Ethical hacking

Farzeen Mohd Imran Memon

B.E (INDUSTRIAL ELECTRONICS)
FORMER LECTURER AT REI POLYTECHNIC

Mahmmed Imran Mahmmed Memon

Diploma in Electronics & Video Engineering
Aircraft Maintenance Engineering
B.Sc. Industrial Science
Owner of MI Classes

The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As a coin has two sides with most technological advances, there is a good as well as a dark side: criminal hackers. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. With these concerns and others, the ethical hacker can help. This paper describes ethical hackers: their skills, their attitudes, and how they go about helping their customers and plug up security holes & its counter measures. The ethical hacking process is explained, along with many of the problems globally.

The term ‘hacker’ has a dual usage in the computer industry today. Originally, the term was Defined as:

1. A person who enjoys learning the details of computer systems and how to stretch their capabilities opposed to most users of computers, who prefer to learn only the minimum amount necessary.
2. 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.

As computers became increasingly available at universities, user communities began to extend beyond researchers in engineering or computer science to other individuals who viewed the computer as a curiously exile tool. Whether they programmed the computers to play games, draw pictures, or to help them with the more mundane aspects of their daily work, once computers were available for use, there was never a lack of individuals wanting to use them.

Because of this 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 some- one'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.

When the number of these destructive computer intrusions became noticeable, due to the visibility of the system or the extent of the damage in, 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 some-one 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

What is ethical hacking?

Ethical hacking and ethical hackers are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to by-pass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organizations to improve the system security in an effort to minimize or eliminate any potential attacks.

An Ethical hacker is also known as a White Hat Hacker, He is a Security professional who applies their hacking Skills for defensive purposes on behalf of the owners of Information Systems. Nowadays certified ethical hackers are among the most sought after information security employees in large organizations such as Wipro, Infosys, IBM, Airtel and Reliance among others.
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 ethical hackers would employ the same tools and techniques as in the case neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report back to the owners the vulnerabilities they found and instructions for how to remedy them.

he intruders, but they would neither damage the target systems nor steal information. Instead, they would

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 ethical hackers would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information.

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 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.

The 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 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

Who are ethical hackers?

These early efforts provide good examples of 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 net-working 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 vulner

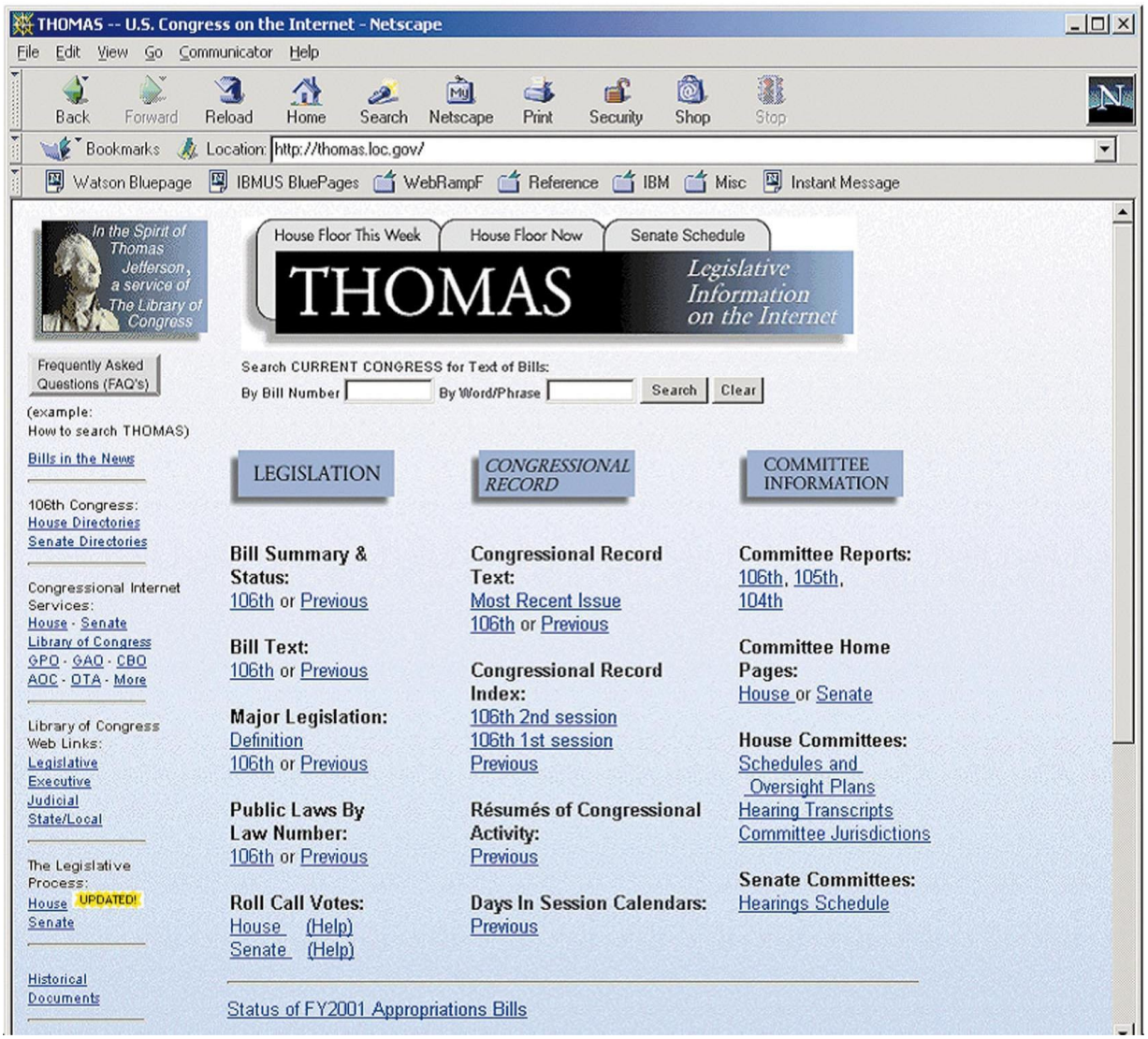
Vulnerability testing, but are equally important when pre-paring the report for the client after the test.

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 ªliveº 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 know its weaknesses. Finally, keeping up with the ever- changing world of computer and network security requires continuous education and review. In the computer security realm, the ethical hacker's task is the harder one. With traditional crime anyone can become a shopkeeper, artist, or any other profession 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.

 ISSN: 2321-8169
243 - 248

Hacked pages globally

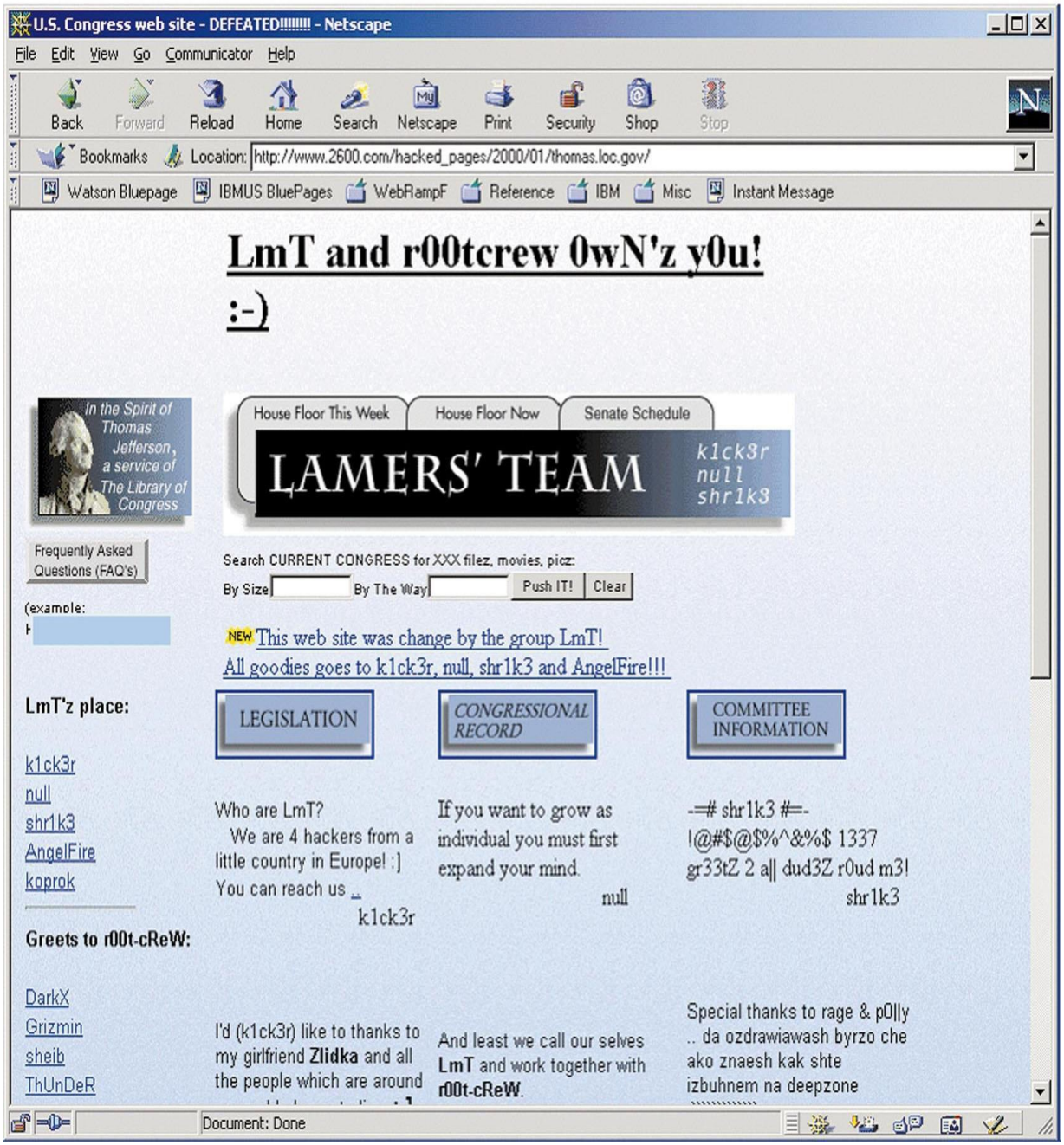
Figure 1: Library of Congress Web page before attack



Some people are under the mistaken impression that their Web site would not be a target. They give numerous reasons, such as it has nothing interesting on it or hackers have never heard of my company. What these people do not realize is that. The goal of many criminal hackers is simple: Do something spectacular and then make sure that all of your pals know that you did it. Another rebuttal is that many hackers simply do not care who your company or organization is; they hack your Website because they can. For example, Web Administrators at UNICEF (United Nations Children's Fund) might very well have thought that no hacker would attack them. However, in January of 1998, their page was defaced. Many other examples of hacked Web pages can be found at archival sites around the Web.

ISSN: 2321-8169
243 - 248

Figure 2 Hacked Library of Congress Web page



Regular auditing, vigilant intrusion detection, good system administration practice, and computer security awareness are all essential parts of an organization's security efforts. A single failure in any of these areas could very well expose an organization to cyber-vandalism, embarrassment, loss of revenue or mind share, or worse. Any new technology has its benefits and its risks. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place.

Certified Ethical Hacker

Certified Ethical Hacker (CEH) is a qualification obtained by assessing the security of computer systems, using penetration testing techniques. The code for the CEH exam is 312-50, and the certification is in Version 9 as of 2016.

Penetration tests are employed by organizations that hire certified ethical hackers to penetrate networks and computer systems with the purpose of finding and fixing security vulnerabilities. While unauthorized hacking, also known as Black Hat hacking, is illegal, penetration testing done at the request of the owner of the targeted systems.

The EC-Council offers another certification, known as Certified Network Defence Architect (CNDA). This certification is designed for United States Government agencies and is available only to members of selected agencies

Certification is achieved by taking the CEH examination after having either attended training at an Accredited Training Centre (ATC), or completed through self-study. If a candidate opts for self-study, an application must be filled out and proof submitted of two years of relevant information security work experience. Those without the required two years of information security related work experience can request consideration of educational background. The current version of the CEH is V9 which uses the EC-Council's exam 312-50, as the earlier versions did. Although the new version V8 has recently been launched, this exam has 125 multiple-choice questions, with a 4-hour time limit, and requires at least a score of 70% to pass. The test delivery will be web based, via Pro metric prime. The exam code varies at different testing centres. The 312-50 exam proctored at Accredited Training Centres (ATC). The earlier v7 had 150 multiple-choice questions and a four-hour time limit. The version 7 and version 8 exams cost US$500 for the actual test and $100 as a non-refundable fee for registration.),

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. 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.

References

1. The Basics of hacking and penetration testing : Ethics Hacking and Penetration Testing Made Easy
2. CEH Certified Ethical Hacker Book
3. The Black Book Ethical Hacking By Brian G. Coffex
4. Certified Ethical Hacker - Wikipedia