International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 07 | July - 2021 ISSN: 2582-3930

ETHICAL HACKING

Ashish Shakya[1], Mohammad Arif[2], Abhay Kumar Singh[3] , Ms. Shikha Agarwal[4].

[123]Department of Information Technology , Raj Kumar Goel Institute Of Technology, Ghaziabad

---

ABSTRACT- The explosive growth of the online has brought many goodies like E-commerce-banking, E-mail, Cloud computing, but there's also a Dark side like Hacking, Backdoors etc. Hacking is that the first big problem faced by Governments, companies, and personal citizens around the world, Hacking involve reading others e-mail, steal their MasterCard number from an on-line ecommerce site, secretly transmitting secrets to the open Internet. An Ethical Hacker can help the people that are suffered by this Hackings. This Paper explains about Ethical Hackers, Their Skills, Their Attitudes, and the way they are going About Helping Their Customers Find and Plug up Security Holes.

1.INTRODUCTION

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

Ethical hacking and ethical hacker are terms use to describe hacking which is performed by a corporation or individual to assist identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and look for any weak points that would be exploited by malicious hackers. This information is then employed by the organization to enhance the system security, in an attempt to attenuate or eliminate any potential attacks. The work that ethical hackers do for organizations has helped improve system security and may be said to be quite effective and successful. Individuals those are interested in becoming an ethical hacker will aim towards a certification to become a Certified Ethical Hacker, or CEH. This certification is granted by the International Council of Ecommerce Consultants (EC-Council). Ethical hackers they ought to be completely trustworthy and powerful programming and network skills. They acquire same skill, mindset, and tools of a hacker but the attacks are done in a non-destructive manner.

2. TYPES OF HACKER

Hackers can be divided in these three groups:

White-Hats:- Good guys, include ethical hackers.
Black-Hats:- Bad guys, include malicious hackers.
Gray-Hats:- Good or bad hacker, depends on the situation.

Ethical hackers generally lie into the white-hat category, but sometimes they are also former gray hats who have become security professionals and use their skills in an ethical manner.

WHITE HAT HACKER

White hats are the great guys, the moral hackers who use their hacking skills for defensive purposes. White-hat hackers are generally security professionals with knowledge of hacking and therefore the hacker toolset and who use this data to locate weaknesses and implement countermeasures. White-hat hackers are main candidates for the exam. White hats are those that hack with permission from the info owner. it's critical to urge permission before beginning any hacking activity. This is what makes a security professional a white hat versus a malicious hacker who can't be trusted.

BLACK HAT HACKER

Black hats are the malicious hackers or crackers use their skills for illegal or malicious purposes. They forced an entry or violate the system integrity of remote systems, with malicious intentions. They gained unauthorized access, black-hat hackers destroy or damages vital data, deny legitimate users service, and cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because of their actions are malicious. This is the general definition of a hacker and what most people consider a hacker to be.

GRAY HAT HACKER

Gray hats are those hackers who may work with both intensive offensively or defensively, depending on the situation. This is the differentiating line between hacker and cracker. Gray-hat hackers are curious in hacking tools and technologies and they are not malicious as black hats. Gray hats are self appointed ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to focus on security problems in a system or educate victims so they secure their systems properly.

3. PHASES OF ETHICAL HACKING

Phases of Ethical Hacking Consists of Five Blocks:

1. Reconnaissance
2. Maintaining Access
3. Scanning & Enumeration
4. Gaining Access
5. Clearing Tracks

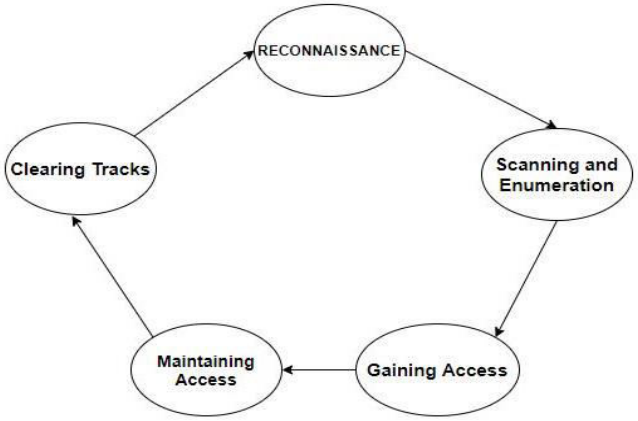

Fig: Phases of Hacking

RECONNAISSANCE

Collecting Initial information and Getting to know the target system is the first step in Ethical Hacking. Reconnaissance is a set of processes and techniques that is used to privately discover and collect information about a target system. There are seven steps mentioned below for Reconnaissance:-

1. Identification of active machines
2. Preliminary information collection
3. Identification of every ports services
4. Network mapping
5. Identification of open ports & access points
6. OS fingerprinting

SCANNING & ENUMERATION

The second step of the ethical hacking is the scanning and enumeration. Scanning is the common technique that is uses by pen tester to find the open door. Scanning is used to determine the weaknesses of the service and product that operate on the port. They need to figure out the OS included, live host, services, intrusion detection, firewalls, perimeter equipment, routing and general networks topology that are parts of the targets organization during this phase. Enumeration is the main priority of network attack.

GAIN ACCESS

Once the observation is finished on the target system and every weakness are tested, then the hackers then attempts with the help of some tools & techniques to gain access of the target system. This mainly focuses on the retrieval of the password. Either bypass techniques (like using konboot) or password cracking techniques that can be used for this by hacker to gain access.

MAINTAINING ACCESS

Once the hacker get the access of the targeted systems, he take all advantage of both the systems and its resources and they use the systems as a catapult pad for testing and harming other system, or they can also retain the low profile & continue to exploit the systems without the genuine user knowing. Those two acts will demolish the organization that leads to a calamity. Rootkits gain entrance to the OS level, while the Trojan horse gain entrance at the program levels. Attackers use the Trojan horses to migrate on the system user passwords, names and credit card information's. Organizations that can use tools for intrusion detection to detect the intruders.

CLEARING TRACKS

For several purposes like avoiding detection & further penalizing for intrusion, an offender will destroy confirmation of his activities and existence. Eliminating evidence that's often mentioned the ' clearing tracks ' is that the requirement for each intruder who must remain anonymous and stop detect back. Generally this steps begins by delete the adulterate logins or all other possible errors messages generated from the attack process on the victim system. For e.g., a buffer overflow attack usually leaves a message that must be cleared within the systems logs. Next attention is concentrated on making changes so as to not log in to potential logins. The 1st thing a systems administrator does to trace the system's uncommon activity is to review all the systems log file, it's necessary for trespasser to use the tool to vary the system logs so that the administrator cannot track them. Making the system appear as if it did before they obtain access & found out backdoor for his or her own use is vital for attackers. Any files that are modified must be swap back to their actual feature's so there's little question into the mind of administrators that the systems are trespasser.

4.TOOLS USED IN ETHICAL HACKING

1. Tools for Reconnaissance: Whois Lookup, Google and NSLookup.
2. Tools for Scanning: Nikto WebsiteVulnerability Scanner, Ping, Tracert, Nmap, Zenmap, Netcraft.
3. Tools for Gaining Access: KonBoot, pwdump7, John the Ripper, Wireshark, Fluxion, Cain and Abel.
4. Tools that are used for the Maintaining Access: Beast, Metasploit Penetration Testing Software, Cain & Abel.
5. Tools for Clearing Tracks: OS Forensics, Metasploit Penetration Testing Software.

5. CONCLUSIONS

The security problems will suffer as long as constructor remain committed to present systems architectures, generated without some security requirements. Proper security is not be a fact as long as there is funding for ad-hoc & security solutions for such insufficient designs and because the delusory results of intrusion team are confirmed as evidence of computer systems security. Regular monitoring, good systems management practice, attentive detection of intrusion & awareness of computer security that's all essential components of the security effort of an organization. In any of those places, only one failure could well exposes a corporation to cyber vandalism, humiliation or even worse, loss of revenue. Each new technology has its advantages and risks. While the moral hackers which will help the customers better appreciate their security needs and keeping their guards in situ is up to customers.

REFERENCES

- “Is Ethical Hacking Ethical?" by Int. J. Eng. Sci. Technol., 2011.
- “Introduction to Ethical Hacking” by S.-P. Oriyano 2017
- "Ethical Hacking and Penetration Testing Guide" by R. Baloch 2017.
- http://www.wikipedia.org/wiki/ethical hacking
- www.computerhope.com
- http://searchsecurity.techtarget.com/
- http://www.pcworld.com/
- http://image.slidesharecdn.com/
- http://www.instructables.com/