Impacts of Ethical Hacking

Mr. Ravinder Mohan Jindal[1], Mrs. Leekha Jindal[2], Ramandeep Kaur[1]
[1]*PG Dept. of Computer Science, HMV Jalandhar*
[2]*PG Dept. of Computer Science, DAV Jalandhar*

Abstract: The status of security on the internet is bad and getting worse. One effect to this state of relationships is term as Ethical Hacking which attempts to increase security defense by identifying and patching known security vulnerabilities on systems owned by other party. As public and private organizations roam more of their serious functions to the Internet, criminals have more chance and reason to gain access to aware in order through the Web application. Thus the need of caring the systems from the irritation of hacking generated by the hackers is to endorse the persons who will punch back the illegal attacks on our computer systems. So, Ethical hacking is an evaluation to test and check an information technology environment for possible feeble links and vulnerabilities. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intention. This paper describes what ethical hacking is, what it can do, an ethical hacking method as well as some tools which can be used for an ethical hack.

Keywords- Vulnerabilities, Hacker, Cracker, Port and Intrusion.

I. INTRODUCTION TO ETHICAL HACKING

The vast progress of Internet has brought many good things like electronic commerce, email, easy access to huge stores of position matter etc. As, with most industrial advances, there is also other face: illegal 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 type of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. So, this article describes ethical hackers, their skills and how they go about helping their clients and plug up security holes. Ethical hackers perform the hacks as security tests for their systems. An ethical hack's results is a exhaustive description of the findings as well as a proof that a hacker with a definite 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 consideration, a kind of training, a test for the security of an information technology environment [1].

II. WORKING OF AN ETHICAL HACKER

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

A. Obeying the Ethical Hacking Commandments: Every Ethical Hacker must follow few basic principles. If he does not follow, bad things can happen. The results are even very dangerous.

B. 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.

C. 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.

D. 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 fed-up conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups.

E. Executing the plan: In Ethical hacking, Time and endurance are important. Be careful when you're performing your ethical hacking tests [4].

III. ETHICAL HACKING PROCESS

The Ethical hacking process needs to be planned in advance. All technical, management and tactically 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:

- Specific systems to be tested.
- Risks that are involved.
- Preparing schedule to carry test and overall timeline.
- Gather and explore knowledge of the systems we have before testing.

- What is done when a major vulnerability is discovered? [4, 6].

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

A. 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.

B. Probe and Attack

This is a phase 2 process. 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.

C. Listening

This is again a phase 2 process i.e. scanning which is a combination of search 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 commercial 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.

D. 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.

E. 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.

F. 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.

G. Cleanup

This could be instructions in the final report on how to remove certain Trojans but most of the time this 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 [4, 9].

IV. SELECTION OF TOOLS IN ETHICAL 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 is more appropriate than a network analyzer. There are various characteristics for the use of tools for ethical hacking which are as follows:

- Adequate documentation
- Detailed reports on the discovered vulnerabilities, including how they can be fixed
- Updates and support when needed
- 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:

A. 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. 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 scanners like other tools, have both odious and suspicious applications- what ISSN: 2319-8753 International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 12, December 2013 Copyright to IJIRSET www.ijirset.com 7579 makes a port scanner high-quality or vice is how it is used. Actually, a port scanner is simultaneously both the most powerful tool an ethical hacker can use in shielding the network of computers and the most dominant tool a cracker can use to produce attacks. The table below shows some of the scanning tools that help in the ethical hacking process: Commercial scanners Network Assoc- Cybercop Sniffers Ether cap, tcpdump Network scanners SATAN, strobe, rprobe War- dialing THC Scan, Login Password crackers John the Ripper, L0pth crack Firewall scanners Fire walk Security and vulnerability scanning Nessus, ISS, cybercop .[V]

B. Password cracking tools

Password cracking does not have to engage fancy tools, but it is a dreary process. If the target doesn't lock you out after a specific number of tries, you can spend an countless amount of time trying every combination of alphanumeric font. 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:

- *Dictionary*- A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly.
- *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.
- *Brute force*- The most time consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken.

There are some common web passwords cracking tools which are as follows:

Brutus: It is a password cracking tool that can perform both dictionary attacks and brute force attacks where passwords are randomly generated from a given character. Brutus can crack the multiple authentication types, HTTP, POP3, FTP, SMB and Telnet. Web cracker It is a simple tool that takes text lists of usernames and passwords, and uses them as dictionaries to implement basic authentication password guessing.

ObiWan: It is a Web password cracking tool that can work through a proxy. **ObiWan** uses wordlists and alternations of numeric or alpha-numeric characters as possible passwords.

C. 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 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 decide a lot of information about a target, like what hosts are available, what services are offered and what OS is running.

D. Vulnerability scanning tools

A Vulnerability scanner allows you to connect to a target system and check for such vulnerabilities as pattern errors. A popular vulnerability scanner is the freely available open source tool Nessus. Nessus is an extremely powerful scanner that can be configured to run a variety of scans. While a ISSN: 2319-8753 International Journal of Innovative Research in Science, Engineering and Technology Vol.2, Issue12,Dec 2013Copyright to IJIRSET www.ijirset.com 7580 windows graphical front end is available, the core Nessus product requires Linux to run. Microsoft's Baseline Security Analyser is 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.

E. Quality Assessment Tools

There are many tools available for use by ethical hacking companies ranging from free open source software such as Nap and THC-Hydra to enterprise-gradesolutions such as CORE IMPACT Pro and Acunetix WVS. Free and open sourcesoftware offers compelling functionality that is regularly updated by a community of users and developers. Commercial testing solution offer cutting-edge functionality, proven reliability, and dedicated research and development.

Various Commercial Tools are-- Pro Acunetix WVS, Metasploit Pro, Nessus, eEye Retina,Rapid7 Nexpose, CST OnLine Digital Forensic Suite (DFS). [II]

V. CONCLUSION

This 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.

VI. 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] http://www.frost.com/upld/get-data.do?id=1568233

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

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

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

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

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

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

[9] Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala , "Ethical Hacking " , International journal of Computer Applications