ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015

An Introduction to Hacking & Hacking Tools

Ms. Saumya John
Dept of Computer Science
BPC College, Piravom, Kerala, India
saumyajobi@gmail.com

Ms. Ceena Paul
Dept of Computer Science
BPC College, Piravom, Kerala, India
ceenapaul.p@gmail.com

Mr. Shajan P.X.
Dept of Computer Science
BPC College, Piravom, Kerala, India
shajanpx@gmail.com

Abstract— **In the past decade public and private sector organizations have migrated more of their critical functions to the Internet, so criminals have more opportunity to gain access to sensitive information. Hence there is a need of protecting the systems from hacking, to overcome from these major issues, the authors in this paper presents a brief description on the term hacking what is Ethical hacking, Black hat hacking, different phases of hacking, Testing strategy and tools used by hackers.**

Keywords—Ethical hacking, Black hat hacking.

I. INTRODUCTION

Vast growth of Internet has made growth in fields like electronic commerce, email, easy access to vast stores of reference material etc. Each day more and more computers get connected to the Internet, wireless devices and networks are blossoming. Due to the advance in technology of the Internet, the government, private industry and the everyday computer user have fears of their data or private information. These types of hackers are called black hat hackers [1] who will secretly steal the organization's information and transmit it to the open internet. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. Malicious hacking [2] 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 this paper describes ethical hackers how they use their skills and how they go about helping their customers and plug up security holes.

II. WORKING OF AN ETHICAL HACKER

The working of an ethical hacker involves the under mentioned steps:

a. Obeying Ethical Hacking Commandments: Every Ethical Hacker must follow few basic principles. If he does not follow, bad things can happen. Most of the time these principles get ignored or forgotten when planning or executing ethical hacking tests. The results are even very dangerous. Web mining can be broadly divided into three distinct categories, according to the kinds of data to be mined.

b. Working ethically: The word ethical can be defined as working with high professional morals and principles. Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical Hacker must be approved and must support the company's goals. No hidden agendas are allowed. Trustworthiness is the ultimate objective. The misuse of information is absolutely not allowed.

c. Respecting Privacy: Treat the information you gather with complete respect. All information you obtain during your testing from Web application log files to clear-text passwords, must be kept private.

d. Not crashing your systems: One of the biggest mistakes is when people try to hack their own systems; they come up with crashing their systems. The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques. You can easily create miserable conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups. Many security assessment tools can control how many tests are performed on a system at the same time. These tools are especially handy if you need to run the tests on production systems during regular business hours.

e. Executing the plan: In Ethical hacking, Time and patience are important. Be careful when you're performing your ethical hacking tests.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015

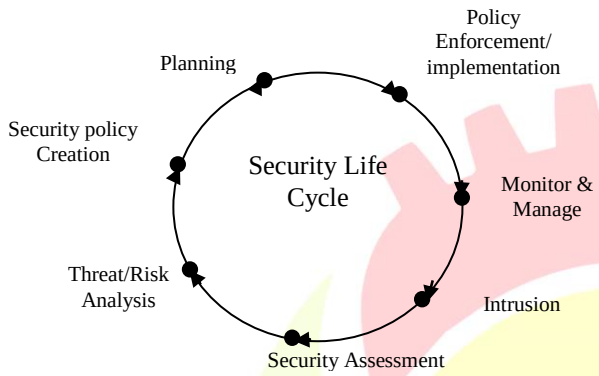

Fig.1. Working of an Ethical Hacker

III. Working of A Black Hat Hacker

An important goal for Black Hats is to gain access to software source code. When a Black Hat gains access to source code they have an opportunity to modify the source in order to introduce vulnerabilities, or to audit the source for bugs. When the target installs or updates the package, the attacker has a sure way to compromise the target. Gaining access to source also enables more potential assets. Perhaps the ultimate target does not run the application in question, but a collaborator or trusted website does. The method of an black hacker involves following steps.

- Information gathering
- Scanning and enumeration
- Gaining access
- Maintaining access
- Covering tracks

A.Information Gathering[3]

This step includes survey and foot printing. This step is preparation part that is employed to assemble the data the maximum amount as potential past to AN attack. The offender tries to search out and exploit a ambiguity by distinguishing patterns of behavior of individuals or systems. Here non-intrusive ways area unit used for making a map of AN organization's network. The ways area unit,

- Target system
- Network design
- Application sort
- Operating system and version
- Server sorts
- Physical location

B.Scanning and Enumeration

During this part, the offender acknowledges target system's informatics address and determines whether or not a system is on the network and additionally they're accessible. Additionally, this part helps to spot the known security loopholes in keeping with system and repair version and defines a user account or system account to be used in hacking the target system. Most account rights will then be exaggerated to permit the account with a lot of access than it had been antecedently granted.

C. Gaining Access

During this section of hacking, hackers exploit exposures exposed throughout the survey and scanning section. They may gain access through dissimilar path like,

- Direct access to a private laptop
- Local space network
- Internet

A common exposure includes stack primarily based buffer overflow, denial of service and hijacking session that has the most objective to realize the possession of the system. Once the system has been hacked, the system management is below the hacker and that they use the system as they need.

D. Maintaining Access

Once gaining access, hackers keep the access for his or her future activities. They will even harden the system and shield their access with backdoors rootkits and Trojans to forestall different hackers. Once the hacker owns the system, they will use it as a base to launch further attacks within which the cooperated system is additionally referred to as zombies.

E.Covering Tracks

In this, hackers would take away all traces of the attack like log files, alarms to safeguard themselves. The purpose of this is to avoid detection by protective personnel to continue exploitation the compromised system and take away proof of hacking to avoid action.

IV. Hacking Phases

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015

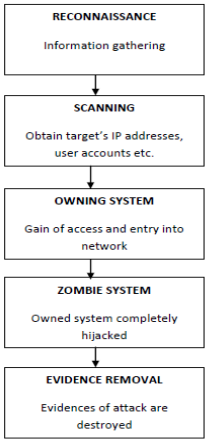

Fig. 2 Hacking Phases

Hacking Can Be Done By Following These Five Phases[4].

Phase 1: Reconnaissance

It can be active or passive: in passive reconnaissance [5]. 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.

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 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.

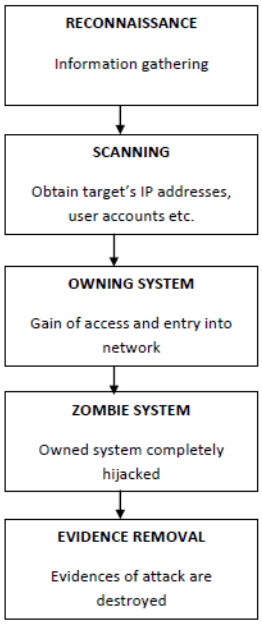

Fig. 2 Hacking Phases

V. TOOLS USED BY HACKERS

There are several common tools used by computer criminals to penetrate network as:

- Trojan horse- These are malicious programs or legitimate software is to be used set up a back door in a computer system so that the criminal can gain access.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015

- Virus- A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents.
- Worm - The worm is a like virus and also a self replicating program. The difference between a virus and a worm is that a worm does not attach itself to other code.
- Vulnerability scanner – This tool is used by hackers & intruders for quickly check computers on a network for known weaknesses. Hackers also use port scanners. This check to see which ports on a specified computer are "open" or available to access the computer.
- Sniffer – This is an application that captures password and other data in transit either within the computer or over the network.
- Exploit – This is an application to takes advantage of a known weakness.
- Social engineering – Through this to obtain some form of information.
- Root kit - This tool is for hiding the fact that a computer's security has been compromised.

VI. TESTING STRATEGY

A. 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.

B. 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 [4] with only limited or no information concerning the organization, prior to conducting the test. The penetration testing team uses publicly available information for example corporate Web site, domain name registry, Internet discussion board, USENET etc, to gather information about the target and conduct its penetration tests. Though blind testing can provide a lot of information about the organization 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 or proprietary information, etc. But it is more time consuming and expensive because of the effort required by the testing team to research the target.

C. *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.

D. 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, 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 [6] 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.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015

VII. CONCLUSION

In this paper authors address the term hacking from several perspective like working of ethical hacking and black hat hacking. Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. Black hat hackers, gains access to source code they have an opportunity to modify the source in order to introduce vulnerabilities, or to audit the source for bugs. Authors give a brief introduction to the different phases of Hacking, Testing strategy and tools used by hackers.

Table 1: Summary of working

Hacker	Working Steps
Ethical	a) Obeying Ethical Hacking Commandments b) Working ethically c) Respecting Privacy d) Not crashing your systems e) Executing the plan
Black Hat	a) Information gathering b) Scanning and enumeration c) Gaining access d) Maintaining access e) Covering tracks

References

[1] 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.

[2] Palmer, C.C.,2001,April 13. "Ethical Hacking", IBM Systems Journal Vol. 40 No.3 2001.

[3] R. Sushmithaand *et al*, "Hacking methods, techniques and their prevention" International journal of Computer Science and Information Technology Research, Vol. 2, Issue 2, pp: (183-189), Month: April-June 2014.

[4] K.Bala Chowdappa et al, "Ethical Hacking Techniques with Penetration Testing", International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393.

[5] EC-Council (n.d.). Ethical Hacking and Countermeasures, online http://www.eccouncil.org/ ipdf/EthicalHacker.pdf (visited on may 2012)

[6] About Effective Penetration Testing Methodology byByeong-HoKANG