International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 5 –NOVEMBER 2014.

Network Security and Business Protection through Ethical Hacking

Dama Anand[#1] and Akki Suresh Babu[*2]

[#]*Asst. Professor, Department of CSE, UshaRama College of Engg & Tech, Telaprolu, Vijayawada, A.P., India*

[*]*E-Tutor, Tutor vista (E-learning), Bangalore, Karnataka, India*

Abstract— Ethical hacking involves computer and network professionals who use their expertise to safeguard the networks of an organization on behalf of its owners. In order to test a security system, they seek vulnerabilities that a malicious hacker could exploit. Ethical hacking is also known as penetration testing, intrusion testing, and red teaming. An ethical hacker is sometimes called a white hat while the other one is called black hat. Ethical hackers collect and assess information on issues like loopholes which are truly a security threat, the depth to which a hacker can get into via one of these holes and the patching requirements in order of priority. The ethical hacker aims to help the organization take anticipatory measures against malicious attacks by attacking the system himself; all the while staying within legal limits. The most important point is that an Ethical Hacker has authorization to probe the target. The reason is that as technology advances and organizations depend on technology increasingly, information assets have evolved into critical components of survival and need to be protected at any cost

Index Terms— Intrusion Testing, automated tools, Business Objectives, security architecture, NDA

I. INTRODUCTION

Businesses of all sizes are increasingly challenged to adopt new technologies such as cloud computing and virtualization and business practices such as bring-your own- device and IT outsourcing. To complicate this challenge, companies face increasingly targeted and sophisticated attacks. Attackers now range from organized crime rings to advanced nation-states and are highly organized, skilled, and motivated. Despite the prevalence of firewalls, IPS, anti-virus and other security technologies, many businesses continue to fall victim to these attacks due to unintentional configuration errors. As a result, companies are beginning to recognize the importance of human experience and analysis in a best-of-breed security architecture.

Ethical hacking companies offer tremendous value in their ability to share their advanced security knowledge and expertise with customers. This service enables businesses to adjust their security technologies, train their staff, and enact security practices that better protect critical systems and sensitive data. Ethical hacking services provide customers with objective and real-world assessments of security weaknesses, vulnerability, risk, and remediation options. As a result, ethical hacking is rapidly gaining attention as an essential security practice that should be performed on a regular basis.

However, businesses must be careful to select a reputable and experienced ethical hacker to ensure an efficient and productive assessment. Customers can better plan and implement a successful ethical hacking consultation by first understanding the challenges and best practices in this market. To better support both technical and business decision makers considering ethical hacking services, Frost & Sullivan has conducted interviews with key industry participants and customers to identify leading challenges and best practices as well as extensive secondary research. This paper presents these findings to provide customers with the knowledge necessary to justify and implement leading ethical hacking services into their security architecture.

II. WHAT ISETHICALHACKING?

The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. As, with most technological advances, there is also other side: criminal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are called black hat hackers. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. So, this paper describes ethical hackers, their skills and how they go about helping their customers and plug up security holes. Ethical hackers perform the hacks as security tests for their systems. This type of hacking is always legal and trustworthy. In other terms ethical hacking is the testing of resources for the betterment of technology and is focused on securing and protecting IP systems. So, in case of computer security, these tiger teams or ethical hackers would employ the same tricks and techniques that hacker use but in a legal manner and they would neither damage the target systems nor steal information. Instead, they would evaluate the target system's security and report back to

the owners with the vulnerabilities they found and instructions for how to remedy them. Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results is a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment.

An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them.

We can easily say that Ethical hacking does perfectly fit into the security life cycle shown in the below figure

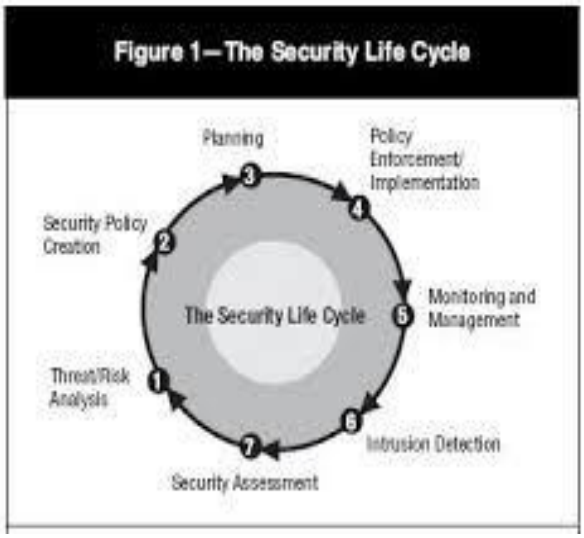

Fig 1: Working of an Ethical Hacker

III. RULES FOR ETHICAL HACKING

The working of an ethical hacker involves the under mentioned steps:

1. Obeying the Ethical Hacking Commandments: Every Ethical Hacker must follow few basic principles. If he does not follow, bad things can happen. Most of the time these principles get ignored or forgotten, when planning or executing ethical hacking tests. The results are even very dangerous.

2. Working ethically: The word ethical can be defined as working with high professional morals and principles Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical Hacker must be approved and must support the company's goals. No hidden agendas are allowed. Trustworthiness is the ultimate objective. The misuse of information is absolutely not allowed.

3. Respecting Privacy: Treat the information you gather with complete respect. All information you obtain during your testing from Web application log files to clear-text passwords — must be kept private.

.

4. Not crashing your systems: One of the biggest mistakes is when people try to hack their own systems; they come up with crashing their systems. The main reason for this is poor

IV. RULES FOR ETHICAL HACKING

The working of an ethical hacker involves the under mentioned steps:

1. Obeying the Ethical Hacking Commandments: Every Ethical Hacker must follow few basic principles. If he does not follow, bad things can happen. Most of the time these principles get ignored or forgotten, when planning or executing ethical hacking tests. The results are even very dangerous.

2. Working ethically: The word ethical can be defined as working with high professional morals and principles Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical Hacker must be approved and must support the company's goals. No hidden agendas are allowed. Trustworthiness is the ultimate objective. The misuse of information is absolutely not allowed.

3. Respecting Privacy: Treat the information you gather with complete respect. All information you obtain during your testing from Web application log files to clear-text passwords — must be kept private.

.

4. Not crashing your systems: One of the biggest mistakes is when people try to hack their own systems; they come up with crashing their systems. The main reason for this is poor increased time and labor costs necessary to identify useful assessment data. Additionally, IT organizations can simply forget to scan certain systems or enable the full suite of testing modules or the scanning tool may not discover more complex vulnerabilities. These missteps can lead to false-negatives and incomplete assessments.

Conversely, ethical hackers are highly proficient with automated tools and manual testing. This experience and proficiency enables the essential service of identifying any missed false-negatives and eliminating false-positives. Therefore, the value of ethical hacking services is the ability to achieve truly comprehensive and actionable assessment

data. In addition, ethical hacking companies can identify the customer's particular security, operational, and compliance objectives before the assessment. These companies can then tailor the assessment and the report to focus on these objectives. The ethical hacking company adds further value by interpreting the results of the assessment data and presenting a prioritized plan of remediation to the customer.

V. SECRITY AND PRIVACY CONCERNS

Ethical hacking has matured and become a more mainstream service in the past decade. However, businesses remain sceptical about the risk inherent with inviting a third-party to attempt to access sensitive systems and resources. Customers fear that ethical hacking companies may leak sensitive data. In many cases, even the knowledge that a business contracted an ethical hacking company can alarm investors and customers, or can make the company a target for hackers. To reduce this risk, businesses should hire only ethical hacking companies that implement practices to ensure privacy and confidentiality. For example, ethical hacking companies should not keep any data or credentials after the consulting engagement. The ethical hacker should turn over this data to the customer along with the final report and then delete the data. Customers should then ensure that all Non-Disclosure Agreements (NDA) are signed prior to the assessment.

VI. CONCLUSION

Given the rapidly advancing sophistication level of cyber threats, businesses cannot afford to rely on untested and unproven security architectures. Businesses in every industry and of any size are now targets for attacks ranging from commodity threats by amateurs to highly-targeted, complex attacks enacted by organized and highly motivated professionals. This represents a monumental challenge for even the most sophisticated organizations due to complex IT environments including security solutions, end-users, policies, and new technologies. In reality, no organization can achieve 100 percent impenetrable security due to the highly dynamic and complex nature of networks and information security systems. However, businesses must increase the effectiveness of their security architectures to the point that they will not be targeted for hackers. The goal should be to achieve a security architecture that would require enough of the attacker's resources to penetrate that would cost the hacker more than the data is worth.

VII. REFERENCES

[1] H.M David, "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1, Feb 23, 2004.

[2] Sanctum Inc, "Ethical Hacking techniques to audit and secure web enabled applications", 2002.

[3] Smith B., Yurcik W., Doss D., "Ethical Hacking: the security justification redux", IEEE Transactions, pp. 375-379, 2002.

[4] B. Reto, "Ethical Hacking", in GSEC Practical Assignment, Version 1.4b, Option 1, Nov 24, 2002.

[5] B. Kevin, "Hacking for dummies", 2nd edition, 408 pages, Oct 2006.

[6] D. Manthan "Hacking for beginners", 254 pages, 2010.

[7] my.safaribooksonline.com/.../introduction-to-ethical-hacking-ethics-legality.

[8] J. Danish and A. N. Muhammad, "Is Ethical Hacking Ethical? " , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.

[9] Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala , "Ethical Hacking " , International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010.

[10] media.techtarget.com/searchNetworking- Introduction to ethical hacking-Tech Target.