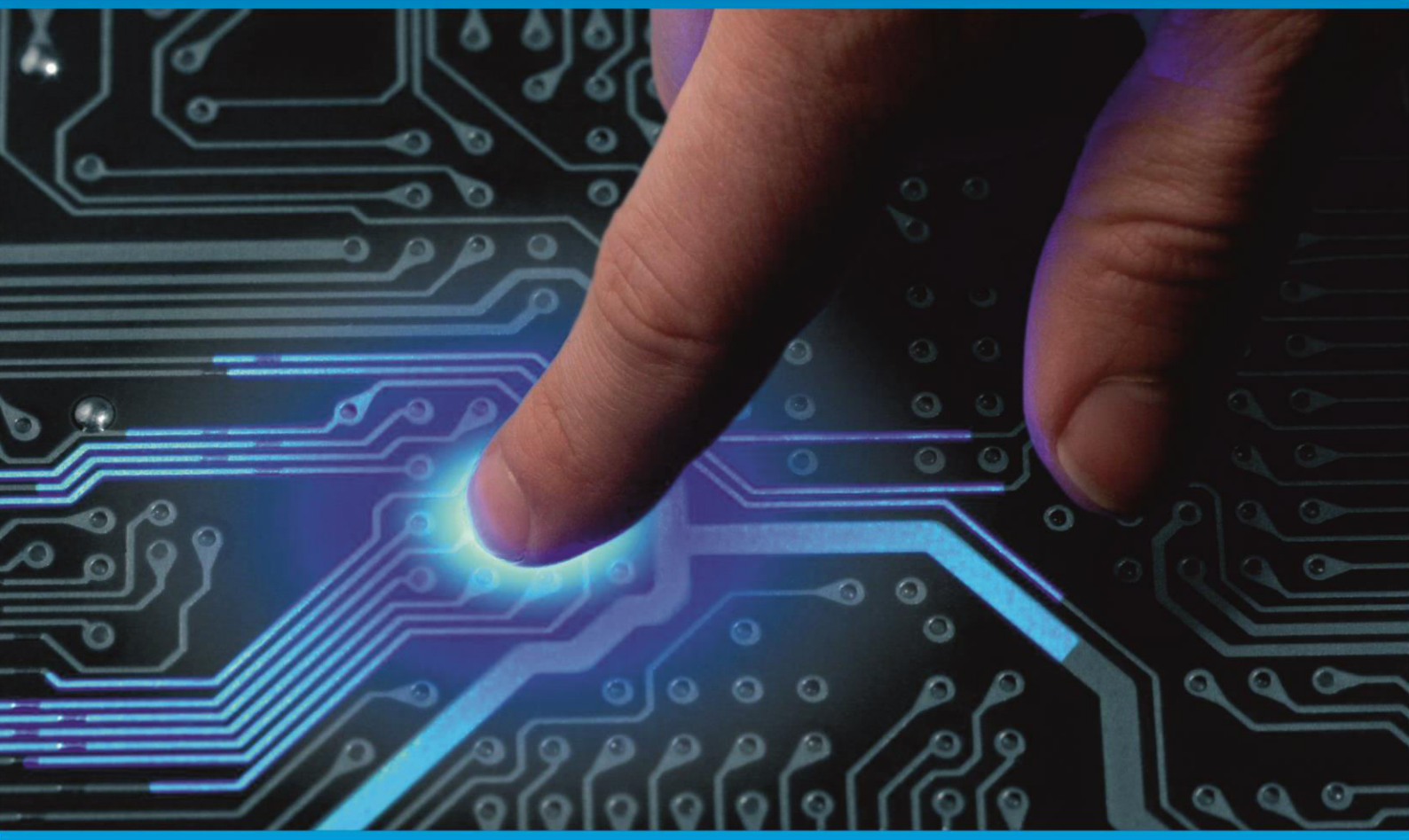
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903128|

A Study on Ethical Hacking

Srushti Dalavi [1], Dr.Vaishali Sanvilkar[2]

Student, Department of M.C.A, P.E.S.'s Modern College of Engineering Pune, Maharashtra, India[1]

Head of the Department, Department of M.C.A, P.E.S.'s Modern College of Engineering Pune, Maharashtra, India[2]

ABSTRACT: Ethical hacking can be defined as a process where an authenticated person, who is a computer and network expert, attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test the system an ethical hacker will use an equivalent principle because the usual hacker uses, but reports those vulnerabilities rather than using them for his or her own advantage. Ethical hackers offer a security net to your organization. Hackers will keep your network, email, systems, and database security. We can run up to them as soon as we start noticing any glitch. In fact, within the presence of those people, glitches are addressed even before you notice. Ethical hackers are hired by big organizations to seem into the vulnerabilities of their systems and networks and develop solutions to stop data breaches.

KEYWORDS: Malicious hacker , black hat hacker, Grey hat hacker ,white hat hacker

I. INTRODUCTION

In this evolving period Internet, computer security has become a major concern for businesses and governments. They want to be able to take advantage of the Internet for their own purpose.

At many times, the potential customers of these services are worried about maintaining control of their personal information that varies from credit card numbers to social security numbers and personal address .In their search for a way to approach the problem related, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to possess independent computer security professionals plan to force an entry their computer systems. In computer security, these "ethical hackers" would use identical tools and techniques because of the intruders, but they may neither damage the target systems nor steal information. Rather than that, they may evaluate the target systems' security and report back to the owners with the vulnerabilities they found and directions for the simplest way to remedy them.

Every good ethical hacker should know the methodology chosen by the hacker like reconnaissance, host or target scanning, gaining access, maintaining access and clearing tracks. For ethical hacking we should know about the various tools and methods that can be used by a black hat hacker apart from the methodology used by him/her. From the purpose of view of the user one should know at least a number of these because some hackers make use of these who aren't conscious of the varied hacking methods to hack into a system. Also when thinking from the point of view of the developer, he/she also should be aware of these since he should be able to close holes in his/her software even with the usage of the various tools. With the arrival of the latest tools the hackers may make new tactics. But a minimum of the software is going to be immune to a number of the tools.

II. LITERATURE SURVEY

i. **Phreakers and tiger teams:**It was during the 1970s that the waters began to urge muddied. With the growing popularity of computers, individuals who understood systems and programming languages were getting down to see the probabilities in testing those systems to know their capabilities.This was also the time that “phreaking” began to realize widespread notoriety. Phreaker began to know the character of telephone networks. Many individuals were ready to use devices that mimicked the dialing tones so as to route their own calls, which allowed them to form involves free .Arguably, this was one among the primary times that hacking was used for illegal purposes by an outsized number of individuals .Simultaneously, however, governments and corporations were starting to see the benefit in having technical experts actively hunt down the weaknesses during a system for them, thus allowing them to unravel those problems before they might be exploited. These were referred to as “tiger teams” and therefore the American government was especially keen on using them to strengthen their defences.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903128|

ii. **The rise of the black hat hacker:**Near about the 1980s and 1990s, the term hacker began to be associated almost exclusively with criminal activity. The amazing popularity of the private computer as a tool for both businesses and individuals meant that tons of important data and details were now stored not in physical form but in computer programs. Hackers began to ascertain the chances of stealing information that would then be sold on or wont to defraud companies.[1]

iii. **Sophisticated modern cybercriminals:**It is estimated that quite 30,000 websites are hacked every single day, which matches to point out the size of recent hacking and the way it can affect businesses of all sizes. Hackers range from inexperienced "script kiddies" making use of hacking tools written by others to stylish modern cybercriminals who will stop at nothing to urge what they need .While we might consider hackers as operating exclusively from behind their computer screens, it's also true that black hat hackers will search for alternative methods to interrupt down systems. These methods could include everything from cracking passwords to using sorts of social engineering during which victims might be tricked into delivering personal details or sensitive organizational information.

iv. **The renaissance of the ethical hacker:**As hackers become smarter and more persistent, it's become increasingly important for companies to possess adequate defences against them. This is why we've seen the concept of ethical hacking increasingly utilized by cybersecurity firms as the simplest way to combat the matter .Ethical hacking is now commonplace – it's even possible to become what's referred to as a licensed Ethical Hacker.

v. **How ethical hackers can help businesses:**It's easy to ascertain how businesses can take pleasure in using ethical hackers. A white hat hacker can mimic a true cyber attack that black hat hackers would plan to perform using all equivalent strategies that a real attack would use. If a business's defences have a weakness, the moral hacker is going to be ready to expose it in order that it is often fixed before a true hack occurs.

III. TYPES OF HACKERS

i. **White Hat Hacking :** This hacking is completed for the great deed. In this sort of hacking the skill is employed for legal purposes and to save lots of and protect the info of any organization or for a person . These are paid employees working for companies as security specialists. All white hat hackers use their knowledge and skills for the good of others. White Hat Hacking is practiced. [5]White-hat hackers are often mentioned as ethical hackers. White-hat hackers disclose every vulnerability they find within the company's security system in order that it are often fixed before they're being exploited by malicious actors

ii. **Black Hat Hacking :** This hacking is completed illegally and is maliciously used for private gain. Black hat hackers usually have extensive knowledge about breaking into computer networks bypassing security protocol.Black hat hackers or unethical hackers perform hacking to fulfill their selfish intentions .

iii. **Grey Hat Hacking :** Such quiet hacking is the mixture of both Black Hat and White Hat Hacking. Grey Hat Hacking is completed for the protection of national level. Grey-hat hackers surf the internet and hack into computer systems to notify the administrator or the owner that their system/network contains one or more vulnerabilities that possesses to be fixed immediately.

IV. HACKING PHASES

i. **Foot Printing or Reconnaissance:**Refers to the method of assembling the maximum amount of data as doable concerning the target system to seek out ways in which to penetrate into the system. An associate moral hacker has got to pay the bulk of his time in identifying a corporation, gathering data concerning the host, network and folks associated with the organization.Information like science address, Whois records, DNS data, associate OS used, worker email id, Phone numbers etc is collected.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903128|

Footprinting helps to:

a) Know Security Posture – the information gathered can facilitate North American countries to urge an summary of the safety posture of the corporate like details concerning the presence of a firewall, security configurations of applications etc.
b) Reduce Attack space – will establish a {particular} vary of systems and focus on particular targets solely. this can greatly scale back the quantity of systems we tend to ar direction on.
c) Identify vulnerabilities – we are able to build associate data information containing the vulnerabilities, threats, loopholes accessible within the systemof the target organization.
d) Draw Network map – helps to draw a network map of the networks within the target organization covering topology, trustworthy routers, presence of server and alternative data.

ii. Scanning: Once the wrongdoer has enough data to know however the business works and what data of import can be accessible, he or she begins the method of scanning perimeter and internal network devices trying to find weaknesses, including

a) Open ports
b) Open services
c) Vulnerable applications, together with operative systems
d) Weak protection of information in transit
e) Make and model of every piece of LAN/WAN instrumentation
f) Shutting down all surplus ports and services
g) Allow crucial devices, or devices housing or process sensitive data, to retort solely to approved devices
h) Closely manage system style, resisting makes an attempt to permit direct external access to servers except below special circumstances and forced by end-to-end rules outlined in access management lists
i) Maintain correct patch levels on end and LAN/WAN systems

iii. Attack and Gaining Access: Gaining access to resources is the whole purpose of a modern attack. The same old goal is to either extract data of import to the wrongdoer or use the network as a launch website for attacks against alternative targets. In either scenario, the wrongdoer should gain some level of access to at least one or additional network devices.In addition to the defensive steps delineated on top of, security managers ought to build each effort to make sure end-user devices and servers aren't simply accessible by unauthenticated users. This includes denying native administrator access to business users and closely observing domain and native admin access to servers.

iv. Maintaing Access: Having gained access, associate wrongdoers should maintain access long enough to accomplish his or her objectives. Although associate wrongdoer reaching this part has with success circumvented your security controls, this part will increase the attacker's vulnerability to detection.

v. Escalating Privilege, Covering Tracks and making Backdoors:After achieving his or her objectives, the wrongdoer usually takes steps to cover the intrusion and doable controls left behind for future visits. Again, additionally to anti-malware, personal firewalls, and host-based IPS solutions, deny business users native administrator access to desktops. Alert on any uncommon activity, any activity not expected supported your information of however the business works. To form this work, the safety and network groups should have a minimum of the maximum amount of information on the network because the wrongdoer has obtained throughout the attack method.

V. ADVANTAGES AND DISADVANTAGES

i. ADVANTAGES:

a) All depends upon the trustworthiness of the moral hacker
b) Hiring professionals is expensive5.1 Advantages
c) Provides security to banking & financial establishes Prevents websites defacements
d) An evolving technique
e) To catch a thief you've got to think sort of a thief

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021. 0903128|

ii. DISADVANTAGE:

a) All depends upon the trustworthiness of the moral hacker
b) Hiring professionals is expensive

VI. CONCLUSION

Ethical hackers help companies in finding out vulnerabilities and possible security leaks of their computer systems and also to protect them from any potential threat. In future e thical hacking as a career has promising prospects .The Hacking process has both its benefits and risks. They can either bankrupt a company or protect the data, increasing the revenues for the company. The battle between the white hat hackers and the black hat hackers is a long war, which has no end. Ethical Hackers help companies to understand the present hidden problems in their servers and corporate network.[3] Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and the way they could be exploited.[2]This also concludes that hacking is a crucial aspect of computer world. Hacking deals with both sides of being good and bad. It plays a vital role in maintaining and saving a lot of secret information, whereas malicious hacking can destroy everything. It all depends is the intention of the hacker. It is near about impossible to fill a niche between ethical and malicious hacking as human mind can't be conquered, but security measures are often tighten [3]

REFERENCES

[1]https://www.biharihacker.in/2020/10/all-history-of-ethical-hacking-and.html
[2]Gurpreet K. Juneja,"Ethical hacking :A technique to enhance information security"international journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013
[3] K.BalaChowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393
[4]https://www.eccouncil.org/ethical-hacking/ hacking phases
[5]https://www.slideshare.net/ShravanSanidhya1/presentation-on-ethical-hacking-ppt#:~:text=%EF%82%97%20That%20is%20black%20hat,using%20them%20for%20defensive%20purposes
Types of hacker
[6]https://www.slideshare.net/vishalkumar245/introduction-ethical-hacking
[7]https://www.seminarsonly.com/computer%20science/Ethical-hacking.php
[8]https://searchsecurity.techtarget.com/definition/ethical-hacker
[9]https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_hacker_types.htm

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details