The Network Hackers: Security Providers of Network in Emerging and Continuous way

*Er. Jiaur Rahman Ahmed, **Er. Deepak Kumar Garg, ***Er.Aminur Rahman
*Lecturer,Department of Computer Science,Guru Kashi University,Talwandi Sabo ,Bathinda,Punjab
**Lecturer,Department of Computer Science,Guru Kashi University,Talwandi Sabo ,Bathinda,Punjab
***Lecturer,Department of Computer Science,Jasdev Singh Sandhu Institute of Engineering and Technology,Patiala,Punjab

Abstract
The growth of the Internet has brought easy access to online business, electronic commerce, emails and new avenues of information distribution as well as advertising. Although the most technological advancement there is always a dark side the criminal hackers where they represent a threat to these information avenues. The term "hacker" instantly brings thoughts of an evil, unscrupulous person who steals data and breaks into corporate networks. However, there are advantages to hiring a hacker as a part of your information technology group. A company that maintains a website and internal network can benefit from the experiences developed by the hacker. Not all hackers are criminals, and some of them penetrate network security in an attempt to educate users.Despite the fact that companies, governments, and individuals around the world are anxious to be a part of such revolution, there are always a fear of hackers who will break into their web servers and steal their data and sensitive information. With these concerns the ethical hacker can help eliminate such fear and find optimum solutions to these problems.
Keywords: Denial-of-Service, Network Security, FTP, Ethical Hacking.

Introduction

With the fast growth of the Internet technologies, computer security has become a major concern for governments and business where the possibility of being hacked is proportional to the security implemented in their infrastructure. In an effort to find a proper approach to the problem, organizations came to realize that on of the best solution to the problem is to evaluate the intruder threat where computer security professionals can be hired to attempt to break into their computer systems. Such approach is similar to having independent auditors to verify an organization's bookkeeping records. With the same concept, professional security team "ethical hackers" will employ the same tools and techniques used by intruders to investigate the security gaps and vulnerabilities without damaging the target systems or steal information. Once such process is complete, the security team will report back to the owners with the vulnerabilities they found and instructions on how to eliminate such security gaps.

What is Ethical Hacking

Professional ethical hackers possess a variety of skills and must be completely trustworthy since while testing the client's systems security they may discover information about their clients that should remain secrets. Ethical hackers must be trusted to exercise tight control over any information that might be a target of misused by intruders. Due to the sensitivity of the

information gathered during the evaluation of the vulnerable systems, strong measures are required to be taken into considerations to ensure that the security of the systems being employed by the ethical hackers are intact. During the evaluation of a system's security, the ethical hackers seek the answers to some of the following questions:

- What can an intruder see on the target systems?
- What can an intruder do with the information captured?
- What is organization trying to protect?
- How much effort, time, and money are an organization is willing to expend to obtain adequate protection?

Once the answers to the above questioned were determined, a security evaluation plan is drawn up by the ethical hackers where it can identify the system to be tested, how such systems will be tested, and determining any limitations implemented in the testing plan. In a society so dependent on computers and networks, breaking through somebody's systems is considered anti-social behaviors, and as such organizations and business investing the best they can to have the best security in place to protect their interests and their information. However, with the best security and best security policy in place, a break-in still occurs by determined hackers. The only solution for organizations and businesses to avoid such problem could lie in the form of ethical hackers where such group get paid to hack into supposedly secure networks and expose flaws. No matter how layered and extensive the security architecture is constructed within any organization's infrastructure, the potential for external intrusion still unknown until its defenses are realistically tested. Despite the fact that most organizations usually hire security specialists to protect their domains, the fact remains that security breaches happen due to the lack of knowledge about the organization's systems, and its potential vulnerabilities. The solution to solve such vulnerabilities is for organizations to hire ethical hackers where they can test and determine such vulnerabilities through different ways of breaking into the systems and presenting the right solutions for such organizations to eliminate the existing security gaps within their security infrastructure.

IIS Security Issues

Internet Information Server (IIS) had many vulnerability issues in the past that affected a lot of organizations and small business, and some of these vulnerabilities are:

- **Denial-of-Service attacks** – such attack is related to a stack overflow in the IIS FTP module. When IIS is configured to allow anonymous FTP, the attackers could log in and create a long directory name that can create an overflow condition. The solution for such problem as suggested by Microsoft is to turn off the FTP serves unless it is needed. Also, IIS should be implemented to prevent the creation of new directories.
- **An Elevation of privilege attacks** – such attack is launched by creating crafted anonymous HTTP that can request to gain access to a location that usually requires authentication. Such attack can be mitigated by enforcing the file system based ACL where the attacker will be restricted to the permissions granted to the anonymous user account within the system.
- **Zero-day attacks** – such attack exploit code that can be used to create Denial of Service (DoS) condition on Windows Server 2003 and Windows XP without requiring write access to the server file systems. To mitigate such attack, the NTFS file system need to be modified to disallow the directory creation by FTP users and also disallow FTP write access to anonymous users (Prince, 2009).
- **File Transfer Protocol (FTP) attacks** – such attack will happen when a certain code runs to install unauthorized software on the IIS. Such attack can happen only when the FTP is enabled, and as such; the attacks can be mitigated by disable the FTP capability on the IIS (Protalinski, 2009).

IE Security Issues

Internet Explorer (IE) is used by many users cross the world, and such client application faces many security threats that can compromise the user's computer and the server security. Some of the security threats that IE faces over the past years are:

- **Crafted script (phishing site) attack** – Such attack will create a crafted html local resource link with a script that will display a fake content of a trusted site. Once the link is clicked, it will display "Navigation Cancelled" page to push the victim to refresh the page, and the attack will provide the fake content to the user. To avoid such attack, users must be aware of the attack and don't trust the "Navigation Cancelled".
- **Inline Frames Attack** – such attack happen via iframes where such frames are used to serve web ads which comes from different domain than the content that appears on the

same web page. Such iframes don't have restricted access to a document's frames within the Internet Explorer and as such, attackers can modify the contents of the iframes to direct users to different domains .

- **Code Execution Attack** – such attack happens when the attackers code host a malicious crafted web page and run the code if the user was convinced to visit the web page, and press the F1 key to response to a pop-up page (Naraine, 2010).
- **System File Attack** – Such attack can be initiated based on a system file that is part of the Windows system files. In such attack the attacker will take control over the user's computer via IE feature that lets the browsers control other Microsoft applications which run under a Windows system. Such control will be gained by the attacker during the user's visit to the attacker's web site (Thurrott, 2005).

Penetration Test: Security

Penetration testing (also called pen testing) is the practice of testing web applications, computer systems, and network to find vulnerabilities that any intruder may exploit. Such test can be automated with software applications or can be performed manually. In either way, the process encompasses gathering information about the target system, identifying possible entry points, attempting to break in (either for real or virtual) and reporting back such findings to the client. The main objective of penetration testing is to determine security weaknesses, and also testing how an organization's security policy compliant with standard security guidelines.

Some clients insist that as soon as the ethical hackers gain access to their network or to one of their systems, the evaluation should halt, and the client should be notified. Such short of ruling should be discouraged since it prevents the client from learning more about what ethical hackers might discover more about their systems vulnerabilities, and other issues that might harm their systems. Organizations and companies should allow enough time for the penetration test to be done properly since last minute evaluations are of little use, and the implementation of corrections for discovered security problems might take more time than is available, and may introduce new system problems. In order for the client to receive a valid evaluation, the client must be cautioned to limit prior knowledge of the test as much as possible for ethical hacker to run a real live test. Having such knowledge known to the organization's employees will make the hacking process unreal since client's employee will be running ahead of the ethical hackers

locking doors and windows. Having a limited number of people at the target organization who know of the impending evaluation, it becomes possible for the evaluation to reflect the organization's actual security exposure to the outside world.

Once the contractual agreement with ethical hackers is in place, the testing may start as defined in the agreement. It's important to point out that penetration test itself poses some risks to the client networks and systems, since criminal hackers might monitor the transmissions of the ethical hackers and learn the same information about the client during such test. In such case, if the ethical hackers identify weakness in the client's security, the criminal hackers could potentially attempt to exploit such vulnerabilities, and as such; implementing the best approach to avoid such dilemma is very important. One of these approaches is for ethical hackers to maintain several addresses around the Internet from which the transmission will emanate and to switch origin addresses often. A complete log of the test performed by the ethical hackers is always a good idea to be maintained for the final report, and also to identify any unusual event that might happen during the test. In many cases, additional intrusion monitoring software can be deployed at the target to ensure that all the testes are coming from the ethical hacker's machines.

The line between criminal hacking and computer virus writing is becoming increasingly blurred, and as such; many clients request from ethical hackers to perform testing to determine the client's vulnerabilities to web-based virus and email. However, it is far better for the client to deploy strong antivirus software, to keep it up to date, and implement a clear and simple policy within an organization to report any incidents. There are several kinds of testing that can be done during the penetration test, and any combination of the following may be called for:

- **Remote network –** This test simulate the intruder launching an attack across the Internet. The primary defences that must be defeated are filtering routers, firewalls, and web servers.
- **Remote dial-up network –** This test simulates the intruder launching an attack against the client's modem pools. The primary defences that must be defeated are the user authentication schemes.
- **Local network –** This test simulates authorized person has a legal connection to the organization's network. The primary defences that must be defeated are internal web servers, Intranet firewalls, server security measures and e-mail systems.

- **Stolen laptop computer –** This test makes use of the laptop computer of a key employee within the organization. The test will examine the computer for passwords stored in dial-up software corporate information assets, and personal information.
- **Social engineering –** This test will evaluate the target organization's staff as to whether it would leak information to someone. In such test, the ethical hacker will be calling the organization's computer help line and asking for the external telephone numbers of the modem pool. Defending against such attack is hard, because people and personalities are involved.
- **Physical entry –** This test examine the physical penetration of the organization's building. Security guards or police could become involved if the ethical hackers fail to avoid detection.
- Penetration test usually have strategies, and such strategy include the following:
- **Target testing –** Such test is performed by the penetration testing team (Ethical hackers) in coordination with the organization's IT team. It is sometimes referred to as a "light-turned-on" approach since everyone can see the test being carried out.
- **External testing –** This type of pen test targets a company's external visible servers or devices including web servers, firewalls, domain name servers (DNS), or email servers. The objective of such test is to find out if outside attackers can get in, and how far they can get in and gain access.
- **Internal testing –** this test mimics an inside attack behind the firewall by an authorized user with standard access privileges. Such test is useful for estimating how much damage a disgruntled employee could cause.
- **Blind testing –** Such test simulates the procedures and actions of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand.
- **Double blind testing –** Such test is conducted while one to two people within the organization might be aware of the test. The test can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

Final Penetration Report

The final report represents a collection of all of the ethical hacker's discoveries as the result of the penetration test evaluation. Vulnerabilities found during such test are explained, and the steps to avoid such vulnerabilities were specified through specific procedures to close any security gaps discovered during such process. The report also offers advices on how to raise awareness, and advice on how to close the vulnerabilities and keep them closed. The report is considered to be a very sensitive issue since such vulnerabilities found and stated in such report if it fell into the wrong hands might be used against the company's vulnerabilities to gain access to sensitive information within the company networks.

The ethical hackers would have an ongoing responsibility to ensure the safety of any information they retain, and as such; in most cases all information related to the work is destroyed at the end of the contract.

Conclusion

Hacking is the complement of Security perspective in Network. The idea of testing the security of a system by trying to break into it is not a new idea such test were done long time ago by many automobile companies during the crash-testing cars to identify the weakest points of their products. From a practical standpoint the security problem will remain as long as manufacturers remain committed to current system architectures without a firm requirement for security. A single failure in any of these areas could very well expose an organization to cyber-vandalism, and loss of revenue and client's information. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place. Finally, attackers will always find their way to the security gaps within any application and software, and it's important for such application and software to follow all the security updates and patches to prevent such threat to the computer systems by ethical hackers.

References

Claburn, T. (2009) Microsoft Expands IIS Vulnerability Warning [Online]. Available from:http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=219501448 (Accessed: 06 November 2010).

Claburn, T. (2009) Microsoft Internet Explorer Vulnerability Warning Issued [Online]. Available from:http://www.informationweek.com/news/internet/browsers/showArticle.jhtml?articleID=208801757 (Accessed: 06 November 2010).

Naraine, R. (2010) Microsoft Investigating new IE browser vulnerability [Online]. Available from:http://www.zdnet.com/blog/security/microsoft-investigating-new-ie-browser-vulnerability/5560 (Accessed: 06 November 2010).

Prince, B (2009) Microsoft IIS Vulnerability Get Hit By Attacks [Online]. Available from: http://www.eweekeurope.co.uk/news/news-security/microsoft-iis-vulnerability-gets-hit-by-attacks-1767 (Accessed: 06 November 2010).

Prince, B. (2007) Microsoft Investigates IE7Vulnerability [Online]. Available from: http://www.eweek.com/c/a/Security/Microsoft-Investigates-IE-7-Vulnerability/ (Accessed: 06 November 2010).

Protalinski, E. (2009) IIS vulnerability under limited attacks [Online]. Available from: http://arstechnica.com/microsoft/news/2009/09/microsoft-investigating-possible-vulnerability-in-iis.ars (Accessed: 06 November 2010).