Ethical Hacking

Nandini Bhardwaj,
Ayushi Saxena
,Namit Gupta
College of Computing science and technology
Nandinibhardwaj394@gmail.com,
aayushi.saxenaa25@gmail.com,
namit.k.gupta@gmail.com

Abstract: The explosive growth of the Internet has brought many good things such as E-commerce banking, E-mail, Cloud Computing, but there is also a Dark side such as Hacking, Backdoors etc. Hacking is the first big problem faced by Governments, companies, and private citizens around the world , Hacking includes reading others e-mail, steal their credit card number from an on-line shopping site, secretly transmitting secrets to the open Internet. An Ethical Hacker can help the people who are suffered by this Hackings. This Paper Describes about Ethical Hackers, Their Skills, Their Attitudes, and How They Go About Helping Their Customers Find and Plug up Security Holes.

Introduction

The increasingly growth of internet has given an entrance passage to many things: e-commerce, email, social networking, and online shopping & information distribution. As the technology advances it has its dark side; hackers. Govt. organization, private citizen & many companies of the world wants to be the part of this revolution. Being afraid of hackers as they could break into the web-server. To counter attack them ethical hackers are used in the Govt. organization, companies etc. This paper describes the skills, attitude & how they helps the customer with the increasingly growth rate of internet network security has been a measure concern of Govt.& private organization. As different organization wants to take advantage of the internet but fail to do so, because of the possibility of being hacked. To minimize the risk of being hacked by the hackers the organizations realized the best possible ways to introduced the independent computer security professionals to make their way out. In computer security the ethical hackers employ's some tools & techniques that would neither damaged the system nor still information from it. Instead they would evaluate ways to secure then system & report back the owner with the threat they had found & how to cure them

Types of Hacker

1. ***Whitehat Hackers****:* These are the individuals that perform ethical hacking to help secure companies and organizations. Their belief is that you must examine your network in the same manner as a criminal hacker to better understand its vulnerabilities. A white hacker does it with no criminal intent in mind. Companies around the world, who want to test their systems, contract white hackers.

2. ***Script Kiddies*****:** Script kiddie is a pejorative term for a computer intruder with little or no skill; a person who simply follows directions or uses a cookbook approach — typically using other people's scripts and shellcodes — without fully understanding the meaning of the steps they are performing.

3. ***Crackers***: Those who will enter your computer just for the fun of it, or prove their technical skills.

4. ***Gray-hat Hackers****:* These individuals typically follow the law but sometimes venture over to the darker side of blackhat hacking. It would be unethical to employ these individuals to perform security duties for your organization as you are never quite clear where they stand.

5. ***black hat Hacker:*** A black hat hacker, also known as a cracker or a dark side hacker. He uses his skills with a

criminal intent. Some examples are: cracking bank accounts in order to make transference to their own accounts, stealing information to be sold in the black market, or attacking the computer network of an organization for money.

History Of Hacking

HISTORY OF HACKING 1939: The "bombe" became the world's first ethical hacking machine. It was used by the British to decipher encrypted German messages during WWII

1960: The Computer Penetration was first discussed by leading experts with the mention of deliberate tests by professionals.

1971: The first "Tiger-Team" was formed. USAF contracted James Anderson to test time-sharing systems.

1974: The US Air Force conducts one of the first ethical hacks to test the security of the Multics OS .

1986: The US Computer Fraud and Abuse Act makes black and grey hat hacking a criminal offense.

1995: Dan Farmer & Wietse Venema released SATAN, an automated vulnerability scanner, which becomes a popular hacking tool.

1999: Software security goes mainstream with the release of Microsoft Window's 98.

2003: OWASP releases the first OWASP testing guide to teach best practices in penetration testing

2009: PTES is founded leading to an increase in ethical hacking jobs. They offer business and security service providers a common language and scope for performing penetration testing.

2014: Worldwide security spending reaches $71.1 billion. Security executives begin to use on demand penetration testing services for cost effective ethical hacking. Pros of ethical hacking – i. For solving a problem we have to think like a criminal(black hat, grey hat). ii. Helps us to create secure systems less vulnerable to external attacks. iii. Finding the loops in the security of the systems. Cons of ethical hacking i. Provides a detailed analysis of what is happening. ii. We have to secure the sensitive information iii. A secured feeling secured even when an external attack already happeninng

Facts of Ethical Hacking

1. India leads the world in ethical hackers; 23% live there (the U.S. is number two with 20%).

2. Top ethical hackers in India make 16 times the median salary for a software engineer in that country

3. 58% call themselves "self-taught," but many report they've taken at least some computer science classes

4. Top motivations are "the opportunity to learn tips and techniques," "to be challenged, and "to have fun"; "making money" was 4th

5. 37% hack as a hobby

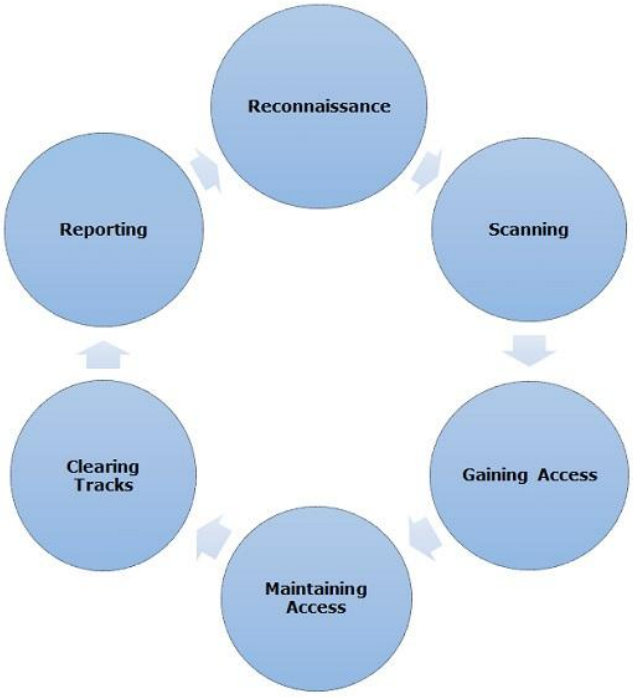
6. 12% make more than $20,000 annually

7. 3% make more than $100,000 annually

8. 1% make more than $350,000 annually

9. Young person's game: 90% of hackers are younger than

Process of Ethical Hacking:



Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

Gaining Access:

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

Maintaing Access:

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

Clearing Tracks:

This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

Reporting:

Reporting is the last step of finishing the Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

Scanning:

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Quick Tip:

The processes are not standard. You can adopt a set of different processes and tools according to your techniques that you are comfortable with. The process is of least significance as long as you are able to get the desired results.

Tools of Hacking

Netsparker:

Netsparker is an easy to use web application security scanner that can automatically find SQL Injection, XSS and other vulnerabilities in your web applications and

web services. It is available as on-premises and SAAS solution.

□□***Acunetix:***

Acunetix is a fully automated ethical hacking solution that mimics a hacker to keep one step ahead of malicious intruders. The web application security scanner accurately scans HTML5, JavaScript and Single-page applications. It can audit complex, authenticated webapps and issues compliance and management reports on a wide range of web and network vulnerabilities.

□□***Probely:***

Probely continuously scans for vulnerabilities in your Web Applications. It allows its customers to manage the life cycle of vulnerabilities and provides them with some guidance on how to fix them. Probely is a security tool built having Developers in mind.

□□***Brupe Suit:***

Burp Suite is a useful platform for performing Security Testing of web applications. Its various tools work seamlessly together to support the entire pen testing process. It spans from initial mapping to analysis of an application's attack surface.

□□***Angry IP Scanner:***

Angry IP Scanner is open-source and cross-platform ethical hacking tool. It scans IP addresses and ports.

Conclusion:

"Ethical Hacking" seems to be a new buzz tools although the process of hacking which contain a cycle. Nevethless, ethical hacking provides results which can be used to strength a information technology environment. Ethical hacking provides data which is based on real tests, which have been successful after all. Problems detected by an ethical hack are for real and should be treated in such a way – fixing the security holes is required. An ethical hack per se doesn't fix or improve the security at all – it does provide information about what should be fixed.

References

[1] Twincling Society Ethical Hacking Seminar. 2006. RetrievedMarch272009.

[2] Krutz, Ronald L. and Vines, Russell Dean. The CEH Prep Guide: T Comprehensive Guide to Certified Ethical Hacking. PublishedJohnWiley and Sons, 2007.

[3] Palmer, Charles. Ethical Hacking. Published in IBM Systems Journal: End-to-End Security, Volume 40, Issue 3, 2001.

[4] Tiller, James S. The ethical hack: a framework for business value penetration testing. Published by CRC Press, 2005.

[5] Beaver, Kevin and McClure, Stuart. Hacking For Dummies. Published by For Dummies, 2006.

[6] Certified Ethical Hacking Seminar. 2006. Retrieved March 27, 2009.

[7] Certified Ethical Hacking EC-Council. 2009. Retrieved March 27, 2009.

[8] Certified Ethical Hacking EC-Council. 2009. Retrieved March 27, 2009.

[9] Ethical Hacking Jobs. 2009. Retrieved March 27, 2009.D'Ottavi, Alberto. Interview: Father of the Firewall. 2003. Retrieved March 27, 2009