Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 43 No. 4 (2022)

Cyber Security Practices Ethical Hacking and its Significance in Modern

[1] Ashwini Bari, [2] Anil Yadav, [3] Sahil Suman, [4] Ramit Ranjan

[1] Asst. Professor
Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur
[2] Assistant Professor
Computer Science Engineering
Arya Institute of Engineering Technology & Management, Jaipur
[3] Science Student
Assembly of God Church School, Bettiah, Bihar
[4] Science Student
S.D.S Senior Secondary School, Chhapra, Bihar

Abstract: Someone who is an ethical hacker is a computer and network expert who breaks into security systems on behalf of their owners to find holes that a bad hacker could use. The internet's rapid rise has led to many good things, such as: shopping, e-mail, shared computers, and new Places for ads and information to be sent through What people in business and the government worry about most these days is ethical hacking, which is also called attack testing, penetration testing, or red teaming. Concerns about being "hacked" are raised by businesses, and possible customers are worried about keeping personal information safe.
Keywords: cybercrime, clearing Tracks, computer security, Ethical hacking, scanning and Enumeration.

1. Introduction:

Ethics-based hacking is becoming more common in many areas of life, especially in the computer business. People who want to protect the common area and data should talk to each other using the right technology. Because hackers are so smart, ethical hacking has become the newest and most cutting-edge way to use computers.

All businesses, big and small, use this as their first line of defense to keep their info safe. These days, it is hard to figure out what people really want, and it's even harder to figure out why ethical hackers break into systems that aren't completely secure.

In general, ethical hackers are allowed to break into what seems to be a secure computer system without doing any harm, but with the goal of finding weak spots so they can use that information to make things safer. Some companies tell their local security officer or manager that an attack like this is going to happen—it is usually called a "penetration test"—and they may even be able to watch the hacker work, but most of the time, they are not. Only senior staff and maybe two or three board members know about the attack.

There is a wide range of classifications in the general field of ethical hacking.

Hacking with ethics

Hacker with morals

Two white hats Someone who hacks for a good cause is called an ethical hacker. People who are good are mostly ethical hackers. They are allowed by law to mess with other people's programs. Ethical hackers look for cracker-friendly ports, websites, and bugs that can be used by crackers. As soon as someone knows where a device is weak, it is easy to hit it. People who use the internet need to know how hackers can get into their networks to stay safe.

Reconnaissance, keeping access, Scanning, and listing, getting access Clearing tracks, Scanning, and listing. The second step in penetration testing and ethical hacking is to list and scan everything that is there. Pen testers often use scanning to find an open door. They also use scanning to find out where the service that works on the port is weak. Getting inside. Once the observation is over and all the weak spots have been tried, hackers use tools and techniques to try to get in. The main goal of this is getting the password back. Either bypass

techniques or password breaking methods can be used by hackers to do this. Keeping entry open.

Once the hacker gets into the targeted systems, he can use them and their resources to his advantage and use them as a launching pad to test and damage other systems. He can also stay hidden and keep using the systems without the real user's knowledge, which is bad for business and causes a disaster.

2. Literature Review:

Past research has targeted on ethical hacking, which entails professionals in pc networks trying out safety systems on behalf in their proprietors to discover vulnerabilities that malicious hackers may want to exploit. With the rapid increase of the net, which has added about many fine traits like e-commerce, email, collaborative paintings, and new avenues for marketing and facts sharing, moral hacking has gained good sized attention. It has grown to be a number one issue for businesses and governments. This practice, additionally referred to as intrusion trying out, penetration checking out, or pink teaming, aims to perceive and fasten security weaknesses. Organizations are concerned about the hazard of being hacked, and capability customers are concerned approximately safeguarding their private statistics. Past studies have contributed to information the significance of moral hacking in an increasingly virtual world.

3. Conclusion:

The security problems will endure as long as constructor remain committed to present systems architecture, generated without some requirements. Proper security will not be a fact if there is funding for ad-hoc & security solutions for these insufficient designs & if the instructions team are recognized as evidence of computer system security. Regular monitoring, attentive detection of instruction, good systems management practice & awareness of computer security that all essential components of the security efforts of an organization. In preceding sections, we saw the methodology of hacking why should we aware of hacking and some tools which a hacker may use. Now we can see what can we do against hacking or protect ourselves form hacking.

The first thing we should do is keep ourselves updated about that software we and using for official and reliable sources. Educate the employee and the users against black hat hacking.

Many types of ethical hacking Depending knowledge of hacking in this many hackers good hacking it’s no form harm it is maintained safety of and security and check the vulnerabilities in the current system.

Hacktivists: In this activity hacker hacking any computer system illegal hacker can send a large massage in the main page in the massage they give something illegal hacker hacking.

Cyber warriors: Cyber warriors use any computer use to ethical hacking you do hired organization hired ethical hacking and find out an ethical hacker it is weakness a cache her to save the information.

4. Future scope

Certainly! The prospects for ethical hacking in India are quite vibrant. Ethical hackers are like digital detectives who concentrate on expertise pc networks and uncovering any weak spots in protection systems. They do that to prevent terrible hackers from exploiting those vulnerabilities. As the internet has grown explosively, it has introduced us many true things like online purchasing, emails, collaborative paintings, and new methods to market it and share facts. However, it has additionally given upward thrust to numerous protection issues. This is wherein moral hacking comes in. It turns out to be a pinnacle priority for agencies and governments.

Ethical hacking is sometimes additionally referred to as intrusion trying out or penetration testing. It entails simulating cyber-assaults to discover and fasten any weaknesses before the terrible men can take advantage of them. In easy phrases, it is like having a pleasant virtual superhero who checks your defenses to make sure they may be sturdy. Organizations are truly involved about the opportunity of being "hacked." They need to maintain their facts and structures secure from cybercriminals. And even ordinary human beings are worried about their non-public records, like financial institution info or non-public messages, staying secure online.

So, the destiny of moral hacking in India is all about protecting groups and individuals from cyber threats. It gives many exciting opportunities within the discipline of cybersecurity, ensuring that your digital

existence stays safe and sound.

References

[1] S.- p oriyano," Instructions to Ethical hacking," in CEHTMV9 ,2017
[2] B. sahare, a Naik, and s. khandey," study of Ethical hacking " int j. computer science Trends technology., 2014.
[3] S. patil, a. jangrJangra M. bhale, A. Raina, and p. kulkarni, " Ethical hacking: The need for cybersecurity. " In IEEE International conference on power, control, signals, and instrumentation engineering.
[4] G. R Lucas," cyber warfare," in the Ashgate Research companion to Militara Ethics, 2016
[5] Simplilearn.com, “ethical hacking” is an authorized practical of detecting vulnerabilities in an application, system, or organization’s infrastructure and bypassing system security to identify potential data breaches and threats in a network.
[6] Hackers’ identity and exploit gaps and weakness in computer systems. Ethical hackers identify the same weakness, but do so with the intention of fixing them. (University of Denver boot campus)
[7] Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical hacking: Educating future cybersecurity professionals. In Proceedings of the EDSIG Conference ISSN.
[8] Hawamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., & Al-Rawashdeh, G. Cyber security, and ethical hacking: The importance of protecting user data. Solid State Technology.
[9] Manjikian, M. (2017). Cybersecurity ethics: an introduction. Routledge.
[10] Radziwill, N., Romano, J., Shorter, D., & Benton, M. (2015). The ethics of hacking: Should it be taught? Faily, S. (2014). Ethical hacking assessment as a vehicle for undergraduate cyber-security education.
[11] Prasad, S. T. (2014). Ethical hacking and types of hackers. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE).
[12] Rathore, N. (2015). Ethical hacking and security against cybercrime. i-manager's Journal on Information Technology.
[13] Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley.
[14] Anley, C., Heasman, J., & Lindner, F. (2007). "The Shellcoder's Handbook: Discovering and Exploiting Security Holes." Wiley.
[15] Jain, M., Kaushik, M. and Kumar, G. (2015) “Reliability analysis for embedded system with two types of faults and common cause failure using Markov process,” in Proceedings of the Sixth International Conference on Computer and Communication Technology 2015. New York, NY, USA: ACM.
[16] Kaushik, M. et al. (2015) “Availability analysis for embedded system with N-version programming using fuzzy approach,” International Journal of Software Engineering Technology and Applications, 1(1), p. 90. doi: 10.1504/ijseta.2015.067533.
[17] R. Kaushik, O. P. Mahela and P. K. Bhatt, "Power Quality Estimation and Event Detection in a Distribution System in the Presence of Renewable Energy" in Artificial Intelligence-Based Energy Management Systems for Smart Microgrids, Publisher CRC Press, pp. 323-342, 2022, ISBN 9781003290346.
[18] T. Manglani, R. Rani, R. Kaushik and P. K. Singh, "Recent Trends and Challenges of Diverless Vehicles in Real World Application", 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 803-806, 2022.
[19] R. K. Kaushik Anjali and D. Sharma, "Analyzing the Effect of Partial Shading on Performance of Grid Connected Solar PV System", 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-4, 2018.
[20] R. Kaushik, O. P. Mahela, P. K. Bhatt, B. Khan, S. Padmanaban and F. Blaabjerg, "A Hybrid Algorithm for Recognition of Power Quality Disturbances," in IEEE Access, vol. 8, pp. 229184-229200, 2020.