International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

A Green Thumb to Fortify Information Redemption

V T RAM PAVAN KUMAR. M

Assistant Professor, Dept of MCA, ,KBNCollege, Vijayawada, Andhra Pradesh, India.

***Abstract*— 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 with most technological advances, there is also 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 find and plug up security holes. The ethical hacking process is explained, along with many of the problems that the Global Security Analysis Lab has seen during its early of ethical hacking for IBM clients.**

I. INTRODUCTION

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

HACKER

1. 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.

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 deby C. C. Palmer scribe 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 flexible 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.

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 a as 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?

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.2

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" 3 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." 4 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.5–7

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**) use don't 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.

Unlike the way some one 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.. 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.

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?

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

A surprising number of clients have difficulty precisely answering the first question: a medical center might say "our patient information," an engineering firm might answer "our new product designs," and a Web retailer might answer "our customer database."

All of these answers fall short, since they only describe targets in a general way. The client usually has to be guided to

succinctly describe all of the critical information assets for which loss could adversely affect the organization or its clients. These assets should also include secondary information sources, such as employee names and addresses (which are privacy and safety risks), computer and network information (which could provide assistance to an intruder), and other organizations with which this organization collaborates (which provide alternate paths into the target systems through a possibly less secure partner's system).

A complete answer to (2) specifies more than just the loss of the things listed in answer to (1). There are also the issues of system availability, wherein a denial-of-service attack could cost the client actual revenue and customer loss because systems were unavailable. The world became quite familiar with denial-of-service attacks in February of 2000 when attacks were launched against eBay**, Yahoo!**, E*TRADE**,CNN**,and other popular Websites. During the attacks, customers were unable to reach these Web sites, resulting in loss of revenue and "mind share." The answers to (1) should contain more than just a list of information assets on the organization's computer. The level of damage to an organization's good image resulting from a successful criminal hack can range from merely embarrassing to a serious threat to revenue. As an example of a hack affecting an organization's image, on January 17, 2000, a U.S. Library of Congress Web site was attacked. The original initial screen is shown in Figure 1, whereas the hacked screen is shown in Figure 2. As is often done, the criminal hacker left his or her nickname, or handle, near the top of the page in order to guarantee credit for the break-in.

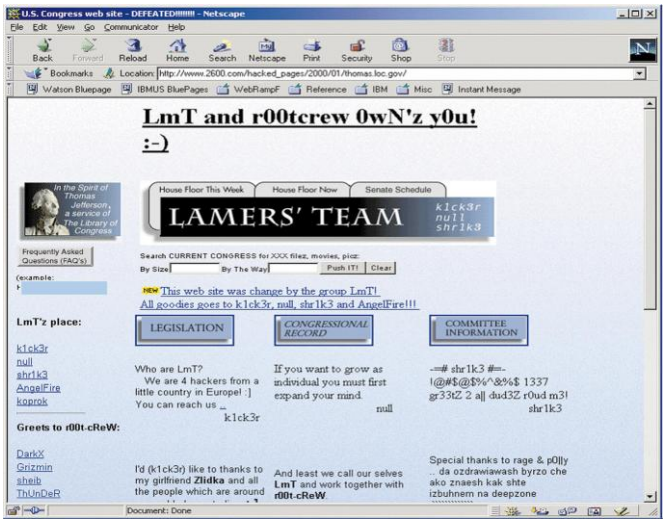


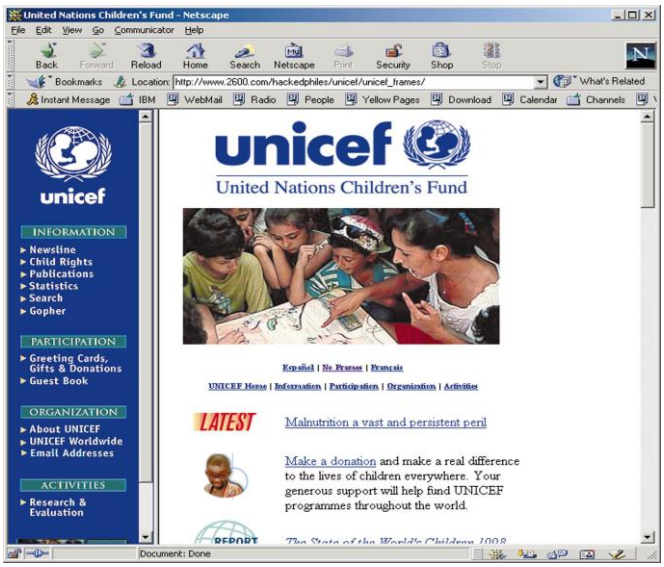
FIG 1: LIBRARY OF CONGRESS WEB PAGE AFTER ATTACK

Some clients are under the mistaken impression that their Web site would not be a target. They cite numerous reasons, such as "it has nothing interesting on it" or "hackers have never heard of my company." What these clients do not realize is that every Web site is a target. 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 Web site 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 as shown in Figures 3 and 4. Many other examples of hacked Web pages can be found at archival sites around the Web.

Answers to the third question are complicated by the fact that computer and network security costs come in three forms. First there are there al monetary costs incurred when obtaining security consulting, hiring personnel, and deploying hardware and software to support security needs. Second, there is the cost of usability: the more secure a system is, the more difficult it can be to make it easy to use. The difficulty can take the form of obscure password selection rules, strict system configuration rules, and limited remote access. Third, there is the cost of computer and network performance. The more time a computer or network spends on security needs, such as strong cryptography and detailed system activity logging, the less time it has to work on user problems.

II. THE ETHICAL HACK ITSELF

Once the contractual agreement is in place, the testing may begin as defined in the agreement. It should be noted that the testing itself poses some risk to the client, since a criminal hacker monitoring the transmissions of the ethical hackers could learn the same information. If the ethical hackers identify a weakness in the client's security, the criminal hacker could potentially attempt to exploit that vulnerability. This is especially vexing since the activities of the ethical hackers might mask those of the criminal hackers. The best approach to this dilemma is to maintain several addresses around the Internet from which the ethical hacker's transmissions will emanate, and to switch origin addresses often. Complete logs of the tests performed by the ethical hackers are always maintained, both for the final report and in the event that something unusual occurs. In extreme cases, additional intrusion monitoring software can be deployed at the target to ensure that all the tests are coming from the ethical hacker's machines. However, this is difficult to do without tipping off the client's staff and may require the cooperation of the client's Internet service provider.



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 Webservers, 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 helpline 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.

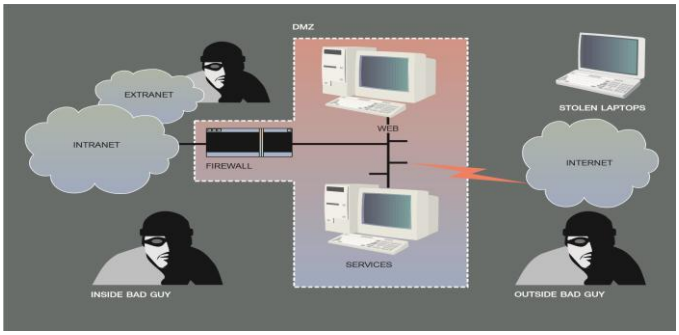
Physical entry. This test acts out a physical penetration of the organization's building. Special arrangements must be made for this, since security guards or police could become involved if the ethical hackers fail to avoid detection. Once inside the building, it is important that the tester not be 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.

III. THE FINAL REPORT

The final report is a collection of all of the ethical hacker's discoveries made during the evaluation. Vulnerabilities that were found to exist are explained and avoidance procedures specified. If the ethical hacker's activities were noticed at all,

Figure 5 Different ways to attack computer security



the response of the client's staff is described and suggestions for improvements are made. If social engineering testing exposed problems, advice is offered on how to raise awareness. This is the main point of the whole exercise: it

does clients no good just to tell them that they have problems. The report must include specific advice on how to close the vulnerabilities and keep them closed. The actual techniques employed by the testers are never revealed. This is because the person delivering the report can never be sure just who will have access to that report once it is in the client's hands .

IV. CONCLUSION

The idea of testing the security of a system by trying to break into it is not new. Whether an automobile company is crash-testing cars, or an individual is testing his or her skill at martial arts by sparring with a partner, evaluation by testing under attack from a real adversary is widely accepted as prudent. It is, however, not sufficient by itself. As Roger Schell observed nearly 30 years ago:

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.

V. CITED REFERENCES AND NOTES

[1] E. S. Raymond, The New Hacker's Dictionary, MIT Press, Cambridge, MA (1991).

[2] S. Garfinkel, Database Nation, O'Reilly & Associates, Cambridge, MA (2000).

[3] The first use of the term "ethical hackers" appears to have been in an interview with John Patrick of IBM by Gary Anthens that appeared in a June 1995 issue of ComputerWorld. 4. P. A. Karger and R. R. Schell, Multics Security Evaluation: Vulnerability Analysis, ESD-TR-74-193, Vol. II, Headquarters Electronic Systems Division, Hanscom Air Force Base, MA (June 1974).

[4] S.M.GoheenandR.S.Fiske,OS/360ComputerSecurityPenetration Exercise, WP-4467, The MITRE Corporation, Bedford, MA (October 16, 1972).

[5] R. P. Abbott, J. S. Chen, J. E. Donnelly, W. L. Kingsford, andS.T.Tokubo,SecurityAnalysisandEnhancementsofComputer Operating Systems, NBSIR 76-1041, National Bureau of Standards, Washington, DC (April 1976).

[6] W. M. Inglis, Security Problems in the WWMCCS GCOS System, JointTechnicalSupportActivityOperatingSystemTechnical Bulletin 730S-12, Defense Communications Agency (August 2, 1973).

[7] D.FarmerandW.Z.Venema,"ImprovingtheSecurityofYour Site by Breaking into It," originally posted to Usenet (December 1993); it has since been updated and is now available at ftp://ftp.porcupine.org/pub/security/index.html#documents.

[8] See http://www.faqs.org/usenet/. Who can really determine who said something first on the Internet?

[9] See http://www.cs.ruu.nl/cert-uu/satan.html. This strategy is based on the ideal of raising the security of the whole Internet by giving security software away. Thus, no one will have any excuse not to take action to improve security.