Global Scientific JOURNALS
GSJ: Volume 10, Issue 5, May 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

Ethical Hacking Techniques and penetration testing

Zara Mubeen, Bilal Hassan, Faisal Rehman
Department of computer science and information technology
Lahore Leads University
zararamzan060@gmail.com, bilal.mughal098@gmail.com, faisalrehman0003@gmail.com

Abstract- The modern world is changing and changing rapidly. The huge number of inventions is constantly expanding. Information is getting double in less than a year. The advancement of technology has played the important role in our life. In this era, the most thing to be concern is computer security for companies and organizations. Unfortunately, the data we share over the internet is not secure in any way. Cyber-attacks are getting complex and it is hard to detect them

. The security of data is the most important thing that needs to talk about. Hacking means getting control on other person's accounts. Hacking is an uncertified intrusion into a computer on the matrix. The person committed in hacking venture is commonly assigned to as a hacker. This paper covers the different types of hacking and ethical hacking techniques.

Keywords - Hacking, Ethical Hacking, Cyber-attack

Introduction

A network security system depends on layers of security and it consists of more than one component including in to the network for scanning network and security software and hardware. All modules work in conjunction to rise the comprehensive computer network security. There are 50 nations who tracked down their technique for network safety. The liveliest control of fence on the way to the security, there are 25 nations that found and show the strategy of cyber security, US of America, Germany, United Kingdom, Australia, Switzerland, Norway, Sweden, Canada, Spain, Estonia, Singapore, Finland, Russia, Poland, France, Algeria, New Zealand, Europe, Brazil, India, Netherlands, Japan, Malaysia, Italy [1].

The social are prudent changes due to these innovations are unmatched on one hand yet as each image has two sides, the innovations additionally have a more obscure side on the other hand also[1]. It prompts the presence of new classes of wrongdoings notwithstanding carrying out the traditional violations utilizing arising innovations.

Moreover, the impacts of indecent conduct can be more extensive when contrasted with before due to the advancement of ICT which wiped out the idea of topographical limits. Pakistan is additionally dealing with the issue of network safety and is not liberated from this problem [2]. In Pakistan, the exceptional development, openness of PC supplies, and development in web access suppliers prompt learning and communicate.

Youngsters between the ages of 13 and 17 are investing more energy in their cell phones and

less time getting to online media stages on their web programs. Nelson Studios shows that youngsters' cell phone information utilization significantly increased in 2011 (Nelson, 2011; Osborne, 2012). Stages like Facebook can now routinely gather information from north of 500 million dynamic clients through its Messenger application, in addition to 30 billion messages every day by means of their as of late procured WhatsApp (Weissenthal, 2014). Pass by In the United Kingdom, 81% of adolescents approach portable (Spence, 2013), while in the United States, 88% (Lane Hart, 2015). But then, little is had some significant awareness of the different manners by which applications make and offer information. On the other hand, pair of people does use this surprising alteration for illegal motive as fine. Hacking is just like digital crime or digital theft. Hackers can hack anything connected to the internet like websites, accounts

even bank servers. These days the computer network security is a big matter that demands to be considered. Organizations use the internet in a wide variety of application management, database access, etc.

The word ethical hacking is the phrase used to report hacking achieve by a company or original to recognize future pitfall on a computer or mesh. They are permitted by the company or organization to hack their systems for security purposes. Ethical hacking is a responsibility. To become an ethical hacker someone should have complete knowledge about hacking [15].

Literature review

The new technologies of mobiles, Cloud computing, e-commerce, and mobile applications are mainly changing the world's vision and viewpoint of business The business agencies are preparing new strategies to gain the benefits of new technology [5]. According to the survey, the ratio of online transactions are almost eighty percent of the total transaction.[5] As the online business and interaction with social media are increasing day by day. Trillions of data are stored on the computer servers over the network so the ratio of cyber- attacks also [6] increased.

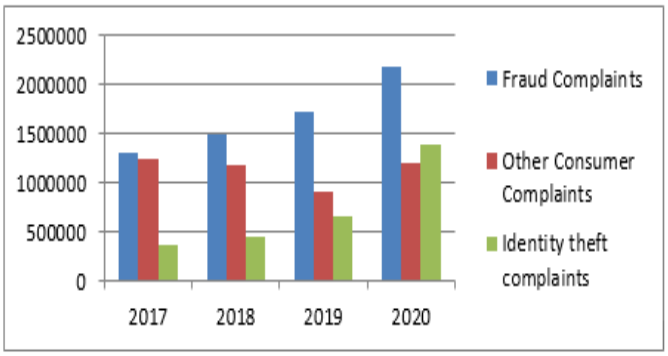


Figure.1 Ratio of cyber attacks

In 2017 according to the record there are 15000 plus complains regarding cyber crime. It increase up to 200000 and in 2020 instead of decreasing it increased up to more than 200000.

With the rise of cyber-attacks, the demand for cyber security professionals is also adding who retain the network penetration testing [7] and enjoy the ethical hacking chops, performed to assure the security of the system.

Hackers are the people who see far away the extremities and limitations imposed by others and look forward to using their skills toward upgrading or sharing knowledge [4] .

Ethical hacking allows you to attempt to bypass the system security and find the weakest point of the system that could be taken advantage of the black hat hacker. Many institutions offer the ethical hacking courses. To begin with hacking, the affiliation manifest the sharp way to admit any interference into their network or system is to hire their own experts who would strive to enter in their systems and find if there are any intrusion pitfalls. These professionals, known as "Red brigades" or "ethical hackers", follow the same way and tools like that of hateful hackers, but the difference is in their intentions [6].

Red teams or ethical hackers have clear plans to

assure the security of the systems. Someone who is interested in getting an ethical hacker can work towards instrument to come a Pokka Ethical Hacker, or CEH[8] . Ethical hacking is nothing but the law of the internet. When they exercise them[1] someone can be a professional ethical hacker.

But there are some white hat hackers (ethical hackers) who wear black hats whenever they need them. They use their power to help themselves without being caught at the expense of others. Unfortunately, some of the experts use their power to harm society [9]. Corruption can be seen as a big issue in ethical hacking. An ethical hacker can do the job with honesty but understanding their schemes or desires are arguable [9].

There are many challenges we have to face to overcome cyber- crises. In fact during covid 19 the ratio of cyber harassment increases. Here is the table containing the data of harassment complaints.

Table.1

Cases of cyber harassments

Covid 19 and cyber harassment cases		
Sr #	**Months**	**Complaints**
1	March	58
2	April	78
3	May	188
4	June	413
5	July	697
6	August	309
7	September	473

Purpose (Problem statement)

The intrusion of computers it becomes the serious issue in this era. Unfortunately, the less able and less mindfulness would bring down the systems by damaging the systems. The directors also have to repair the systems. For the system security, they have to hire some ethical hackers and should also follow the precautions. The main purpose of this paper is to define the techniques of ethical hacking.

1. Types of Hacking/Hackers

The hacking the two of busted down into three diverse designate. The word Hat has its origins in Old West films in which the Saints hat tone was white and the bodies' hat was dark. It can either be talk that the white the shading, the more uncertain it is to be disable. The White Hat Hackers are business- approve and paid persons with good design and ethical also known as "IT Artisan"[3]. Their task is to cover the Internet, occupation, networks and computer method from hackers. Some concern pays IT experts to try and hack into their own systems and computers to check the security. The white hat hacker is also known as an noble hacker [12].

Dissimilar the white hat hackers, the plan of the black hat hackers is to harm the systems and the web. They pound security and crush into the web to spoiled and damaged data to give the network futile. Websites, take data, and enhance security. They breach plan and sign to smash into the system or uncertified systems. That's all that for their own private activity, such as wealth. They are also called as searchers or malicious hackers. They steal private information like passwords or any other data to take the hand over the whole system. They do such article just to complete their ego, for fun, occasionally for money [13]. Hackers can be classifying into three major sorts.

1. Black Hat Hacker 2. White Hat hackers.

3. Grey Hat hackers.

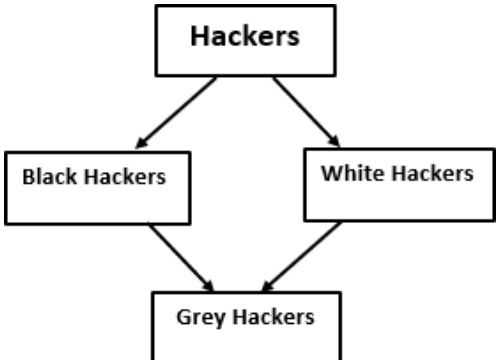
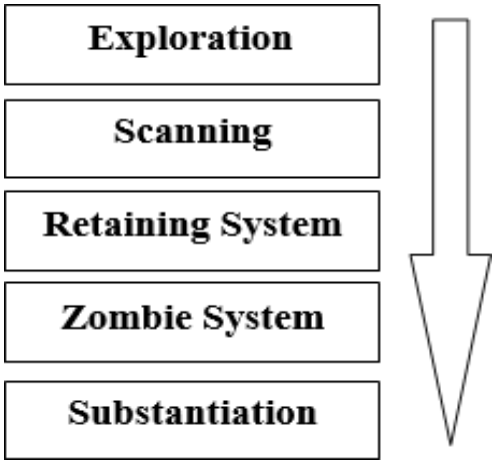


Figure.2 Types or hackers

i. Black Hat Hackers

To recognize a black hacker is just to indicate that they have certain level of expertise in attacking and destroying the systems and networks. Black hats attack the system with the different motives



in mind. They do all these activities to take the advantage of the system they may using the system to reach the other system on the same network. Black hats do all the malicious activities for sake of money or destroying the system. They often called crackers. Black hats have less ethics. They even don't care about the ethics or laws [14].

ii. White Hat Hackers

Ethical hacking is very stoic. They just claim. Time and obduracy to intervene and search the system security flaws. This can be an important feature of patience it will also be seen in the malicious hacker because he will also maintain it. Be patient and detector the attack system for weeks or perhaps for months and will wait for the availability to attack the choose target. The distinction is that the ethical hacker will show restraint to test the target opposed to any security. Breach while a malicious hacker will be patient to collect details and find an opportunity related to attacking the target system. It very well may be seen that all methods and abilities are moral and hackers in light of perniciousness. This is just the intention of hackers [4]. This makes them different. There is always a moral hacker. Use these way and chops to find out your weaknesses. Target framework and how to manage any horrible attacks, while an awful programmer will constantly attempt. Use design and expertise to hit the objective. Destroying and destroying it for particular gain like plutocrat. To know the true intention of a person who is involve in ethical hacking is delicate. It is another big issue that needs to be talked about because white hat hackers wear black hats whenever they want or need and use their chops in a wrong way.

1. Hacking Phases

The companies and organizations hire the ethical hackers to stop the cyber-attacks. This work can be done in different phases. It takes a lot of effort and skills to identify the real vulnerabilities.

Figure.3 Phases of hacking

i. Exploration

Can be dynamic or latent. In passive surveillance, data is gathered concerning the thing without knowing the designed organization or person. This must be finished via looking for target data on the internet or purchasing the hand of the designated organization anything he desires to uncover and give valuable data to the Hacker. This cycle is additionally called generally data. In this methodology, the Hacker doesn't assault the arrangement of the organization network for adding data.

While in active surveillance, the hacker enters the network to discover individual hosts, IP addresses, and network services. This process is

also called "**Door window**". In this technique, there is a high threat of being caught than inactive Surveillance.

ii. Scanning

The output stage utilizes the data put away in stage 1 to examine the network. The hacker uses tools similar as dialers, harborage scanners, etc. to search the network for entry in the system and in the company network.

Ethical hackers can scan the suspectable points through which a company's system can be hacked or exploited This process is easy because to perform vulnerabilities scans there are many tools available. Ethical hackers create maps of networks which includes finding firewall and different networks or routers help them to perform this stage.

iii. Retaining System

This is the true real hacking phase and the hackers use information, which is discovered in two former phases to attack, and in the original network (LAN, no matter wired or wireless),

original PC access, internet or offline. This process is called **retaining the system**.

He destroys all the suspectable point and get control over the system he has hacked. Once he gets control on the system then he can steal all the data and destroy the system for his benefit. But ethical hackers use this skill in ethical way.

iv. Zombie System

Once the hacker has gained access to the system or network, he claims that he is penetrating for unborn attacks (or fresh attacks) and makes changes to the system that other hackers or security help cannot enter and pierce the attacked system. In such a situation the power system mentioned in phase 3 is known as the **zombie system.**

v. Substantiation

In this phase, the hacker eliminates and obliterates all validation and hints of the hacking, comparative as log lines or reprobation's from the interruption disclosure framework, so that these cannot be prohibited and followed, which additionally keeps him from the interruption of the framework. When the framework has been tended to by a hacker, there are beautiful test style known as infiltration tests to figure out programmer and saltine.

2. Penetration testing

Penetration tests, also called creatures, are part of ethical hacking and specifically concentrate on only breaking into information systems. So how does penetration testing differ from ethical hacking? Wide range to cover systems. Ethical hacking has further places and liabilities than penetration testing. It is a simulated cyber attack towards your device to test for suspect able vulnerabilities. In the environment of internet mileage security, penetration checking out is generally used to enhance an internet mileage firewall.

Phases of Penetration Test

There are six phases of penetration tests.

Figure.4 Phases of penetration testing

i. Planning

The first phase of the penetration test involves determining the scope and objectives of the test. This will start just when you are utilizing black box, white box or dim box entrance test strategy.

ii. Information Gathering

In this stage the hacker or entrance analyzer attempts to figure out the data however much as could reasonably be expects regarding the objective. It data about end utilizes, framework, applications, and that's just the beginning. The data is utilized to be precise in the entrance test, utilized a far reaching outline of the framework to get what precisely should be checked and surveyed. A portion of the strategies utilized at this stage can incorporate web index inquiries, space name look, web fingerprint, social designing, and even hunt controls, records to track down private data.

iii. Scanning and Detection

The scanning and detection stage is utilized to figure out how the objectives framework responds to different assault endeavors. The infiltration analyzer will probably utilize mechanized entrance testing devices to search for any underlying weaknesses. Static scanning and detection investigation are two sorts of approaches utilized by the infiltration analyzer. Static scanning looks at an applications code to anticipate how it will answer to an attack. Dynamic investigation screens an applications cod as it runs and gives a constant perspective on how it is functioning.

iv. Attack

When a pen tester has a full understanding of the parts to be tested, it attacks in a simulated, controlled environment. The tester attempts a real cyber attack and can take control of a device to extract data.

v. Maintain Access

Once the tester reached the target they try to expand and maintain long term access on it. The purpose of this phase is to see if the weakness can be used to gain a permanent presence in the targeted system for long to gain the depth access to a bad actor. The idea is to mimic the determine high-level threats that often remain in the system for long time to steal highly sensitive data from an organization.

v. Analysis

Once the pen tester reached the target he will then generate a report in the form of summery containing details of each steps and vulnerabilities and how they clean it after the test and make suggestions to secure the system.

Future Recommendation

The security teams will grab on hackers' exploits. It is a never ending fight that becomes more complicated with every technological advance. The challenges become double when companies launch IoT devices without the right security settings. Ideally, security should be so simple that anyone who use the device can simply turn it on and safely and operate it. The defender does not have everything secure [25]. There is always a week point is the system and pen tester find that week point and gets into the system to make it more secure.

The best way to discover and respond to threats on time is to combine AI with cyber security. AI scans the system immediately unlike human and find the coming threats. AI will find out and respond to threats as early unlike human. AI takes care of the cybersecurity simulations that can bore your cybersecurity personnel, while imitating the best human qualities and eliminating flaws.

It helps to assess the underlying security threats and prevent them on a permanent basis. It also analyzes your network in depth to see if there are security holes that could damage your network. As we know there is much data available on internet related to hacking and speed up the training process. They should replace pen testing with AI version of hacking. AI based testing make sure that there is no defects or holes left after testing. This makes the system’s

security much more powerful than manual pen testing. AI based pen testing can test the large number of systems in less time with good results [27].

In spite of that there are some steps that we should take to avoid cyber-crimes.

a) **A. Understanding Cyber Crimes Trends**

Must be sensitive to this issue. Our government should arrange the programs to spread the public awareness regarding cyber-crimes issues. People need to be taught about computer crimes and the knowledge of internet [27]. The instructed people should be able to identify, prevent and minimize the computer threats.

b) **B. Strain the Internet traffic**

Some countries, like China and Saudi Arabia, have executed Internet filtering for ISPs and clients at the governmental level. The government should stop illegal access to the website. Websites promoting or possessing keywords such as terrorism, bomb-making tricks and pornography should be blocked. Appropriate legislation is needed to filter incoming Internet traffic before Internet users can access it. The government should block the website which is a big threat to the country [29][30]. ISPs should be instructed to install DDoS and anti-spam precautions**.**

c) **C. Execution of cyber security laws**

Laws aimed at protecting the cyber community from wanted crimes seem to be on the rise. Non-commercial issues, especially in Pakistan, are not enough to protect the use of the Internet to spread extremist ideologies. Extremists carried out illegal activities on social media all over the world and especially in Pakistan. These activities affect not only the autonomy and confidence of individuals but also of institutions. Comprehensive policies are needed to combat cyber terrorism and cyber extremism. These laws can be harmonized with the international community to combat terrorism rather than cyber terrorism.

Other Recommendations

Other recommendations include enhancing the development of expert police and forensic computing resources. Help the International Computer Emergency Response Team (CERT) community, including through funding, as a potential resource that can prevent or alleviate the massive Internet problem. Fund research in areas such as: Strong Internet Protocol, Hazard Analysis, Emergency planning and disaster propagation analysis, human factors in the use of computer system, security economics.

Conclusion

Due to the lack of awareness Pakistani society is facing many cyber problems. Therefore, the proper understanding and proper awareness about cyber-crimes are necessary to control them.

Hacking has both benefits and risks as well. They may destroy the company in unethical way or protect the company by using ethical hacking skills. The battle of good and evil between ethical and unethical hackers in never-ending battle. It concludes that cyber security is the major issue. Our governments should make strict rules for cyber security.

Overview

In this paper we discuss social media problems and cyber security issues in this world. Also discuss how cyber crimes are increasing with the advancement of technology. We discuss different types of hacking, hacking phases and ethical hacking and penetration testing. We discussed that how cyber security can be improve with AI.

References

[1] G, N, Reddy and G, J, U, Reddy, A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES.

[2] F, Neri C, Aliprandi F, Hateci, M. Cuadros, and T. By, Sentiment analysis on social media. *Proc. 2012 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal.*

Mining, ASONAM 2012. no. August pp. 919....926, 2012, doi: 10,1109//ASONAM,2012,164.

[3] J.-P. A. Yaacoub. H. N. Noura. O. Salman, and A. Chehab, "A Survey on Ethical Hacking: Issues and Challenges, pp. 1/46, 2021, [Online]. Available: http:://arxiv.org//abs/2103.15072.

[4] D. Pace and A, A, Jagnarine/ The Role of White Hat Hackers in Information Security," *Honor, Coll. Theses. Pap.* p. 14 2005.

[5] S. Ullah, M. Amir, M. Khan, H. Asmat, and K. Habib, "Pakistan and cyber crimes: Problems and preventions," *2015 1st Int. Conf. Anti-Cybercrime, ICACC 2015*, no. February, 2015, doi: 10.1109/Anti-Cybercrime.2015.7351951.

[6] J. Sathya and T. Manivannan, Open Access . pp. 91–96, 2019.

[7] K. B.. Chowdappa, S. S. Lakshmi, and P. N. V. S. Pavan Kumar. /Ethical Hacking Techniques with Penetration Testing,/. *K.Bala Chowdappa al, Int. J. Comput. Sci. Inf. Technol.* vol. 5, no. 3 pp 3389–3393. 2014.

[8] K. P. Vinitha, "Ethical Hacking," vol. 4, no. 06, pp. 2015–2017, 2016.

[9] D. Jamil, /Is Ethical Hacking Ethical?,. *Int. J. Eng. Sci. Technol.* vol. 3, no. 5, pp. 3758–3763, 2011.

[10] Golightly, Lewis & Chang, Victor & Xu, Qianwen. (2021). Towards Ethical Hacking //The Performance of Hacking a Router' 10.1007/978-3-030- 72120-6_17.

[11] Walters, Robert & Novak, Marko. (2021). Cyber Security. 10.1007/978-981-16-1665- 5_2.

[12] Belliger, Andréa & Krieger, David & Belliger. Andrea & Krieger, D. (2020). HACKING/ DIGITIAL /ETHICS Introduction.Ethical Hacking, and Hacking Ethics.

[13] Bekaroo, Veediasha & Velvindron, Loganaden. (2019). Cyber Psychology. /A qualitative study to deviate black hat hacker teenagers towards white hat hacker teenagers .in Mauritius. 10.31234/osf.io/t7bm3.

[14] Pelton, Joseph & Singh, Indu. (2015). Who Will Control the Future, Black Hat Hackers or the Hacked?. 10.1007/978-3-319- 19953-5_7.

[15] Haq, Qamar. (2019). /Cyber Security and Analysis of Cyber Crime Laws to Restrict Cyber Crime in Pakistan/. International Journal of Computer Network and Information Security. 11. 62-69. 10.5815/ijcnis.2019.01.06.

[16] Hossain Faruk, Md Jobair & Miner, Paul & Coughlan, Ryan & Masum, Mohammad & Shahriar, Hossain & Clincy, Victor & Cetinkaya, Coskun. (2021). Smart Connected Aircraft: Towards Security, Privacy, and Ethical Hacking.

[17] Kaushik, Keshav & Bhardwaj, Akashdeep. (2021). Call for Book Chapter - Ethical Hacking and Penetration Testing Unleashed (EHPT2022).

[18] 10.13140/RG.2.2.16133.27364.

[19] Hamza, Anis. (2021). ANIS HAMZA - Network Ethical Hacking for beginners (Kali - Hands- on).

[20] Abu-Shaqra, Baha. (2021). Ethical Hacking Sociotechnology. 10.13140/RG.2.2.14630.04161.

[21] Alhawamleh, Ahmad & Alorfi, Almuhannad & Al-Gasawneh, Jassim & Al- Rawashdeh, Ghada. (2020). Cyber Security and Ethical Hacking: The Importance of Protecting User Data. Solid State Technology. 63.

[22] Ahmed, Ammar. (2020). Ethical Hacking Coursework. 10.13140/RG.2.2.29809.92007.

[23] Gupta, Sunil. (2019). Ethical Hacking Terminologies: Gain the Basic Concepts of Ethical Hacking. 10.1007/978-1-4842-4348-0_1.

[24] Gupta, Aman & Anand, Abhineet. (2018). Ethical-Hacking-and-Hacking-Attacks.

[25] Khan, Atta ur Rehman. (2008). ETHICAL HACKING.

[26] Baloch, Rafay. (2017). Ethical Hacking and Penetration Testing Guide. 10.4324/9781315145891.

[27] Pradeep, I & Sakthivel, G. (2021). Ethical hacking and penetration testing for securing us form Hackers. Journal of Physics: Conference Series. 1831. 012004. 10.1088/1742-6596/1831/1/012004.

[28] Conteh, Nabie. (2021). Ethical Hacking, Threats, and Vulnerabilities in Cybersecurity. 10.4018/978-1-7998-6504- 9.ch001.

[29] Kaur, Navpreet & Singh, Dr. (2016). ETHICAL HACKING IN WINDOWS ENVIRONMENT. 10.5281/zenodo.46485.

[30] Davoodnia, Behzad & Davoodnia, Ali & Zolfy Lighvan, Mina. (2019). /Advanced Wireless Penetration Testing and Ethical Hacking (in Farsi)/.

[31] Faily, Shamal. (2017). /Ethical ethical hacking? Ethical Dilemmas and Dimensions in Penetration Testing/. 10.13140/RG.2.2.31581.51688.

[32] Saha. Sanchita & Das Abhijeet & Kumar, Ashwini & Biswas, Dhiman & Saha, Subindu. (2020). Ethical Hacking/ Redefining Security in Information System. 10.1007/978-981-15-0361-0_16.