ETHICAL HACKING: Need of Security

SHUBHAM PATIL[1], AKSHATA DHOLE[2], ANUJA NILAK[3], ROHAN POL[4], POURNIMA KAMBLE[5]

Student, Computer Technology, Bharati Vidyapeeth Institute of Technology, Maharashtra, India[1,2,3,4]

Professor, Computer Technology, Bharati Vidyapeeth Institute of Technology, Maharashtra, India[5]

ABSTRACT

Cybercrime is a computer oriented crime that involves a computer and a network. Cybercrimes include most of the times profit oriented criminal activities. Hacking is the set of instruction using which we can interrupt between the client and server. In Intentional hacking hackers who attacks on the any client servers with the moto to harm the system and communication between the server's Unintentional hackers are those who may sometimes intemperate laws but doesn't have intention to harm or to steal. These type of hackers either work with an organization or under government. In this, we have explained different types of hacker in detail and how the systems are basically hacked by the hackers and how the positive and negative side of the hacking.

Keywords: *hacking, vulnerability, spoofing, sniffing.*

1. INTRODUCTION

Hacking This crime is related to the act of gaining illegal access to a computer system or network and some time making unauthorized use of such access. Also, it is the act by which other forms of cyber-crime like fraud, terrorism, etc. are committed. Hacking is one of the most well-known types of computer crime. A hacker is someone who find out and exploits the weaknesses of a computer system or network.

It is referring to the unauthorized access of another's computer system. To put programs into system known as viruses, worms, and Trojan Horses that can shut down or destroy an entire computer network.

Hacking is also carried out as a way to take credit card numbers, internet password, and other personal information. By accessing the address of person, hackers are able to steal these types of items from millions of internet users all at once. Hacking is also having some advantages such as we can spy on terrorism and stop the harm before the damage. Also hacking can be use in big companies to test security measures. Teaching Hacking techniques to students make them prepare for any type of hacker attack on their system. Also using hacking techniques, we can create the best type of security to maintain the information and network. The top security designers are hackers who creates security measurements for companies.

2. LITERATURE REVIEW

Fortinet global security strategist Derek Manky pointed out "Every minute, we are seeing about half a million attack attempts that are happening in cyber space" [1]. In addition, hackers are launching more sophisticated attacks on every possible weakness in our computer network system and trying to damage or crush our security system.

In cybersecurity education are concentrating on defensive techniques such as cryptography, intrusion detection, firewalls, and access control or offensive techniques such as buffer overflow attacks, exploitation, and post-exploitation [2]. conducting hands-on ethical hacking that exist in computer systems is the first and the most important step in protecting our security system.

A user study by Garfinkel and Miller [3], states that many users may still be vulnerable in spite of having strong passwords. The future is life bounded in internet hence, security is the most important factor to be taken care of. This is why people should learn ethical hacking.

Ethical hacking entails the usage of same tools and practices the bad guys make use of, however it also involves wide range forefront planning, a set of precise tools, multifaceted testing methodologies [4], and adequate report to fix any problems before the bad guys exploit our privacy.

3. METHODOLOGY

Hacker is the person who steals user name and password of authorized users account and tries to get entry into it and access that account or software. Usually hacker is expert in programming and its related problems. Hacking is one of most well-known type of crime in world. Hacking is the process of modification of the features of the system for achieving the goal of a person who is outside the system. Hacking usually involves illegally gaining access to commercial database, one or more computer, take them offline or online either for malicious purposes or financial gain. Hacking is the life style of hackers.

Hacking is carried out as a way to talk credit card no, internet passwords, other personal information. Hackers are able to steal these type of items from millions of internet users.

Techniques of ethical hacking:

1)Information gathering: The analyzers gather as much data about the web application as could be allowed and gain comprehension of its rationale.

2) Vulnerability scanning: Web server vulnerabilities, confirmation instrument vulnerabilities, input-based vulnerabilities and work particular vulnerabilities are analyzed.

3)Exploitation: The analyzers ought to have a smart thought of the zones that is destined to be directed for misuses. With the rundown

of vulnerabilities available, the two applications were then misused.

4)Test Analysis: It is essential that the objective substance knows about commonplace assailant usual way of doing things, procedures and devices assailants depend on, abuses they utilize, and any unnecessary introduction of information the objective is experiencing.

There are different types of hackers:

1) **White Hat Hacker**

    White hacker is also known as "Ethical Hacker". He is the Computer Security specialist and because of that they know about computer networks and security provided by the system. He is the person who spends lots of time to find hacking

    White hat hackers are capable of making changes to the hardware and software of system. They do not hack the system with bad intentions but hack for checking the security of the system. White hackers use their skill to benefit the society. Big companies who feels the importance of computer security signs white hackers for checking of their security.

2) **Black hat hacker**

    Black hat hackers are also known as "Crackers or Dark-side hackers". They also known as "social misfits" and "criminals". They enter into the computer or network with malicious intention in authorized or unauthorized way.

    They are cybercriminals whose intent is entirely malicious without invitation. They plunder computer systems for their own gain at considerable expense to their victims. They destroy files, data etc. Black

hat hackers try to exploit all possible vulnerabilities before organization come to know the flaws in their computer security system.

They crack the bank account and modify it and steal the information for selling it into black market etc.

3) Gray hat hacker

A gray hat hacker is a person who is exactly between white hat hacker and black hat hacker. This person can use his skills either for legal or illegal acts. These people are actually on the "cutting edge" of the computer and network industry.
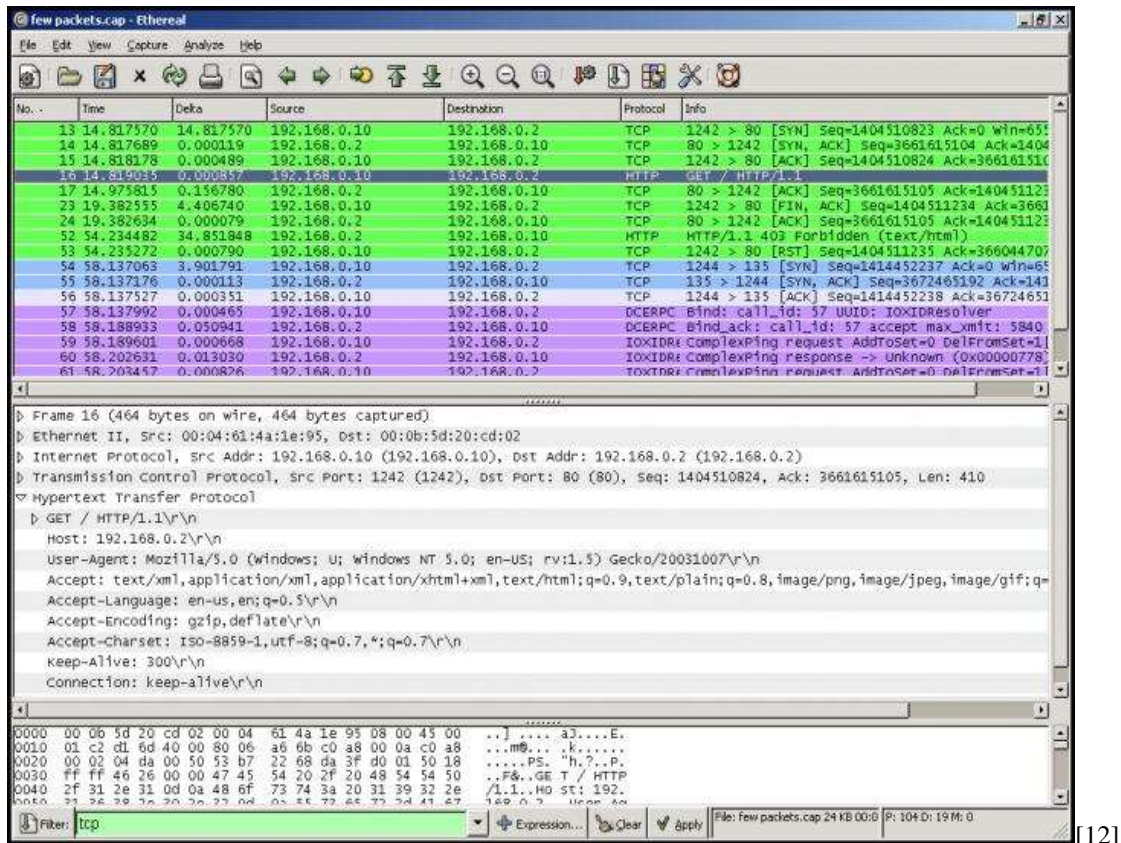
Gray hat hackers don't do this act for his personal gain. They try to prove that he is accomplished person in hacking. These hackers may hack into a computer system to notify the administrator that their system is vulnerable and then offer to repair it. They are doing it for a good purpose but still demanding personal gain. Once the person does it for money he becomes a black hacker.

Positive side of hacking

- Hackers are always very familiar with computer systems and can easily find the security vulnerabilities.

- Not all hackers do dirty works.

Negative side of hacking

- Destroy data or make the network unusable for those who are authorized to use the network with malicious intent or for personal gain.

- If a website is hacked, it may lose not only essential data but also a great no of customers because the website is not operational during that period.

- Because of viruses, worms, Trojan horse's entire computer system may hack.

- On the individual level, hackers may also able to gain unauthorized access into our computers to steal what we have stored such as credit card numbers, bank account details, address books or other personal, financial or business information

- If hackers hack any popular company then it damages its reputation, loss the information and because of hacking they have to suffer from financial loss.

- Illegal use of people identities is increase.

[12]

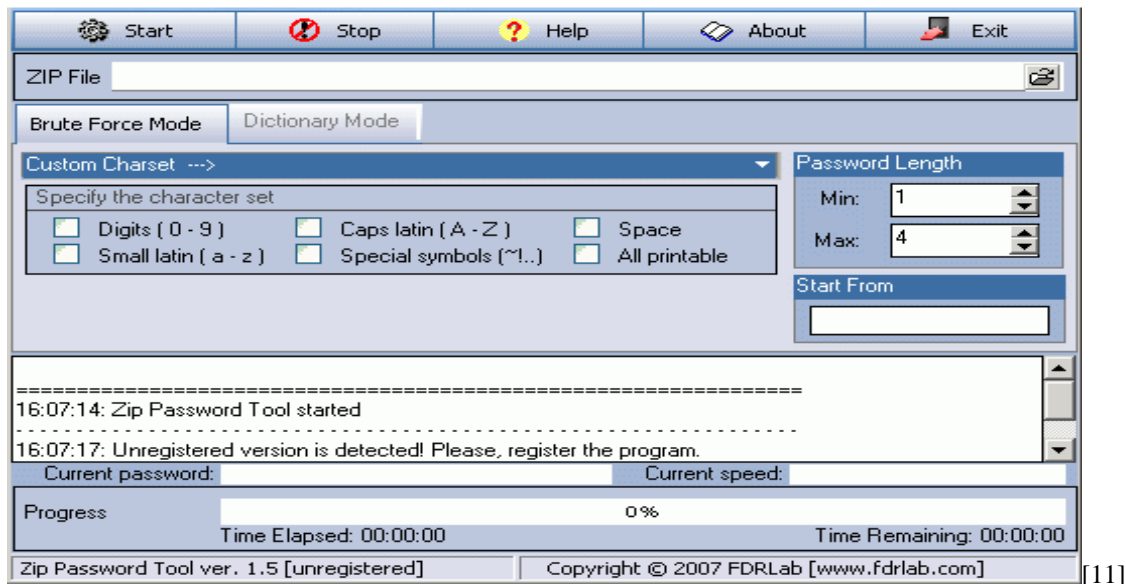
[12]

Fig 1: Wi-Fi Hacking Interface

[11]

Fig 2: Zip File Hacking Interface

6. Conclusion

Moral Hackers assist associations with understanding the present shrouded issues in their servers and corporate system. Moral Hacking is an apparatus, which if appropriately used, can demonstrate valuable for understanding the shortcomings of a system and how they may be abused. Hacking has the two its advantages and dangers. Programmers are extremely various. They may bankrupt an organization or may secure the information, expanding the incomes for the organization. What all depends is the intension of the programmer. It is relatively difficult to fill a hole amongst moral and pernicious hacking as human personality can't be vanquished, yet safety efforts can be fix.

7. REFERENCES

[1] H. Taylor, (2015, December 28), "Huge Cybersecurity Threats Coming in 2016," Retrieved from http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in- 2016.html

[2] M. Mink, and F. C. Freiling, "Is Attack Better Than Defense? Teaching Information Security the Right Way," Proceedings of the 3rd annual conference on Information security curriculum development, Kennesaw, Georgia, pp. 44-48, 2006.

[3] Simson Garfinkel and Robert Miller. Johnny 2: A user

test of key continuity management with s/mime and outlook express. Symposium on Usable Privacy and Security (SOUPS 2005), July 6-8, 2005, Pittsburgh, PA.

[4] Wiley Publications, "Introduction to Ethical Hacking," available at

www.media.wiley.com

[5] website: https://www.tutorialspoint.com/ethical_hacking/ethical_ha cking_reconnaissance.html

[6] Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer. Social Phishing. Magazine Communications of the ACM

[7] Website: http://www.digit.in/technology-guides/fasttrack-to-cyber- crime/the-12-types-of-cyber-crime.html

[8] Aaron Emigh. Online identity theft: Phishing technology, chokepoints and countermeasures. ITTC Report on Online Identity Theft Technology and Counter measures; http://www.anti- phishing.org/Phishing-dhs-report.pdf, October 2005.

[9] website: http://whatishacking.org/ What is Hacking?

[10] website: http://www.articlesbase.com/security-articles/ethicalhacking-an-introduction-402282.html

[11] Website: www.fdrlab.com Zip file Hacking Interface.

[12] Website: http://community.arubanetworks.com/t5/Controllerless-Networks/Wifi-Calling-Verizon-not-working-IAP-225-8-3-0-1/td-p/443758 Wi-Fi Hacking Interface.