Volume 5, Issue 4, 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Ethical Hacking: A Security Technique

[1]Sonal Beniwal, [2]Sneha

[1]Astt. Lect. CSE/IT Deptt., B.P.S.M.V

[2]M.Tech, B.P.S.M.V

Abstract: As public and private organizations migrate more of their critical functions to the Internet, criminals have more opportunity and incentive to gain access to sensitive information through the Web application. Thus the need of protecting the systems from the nuisance of hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. So, to overcome from these major issues, ethical hackers or white hat hackers came into existence. One of the fastest growing areas in network security, and certainly an area that generates much discussion. The main purpose of this study is to reveal the brief idea of the ethical hacking and its affairs with the corporate security.

Keywords: Hacking, Ethical Hacking, Attack types, Hacking tools.

I. INTRODUCTION

The Internet is still growing1 and e-commerce is on it's advance. The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. More and more computers get connected to the Internet, wireless devices and networks are booming. Due to the advance technology of the Internet, the government, private industry and the everyday computer user have fears of their data or private information being comprised by a criminal hacker. These types of hackers are called black hat hackers 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. So, this paper describes ethical hackers, their skills and how they go about helping their customers and plug up security holes. So, in case of computer security, these tiger teams or ethical hackers would employ the same tricks and techniques that hacker use but in a legal manner and they would neither damage the target systems nor steal information. Instead, they would evaluate the target system's security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.

This paper will define ethical hacking, list some of the commonly use terms for attackers, provide a list of the standard services offered via ethical hacking to combat attackers, discuss the three common group of

II. WHAT IS HACKING?

Hacking is not a simple operation or sequence of commands as many people think. Hacking is a skill. Hacking is not a specific term, there are many types of hacking. Hacking is unauthorized use of computer and network resources. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose. People who engage in computer hacking activities are often called hackers. Hacker A programmer who breaks into someone else's computer system or data without permission.

2.1 Ethical hacking

It is also known as penetration testing or white-hat hacking . The science of testing your computers and network for security vulnerabilities and plugging the holes you find before the bad guys get a chance to exploit them. Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass way past the system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, in an effort to minimize or eliminate, any potential attacks. To catch a thief, think like a thief. That's the basis for ethical hacking. ...involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is legal. Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It's part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

2.2 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.

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.

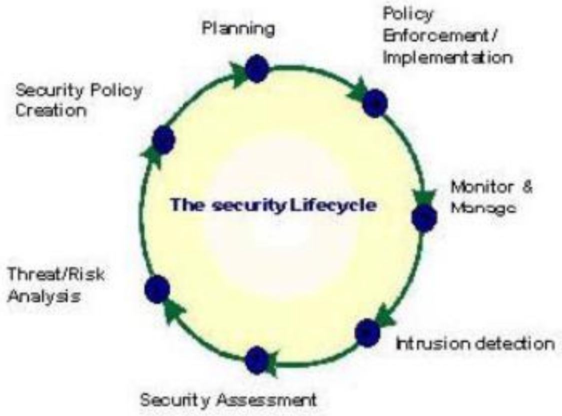

Figure: Working Of Ethical Hacker

III. HACKING HISTORY

3.1 Pre-History:-

- 1960sThe Dawn of Hacking original meaning of the word "hack" started at MIT; meant elegant, witty or inspired way of doing almost anything; hacks were programming shortcuts.

3.2 Elder Days (1970-1979):-

- 1970s: Phone Phreaks and Cap'n Crunch: One phreak, John Draper (aka "Cap'n Crunch"), discovers a toy whistle inside Cap'n Crunch cereal gives 2600-hertz signal, and can access AT&T's long-distance switching system.
- Draper builds a "blue box" used with whistle allows phreaks to make free calls.
- Steve Wozniak and Steve Jobs, future founders of Apple Computer, make and sell blue boxes. THE GOLDEN AGE (1980-1991)
- 1980: Hacker Message Boards and Groups Hacking groups form; such as Legion of Doom (US), Chaos Computer Club (Germany).
- 1983: Kids' Games Movie "War Games" introduces public to hacking.

3.3 The Great Hacker War:-

- Legion of Doom vs. Masters of Deception; online warfare; jamming phone lines.
- 1984: Hacker 'Zines Hacker magazine 2600 publication; online 'zine Phrack.

3.4 Crackdown (1986-1994):-

- 1986: Congress passes Computer Fraud and Abuse Act; crime to break into computer systems.
- 1988: The Morris Worm Robert T. Morris, Jr., launches self-replicating worm on ARPAnet.
- 1989: The Germans, the KGB and Kevin Mitnick.
- German Hackers arrested for breaking into U.S. computers; sold information to Soviet KGB.
- Hacker "The Mentor"arrested; publishes Hacker's Manifesto.
- Kevin Mitnick convicted; first person convicted under law against gaining access to interstate network for criminal purposes.
- 1993: Why Buy a Car When You Can Hack One? Radio station call-in contest; hacker-fugitive Kevin Poulsen and friends crack phone; they allegedly get two Porsches, $20,000 cash, vacation trips; Poulsen now a freelance journalist covering computer crime.
- First Def Con hacking conference in Las Vegas

3.5 Zero Tolerance (1994-1998):-

- 1995: The Mitnick Takedown: Arrested again; charged with stealing 20,000 credit card numbers
- 1995: Russian Hackers Siphon $10 million from Citibank; Vladimir Levin, leader.
- 1999 hackers attack pentagon, MIT, FBI websites.
- 1999: E-commerce Company attacked; blackmail threats followed by 8 million credit card numbers stolen.

IV. TYPES OF ATTACKS

4.1 Nontechnical attacks

Exploits that involve manipulating people ,end users and even yourself, are the greatest vulnerability within any computer or network infrastructure. Humans are trusting by nature, which can lead to social-engineering exploits. Social engineering is defined as the exploitation of the trusting nature of human beings to gain information for malicious purpose. Other common and effective attacks against information systems are physical. Hackers break into buildings, computer rooms, or other areas containing critical information or property. Physical attacks can include dumpster diving (rummaging through trash cans and dumpsters for intellectual property, passwords, network diagrams, and other information).

4.2 Network-infrastructure attacks

Hacker attacks against network infrastructures can be easy, because many networks can be reached from anywhere in the world via the Internet. Here are some examples of network-infrastructure attacks:

- Connecting into a network through a rogue modem attached to a computer behind a firewall.
- Exploiting weaknesses in network transport mechanisms, such as TCP/IP and NetBIOS.
- Flooding a network with too many requests, creating a denial of service (DoS) for legitimate requests.
- Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text, Piggybacking onto a network through an insecure 802.11b wireless configuration.

4.3 Operating-system attacks

Hacking operating systems (OSs) is a preferred method of the bad guys. OSs comprise a large portion of hacker attacks simply because every computer has one and so many well-known exploits can be used against them. Occasionally, some operating systems that are more secure out of the box, such as Novell NetWare and the flavors of BSD UNIX, are attacked, and vulnerabilities turn up. But hackers prefer attacking operating systems like Windows and Linux because they are widely used and better known for their vulnerabilities. Here are some examples of attacks on operating systems:

- Exploiting specific protocol implementations
- Attacking built-in authentication systems.
- Breaking file-system security.
- Cracking passwords and encryption mechanisms.

4.4 Application and other specialized attacks

Applications take a lot of hits by hackers. Programs such as e-mail server software and Web applications often are beaten down:

- Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) applications are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these programs from the Internet.
- Malicious software (malware) includes viruses, worms, Trojan horses, and spyware. Malware clogs networks and takes down systems.
- Spam (junk e-mail) is wreaking havoc on system availability and storage space. And it can carry malware. Ethical hacking helps reveal such attacks against your computer systems.

V. GROUPS OF HACKERS

5.1 White Hats are the good guys, the ethical hackers who use their hacking skills for protective purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures..

5.2 Black Hats are considered the bad guys: the malicious hackers or crackers use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and basically cause problems for their targets.

5.3 Grey Hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Both are powerful forces on the Internet, and both will remain permanently. And some individuals qualify for both categories. The existence of such individuals further clouds the division between these two groups of people.

VI. THE INTRUDER'S MAIN MOTIVES ARE

- To perform network scanning to find out vulnerable hosts in the network.
- To install an FTP server for distributing illegal content on network (ex. pirated software or movies)
- To use the host as a spam relay to continuous flood in the network.
- To establish a web server (non-privileged port) to be used for some phishing scam.

VII. 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.
- **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.

VIII. TYPES OF HACKING

8.1 Inside Jobs

Most security breaches originate inside the network that is under attack. Inside jobs include stealing passwords (which hackers then use or sell), performing industrial espionage, causing harm (as disgruntled employees), or committing simple misuse. Sound policy enforcement and observant employees who guard their passwords and PCs can thwart many of these security breaches.

8.2 Rogue Access Points

Rogue access points (APs) are unsecured wireless access points that outsiders can easily breech. (Local hackers often advertise rogue APs to each other.) Rogue APs are most often connected by well-meaning but ignorant employees.

8.3 Back Doors

Hackers can gain access to a network by exploiting back doors administrative shortcuts, configuration errors, easily deciphered passwords, and unsecured dial-ups. With the aid of computerized searchers (bots), hackers can probably find any weakness in your network..

8.4 Denial of Service

DOS attacks give hackers a way to bring down a network without gaining internal access. DOS attacks work by flooding the access routers with bogus traffic (which can be e-mail or Transmission Control Protocol, TCP, packets).

8.5 Distributed Doss

(DDOSS) are coordinated DOS attacks from multiple sources. A DDOSS more difficult to block because it uses multiple, changing, source IP addresses.

8.6 Anarchists, Crackers, and Kiddies

Anarchists are people who just like to break stuff. They usually exploit any target of opportunity. Crackers are hobbyists or professionals who break passwords and develop Trojan horses or other SW (called wares). They either use the SW themselves (for bragging rights) or sell it for profit. Script kiddies are hacker wannabes. They have no real hacker skills, so they buy or download wares, which they launch. Other attackers include disgruntled employees, terrorists, political operatives, or anyone else who feels slighted, exploited, ripped off, or unloved.

8.7 Sniffing and Spoofing

Sniffing refers to the act of intercepting TCP packets. This interception can happen through simple eavesdropping or something more sinister. Spoofing is the act of sending an illegitimate packet with an expected acknowledgment (ACK), which a hacker can guess, predict, or obtain by snooping.

IX. CONCLUSION

This paper addressed ethical hacking from several perspectives. Ethical hacking seems to be a new buzz word although the techniques and ideas of testing security by attacking an installation aren't new at all. But, with the present poor security on the internet, ethical hacking may be the most effective way to plug security holes and prevent intrusions. On the other hand ethical hacking tools have also been notorious tools for crackers. So, at present the tactical objective is to stay one step ahead of the crackers. 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. After all, ethical hacking will play a certain role in the security assessment offerings and certainly has earned its place among other security assessments. In conclusion, it must be said that the ethical hacker is an educator who seeks to enlighten not only the customer, but also the security industry as a whole. In an effort to accomplish this, let us welcome the Ethical Hacker into our ranks as a partner in this quest.

REFERENCES

[1] Sanctum Inc, “Ethical Hacking techniques to audit and secure web enabled applications”, 2002.
[2] B. Reto, “Ethical Hacking”, in GSEC Practical Assignment, Version 1.4b, Option 1, Nov 24, 2002.
[3] B. Kevin, “Hacking for dummies”, 2nd edition, 408 pages, Oct 2006.
[4] Smith B., Yurcik W., Doss D., “Ethical Hacking: the security justification redux”, IEEE Transactions, pp. 375-379, 2002.
[5] y.safaribooksonline.com/.../introduction-to-ethical-hacking-ethics-legality.
[6] J. Danish and A. N. Muhammad, “Is Ethical Hacking Ethical? “ , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.
[7] Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala , “Ethical Hacking, International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010.
[8] edia.techtarget.com/searchNetworking- Introduction to ethical hacking-Tech Target.
[9] 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.
[10] D. Manthan “Hacking for beginners”, 254 pages, 2010.
[11] Ajinkya A., Farsole Amruta G., Kashikar Apurva Zunzunwala"Ethical Hacking", in 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 10
[12] David Melnichuk," The Hacker’s Underground Handbook ", at http://www.learn-how-to-hack.net
[13] Marilyn Leathers " A Closer Look at Ethical Hacking and Hackers" in East Carolina University ICTN 6865.
[14] Ethical hacking by C. C. Palmer