International Journal for Rapid Research in Engineering Technology & Applied Science
Vol 4 Issue 7 July 2018
ISSN (Online): 2455-4723

A Study of Hacking

Dr.Sanjay Maheshwari *
Vishisht School of Management,DAVV,Indore, MP,45001,India *
Sanjay.bhangdia@gmail.com *

Abstract: The word "hacking" has two definitions. The first definition refers to the hobby/profession of working with computers. The second definition refers to breaking into computer systems. While the first definition is older and is still used by many computer enthusiasts (who refer to cyber-criminals as "crackers"), the definition is much more commonly used. In particular, the web pages here refer to "hackers" simply because our web-server logs show that everyone who reaches these pages are using the second definition as part of their search criteria. The paper is focused to study the hacking problem and measures to be adopted.

Keywords: Hacker, Cyber Crime, Crackers, Signals.

Introduction

The word "hacking" has two definitions. The first definition refers to the hobby/profession of working with computers. The second definition refers to breaking into computer systems. While the first definition is older and is still used by many computer enthusiasts (who refer to cyber-criminals as "crackers"), the definition is much more commonly used. In particular, the web pages here refer to "hackers" simply because our web-server logs show that everyone who reaches these pages are using the second definition as part of their search criteria. A hacker can "hack" his or her way through the security levels of a computer system or network. This can be as simple as figuring out somebody else's password or as complex as writing a custom program to break another computer's security software. Hackers are the reason software manufacturers release periodic "security updates" to their programs. While it is unlikely that the average person will get "hacked," some large businesses and societies receive multiple hacking attempts a day. 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.

Integrity: - Integrity means that data cannot be customized without approval. This means that the data seen by the allowed persons should be correct or the data should maintain the property of integrity.

Availability: - This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

What is ethical hacking? :- Ethical hacking and a ethical hacker are terms that describe hacking performed to help a company or individual identify potential threats on the computer or network. An ethical hacker attempts to hack their way past the system security, finding any weak points in the security that could be exploited by other hackers. The organization uses what the ethical hacker finds to improve the system security, in an effort to minimize, if not eliminate any potential hacker attacks.

Benefits of ethical hacking: - There are many terrorists and terrorist societies that are trying to create havoc in the world with the use of computer technology. They break into various government defense systems and then use this for their terrorist activities.

Preventive action against the terrorists can be taken by the ethical hackers. This can be done because the ethical hackers use their expertise to create alternate information that is false, of the hackers to get while the real information that is necessary and important is hidden from the terrorists.

The ethical hackers are also used to try and test the existing defense systems. These people are also used to build a foolproof system that prevents the breakdown of the existing system.

Who are ethical hackers? : - doing well ethical hackers hold a range of skills. First and primary, they must be fully constant. While testing the security of a client's systems, the ethical hacker may take in 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 assessment, 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. 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 resolution. This is a critical trait, since criminal hackers are known to be particularly patient and willing to monitor systems for days or weeks while waiting for an occasion. Finally, keeping up with the ever-changing world of computer and network security requires nonstop education and review.

Active who is an easy-to-use network tool you can use to find any information about the owners of IP address or Internet domain? You can determine the country, personal and postal addresses of owner, and/or user of IP address and domains.

When a search is completed, the following reports will be displayed:

- DNS Records – A DNS i.e. "Domain Name System" resolves individual host names to their corresponding IP addresses. A computer on the Internet configured as a host may actually resolve to several IP addresses and host names.
- Domain Owner – This report displays information about the domain holder i.e. "registrant". In addition, information is included here about TLD (Top Level Domain) with a link to the domain registrar and the name of the country.
- IP Address – Each IP address is assigned to an individual or a society. Rarely, it may totally differ from the domain owner. Typically, small sites use IPs assigned to their hosting company or network provider, so this information can help you to settle on the objective location of the website or remote computer.
- HTTP Headers – Shows HTTP (Hyper Text Transfer Protocol) headers. It allows you determine web server software; date the document was created, and so on.

What do ethical hackers do?

Does anyone at the target notice the intruder's attempts or successes? :- This is 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, expend weeks or months trying and will usually in time do well.

When the client needs a valuation, there is quite a bit of conversation and paperwork that must be done up front.

-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?

All of these answers fall small, since they only explain targets in a general way. The client generally has to be guided to succinctly explain all of the critical information assets for which loss could harmfully affect the society or its clients. These assets should also include secondary information sources, such as employee names and addresses, 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).

Some customers insist that as soon as the ethical hackers gain access to their network or to one of their systems, the valuation should halt and the client be notified. This sort of ruling should be discouraged, because it prevents the client from learning all that the ethical hackers might discover about their systems. It can also lead to the client's having a false sense of security by thinking that the first security hole found is the only one present.

The ethical hack itself: -If the ethical hackers be familiar with a limitation in the client's security, the criminal hacker could potentially try to increase that responsibility. This is particularly 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. The line between criminal hacking and computer virus writing is becoming increasingly blurred. When requested by the client, the ethical hacker can perform testing to determine the client's susceptibility to e-mail or Web-based virus vectors.

There are several kinds of testing. Any combination of the following may be called for:

- Local network. This test simulates an employee or other authorized person who has a legal relationship to the organization's network.
- Physical entry test acts out a physical penetration of the organization's building. The primary defenses here are a strong security policy, security guards, access controls and monitoring, and security awareness.
- Remote network. This test simulates the intruder launching an attack across the Internet.
- Remote dial-up network. This test simulates the intruder launching an attack against the client's modem pools.
- Social engineering. This test evaluates the target organization's staff as to whether it would leak information to someone.

- 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.

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. 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 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.

Analogy with Building Robbing methodology of a hacker is similar to the one used for usual thefts. Let's consider the case of a bank robbery. As described above there are mainly five steps in hacking like reconnaissance, scanning, and gaining access, maintaining access and clearing tracks. But it is not the end of the process. The various stages in the hacking methodology are

Reconnaissance, Scanning & Enumeration, Gaining access, maintaining access, clearing tracks.

Google: - Google is one of the most famous search engines used in the Internet. Using some kind of particular keywords for searching we can find much such information that is put in publicly. One of the main advantages of Google is its advanced search option. The advanced search have many options like searching for particular domain, documents published after a particular period of time, files of particular format, particular languages etc.

Sam spade is a simple tool which provides us information about a particular host. This tool is very much helpful in finding the addresses, phone numbers etc.

Port Scanning:-A port scan is a method used by hackers to determine what ports are open or in use on a system or network. By scanning the ports over a much longer period of time you reduce the chance that the target will trigger an alert.

Email Tracker and Visual Route: - We often used to receive many spam messages in our mail box. We don`t know where it comes from. Email tracker is software which helps us to find from which server the mail does actually came from

Pingers :-Pingers and yet another category of scanning tools which makes use of the Internet Control Message Protocol(ICMP) packets for scanning.

War Dialing:- The war dialers are a hacking tool which is now illegal and easier to find out. A war dialer is a computer program used to identify the phone numbers that can successfully make a connection with a computer modem.

Super Scan is a powerful TCP port scanner, that includes a range of additional and Nmap ("Network Mapper") is a free and open source utility for network exploration or security auditing. Details are the ability of a hacker to convince some servers to give them information that is vital to them to make an attack. By doing this the hacker aims to find what resources and shares can be found in the system, what valid user account and user groups are there in the network, what applications will be there etc. Hackers may use this also to find other hosts in the entire network

Password Cracking :-Many types of password cracking strategies are used today by the hackers which are described below. Dictionary cracking ,Brute force cracking ,Hybrid cracking, Social Engineering

Loft crack :- This software uses the various password cracking methodologies. This is very high profile software which uses dictionary cracking then brute force cracking.

Maintaining Access :- In the network scenario the hacker will do it by uploading some software like Trojan horses, sniffers, key stroke loggers etc.

-Key stroke loggers are actually tools which record every movement of the keys in the keyboard.

-The hackers will place these Trojan softwares inside the network and will go out. Then after sometimes when he come back the Trojan software either authenticate the hacker as a valid user or opens some other ports for the hacker to get in.

- wrapper softwares actually do is they will place the malicious data in to the white spaces in the harmless data. Actually what they does is that they will insert the data into the white spaces that may be present in the files.

Win zapper is another tool which is used for clearing the tracks. This tool will make a copy of the log and allows the hackers to edit it.

The ending report

The real delivery of the statement is also a sensitive issue. If vulnerabilities were found, the report could be extremely risky if it fell into the wrong hands. A participant might use it for corporate espionage, a hacker might use it to break into the client's computers, or a prankster might just post the report's contents on the Web as a joke. The ending report is usually delivered directly to an officer of the client society in hard-copy form. The ethical hackers

would have an ongoing liability to make sure the safety of any information they hold, so in most cases all information related to the work is destroyed at the end of the contract.

Conclusions

The research paper concludes on a note that good auditing and consideration of security measures from time to time and vigilance intrusion detecting and good systems administration can be very effective ways of securing and fortifying the company's network.The design 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, assessment by testing under attack from a real adversary is usually accepted as prudent.

Now we can see what we can do against hacking or to protect ourselves from hacking. The first thing we should do is to keep ourselves updated about those softwares we and using for official and reliable sources. Educate the employees and the users against black hat hacking. Use every possible security measures like Honey pots, Intrusion Detection Systems, Firewalls etc. Every time make our password strong by making it harder and longer to be cracked.

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.

References

1. www.research.ibm.com
2. www.EzineArticles.com/?expert=P._Walsh
3. www.insecure.in
4. http://www.eccouncil.org/
5. http://www.saching.com/Article/Ethical-hacking-and-its-various-benefits/5052
6. http://www.computerhope.com/jargon/e/ethihack.htm
7. http://www.iss.net/security_center/advice/Underground/Hacking/default.htm
8. http://definitions.uslegal.com/c/computer-hacking/
9. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212220,00.html
10. http://www.windowsecurity.com/articles/Different-Shades-Hackers.html
11. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci550882,00.html
12. http://www.catb.org/jargon/html/T/tiger-team.html
13. http://en.wikipedia.org/wiki/Tiger_team
14. (http://www.nsa.gov/public_info/press_room/2010/cdx.shtml
15. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci555449,00.html
16. http://en.wikipedia.org
17. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci550815,00.html
18. http://geodsoft.com/howto/password/cracking_passwords.htm
19. http://www.microsoft.com/security/antivirus/prevent.aspx