Review on Ethical Hacking

Danish sharma1,Rituraj Chandra2, C.K Raina3
Student CSE department,AIT Chandigarh,Punjab,India

ABSTRACT: As We all know web is developing at a fast speed and the state of security on the internet is very poor. All the data is given to everybody in single tick. Hacking is a process in which, a person or team exploits the weakness in a system for self-proceeds or indulgence. Ethical Hacking is an activity which focuses on the vulnerability in a system and discovers the weakness and try to rectify the security weakness of a system. Ethical hacker plays a vital role in protecting the valuable and sensitive data in a system. He endeavors to copy the expectation and activities of noxious programmers without bringing about mischief. This paper tries to portray thought of ethical hacking, tools and every one of its angles in general.

KEYWORDS: Ethical Hacking, Hacking Phases, Penetration,Hacking tools.

Introduction

With the rapid growth of the cyber technology world, computer security has become a foremost concern for governments and business peoples where the possibility of being hacked is comparative to the security implemented in thei infrastructure. Professional
ethical hackers use the same methods and techniques used by hackers to investigate the security flaws and vulnerabilities without affecting the target systems or sensitive data.
Once ethical process is complete, the security team will give the details report to the
owners with the vulnerabilities they found and instructions on how to eradicate such security flaws.

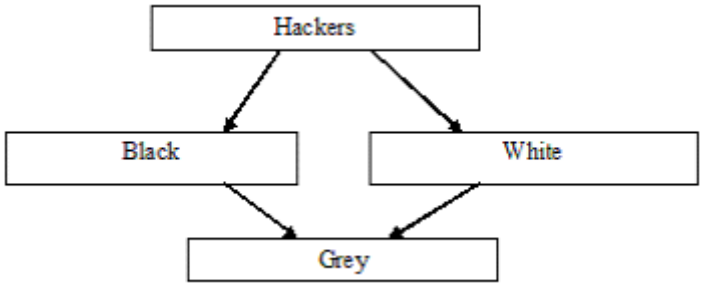
What is Ethical Hacking?

Ethical hacking is also known as “Penetration Hacking” or “Intrusion Testing” or “Red Teaming”. Ethical hacking is defined as the practice of hacking without malicious intent. the Ethical Hackers and Malicious Hackers are different from each other and playing their important roles in security .According to Palmer (2004, as quoted by Pashel, 2006): “Ethical hackers employ the same tools and techniques as the intruders, but they neither damage the target systems nor steal information. Instead, they evaluate the target systems’ security and report back to owners with the vulnerabilities they found and instructions for how to remedy them”. The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. As, with most technological advances, there is also other side: criminal hackers who will secretly steal the organization’s information and transmit it to the open internet. These types of hackers are called black hat hackers. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical

Ethical hackers or white hat hackers. Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results is a detailed report of the findings as well as a testimony that ahacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them. We can easily say that Ethical hacking does perfectly fit into the security life cycle shown in the below figure

Fig. 3 Security Life Cycle

TYPES OF HACKING/HACKERS



The hacking can be classified in three different categories, according to the shades or colours of the "Hat". The word Hat has its origin from old western movies where the colour of Hero's' cap was "White" and the villains' cap was "Black". It may also be said that the lighter the colour, the less is the intension to harm.

A.White Hat Hackers

White Hat Hackers are authorized and paid person by the companies, with good intends and moral standing. They are also known as "IT Technicians". Their job is to safeguard Internet, businesses, computer networks and systems from crackers. Some companies pay IT professionals to attempt to hack their own servers and computers to test their security. They do hacking for the benefit of the company. They break security to test their own security system. The white Hat Hacker is also called as an Ethical Hacker in contrast to White Hat Hackers

.

B. BlackHat Hackers

The intension of Black Hat Hackers is to harm the computer systems and network. They break the security and intrude into the network to harm and destroy data in order to make the network unusable. They deface the websites, steal the data, and breach the security. They crack the programs and passwords to gain entry in the unauthorized network or system. They do such things for their own personal interest like money. They are also known as "Crackers" or Malicious Hackers Other than white hats and black hats.

C. Grey hat hackers

Another form of hacking is a Grey Hat. As like in inheritance, some or all properties of the base class/classes are inherited by the derived class, similarly a grey hat hacker inherits the properties of both Black Hat and White Hat. They are the ones who have ethics. A Grey Hat Hacker gathers information and enters into a computer system to breech the security, for the purpose of notifying the administrator that there are loopholes in the security and the system can be hacked. Then they themselves may offer the remedy. They are well aware of what is right and what is wrong but sometimes act in a negative direction. A Gray Hat may breach the organizations' computer security, and may exploit and deface it. But usually they make changes in the existing programs that can be repaired. After sometime, it is themselves who inform the administrator about the company's security loopholes. They hack or gain unauthorized entry in the network just for fun and not with an intension to harm the Organizations' network. While hacking a system, irrespective of ethical hacking (white hat hacking) or malicious hacking (black hat hacking), the hacker has to follow some steps to enter into a computer system, which can be discussed as follows.

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?

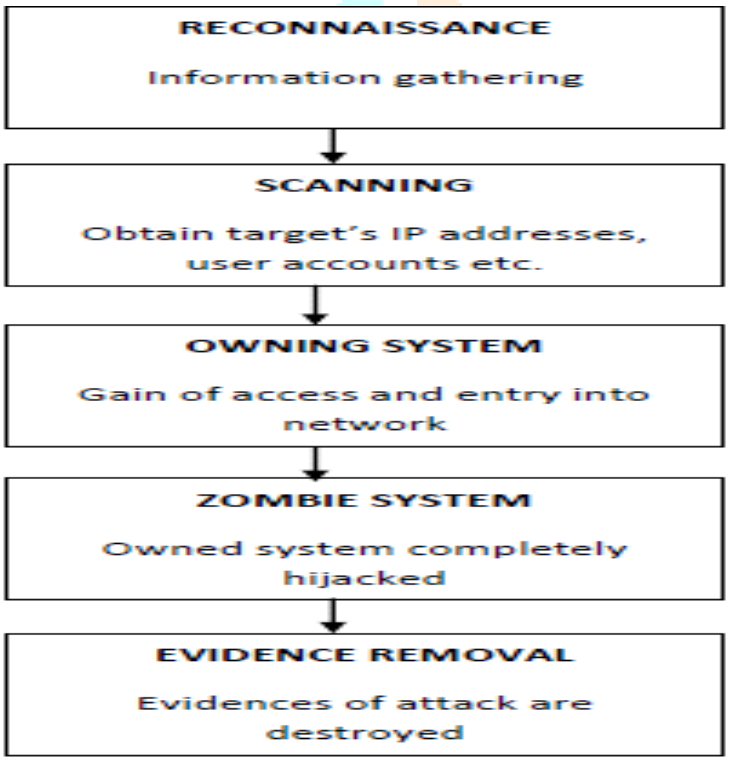
HACKING PHASES

Hacking Can Be Done By Following These Five Phases:
Phase 1: **Reconnaissance**: can be active or passive: in passive reconnaissance the information is gathered regarding the target without knowledge of targeted company (or individual). It could be done simply by searching information of the target on internet or bribing an employee of targeted company who would reveal and provide useful information to the hacker.
This process is also called as "information gathering". In this approach, hacker does not attack the system or network of the company to gather information. Whereas in active reconnaissance, the hacker enters into the network to discover individual hosts, ip addresses and network services. This process is also called as

"rattling the doorknobs". In this method, there is a high risk of being caught as compared to passive reconnaissance

Phase 2: **Scanning**: In scanning phase,the Information Gathered In Phase 1 Is Used To Examine The Network. Tools Like Dialers', Port Scanners Etc. are being Used by the Hacker to Examine the Network So As To Gain Entry in the Company's System And Network.
passive reconnaissance.
Phase 3: Owning the System: This Is The Real And Actual Hacking Phase. The Hacker Uses The Information Discovered In Earlier Two Phases To Attack And Enter Into The Local Area Network (LAN, Either Wired Or Wireless), Local Pc Access, Internet Or Offline. This Phase Is Also Called As "Owning The System"

Phase 4: **Zombie System**: Once the hacker has gained the access in the system or network, he maintains that access for future attacks (or additional attacks), by making
changes in the system in such a way that other hackers or security personals cannot then enter and access the attacked system. In such a situation, the owned system (mentioned in Phase 3) is then referred to as "Zombie System".



Phase 5: Evidence Removal: In this phase, the hacker removes and destroys all the evidences and traces of hacking, such as log files or Intrusion Detection System Alarms, so that he could not be caught and traced. This also saves him from entering into any trial or legality. Now, once the system is hacked by hacker, there are several testing methods available called penetration testing to discover the hackers and crackers.

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.

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

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.

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.

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.

Benefits of Ethical Hacking

• This type of “test” can provide convincing evidence of real system or network level threat exposures through proof of access. Even though these findings may be somewhat negative, by identifying any exposure you can be proactive in improving the overall security of your systems.

• However, information security should not be strictly limited to the mechanics of hardening networks and computer systems. A mature security information program is a combination of policies, procedures, technical system and network standards, configuration settings, monitoring, and auditing practices. Business systems, which have resisted simple, direct attacks at the operating system or network level, may succumb to attacks that exploit a series of procedural, policy, or people weak points.

• An ethical hack, which tests beyond operating system and network vulnerabilities, provides a example, should your ethical hack prove that your firewalls could withstand an attack because there was no breach, but no one noticed the attacks, you may be better prepared to make a case for improving intrusion detection broader view of an organization’s security. The results should provide a clear picture of how well your detection processes works as well as the response mechanisms that should be in place. “Tests” of this sort could also identify weakness such as the fact that many systems security administrators may not be as aware of hacking techniques as are the hackers they are trying to protect against. These findings could help promote a need for better communication between system administrators and technical support staff, or identify training needs.

• Quite often, security awareness among senior management is seriously lacking.
traditional diagnostic work primarily deals with the possibility of a threat and this often leads to a casual view of the threat, deferring the need to immediately address the requirements. Through an ethical hacking exercise, especially if the results are negative, senior management will have a greater understanding of the problems and be better able to prioritize the requirements. For improving intrusion detection.

B. Limitations of Ethical Hacking

• Ethical hacking is based on the simple principle of finding the security vulnerabilities in systems and networks before the hackers do, by using so-called “hacker” techniques to gain this knowledge. Unfortunately, the common definitions of such testing usually stops at the operating systems, security settings, and “bugs” level. Limiting the exercise to the technical level by performing a series of purely technical tests, an ethical hacking exercise is no better than a limited “diagnostic” of a system’s security.

• Time is also a critical factor in this type of testing. Hackers have vast amounts of time and patience when finding system vulnerabilities. Most likely you will be engaging a "trusted third party" to perform these test for you, so to you time is money. Another consideration in this is that in using a "third party" to conduct you tests, you will be providing "inside information" in order to speed the process and save time. The opportunity for discovery may be limited since the testers may only work by applying the information they have been given.

• A further limitation of this type of test is that it usually focuses on external rather than internal areas, therefore, you may only get to see half of the equation. If it is not possible to examine a system internally, how can it be established that a system is "safe from attack", based purely upon external tests? Fundamentally this type of testing alone can never provide absolute assurances of security. Consequently, such assessment techniques may seem, at first, to be fundamentally flawed and have limited value, because all vulnerabilities may not be uncovered.[9]

Time is also a critical factor in this type of testing. Hackers have vast amounts of time and patience when finding system vulnerabilities. Most likely you will be engaging a "trusted third party" to perform these test for you, so to you time is money. Another consideration in this is that in using a "third party" to conduct you tests, you will be providing "inside information" in order to speed the process and save time. The opportunity for discovery may be limited since the testers may only work by applying the information they have been given.

• A further limitation of this type of test is that it usually focuses on external rather than internal areas, therefore, you may only get to see half of the equation. If it is not possible to examine a system internally, how can it be established that a system is "safe from attack", based purely upon external tests? Fundamentally this type of testing alone can never provide absolute assurances of security. Consequently, such assessment techniques may seem, at first, to be fundamentally flawed and have limited value, because all vulnerabilities may not be uncovered

CONCLUSION

In this paper firstly we introduced the concepts of system hacking, types of hacking, 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 , benefits and limitations then we discussed various opportunities available to an ethical hacker as a professional.

REFERENCES

[1] Wikipedia
[2] http://www.articlesbase.com/security-articles/ethical-hacking-an-introduction-402282.html
[3] http://www.ehacking.net/2011/06/top-6-ethical-hacking-tools.html#sthash.nszGZw4y.dpuf
[4] OWASP. "Web Application Penetration Testing,"
http://www.owasp.org/index.php/Web_Application_Pene tration_Testing.
[5] Gurpreet K. Juneja,"Ethical hanking :A technique to enhance information security"international journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013
[6] H.M David, "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1,
Feb 23, 2004
[7] https://www.researchgate.net/publication/271079090