MANTECH Publications

Journal of Research in Computer Science and Engineering
Volume 8 Issue 1
ISSN- 2457-0818 (Online)

Scope and Challenges in Ethical Hacking

G sravan[1], Dr Ankita Nigam

Student[1], Professor[2]

Department of Computer Science and Engineering

Princeton Institute of Engineering and Technology of Women, Hyderabad, India

Corresponding Authors' Email id:-*sravaniguduru5813@gmail.com[1], ankita270481@gmail.com[2]*

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 online 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.

Keywords :- *Hacking, e-mail , backdoors.*

INTRODUCTION

Ethical Hacking can be defined as a legal access of an Internet geek or group in any organization's online property after their official permission. An Ethical Hacker can help the people who are suffered by this Hackings. Ethical Hacking can be defined as a legal access of an Internet geek or group in any organization's online property after their official permission. A good hacker, or security professional acting as an ethical hacker, just has to understand how a computer system works and know what tools to employ in order to a security weakness. By learning the same skills and employing the software tools used by hackers, you will be able to defend your computer networks and systems against malicious attacks. 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 system

Page 57-63 © MANTECH PUBLICATIONS 2023. All Rights Reserved

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 The work that ethical hackers do for organizations has helped improve system security and can be said to be quite effective and successful. Individuals interested in becoming an ethical hacker can work towards a certification to become a Certified Ethical Hacker, or CEH. This certification is provided by the International Council of E-Commerce Consultants (EC- Council). Ethical hackers they should be completely trustworthy and strong programming and computer network skills. They posses same skill, mindset, and tools of a hacker but the attacks are done in a non-destructive manner.

TYPE OF ETHICAL HACKERS

Hackers can be divided into three groups:

White-Hats Good guys, include ethical hackers

Black-Hats Bad guys, include malicious hackers

Gray-Hats Good or bad hacker; on the situation Ethical hackers usually fall into the white-hat category, but sometimes they're former gray hats who have become security professionals and who now use their skills in an ethical manner.

White-hats

White hats good guys, the ethical hackers who use their hacking skills for defensive 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. White-hat hackers are prime candidates for the exam. White hats are those who hack with permission from the data owner. It is critical to get permission prior to beginning any hacking activity. This is what makes a security professional a white hat versus a malicious hacker who cannot be trusted.

Black-Hats

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

Page 57-63 © MANTECH PUBLICATIONS 2023. All Rights Reserved

easily be differentiated from white-hat hackers because their actions are malicious. This is the traditional definition of a hacker and what most people consider a hacker to be.

Gray-Hats

Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Gray-hat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats are self proclaimed ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to highlight security problems in a system or educate victims so they secure their systems properly.

SOME OF THE FAMOUS ETHICAL HACKERS

Some of the famous Ethical hackers are Benild joseph, PranavMistry, Andrianlemo (Black Hat),Jonathan James, Linus to r vats(white Hat), Stephan woniaketc . Benild Josephthe 20 years old world renowned Ethical Hacker | Information Security Consultant | Speaker | Author in Indian IT Industry was born in Calicut, A City of Kerala. Currently acting asthe Chief Executive Officer of "Th3 art of h@ckin9"– International IT Security Project. He has his credit to many registered and pending patents in cyber forensic and information security domain. He specializes in Web Application security, Penetration testing and Forensic investigation. His research interests include Computer Security, Networking, Data Forensic, Virtualization, Web Application Vulnerability and Information Security. Pranav Mistry is a research assistant and a PhD candidate at MIT Media Lab. Sixth Sense has recently attracted global attention. Among some of his previous work, Pranav has invented Mouse less - an invisible computer mouse; intelligent sticky notes that can be searched, located and can send reminders and messages; a pen that can draw in 3D; and a public map that can act as Google of physical world. Pranav has commercialized his invention, the sixth sense and Sixth Sense is now being actively usedat NASA. It is rumored that Facebook tried to acquire the technology from Pranav for a reportedly $2 billion and 5% ownership of Facebook, but Pranav decided to open source it instead. He is currently working with Samsungcompany presently.

Page 57-63 © MANTECH PUBLICATIONS 2023. All Rights Reserved

PHASES OF HACKING

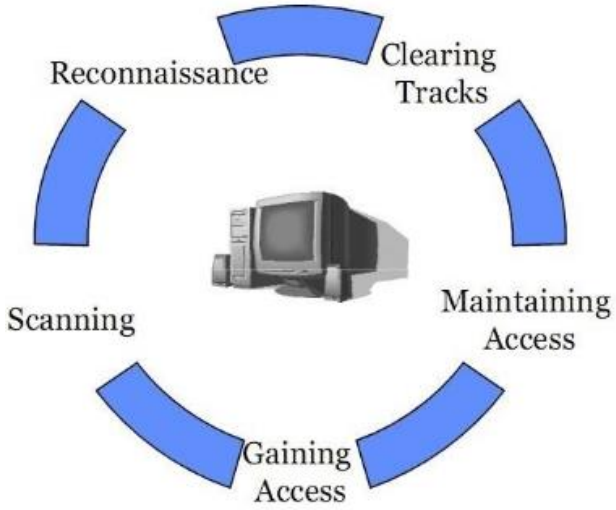


Fig : 1- Phases of ethical hacking

Phase1—Reconnaissance
Phase 2—Scanning
Phase 3—Gaining Access
Phase 4—Maintaining Access
Phase 5—Covering Tracks

Phase 1: Passive and Active Reconnaissance

Passive reconnaissance involves gathering information regarding a potential target without the targeted individual's or company's knowledge. However, it's usually done using Internet searches or by Goggling an individual or company to gain information. This process is generally called information gathering. Social engineering and dumpster diving are also considered passive information-gathering methods. Sniffing the network is another of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing network traffic is similar to building monitoring: A hacker watches the flow of data to see what time certain transactions take place and where the traffic is going.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This usually involves more risk of detection than passive reconnaissance and is sometimes called rattling the doorknobs. Active reconnaissance can give a hacker an indication of security measures in place, but the process also increases the chance of being caught or at least raising

Page 57-63 © MANTECH PUBLICATIONS 2023. All Rights Reserved

suspicion. Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. This information may enable a hacker to find vulnerability in that OS version and exploit the vulnerability to gain more access.

Phase2: Scanning

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase can include dialers, port scanners, network mappers, sweepers, and vulnerability scanners.

Hackers are seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts.

Phase 3: Gaining Access

This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline. Gaining access is known in the hacker world as owning the system

Phase 4: Maintaining – Access

Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, root kits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

Phase 5: Covering Tracks

Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms.

AN ETHICAL HACKER'S SKILL

Ethical hackers who stay a step ahead of malicious hackers must be computer systems experts who are very knowledgeable about computer programming, networking, and operating systems. In-depth knowledge about highly targeted platforms (such as Windows, UNIX, and Linux) is also a requirement. Patience, persistence, and immense

Page 57-63 © MANTECH PUBLICATIONS 2023. All Rights Reserved

perseverance are important qualities for ethical hackers because of the length of time and level of concentration required for most attacks to pay off. Networking, web programming, and database skills are all useful in performing ethical hacking and vulnerability testing. Most ethical hackers are well rounded with wide knowledge on computers and networking. In some cases, an ethical hacker will act as part of a "tiger team" who has been hired to test network and computer systems and find vulnerabilities. In this case, each member of the team will have distinct specialties, and the ethical hacker may need more specialized skills in one area of computer systems and networking. Most ethical hackers are knowledgeable about security areas and related issues but don't necessarily have a strong command of the countermeasures that can prevent attacks

MPORTANCE OF ETHICAL HACKING

Ethical hacking important for some of the services like Application Testing, War Dialing, Network Testing, Wireless Security, System Hardening etc. It used to judge the security programs of the organization. It makes software and codes and more efficient of organizations. Ethical hacking faces the organizations security risk .

ADVANTAGE AND DISADVANTAGE

Advantage

- This prevents identity theft and the leaking of vital information
- It allows them to implement stronger security measures.
- It is also beneficial to help government entities to protect major computer system from being compromised in a way that national security would be an issue
- Ethical hacking also help families of deceased people to access account to see what their final vital transmissions may have been or gain access to some accounts to close them down.

Disadvantage

- This may corrupt the files of an organization.
- Basic problem with this is trustworthiness of the Ethical hacker. • Ethical hacker might use the information maliciously

FUTURE SCOPE OF ETHICAL HACKERS

As it as evolving branch the scope of enhancement in technology is immense. No ethical hackers can ensure the system security by using the same technique repeatedly. He would have to improve, develop and explore efficient new avenues

Page 57-63 © MANTECH PUBLICATIONS 2023. All Rights Reserved

repeatedly. More enhanced software's should be used for optimum protection. Tools used, need to be updated regular l and more efficient once need to be developed.

CONCLUSION

Ethical hacking is legal way to securing your system. Main way that system in hands of ethical hacker so that he can make your system full proof. It is a part of overall security program. System administrator should always try to find the loop holes in to the system and make preventive majors. Ethical hackers possess same skill, mindset and tools of a hacker but the attacks are done in a nondestructive manner.

REFERENCES

1. http://www.wikipedia.org/wiki/ethical hacking
2. www.computerhope.com
3. http://searchsecurity.techtarget.com
4. http://www.instructables.com

Page 57-63 © MANTECH PUBLICATIONS 2023. All Rights Reserved