ETHICAL HACKING
(Tools, Techniques and Approaches)

Brijesh Kumar Pandey
Dept. of MCA
TIMSCDR
Mumbai, India
brijesh.pandey@thakureducation.org

Alok Singh
Dept. of MCA
TIMSCDR
Mumbai, India
Singh.alok@thakureducation.org

Lovely lakhmani Balani
Dept. of MCA
TIMSCDR
Mumbai, India
lovely.lakhmani@gmail.com

***Abstract*— 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. [1] This paper describes ethical hackers: their skills, their attitudes, and how they go about helping their customers find and plug up security holes. The ethical hacking process is explained, along with many of the challenges and opportunities in the field of ethical hacking.**

***Index Terms*—Ethical hacking, vulnerability analysis, exploitation, Information gathering, Information security.**

I. INTRODUCTION

The term "hacker" has a dual usage in the computer industry today. Originally, the term was defined as:

"A person who enjoys learning the details of computer systems and how to stretch their capabilities-as opposed to most users of computers, who prefer to learn only the minimum amount necessary. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming".

This complimentary description was often extended to the verb form "hacking," which was used to describe the rapid crafting of a new program or the making of changes to existing, usually complicated software.

Because of the increasing popularity of computers and their continued high cost, access to them was usually restricted. When refused access to the computers, some users would challenge the access controls that had been put in place. They would steal passwords or account numbers by looking over someone's shoulder, explore the system for bugs that might get them past the rules, or even take control of the whole system. They would do these things in order to be able to run the programs of their choice, or just to change the limitations under which their programs were running.

Initially these computer intrusions were fairly benign, with the most damage being the theft of computer time. Other times, these recreations would take the form of practical jokes. However, these intrusions did not stay benign for long. Occasionally the less talented, or less careful, intruders would accidentally bring down a system or damage its files, and the system administrators would have to restart it or make repairs. Other times, when these intruders were again denied access once their activities were discovered, they would react with purposefully destructive actions. When the number of these destructive computer intrusions became noticeable, due to the visibility of the system or the extent of the damage inflicted, it became "news" and the news media picked up on the story. Instead of using the more accurate term of "computer criminal," the media began using the term "hacker" to describe individuals who break into computers for fun, revenge, or profit. Since calling someone a "hacker" was originally meant as a compliment, computer security professionals prefer to use the term "cracker" or "intruder" for those hackers who turn to the dark side of hacking. For clarity, we will use the explicit terms "ethical hacker" and "criminal hacker" for the rest of this paper.

1) What is ethical hacking?

With the growth of the Internet, computer security has become a major concern for businesses and governments. They want to be able to take advantage of the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being "hacked." 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 similar to having independent auditors come into an organization to verify its bookkeeping records. In the case of computer security, these "tiger teams" or "ethical hackers" would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.

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 a two-level (secret/top secret) system." Their evaluation found that while Multics was "significantly better than other conventional systems," it also had " … vulnerabilities in hardware security, software security, and procedural security" that could be uncovered with "a relatively low level of effort." The authors performed their tests under a guideline of realism, so that their results would accurately represent the kinds of access that an intruder could potentially achieve. They performed tests that were simple information-gathering exercises, as well as other tests that were outright attacks upon the system that might damage its integrity. Clearly, their audience wanted to know both results. There are several other now unclassified reports that describe ethical hacking activities within the U.S. military.

With the growth of computer networking, and of the Internet in particular, computer and network vulnerability studies began to appear outside of the military establishment. Most notable of these was the work by Farmer and Venema, which was originally posted to Usenet in December of 1993. They discussed publicly, perhaps for the first time, this idea of using the techniques of the hacker to assess the security of a system. With the goal of raising the overall level of security on the Internet and intranets, they proceeded to describe how they were able to gather enough information about their targets to have been able to compromise security if they had chosen to do so. They provided several specific examples of how this information could be gathered and exploited to gain control of the target, and how such an attack could be prevented.

Farmer and Venema elected to share their report freely on the Internet in order that everyone could read and learn from it. However, they realized that the testing at which they had become so adept might be too complex, time-consuming, or just too boring for the typical system administrator to perform on a regular basis. For this reason, they gathered up all the tools that they had used during their work, packaged them in a single, easy-to-use application, and gave it away to anyone who chose to download it. Their program, called Security Analysis Tool for Auditing Networks, or SATAN, was met with a great amount of media attention around the world. Most of this early attention was negative, because the tool's capabilities were misunderstood. The tool was not an automated hacker program that would bore into systems and steal their secrets. Rather, the tool performed an audit that both identified the vulnerabilities of a system and provided advice on how to eliminate them. Just as banks have regular audits of their accounts and procedures, computer systems also need regular checking. The SATAN tool provided that auditing capability, but it went one step further: it also advised the user on how to correct the problems it discovered. The tool did not tell the user how the vulnerability might be exploited, because there would be no useful point in doing so.

2) Who are ethical hackers?

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 to exercise tight control over any information about a target that could be misused. The sensitivity of the information gathered during an evaluation requires that strong measures be taken to ensure the security of the systems being employed by the ethical hackers themselves: limited-access labs with physical security protection and full ceiling-to-floor walls, multiple secure Internet connections, a safe to hold paper documentation from clients, strong cryptography to protect electronic results, and isolated networks for testing.

Ethical hackers typically have very strong programming and computer networking skills and have been in the computer and networking business for several years. They are also adept at installing and maintaining systems that use the more popular operating systems (e.g., UNIX or Windows NT) used on target systems. These base skills are augmented with detailed knowledge of the hardware and software provided by the more popular computer and networking hardware vendors. It should be noted that an additional specialization in security is not always necessary, as strong skills in the other areas imply a very good understanding of how the security on various systems is maintained. These systems management skills are necessary for the actual vulnerability testing, but are equally

important when preparing the report for the client after the test.

Finally, good candidates for ethical hacking have more drive and patience than most people. Unlike the way someone breaks into a computer in the movies, the work that ethical hackers do demands a lot of time and persistence. This is a critical trait, since criminal hackers are known to be extremely patient and willing to monitor systems for days or weeks while waiting for an opportunity. A typical evaluation may require several days of tedious work that is difficult to automate. Some portions of the evaluations must be done outside of normal working hours to avoid interfering with production at "live" targets or to simulate the timing of a real attack. 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-changing world of computer and network security requires continuous education and review.

One might observe that the skills we have described could just as easily belong to a criminal hacker as to an ethical hacker. Just as in sports or warfare, knowledge of the skills and techniques of your opponent is vital to your success. In the computer security realm, the ethical hacker's task is the harder one. With traditional crime anyone can become a shoplifter, graffiti artist, or a mugger. Their potential targets are usually easy to identify and tend to be localized. The local law enforcement agents must know how the criminals ply their trade and how to stop them. On the Internet anyone can download criminal hacker tools and use them to attempt to break into computers anywhere in the world. Ethical hackers have to know the techniques of the criminal hackers, how their activities might be detected, and how to stop them.

Given these qualifications, how does one go about finding such individuals? The best ethical hacker candidates will have successfully published research papers or released popular open-source security software. The computer security community is strongly self-policing, given the importance of its work. Most ethical hackers, and many of the better computer and network security experts, did not set out to focus on these issues. Most of them were computer users from various disciplines, such as astronomy and physics, mathematics, computer science, philosophy, or liberal arts, who took it personally when someone disrupted their work with a hack.

One rule that IBM's ethical hacking effort had from the very beginning was that we would not hire ex-hackers. While some will argue that only a "real hacker" would have the skill to actually do the work, we feel that the requirement for absolute trust eliminated such candidates. We likened the decision to that of hiring a fire marshal for a school district: while a gifted ex-arsonist might indeed know everything about setting and putting out fires, would the parents of the students really feel comfortable with such a choice? This decision was further justified when the service was initially offered: the customers themselves asked that such a restriction be observed. Since IBM's ethical hacking group was formed, there have been numerous ex-hackers who have become security consultants and spokespersons for the news media. While they may very well have turned away from the "dark side," there will always be a doubt.

3) What do ethical hackers do?

An ethical hacker's evaluation of a system's security seeks answers to three basic questions:

- What can an intruder see on the target systems?
- What can an intruder do with that information?
- Does anyone at the target notice the intruder's attempts or successes?

While the first and second of these are clearly important, the third is even more important: If the owners or operators of the target systems do not notice when someone is trying to break in, the intruders can, and will, spend weeks or months trying and will usually eventually succeed.

When the client requests an evaluation, there is quite a bit of discussion and paperwork that must be done up front. The discussion begins with the client's answers to questions similar to those posed by Garfinkel and Spafford:

1. What are you trying to protect?
2. What are you trying to protect against?
3. How much time, effort, and money are you willing to expend to obtain adequate protection?

II. PLANNING THE TEST

Aspects that should be focused on:

a) Who should perform penetration testing?

b) How often the tests have to be conducted?

c) What are the methods of measuring and communicating the results?

d) What if something unexpected happens during the test and brings the whole system down?

e) What are the organization's security policies?

III. THE MINIMUM SECURITY POLICIES THAT AN ORGANIZATION SHOULD POSSESS

a) Information policy

b) Security policy

c) Computer use

d) User management

e) System administration procedures
f) Incident response procedures
g) Configuration management
h) Design methodology
i) Disaster methodology
j) Disaster recovery plans.

IV. ETHICAL HACKING AS A DYNAMIC PROCESS

Ethical hacking is a dynamic process since running through the penetration test once gives the current set of security issues which subject to change over time therefore penetration testing must be continuous to ensure that system movements and installation of new applications do not introduce new vulnerabilities in the system.
Areas to be tested:

- Application servers
- Firewalls and security devices
- Network security
- Wireless security

Multi layered assessment:

Various areas of security are evaluated using a multilayered approach.

- Each area of security defines how the target will be assessed.
- An identified vulnerability at one layer may be protected at another layer minimizing the associated risk of the vulnerability.

V. WEAPONS OF AN ETHICAL HACKER

Automatic tools has changed the world of penetration testing/ethical hacking, IT security researcher has been developed and currently developing different tools to make the test fast, reliable and easier task. Without automatic tools, the hacking process is slow and time consuming. in this paper we summarize the best tools that are widely used in the world of hacking:

Nmap

Nmap is a best tool ever that are used in the second phase of ethical hacking means port scanning, Nmap was originally command line tool that has been developed for only Unix/Linux based operating system but now its windows version is also available and ease to use. It is use for Operating system fingerprinting too.

Nessus

Nessus is the world most famous vulnerability scanner, Nessus has been developed by Tenable network security, it is available for free of cost for non-enterprise environment means for home user. It is a network vulnerability scanner and use for finding the critical bugs on a system.

Nikto

Nikto is a free and open source tool, It checks for outdated versions of over 1000 servers, and version specific problems on over 270 servers, It find out the default files and programs. It is a best tool for web server penetration testing.

Kismet

Now a days Wardriving or Wireless LAN(WLAN) hacking is in market and different companies hire penetration tester for doing test on wireless network, this test requires some tools, so Kismet is a best choice for do this. Kismet identifies networks by passively collecting packets and detecting networks, which allows it to detect (and given time, expose the names of) hidden networks and the presence of non-beaconing networks via data traffic.

MetaSploit

The best tool ever, Metasploit contain a database that has a list of available exploit and it is easy to use and best tool for doing penetration testing, Metasploit framework is a sub project and is use to execute exploit code against a machine and get the desire task done.

NetStumbler

Once again for wardriving, well netstumbler are available for windows based operating system, it works on windows based operating system.It can detect WiFi that is IEEE 802.11b, 802.11g and 802.11a networks. MiniStumbler is also available and works on Windows CE based system. [2]

Techniques of ethical hacking:

- Information gathering
- Vulnerability scanning
- Exploitation
- Test Analysis

- **Information Gathering**

  In this step, the testers collect as much information about the web application as possible and gain understanding of its logic. The deeper the testers understand the test target, the more successful the penetration testing will be [3]. The information gathered will be used to create a knowledge base to

act upon in later steps. The testers should gather all information even if it seems useless and unrelated since no one knows at the outset what bits of information are needed. This step can be carried out in many different ways: by using public tools such as search engines; using scanners; sending simple HTTP requests or specially crafted requests [4]; or walking through the application.

- **Vulnerability Analysis**
  Using the knowledge collected from the information gathering step, the testers then scan the vulnerabilities that exist in the web application. The testers can conduct testing on configuration management, business logic, authentication, session management, authorization, data validation, denial of service, and web services [4]. In this step, web server vulnerabilities, authentication mechanism vulnerabilities, input-based vulnerabilities and function-specific vulnerabilities are examined.

- **Exploitation**

  After the vulnerability analysis step, the testers should have a good idea of the areas that will be targeted for exploits. With the list of vulnerabilities on hand, the two applications were then exploited.

- **Test Analysis Phase**

  This phase is the interface of the results, the testers and the target entity [3]. It is important that the target entity is aware of typical attacker modus operandi, techniques and tools attackers rely on, exploits they use, and any needless exposure of data the target is suffering from.

VI. Approaches towards Ethical hacking (PENTEST)

. Any combination of the following may be called for:

- *Remote network*. This test simulates the intruder launching an attack across the Internet. The primary defenses that must be defeated here are border firewalls, filtering routers, and Web servers.
- *Remote dial-up network*. This test simulates the intruder launching an attack against the client's modem pools. The primary defenses that must be defeated here are user authentication schemes. These kinds of tests should be coordinated with the local telephone company.
- *Local network*. This test simulates an employee or other authorized person who has a legal connection to the organization's network. The primary defenses that must be defeated here are intranet firewalls, internal Web servers, server security measures, and e-mail systems.
- *Stolen laptop computer*. In this test, the laptop computer of a key employee, such as an upper-level manager or strategist, is taken by the client without warning and given to the ethical hackers. They examine the computer for passwords stored in dial-up software, corporate information assets, personnel information, and the like. Since many busy users will store their passwords on their machine, it is common for the ethical hackers to be able to use this laptop computer to dial into the corporate intranet with the owner's full privileges.
- *Social engineering*. This test evaluates the target organization's staff as to whether it would leak information to someone. A typical example of this would be an intruder calling the organization's computer help line and asking for the external telephone numbers of the modem pool. Defending against this kind of attack is the hardest, because people and personalities are involved. Most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who “forgot” his or her badge. The only defense against this is to raise security awareness.
- *Physical entry*. This test acts out a physical penetration of the organization's building. Special arrangements must be made for this, since security guards or police could become involved if the ethical hackers fail to avoid detection. Once inside the building, it is important that the tester not be detected. One technique is for the tester to carry a document with the target company's logo on it. Such a document could be found by digging through trash cans before the ethical hack or by casually picking up a document from a trash can or desk once the tester is inside. The primary defenses here are a strong security policy, security guards, access controls and monitoring, and security awareness.

Each of these kinds of testing can be performed from three perspectives: as a total outsider, a “semi-outsider,” or a valid user.

A total outsider has very limited knowledge about the target systems. The only information

used is available through public sources on the Internet. This test represents the most commonly perceived threat. A well-defended system should not allow this kind of intruder to do anything.

A semi-outsider has limited access to one or more of the organization's computers or networks. This tests scenarios such as a bank allowing its depositors to use special software and a modem to access information about their accounts. A well-defended system should only allow this kind of intruder to access his or her own account information.

A valid user has valid access to at least some of the organization's computers and networks. This tests whether or not insiders with some access can extend that access beyond what has been prescribed. A well-defended system should allow an insider to access only the areas and resources that the system administrator has assigned to the insider.

VII. OPPORTUNITIES AND CHALLENGES

Ethical Hacking also known as Internet Security is very different from traditional Security. Internet security is more on a proactive basis as compared to traditional security. While traditional security is based on catching the criminals, internet security has Ethical Hackers that try to hack into a company/organization before an 'attack' so they are able to find any weak links. Ethical Hackers are hired by companies to hack their own respective company and be able to identify any loopholes where an ill-intentioned hacker could create damage so that the company can buff its security and cover the cracks. They use their creativity and skills to make the internet world of a company a foolproof and safe place for both the owners and the clients. These 'Cyber Cops' prevent Cyber Crimes and protect the cyber space.

The ethical hack itself poses some risk to the client:
Criminal hacker monitoring the transmissions of ethical hacker could trap the information.

VIII. CONCLUSION

In this paper firstly we introduced the concepts of system security, hacking, hacker, ethical hacking aka pen testing. Then in next section we discussed various tools, techniques and approaches which are normally constitutes weaponry of a seasoned hacker. In our paper we explained how ethical hacking is a continuous and dynamic process, then we discussed various opportunities available to an ethical hacker as a professional.

REFERENCES

[1] http://www.articlesbase.com/security-articles/ethical-hacking-an-introduction-402282.html

[2] http://www.ehacking.net/2011/06/top-6-ethical-hacking-tools.html#sthash.nszGZw4y.dpuf

[3] OWASP. "Web Application Penetration Testing," http://www.owasp.org/index.php/Web_Application_Pene tration_Testing.

[4]http://www.corecom.com/external/livesecurity/pentest.html

[5]http://www.networkdefense.com/papers/pentest.html

[6] Internet Security Systems, Network and Host-based Vulnerability Assessment

[7]http://www.infosecinstitute.com/blog/ethicalhacking_computer_forensics.html

[8]http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083715,00.html

[9]http://www.owasp.org/index.php/Testing:_Information_Gathering

View publication stats