits of ethical hacking? I get this asked quite a bit. The benefits of ethical hacking are a little different than the benefits of network defence or perimeter defence, because ethical hacking helps any system owner or business owner find the vulnerabilities before an attacker does, in a way so that the attacker would find if they were actually committing an attack. That's why ethical hacking uses these attacker techniques. That's why it actually uses the real tools, technologies, methodology and approaches that an attacker would, rather than using a SAS process that an auditor might use. Or, rather than using the CISSP framework for defence.

Modelling

Modelling an attack always finds vulnerabilities that cannot be found any other way. It helps document both weak security areas, areas where an attacker can get in, and also strong security areas. Areas where an attacker is thwarted, takes forever. Those are the kinds of areas that we don't need to worry about, or maybe need to extend those areas or any security model is the key benefit of ethical hacking. That's really why folks do this. I mentioned a little bit ago that ethical hacking is actually more of an attack technique. It uses attacker tools, approaches and posture of an attacker creating a big difference between ethical hacking and network security.

Network Security

Network security is more about defending and documenting defences. You are finding out about firewalls and putting them up. You will find out about VPN server security and actually instantiate VPN servers. It's typically not about modelling an attack the way an attacker would. Those are very different things. Network security typically entails following best practices or common techniques in order to implement and operate in a secure manner. Ethical hacking is finding the weaknesses in those implementations, weaknesses and then feeding them back into a network security process that helps defend against them and repel those types of potential attacks from future occurrences..

III. CONCLUSION

One of the main aim of the seminars is to make others understand that there are so many tools through which a hacker can get in to a system. There are many reasons for everybody should understand about these basics. Let's check its various needs from various perspectives. Student A student should understand that no software is made with zero vulnerability. So while they are studying they should study the various possibilities and should study how to prevent that because they are the professionals of tomorrow. Professionals should understand that business is directly related to security. So they should make new software with vulnerabilities as less as possible. If they are not aware of these then they won't be cautious enough.

IV. REFERENCES

[1] Hacking: The art of exploitation – John Erickson, 2nd Edition-William Pollock The basics of Hacking and Penetration testing – Patrick Engebretson-Elsevier An unofficial guide of Ethical Hacking – Ankit Fadia, 2nd Edition -Macmillan publishers India Ltd.

[2] The unrevealed secrets of Hacking and Cracking-Prateek Shukla & Navneet Mehra- Unicorn Books Pvt. Ltd.

[3] Windows Hacking 2.0- Ankit Fadia - Vikas Publishing House Pvt. Ltd.Hacking web services – Shreeraj Shah – Delmar Cengage Learning.