RESEARCH ARTICLE OPEN ACCESS

Conceptual Oriented Analysis on the Modern Tools and Techniques to Enrich Security Vulnerabilities in Ethical Hacking

Dr.K.Sai Manoj [1], Ms. K. Mrudula [2], Mrs G.Maanasa [3], Prof.K.Phani Srinivas [4]

CEO [1], Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, AP, India
Director [2], Innogeecks technologies, Vijayawada, AP, India
Research Scholar [3], Acharya Nagarjuna University, Guntur Dist, AP, India
Editor & Reviewer [4], Director R&D Innogeecks Technologies and Amrita Sai Institute of Science &Technology, Vijayawada, AP, India

ABSTRACT

The state of security on the internet is bad and getting worse. One reaction to this state of affairs is termed as Ethical Hacking which attempts to increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. As public and private organizations migrate more of their critical functions to the Internet, criminals have more opportunity and incentive to gain access to sensitive information through the Web application. Thus the need of protecting the systems from the trouble of hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. So, Ethical hacking is an assessment to test and check an information technology environment for possible weak links and vulnerabilities. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This research paper describes what ethical hacking is, what it can do, an ethical hacking methodology as well as some tools which can be used for an ethical hack.

Keywords :— Vulnerabilities, Hacker, Cracker, Port and Intrusion.

I. INTRODUCTION

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.

II. OPERATIONAL MECHANISM OF HACKER

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 planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques. You can easily create miserable conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups. Many security assessment tools can control how many tests are performed on a system at the same time. These tools are especially handy if you need to run the tests on production systems during regular business hours.

5. *Executing the plan:* In Ethical hacking, Time and patience are important. Be careful when you're performing your ethical hacking tests.

.

III. HACKINGPROCESS

The Ethical hacking process needs to be planned in advance. All technical, management and strategical issues must be considered. Planning is important for any amount of testing – from a simple password test to all out penetration test on a web application. Backup off data must be ensured, otherwise the testing may be called off unexpectedly if someone claims they never authorizes for the tests. So, a well defined scope involves the following information:

i. Specific systems to be tested.
ii. Risks that are involved.
iii. Preparing schedule to carry test and overall timeline.
iv. Gather and explore knowledge of the systems we have before testing.
v. What is done when a major vulnerability is discovered?
vi. The specific deliverables- this includes security assessment reports and a higher level report outlining the general vulnerabilities to be addressed, along with counter measures that should be implemented when selecting systems to test, start with the most critical or vulnerable systems.

The overall hacking methodology consists of certain steps which are as follows:

PHASE I – REONNAISSANCE
PHASE II – SCANNING
PHASE III – GAINING ACCESS
PHASE IV – MAINTAING ACCESS
PHASE V – COVERING TRACKS

1. *Reconnaissance:* To be able to attack a system systematically, a hacker has to know as much as possible about the target. It is important to get an overview of the network and the used systems. Information as DNS servers, administrator contacts and IP ranges can be collected. During the reconnaissance phase different kind of tools can be used – network mapping, network and vulnerability scanning tools are the commonly used. Cheops for example is a very good network mapping tool which is able to generate networking graphs. They can be of great help later on during the attack phase or to get an overview about the network. A network mapping tool is very helpful when doing an internal ethical hack. At the end of the reconnaissance phase, an attacker should have a bunch of information about the target. With all these pieces of information, a promising attack path can be constructed.

2. *Probe and Attack:* This is a phase 2 process as shown in the above fig. The probe and attack phase is about digging in, going closer and getting a feeling for the target. It's time to try the collected, possible vulnerabilities from the reconnaissance phase. Tools which can be used during the Probe and Attack phase are many-sided as web exploits; buffer overflows as well as brute-force can be required. Even Trojans like NetBus can be deployed to capture keystrokes, get screenshots or start applications and a host. The probe and attack phase can be very time consuming, especially if brute force attack techniques are used or when individual pieces of software have to be developed or analyzed.

3. *Listening:* This is again a phase 2 process i.e. scanning which is a combination of Probe and attack and listening. Listening to network traffic or to application data can sometimes help to attack a system or to advance deeper into a corporate network. Listening is especially powerful as soon as one has control of an important communication bottleneck. Sniffers are heavily used during the listening phase. Multiple sniffers, from very simple to more complexes, from console based to GUI driven exist for all operating systems. Some sniffers, like better cap can even poison ARP tables to enable sniffing in switched environments and open totally new opportunities for listening to network traffic.

4. *First Access:* This is a phase 3 process which is not about getting root access, it's about getting any access to a

system is it a user or root account. Once this option is available it's time to go for higher access levels or new systems which are now reachable through the acquired system.

Advancement: Phase 4 i.e. Maintaining access is a combination of Advancement and Stealth process. The advancement phase is probably the most creative demanding stage, as unlimited possibilities are open. Sniffing network traffic may unveil certain passwords, needed usernames or e-mail traffic with usable information. Sending mails to administrators faking some known users may help in getting desired information or even access to a new system. Probably one also has to alter configuration files to enable or disable services or features. Last but not least, installing new tools and helpful scripts may help to dig in deeper or to scan log files for more details.

5. *Stealth:* Some systems may be of high value – systems which act as routers or firewalls, systems where a root account could be acquired. To have access to such systems at a later time it is important clean relevant log files.

6. *Takeover:* Takeover is a phase 5 process .Once root access could be attained, the system can be considered won. From there on it's possible to install any tools, do every action and start every services on that particular machine. Depending on the machine it can now be possible to misuse trust relationships, create new relationships or disable certain security checks.

7. *Cleanup:* This could be instructions in the final report on how to remove certain trojans but most of the time this will be done by the hacker itself. Removing all traces as far as possible is kind of a duty for the hacking craft. An ethical hack always poses a certain risks if not properly done. A hacker could use the deployed tools or hide his attacks in all the attacks from the ethical hack. He could also try to attack the attackers system, therefore gain entry to the ethical hackers system and collect all information free of charge and already sorted and prepared. Preparing an ethical hack and hold a high level of security is a challenging task which should only be done by professionals.

IV. SELECTION OF TOOLS FOR HACKING

It is very much essential to make sure that we are using the right tool for ethical hacking process. It is important to know the personal as well as technical limitations. Many tools focus on specific tests, but no one tool can test for everything. The more tools you have, the easier your ethical hacking efforts are. Make sure you that you're using the right tool for the task. For example, to crack passwords, you need a cracking tool such as LC4 or John the Ripper. Similarly, for an in-depth analysis of a Web application, a Web-application assessment tool (such as Whisker or Web Inspect) is more appropriate than a network analyzer (such as Ethereal). There are various characteristics for the use of tools for ethical hacking which are as follows:

i. Adequate documentation
ii. Detailed reports on the discovered vulnerabilities, including how they can be fixed
iii. Updates and support when needed
iv. High level reports that can be presented to managers

These features can save the time and effort when we are writing the report. Time and patience are important in ethical hacking process. We should be careful when we are performing the ethical hacking tests. It is not practical to make sure that no hackers are on our system. Just make sure to keep everything private if possible. Do encrypt the emails and files if possible. The list and description of various tools used in the ethical hacking process are as follows:

Scanning tools: The Scanning tools are quite helpful in the ethical hacking process. In technical detail, a scanner sends a message requesting to open a connection with a computer on a particular port. (A port is an interface where different layers of software exchanges information). The computer has an option of ignoring the message, responding negatively to the message, or opening a session. Ignoring the message is the safest since if there are no open services it may be hard for a cracker to determine if a computer exists. Once a port scan reveals the existence of an open service, a cracker can attack known vulnerabilities. Once a cracker scans all computers on a network and creates a network map showing what computers are running, what operating systems and what services are available, almost any kind of attack is possible including automated scripting program attacks and social engineered attacks. The first scanner was the security administrator's tool for analyzing networks – SATAN introduced by Dan Farmer in 1995. SATAN (Security Administrator tool for analyzing networks) could analyze any system accessible over the internet. But the question here is that why should anyone with internet presence and no interest in cracking other systems learn about scanners? The answer is to learn what crackers will see in their own internet presence since scanners are common attack starting points. Crackers look for unauthorized services such as someone running a server with known problems, an unauthorized server on a high port. Port scanning can be done manually from a single computer to learn about target systems or it can be done automatically by program originating from multiple computers on different networks to a single target system overalongperiodoftime.Portscannerslikeothertools,haveboth offensiveanddefensiveapplications-what makes a port scanner good or evil is how it is used. Actually, a port scanner is simultaneously both the most powerful tool an ethical hacker can use in protecting the network of computers and the most powerful tool a cracker can use to generate attacks. The table below shows some of the scanning tools that help in the ethical hacking process:

Table 1: Tools of Ethical Hacking

Commercial scanners	Network Assoc-Cybercop
Sniffers	Ethercap, tcpdump
Network scanners	SATAN, strobe, rprobe
War- dialing	ThcScan, LoginH
Password crackers	John the Ripper, L0pth crack
Firewall scanners	Firewalk
Security and vulnerability scanning	Nessus, ISS, cybercop

1. Password cracking tools: Password cracking does not have to involve fancy tools, but it is a tedious process. If the target doesn't lock you out after a specific number of tries, you can spend an infinite amount of time trying every combination of alphanumeric characters. It's just a question of time and bandwidth before you break into a system. There are three basic types of password cracking tests that can be automated with tools:

i. Dictionary- A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly.

ii. Hybrid: A common method utilized by users to change passwords is to add a number or symbol to the end. A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt.

iii. Bruteforce: The most time consuming, comprehensive way t o crack a password. Every combination of character is tried until the password is broken.

2. Port Scanning tools: Port scanning is one of the most common reconnaissance techniques used by testers to discover the vulnerabilities in the services listening at well-known ports. Once you've identified the IP address of a target system through foot printing, you can begin the process of port scanning: looking for holes in the system through which you -- or a malicious intruder -- can gain access. A typical system has 2^16 -1 port numbers, each with its own TCP and UDP port that can be used to gain access if unprotected. The most popular port scanner for Linux, Nmap, is also available for Windows. Nmap can scan a system in variety of stealth modes, depending upon how undetectable you want to be. Nmap can determine a lot of information about a target, like what hosts are available, what services are offered and what OS is running.

Vulnerability scanning tools: A Vulnerability scanner allows you to connect to a target system and check for such vulnerabilities as configuration errors. A popular vulnerability scanner is the freely available open source tool Nesses. Nessusis an extremely powerful scanner that can be configured Tourna variety of scans. While a windows graphical front end is available, the core Nesses product requires Linux to run. Microsoft's Baseline Security Analyzer is a free Windows vulnerability scanner. MBSA can be used to detect security configuration errors on local computers or remotely across a network. Popular commercial vulnerability scanners include Retina Network Security Scanner, which runs on Windows, and SAINT, which runs on various Unix/Linux versions.

V. CONCLUSION

This research paper addressed ethical hacking from several perspectives. Ethical hacking seems to be a new buzz word although the techniques and ideas of testing security by attacking an installation aren't new at all. But, with the present poor security on the internet, ethical hacking may be the most effective way to plug security holes and prevent intrusions. On the other hand ethical hacking tools have also been notorious tools for crackers. So, at present the tactical objective is to stay one step ahead of the crackers. Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. After all, ethical hacking will play a certain role in the security assessment offerings and certainly has earned its place among other security assessments. In conclusion, it must be said that the ethical hacker is an educator who seeks to enlighten not only the customer, but also the security industry as a whole. In an effort to accomplish this, let us welcome the Ethical Hacker into our ranks as a partner in this quest.

ACKNOWLEDGMENT

First of all, I am thankful to Honourable Amrita Sai Management for giving me this opportunity and to complete my work. It gives me an immense pleasure and pride to express my deep sense of gratitude to the Innogeecks technologies for their technical support in all the aspects.

AUTHORS' INFORMATION

Dr K Sai Manoj, Founder and Executive Director of Innogeecks Global Services Pvt Ltd, Founder and CEO of Innogeecks Technologies and Founder of 3 start-ups based on IOT and Cloud Computing, is an Enthusiastic learner, Excellent Financial Advisor, Innovative and Visionary Leader, Insightful team builder and strategic planner, who has 10+ years of experience in Financial Services, Equity Research and IT- ITeS services to his credit. He has worked in Reputed Companies like WIPRO Technologies, Fidelity Inverstments.etc., He is Proud of achieving many laurels in the field of Computers and Research. He is a Certified Ethical hacker, Certified Computer hacking forensics Investigator, Certified Security Analyst, Charted Engineer from IEI (India), Certified Blockchain Expert, Microsoft Certified Technology Specialist, AWS Certified Solutions Architect-Associate, Google Analytics Individual Qualification, IBM Block chain Certification, Certified EC Council Instructor and so on.

He has a proven record of having 10+ certifications from the most sought after software giants such as Microsoft, IBM, Google, Face book, EC Council & Amazon besides this he has acted as a reviewer for the Journal of Super Computing (Springer) , Journal of Big Data (Springer) and Journal of the Institution of Engineers (India) – Series B (Springer). And also with his solid financial advice 21 start-ups of Kochi, Bangalore and Vijayawada have tread the success track.

Talking about his research excellence, it is exciting to know that he has filed 3 patents and 4 more are in pipeline and has Published more than 25 research papers in reputed journals like Thomas Reuters, IEEE, Scopus etc., and shows keenness in researching on Cyber Security, Cloud Computing, Big Data / Hadoop, Block chain and Data Analytics.

Ms. K.Mrudula working as a Director for the Innogeecks Technologies. She was completed M.Tech from IIIT Hyderabad .She got more than 6 years of experience in Teaching. She published more than 5 research papers in various International and national research journals. She attended 2 FDP, and 1 workshop.

Mrs.G.Maanasa worked as HR manager in Jaya lakshmi Powercorp Ltd for a Period of 6 years after completing her M.B.A from RVR&JC college of Engineering. She is currently pursuing her doctorate (PhD) in Development of Framework for Tourism Promotion in AP and ICT Integration from Nagarjuna University.

K.PHANI SRINIVAS working as a Director for the Research and Development and He Had Five Years of Industrial Experience as a team Leader in the research areas of Embedded Systems and telecommunications and also He is Having 13 Years of Experience in Academics, Research and Administrative reports. He received so many awards such as a Best Engineer, Best Teacher and also as a Best Researcher. Also He is acting as an Editor/Reviewer for so many top international Journals.

The Focus of His research work is Design of Patch antennas which are Suitable for Defence and Space Based Applications. He received appreciation award in various National and International Conferences. He received Best Coordinator Certificates from IUCEE, IIT ROORKEE, IIT Bhubneswar, NCAT, ELAT and INTEL. He attended WIPRO training Program. He completed one Joint research Program with IIT Kharagpur.He Organized various student level Competitions, workshops, Faculty Development Programs, Guest lectures, Orientation Programs, and Subject Based Seminars with scientists and Academicians. He is doing research work under the valuable Directions of Eminent Scientists. He had done technical Discussions with experts at Space Station, Antenna Research Lab, and Radar station. He Published research articles in Various Scientific Journals. He is an active Editor/Reviewer for the so many top most international journals.

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, Oct2006.

[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, May2011.

[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/search Networking- Introduction to ethical hacking-TechTarget.

[11] A Survey on Protection of Multimedia Content in Cloud Computing, Dr. K.Sai Manoj, Mrudula Kudaravalli,International Journal of Computer Science and Mobile Computing - Vol.6 Issue.11, November-2017, pg. 7-11

[12] INVESTIGATION ON THE DATA SECURITY IN CLOUD COMPUTING USING BIOMETRICS Dr.Sai Manoj.K International Journal of Current Advanced Research Volume 7; Issue 12(B), December 2018; Page No: 16473-16475