Ethical Hacking Techniques with Penetration Testing

S. Ahila
Assistant professor
Dept of CSE
PITS.

A. Devesh Raj
Dept.of CSE
PITS.

G. Prabhu
Dept.of CSE
PITS

Abstract:- **Hacking is an activity in which a person exploits the weakness in a system for self-profit or gratification. Ethical hacking is an identical activity which aims to find and rectify the weaknesses in a system. In the growing era of internet computer security is of utmost concern for the organizations and government. These organizations are using Internet in their wide variety of applications such as electronic commerce, marketing and database access. But at the same time, data and network security is a serious issue that has to be talked about. This paper attempts to discuss the overview of hacking and how ethical hacking disturbs the security. Also the Ethical Hackers and Malicious Hackers are different from each other and playing their important roles in security. This paper studied the different types of hacking with its phases. The hacking can also be categorized mainly in three categories such as white hat, black hat and grey hat hacking. This paper also presents a comparison of the hacking categories with different methods of penetration testing.**

Keywords— Ethical Hacking, Hackers, Hacking Phases.

I. INTRODUCTION

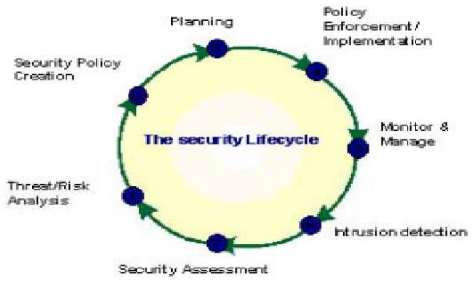


Fig. 1 Security Life Cycle

As cyber attacks increase, so does the demand for information security professionals who possess true network penetration testing and ethical hacking skills. There are several ethical hacking courses that claim to teach these skills, but few actually do. SANS SEC560: Network Penetration Testing and Ethical Hacking truly prepares you to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. You will finish up with an intensive, hands-on Capture the Flag exercise in which you'll conduct a penetration test against a sample target organization, demonstrating the knowledge you mastered in this course. Ethical hacking does perfectly fit into the security life cycle (see Fig 1) . Ethical hacking is a way of doing a security assessment – a current situation (from a technical point of view) can be checked. Like all other assessments (or audits),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 a hacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information. With the growth of internet, computer security is of utmost concern for the organizations and government. These organizations are using Internet in their wide variety of applications such as electronic commerce, marketing and database access. But at the same time, data and network security is a serious issue that has to be talked about. The information such as credit card numbers ,telephone numbers, home addresses, bank account numbers etc. that are available on network may easily be hacked by unsocial elements. This is because of the increasing popularity and use of computers, access to them was limited to authorized or concerned personnel. But when some users were refused to access the computer, they would take it personally, and would challenge the access controls. They would steal passwords and other information by intruding into the system so as to take control of the entire system. They would do such things just to satisfy their ego of not been given the control to access the system, or just for fun, or for money.

Primarily, these computer intrusions were benign but now they have become a serious issue of security. Occasionally the less capable, or less cautious, intruders would unintentionally bring down a system by damaging its files. The system administrator would then have to resume and make repairs to the system. On the other hand, when these intruders were denied access, they would purposefully take destructive actions to harm the organization. When these

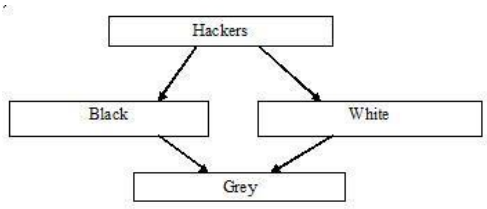
destructive computer intrusions increased in number, they became noticeable, picked up by the media and became "news". The media instead of calling these intruders as "computer criminal," began to call them as "hackers" and described them as individuals who intrudes into some others' computers, may be for fun or revenge, or money. Initially, "hacker" was meant as a compliment, as this person was well verse with computer programming and knowledge, therefore computer security professionals gave a new term "cracker" or "intruder" for those hackers who used their skills for dark side of hackingTo start with hacking, initially organizations decided that the best way to recognize any intrusion into their network or system is to have their own trained professionals who would attempt to break into their systems and would identify, if there are any intrusion threats. These professionals, termed as "Red teams" or "ethical hackers", follow the same steps and tools as that of malicious hackers, but the difference is of their intentions. Ethical hackers have clear intentions to break computer security to save the organization from intrusion attacks. They never reveal the facts and information about the organization. But at any moment of time, if there intentions get sidetracked; they would be the one who would harm the most. This method of recognizing any intrusions into the network and systems was also used by United States Air Force. They conducted a "security evaluation" of the Multics operating systems for a two-level (secret/top secret) system. Their evaluation found that while Multics was significantly better than other conventional systems, it also had loopholes in hardware, software and procedural security. .The hackers performed various penetration tests[4] such as information-gathering, to identify any threat that might damage its integrity.

ABOUT HACKING

Hacking is a brainchild of curiosity. As a result of curiosity, the hacker always wants to know more about information, depending upon his taste. A hacker is a person who enjoys learning the details of computer systems and enhances his capabilities. He is a computer enthusiast and extremely proficient in programming languages, computer systems and networks. Popularly, hackers are referred to someone who penetrates into computer network security systems. It is the hackers who built the Internet and make www to work. The operating system UNIX is a gift from hackers too. Originally, the term hacking was defined as-" 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. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming".

They does not break into systems without authorization rather they are the experts who safeguard the networks of an organization. They attack the organizations' systems to identify any loopholes, if any, in the security, all while staying within the legal limits. Ethical hacking is also known as "Penetration Hacking" or "Intrusion Testing" or "Red Teaming". Malicious hacking is the unauthorized use of computer and network resources. Malicious hackers use software programs such as Trojans, malware and spyware, to gain entry into an organization's network for stealing vital information. It may result to identity theft, loss of confidential data, loss of productivity, use of network resources such as bandwidth abuse and mail flooding, unauthorized transactions using credit or debit card numbers, selling of user's personal details such as phone numbers, addresses, account numbers etc. In general public view, they are the "Criminals of the Cyber World", who has a malicious desire to destroy and harm someone others' network and data. Malicious Hackers are also known as "Crackers". Hackers, be the ethical or malicious, have in depth knowledge of their skills but the only difference that makes them diverse is the intention.

Ethical hackers are very patient. They only demand time and persistence to intrude into the system and find the loopholes in the security. This vital trait of patience can also be seen in malicious hacker as he too would keep the patience and would monitor the target system for weeks or may be for months, and would wait for an opportunity to attack the target. The difference is that an ethical hacker would keep patience to test the target against any security breach while the malicious hacker would keep patience so as to gather information and find an opportunity that is relevant to attack the target system. It may be observed that all techniques and skills employs to both ethical and malicious hackers. It is only the intention of the hackers that makes them diverse. An ethical hacker would always use these techniques and skills to find the weaknesses of the target system and how to deal against any malicious attacks, whereas the malicious hacker would always try to use the techniques and skills to attack the target so as to harm and destroy it for some personal interests like money. It may be said that the ethical hackers' job is tough as compared to malicious one. This is because an ethical hacker would have to identify and understand the changes done in the network by the malicious hacker.



TYPES OF HACKING/HACKER

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

Other than white hats and black hats, 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 breach 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 intention 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.

HACKING PHASES

Hacking Can Be Done By Following These Five Phases.
PHASE 1: RECONNAISSANCE Can Be Active Or Passive: In Passive Reconnaissance[4] 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. Where as 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 Diallers, 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.

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 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".

FIG. 2 HACKING PHASES

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.

TESTING STRATEGIES

• External testing strategy. External testing refers to attacks on the organization's network perimeter using procedures performed from outside the organization's systems, that is, from the Internet or Extranet. This test may be performed with non-or full disclosure of the environment in question. The test typically begins with publicly accessible information about the client, followed by network enumeration, targeting the company's externally visible servers or devices, such as the domain name server (DNS), e-mail server, Web server or firewall.

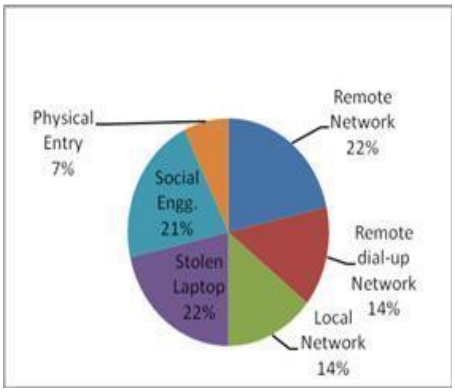
• Internal testing strategy. Internal testing is performed from within the organization's technology environment. This test mimics an attack on the internal network by a disgruntled employee or an authorized visitor having standard access privileges. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network. The techniques employed are similar in both types of testing although the results can vary greatly.

• Blind testing strategy. A blind testing strategy aims at simulating the actions and procedures of a real hacker. Just like a real hacking attempt, the testing team is provided

• with only limited or no information concerning the organization, prior to conducting the test. The penetration testing team uses publicly available information (such as corporate Website, domain name registry, Internet discussion board, USENET and other places of information) to gather information about the target and conduct its penetration tests. Though blind testing can provide a lot of information about the organization (so called inside information) that may have been otherwise unknown, for example, a blind penetration may uncover such issues as additional Internet access points, directly

• connected networks, publicly available confidential/proprietary information, etc. But it is more time consuming and expensive because of the effort required by the testing team to research the target.

• Double blind testing strategy. A double-blind test is an extension of the blind testing strategy. In this exercise, the organization's IT and security staff are not notified or informed beforehand and are "blind" to the planned testing activities. Double-blind testing is an important component of testing, as it can test the organization's security monitoring and incident identification, escalation and response procedures. As clear from the objective of this test, only a few people within the organization are made aware of the testing. Normally it's only the project manager who carefully watches the whole exercise to ensure that the testing procedures and the organization's incident response procedures can be terminated when the objectives of the test have been achieved.



• Targeted testing strategy. Targeted testing or the lights-turned-on approach as it is often referred to, involves both the organization's IT team and the penetration testing team to carry out the test. There is a clear understanding of the testing activities and information concerning the target and the network design. A targeted testing approach may be more efficient and cost-effective when the objective of the test is focused more on the technical setting, or on the design of the network, rather than on the organization's incident response and other operational procedures. Unlike blind testing, a targeted test can be executed in less time and effort, the only difference being that it may not provide as complete a picture of an organization's security vulnerabilities and response capabilities. While there are several available methodologies for you to choose from, each penetration tester must have their own methodology planned and ready for most effectiveness and to present to the client.

TABLE 1 COMPARATIVE STUDY OF PENETRATION TESTING W.R.T THE PERSPECTIVES

Testing Method	Total Outsider	Semi-Outsider	Valid User
Remote Network	√	√	√
Remote dial-up Network	X	√	√
Local Network	X	√	√
Stolen Laptop	√	√	√
Social Engg.	√	√	√
Physical Entry	X	X	√

The chart is prepared based on the categories involved on the data involved considering the presence as 1 and absence as 0. Also the chart for the testing method as penetration test involves for the category. The chart is shown in Fig.3 and Fig.4

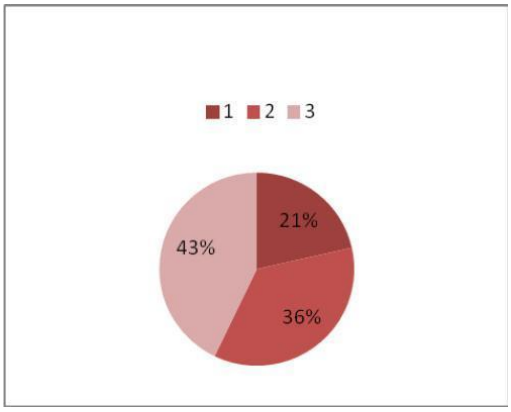


FIG. 3 CATEGORIES AS TOTAL OUTSIDER, SEMI-OUTSIDER AND VALID USER

According to the table described above, the valid user is a hacker who has access to every piece of information and data of the organization, using any testing methods as compared to the other two categories of total or outsider user. Semi outsiders have access to data by all methods accept the physical entry method. The total outsider is involved less as compared to the other two as they cannot access data using some methods like remote dial-up network, Local network and physical entry. This study reveals that a valid user is boon for organization till his intentions are clear; otherwise he is the one who can harm the most as he has access to every information and data. The semi outsider comes after the valid user. And the total outsider user is of least concern.

Here are my top five strategies for network pen testing.

A. TEST ALL THE THINGS

In many environments that I've worked in, the IT security group is primarily concerned with their most sensitive data stores when it comes to penetration tests. This can create huge gaps in the vulnerability identification (and remediation) process that could allow an attacker to easily pivot to sensitive systems. Make sure you hit your sensitive data stores, but pay close attention to the other hosts on your domain that could be compromised and used to get to sensitive data stores.

B . BRUTE FORCE ALL THE SEASONS

If you're testing internally, I can't stress this enough. Do routine audits (weekly, monthly, and/or quarterly) of weak passwords. This can be as simple as doing a quick one password check (Winter2014), to dumping and cracking your domain hashes. If you're going to the dump and crack method, make sure you are taking extra precautions to protect those hashes during and after cracking. Any users identified with a weak password should get a friendly notification email, followed by a forced password reset, if they don't change it by the end of the day. If you want to incentivize users, inform users of the plan to audit passwords and have some small prize for users that are on the good list.

C. AUTOMATED SCANNERS – TRUST, BUT VERIFY

You can typically trust (most) automated scanners, but they can be filled with false positives. Even worse, they may cause you to miss critical (entry point) vulnerabilities that show up in the lower severities. Take memcached for instance. The Nessus plugin[4] shows up as a medium, however I've seen memcached store database and local administrator credentials in cached data. This has resulted in immediate local administrator access to systems. Do your best to fully vet out listening services, even if there's no scan data indicating serious vulnerabilities.

D. CHECK YOUR WEB APPS

We frequently use web applications as entry points during internal penetration tests. For external testing, web apps are an extremely common entry point. Even light testing on internal apps can expose critical vulnerabilities, like directory traversal and SQL injection. Making sure you test your applications along with a network test will help cover your bases.

CONCLUSION

Hacking has both its benefits and risks. Hackers are very diverse. They may bankrupt a company or may protect the data, increasing revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end. While ethical hackers help to understand the companies' their Security needs, the malicious hackers intrudes illegally and harm the network for their personal benefits. An Ethical[5] and creative hacking is significant in network security, in order to ensure that the company's information is well protected and secure. At the same time it allows the company to identify, and in turn, to take remedial measures to rectify the loopholes that exist in the security system, which may allow a malicious hacker to breach their security system. They help organizations to understand the present hidden problems in their servers and corporate network. The study also reveals that the valid users are the ethical hackers, till their intentions are clear, otherwise they are a great threat, as they have access to every piece of information of the organization, as compared to total and semi outsiders.

This also concludes that hacking is an important aspect of computer world. It deals with both sides of being good and bad. Ethical hacking plays a vital role in maintaining and saving a lot of secret information, whereas malicious hacking can destroy everything. What all depends is the intention of the hacker. It is almost impossible to fill a gap between ethical and malicious hacking as human mind cannot be conquered, but security measures can be tighten.

REFERENCE

1. Ozone cyber security
2. Metasploit
3. https://www.sciencedirect.com/ethicalhacking
4. https://kali.training/
5. https://www.hackthebox.eu/