Volume-4, Issue-10, Oct-2015 • ISSN No 2277 - 8160

Research Paper Computer Science

Ethical Hacking and Its Value to Security

C.Nagarani

Assistant Professor in Computer Science, PSG College of Arts and Science, Coimbatore – 641 014.

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. "Ethical Hacking" which attempts to pro-actively increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. Ethical hackers may beta test unreleased software, stress test released software, and scan networks of computers for vulnerabilities.

Ethical hacking can be defined as the practice of hacking without no malicious intention, rather evaluate target system with a hackers perspectives. Hacking is a process to bypass the security mechanisms of an information system or network. 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

This paper aims at putting onward the basic concept of ethical hacking and difference between a hacker and cracker. The swift growth of the Internet has brought many productive and appreciated solutions for our lives such as e-commerce, electronic communication, and new zones for research and data distribution. However, like many other technological progressions, there is also an issue of rising in the total number of criminal hackers. More and more computers get connected to the Internet, wireless devices and networks are flourishing.

Due to the improvement in the proficiency of the Internet, the government, private industry and the everyday computer user have uncertainties of their facts or private information being comprised by a criminal hacker. These type of hackers are called black hat hackers who will furtively snip the organization's data and communicate it to the open internet. So, to overcome from these foremost disputes, another group of hackers emanated and these hackers are named as ethical hackers or white hat hackers.

So, this paper describes ethical hackers, their abilities and how they go about helping their customers and plug up security holes. So, in case of system security, these ethical hackers would employ the same tricks and techniques that hacker use but in a authorized method and they would neither damage the target systems nor steal information. As an alternative, 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.

II.WHAT IS HACKING?

Hacking is not a modest process or categorization of instructions as many ponder. Hacking is a talent / skill / knowledge. Hacking is unlicensed use of computer and network resources. Computer hacking is the art of amending computer hardware and software to achieve an objective outside of the author's unique determination. People who involve in computer hacking activities are called as hackers.

2.1 Ethical hacking

It is also called as penetration testing or white-hat hacking. The knowledge of testing the system nodes and network for security susceptibilities and plugging the fleabags find before the bad guys get an opportunity to mishandle them. Ethical hacking and ethical hacker are terms used to define hacking performed by a company or individual to help identify prospective threats on a computer or network. An ethical hacker attempts to circumvent way past the system security and search for any feeble facts that could be ill-treated by malevolent hackers. This information is then used by the body to improve the system security, in an effort to abate or eradicate any probable attacks Ethical hacking is authorized. Ethical hacking is performed with the target's authorization. The commitment of ethical hacking is to identify susceptibilities from a hacker's viewpoint so systems security can be well enhanced. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

2.2 PHASES OF ETHICAL HACKING

The ethical hacking process can be fragmented down into five distinct phases. An ethical hacker follows processes analogous to those of a spiteful hacker. The phases to gain and maintain entry into a computer system are similar no matter what the hacker's intentions are.

Phase 1: Passive and Active Reconnaissance

Passive reconnaissance involves congregation of information about a prospective target without the targeted individual's or company's knowledge. Sniffing the network is another method of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and additional accessible facilities on the system or network. Sniffing tools are simple and tranquil to use and results a great deal of valued data.

Active reconnaissance can give a hacker an indication of security measures in but the process also increases the chance of being caught or at least raising suspicion. Numerous software tools that accomplish active reconnaissance can be traced back to the computer that is running the tools, thus aggregating the fortuitous of detection for the hacker. Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack.

Phase 2: Scanning

Scanning encompasses taking the data exposed during reconnaissance and using it to examine the network. The various tools that a hacker may employ during the scanning phase may include : Dialers – Port scanners - ICMP scanners - Ping sweeps - Network mappers - SNMP sweepers - Vulnerability scanners

Phase 3: Gaining Access

The third phase is the gaining access where the real hacking takes place. Vulnerabilities wide-open during the reconnaissance and scanning phase are exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network, neither wired nor wireless; local access to a PC; the Internet; or offline. Gaining access is identified in the hacker world as owning the system because once a system has been hacked, the hacker has control and can use that system as they wish.

Phase 4: Maintaining Access

Once a hacker has gained access control to target computers, they intend to keep that access for future exploitation and outbreaks. Sometimes, hackers fortify the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits,

and Trojans.

Phase 5: Covering Tracks
Once hackers have been able to gain control over the target systems, they cover their tracks to avoid detection by security personnel, to continue to use the targeted system, to confiscate indication of hacking, or to avoid legal action.

Phases of Hacking

IV. TYPES OF HACKERS BASED ON THEIR KNOWLEDGE:

Coders:
Coders are real hackers. They are programmers having immense knowledge about many programming languages, networking and working of programs. They are skilled programmers who can find vulnerabilities on their own and create exploits based on those vulnerabilities. They can code their own tools and exploit and can modify existing tools according to their use.

Admins:
These are the computer guys who are not sound enough in programming but holds enough information about hacking and networking. These guys have **Hacking certifications** and can hack any system or network with the help of tools and exploit created by codes

Script kiddies:
This is the most dangerous type of hackers. These type of hackers does not actually know what they are doing. They just use the tools and partial knowledge they gain from internet to attack systems. They do it just for fun purpose and to be famous. They use the tools and exploits coded by other hackers and use them. They have minimum skills.

Types of Hackers based on their motive of hacking:
White Hat Hackers:
White hat hackers are **ethical hackers** with some certifications such as **CEH(Certified Ethical Hacker)**. They break into systems just for legal purposes. Their main motive is to find loopholes in the networks and rectifying them.

Black Hat Hacker:
A black hat hacker may or may not have any **hacking certification** but they hold good knowledge about hacking. They use their skills for destructive purposes. They break into systems and networks either for fun or to gain some money from illegal means.

Gray Hat Hacker:
A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacke. Then they may offer to repair their system for a small fee.d

V. HACKING TECHNIQUES:
A typical hacker attack is not a simple, one-step procedure. It is more likely that the attacker will need several techniques used in combination to bypass the many layers of protection standing between them and root administrative access. The following techniques are not specific to wireless networks. Each of these attacks can take multiple forms, and many can be targeted against both wired and wireless networks.

The Virtual Probe: A popular method that hackers use is pretending to be a survey company. A hacker can call and ask all kinds of questions about the network operating systems, intrusion detection systems (IDSs), firewalls, and more in the guise of a researcher. If the hacker was really malicious, she could even offer a cash reward for the time it took for the network administrator to answer the questions.

Lost Password: One of the most common goals of a hacker is to obtain a valid user account and password. In fact, sometimes this is the only way a hacker can bypass security measures. If a company uses firewalls, intrusion detection systems, and more, a hacker will need to borrow a real account until he can obtain root access and set up a new account for himself.

Sniffing: A sniffer is a program and/or device that monitors all information passing through a computer network. It sniffs the data passing through the network off the wire and determines where the data is going, where it's coming from, and what it is. In addition to these basic functions, sniffers might have extra features that enable them to filter a certain type of data, capture passwords, and more.

VI. POPULAR TOOLS USED BY HACKERS:
Aircrack is one of the most popular wireless passwords cracking tools which you can use for 802.11a/b/g WEP and WPA cracking. Aircrack uses the best algorithms to recover wireless passwords by capturing packets. Once enough packets have been gathered, it tries to recover the password.

AirSnort is another popular tool for decrypting WEP encryption on a wi-fi 802.11b network. It is a free tool and comes with Linux and Windows platforms. This tool is no longer maintained, but it is still available to download from Sourceforge.

WireShark is the network protocol analyzer. It lets you check what is happening in your network. You can live capture packets and analyze them. It captures packets and lets you check data at the micro-level. It runs on Windows, Linux, OS X, Solaries, FreeBSD and others.

CloudCracker is the online password cracking tool for cracking WPA protected wi-fi networks. This tool can also be used to crack different password hashes. Just upload the handshake file, enter the network name and start the tool.

VII. 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. 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.

REFERENCES

[1] Palmer, Charles. Ethical Hacking. Published in IBM Systems Journal: End-to-End Security, Volume 40, Issue 3, 2001. [2] Beaver, Kevin and McClure, Stuart. Hacking For Dummies. Published by For Dummies, 2006 [3] Livermore, Jeffery. What Are Faculty Attitudes Toward Teaching Ethical Hacking and Penetration Testing?. Published in Proceedings of the 11th Colloquium for Information Systems Security Education, 2007. [4] 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. [5] 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. [6] Smith B., Yurcik W., Doss D., "Ethical Hacking: the security justification redux", IEEE Transactions, pp. 375 - 379, 2002. [7] Ethical Hacking and Countermeasures (312-50) Exam. "CEH v8 Exam (312-50)". Retrieved May 27, 2012