Cosmos Multidisciplinary Research E-Journal
Online Available at www.cmrj.in
Recognized International Peer Reviewed Journal
Impact Factor 4.94
ISSN No. 2456-1665

White Hat Hackers and Ethical Hacking

Rahul Laxmikant Gajre
Research Student

Abstract - Information security has become one of the most important concepts in our information and technology driven world as massive growth of the Internet has brought in many good things such as e-commerce, easy access to extensive sources of learning material, collaborative computing, e-mail, Cloud computing and new avenues for enlightenment and information distribution to name a few. Today, since almost all the work is done over the internet, crucial data is sent over the web and other information is placed over the internet. So ensuring data security over the internet is very important and should be taken care of at utmost priority. As with most technological advances, there is also a dark side attached to it, i.e. hacking. Hacking is an activity in which a person (namely hackers) exploits the weaknesses and vulnerabilities in a system for self profit or gratification. With the growing movement of the world from offline to online culture like shopping, banking, sharing information access to sensitive information through the web applications has increased. Thus the need of protecting the systems from hacking arises to promote the persons who will punch back the illegal attacks on the computer systems and will ensure data security. As every coin has two faces, this coin also has one another face which generally acts as a life saver for the victims of hacking. This lifeguard technique is called ethical hacking. Ethical hacking is a technique which is used to identify the weaknesses and vulnerabilities in the system or computer network in order to strengthen the system further to prevent the data.

A white hat hacker is a computer security specialist who does ethical hacking i.e. who breaks into protected systems and networks to test and asses their security. White hat hackers use their skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can detect and exploit them. Although the methods used are similar, if not identical, to those employed by malicious hackers, white hat hackers have permission to employ them against the organization that has hired them for ethical hacking purpose.

Introduction - In today's digital landscape, many of our daily activities rely on the internet. Various forms of communication, entertainment, and financial and work-related tasks are accomplished online. This means that tons of data and sensitive information are constantly being shared over the internet. 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 trouble 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.

In the modern day sense, those who attempt to bypass information security access controls in an effort to pose as authorized users are generally classified as hackers. It is important to remember that a hacker is an unauthorized user who attempts to gain access into a system. They do not have permission to enter the system and do so with the risk of being caught and persecuted based upon established laws. In the new era of computing, there has been this emergence of a new breed of hacker known as the white hat hacker. The goal of the

white hat hacker is very different from their counterparts, known as black hat hackers or crackers. The white hats attempt to infiltrate systems in an effort to help identify weaknesses so they can be patched in time before the black hats find and exploit these same vulnerabilities. Another group, known as the grey hats, are somewhere in the middle as their allegiance to a single side remains unclear. Regardless of the category of hacker, by definition, hackers essentially lack the permission to enter a system or view certain pieces of information. Hackers often trespass into computer networks and can intercept confidential information by using hacking tools and applications or can simply evade authentication and authorization schemes to snoop around. However, since white hat hackers break in to help identify and patch the flaws then evidently intent is really the fundamental idea used in classifying hackers.

Traditionally, hackers are computer geeks who knew almost everything about computers (both hardware and software)and were widely respected for their wide array of knowledge. But over years, the reputation of hackers has been steadily going down. Today, they are feared by most people and are looked upon as icons representing the underground community of cyber population.

Generally there are three different type of hackers.- A black-hat hacker is an individual who attempts to gain unauthorized entry into a system or network to exploit them for malicious reasons. The black-hat hacker does not have any permission or authority to compromise their targets. They try to inflict damage by compromising security systems, altering functions of websites and networks, or shutting down systems. They often do so to steal or gain access to passwords, financial information, and other personal data

Grey hats exploit networks and computer systems in the way that black hats do, but do so without any malicious intent, disclosing all loopholes and vulnerabilities to law enforcement agencies or intelligence agencies. White-hat hackers, on the other hand, are deemed to be the good guys, working with organizations to strengthen the security of a system. A white hat has permission to engage the targets and to compromise them within the prescribed rules of engagement .White-hat hackers are often referred to as ethical hackers. This individual specializes in ethical hacking tools, techniques, and methodologies to secure an organization's information systems.

In the enterprise security arena, white hat hackers have traditionally offered penetration testing (widely known as pentesting) services. In typical pentesting engagements, white hat hackers are hired by organizations that are looking to bolster their defenses. These white hat hackers then seek to hack into their client's networks. In some cases, they may be given a broad charter to try to attack specific assets, such as private networks, applications, and endpoints. Alternatively, they may be given a broad mandate to uncover security gaps, wherever they may be.

By using talented hackers to find gaps, security teams can better test their defenses. In this way, these teams can therefore be better positioned to eliminate gaps and strengthen their defenses—before a real attack happens. Based on the insights a white hat hacker uncovers, teams may need to establish new policies, update or change configurations, or update or replace tools.

Using real attack techniques to proactively find weakness is the best and only way to truly prove the effectiveness of security defenses. White hat hackers often use the same tools and techniques as their black hat counterparts. The techniques employed can range from simple public "root kits" with documented approaches, to complex and sophisticated campaigns that may include social engineering, exploiting endpoint vulnerabilities, presenting attack decoys, spoofing protocols, and more.

What motivates ethical hackers?

Most hackers are motivated by curiosity, and ethical hackers are no exception. They're often motivated by a desire to see what makes things tick, poking around in security systems just for the challenge of finding a way around them. Responsibly reporting their findings is the best way to indulge this desire whilst also staying on the right side of the law.

Many are also driven by a genuine desire to make the world more private and more secure. Exposing flaws in widely-used services and applications means that they're less likely to be used to harm innocent people.

Another big motivating factor for ethical hackers is, of course, cash. A career in pen-testing or red-teaming can be extremely lucrative, and often allows hackers to make a great deal more money than they would as a cyber criminal without fear of reprisals. Similarly, bug bounty programmes can provide incredibly generous payouts for discovering major flaws the current record-holder for the highest-value bug bounty is Google's $112,500 payment to a Chinese researcher who discovered a remote exploit vulnerability in Android.

What Do White Hat Hackers Do?

To put it simply, white hats are offensive security analysts that help companies and organizations gain awareness and strengthen their security and cybersecurity posture. They do this by helping those organizations identify ways to shore up their defenses by:

- Continuously engaging in learning new knowledge, skills, techniques and programming languages.
- Staying abreast of industry changes and technological developments.
- Gathering intelligence about the organization, their IT infrastructure and employees.
- Using various legal and approved methods of digital and physical infiltration.
- Discovering and reporting bugs, vulnerabilities and other weaknesses (sometimes through bug bounty programs).
- Writing or developing code for programs, apps, rootkits, and honeypots.
- Simulating a variety of cyber and social engineering attacks.
- Recommending security improvements based on their findings and industry best practices.

How white hat hackers work

White hat hackers use the same hacking methods as black hats, but the key difference is they have the permission of the system owner first, which makes the process completely legal. Instead of exploiting vulnerabilities to spread code, white hat hackers work with network operators to help fix the issue before others discover it.

White hat hacker tactics and skills include:

1] Social engineering

White hat hackers commonly use social engineering (“people hacking”) to discover weaknesses in an organization’s “human” defenses. Social engineering is about tricking and manipulating victims into doing something they should not (making wire transfers, sharing login credentials, and so on).

2] Penetration testing

Penetration testing aims to uncover vulnerabilities and weaknesses in an organization’s defenses and endpoints so they can be rectified.

3] Reconnaissance and research

This involves researching the organization to discover vulnerabilities within the physical and IT infrastructure. The objective is to gain enough information to identify ways to legally bypass security controls and mechanisms without damaging or breaking anything.

4] Programming

White hat hackers create honeypots that serve as decoys to lure cybercriminals to distract them or help the white hats gain valuable information about the attackers.

5] Using a variety of digital and physical tools

This includes hardware and devices that allow the penetration testers to install bots and other malware and gain access to the network or servers. This also includes -

- pick or bypass physical locks,
- clone ID access cards,
- gain visibility and identify physical security blind spots,
- install bots and other malware, and
- gain access to the network or servers, etc.

For some white hat hackers, the process is gamified in the form of bug bounty programs - competitions that reward hackers with cash prizes for reporting vulnerabilities. There are even training courses, events, and certifications dedicated to ethical hacking.

IMPORTANCE 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.

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.

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,

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.

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.

POPULAR TOOLS USED BY HACKERS:

Air crack 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. Air Snort 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. Wire Shark 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. Cloud Cracker 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

CONCLUSION

Many times, the definition of a white hat hacker just doesn't do them justice. To put it bluntly, white hat hackers are integral to the security of organizations, businesses, and governments. They help those organizations find and mitigate exploitable weaknesses before the bad guys do.

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, mind set and tools of a hacker but the attacks are done in a non- destructive manner.

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.

REFERENCES

[1] http://www.wikipedia.org/wiki/ethical hacking
[2] https://kwhs.wharton.upenn.edu/2019/01/world-white-hat-hacker/
[3] https://blog.eccouncil.org/types-of-hackers-and-what-they-do-white-black-and-grey/
[4] https://www.lifewire.com/hackers-good-or-bad-3481592
[5] Palmer, Charles. Ethical Hacking. Published in IBM Systems Journal: End-to-End Security, Volume 40, Issue 3, 2001.
[6] Beaver, Kevin and McClure, Stuart. Hacking For Dummies. Published by For Dummies, 2006
[7] 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.
[8] 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.
[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] Smith B., Yurcik W., Doss D., "Ethical Hacking: the security justification redux", IEEE Transactions, pp. 375 - 379, 2002.
[11] Ethical Hacking by C.C. Palmer, IBM research division
[12] A Comprehensive Study On Ethical Hacking by Suriya Begum, p. 2277 – 9655