ETHICAL HACKING

Dhruval Shah[1], Rajvi Shah[2], Aditya Nag[3]

[1,2,3]*Computer Department, Thakur College of Engineering and Technology, Maharashtra, India*

---***---

Abstract:- During the development of the Internet, computer security has become a major concern for businesses and governments. We live in security era, where we are securing all our belongings beneath different modes of lock however it's difficult within the case of system security. As nowadays all the information is available online, a large number of users are accessing it, some of them use this information for gaining knowledge and some use it to know how to use this information to destroy or steal the data of websites or databases without the knowledge of the owner. The state of security on web is becoming dangerous and it is becoming worse day by day. So to tackle all such problems "Hackers" come into picture. They are called as Ethical Hackers. This paper describes what is hacking, who are hackers, what is their code of conduct and in what way they are helpful to the society. This paper will also highlight the opportunities in the field of Ethical Hacking.

Keywords:- Hackers, Ethical Hackers, security

1. INTRODUCTION

As the computer technology advances, it has its darker side also; HACKERS. In today world the size of the internet is growing at a very fast rate, a large amount of data is moving online, therefore, data security is the major issue. Today, you'll be able to notice certified moral Hackers operating with a number of the best and largest firms across industries like tending, financial, government, energy and much more!!

Nowadays an outsized range of firms, organizations, organizations, banks, and websites are targeted by the various types of hacking attacks by the hackers. Generally, after hearing the term hacker we all think of the bad guys who are computers experts with bad intensions, who tries to steal, leak or destroy someone's confidential or valuable data without their knowledge. They are the persons with very high computer skills who tries to break into someone else security for gaining access to their personal information, but all the times it is not like that. To overcome the risk of being hacked by the hackers we have Ethical Hackers in the industry, who are also computer experts just like the hackers but with good intensions or bounded by some set of rule and regulations by the various organizations.

1.1 What Is Hacking?

Hacking is that the technique of finding the weak links or loopholes within the laptop systems or the networks and exploiting it to achieve unauthorized access to information or to alter the option of the target computer systems or the networks. Hacking describes the modification within the hardware, code or the networks to accomplish certain goals that don't seem to be aligned with the user goals.. In contrast, it is also called breaking into someone's security and stealing their personal or secret data such as phone numbers, credit card details, addresses, online banking passwords etc. Hackers are classified into three groups:

1. White Hat Hackers
2. Black Hat Hackers
3. Grey Hat Hackers

1.2 What is Ethical Hacking?

With the expansion of the web, pc security has become a significant concern for businesses and governments. They want to be ready to profit of the web for electronic commerce, and alternative pursuits, however they're troubled concerning the likelihood of being hacked.

In the seek for how to approach the matter, organizations came to comprehend that one amongst the most effective ways in which to guage the unwelcome person threat to their interests would be to have freelance pc security professionals decide to burgled their pc systems. This theme is comparable to having freelance auditors inherit a corporation to verify its accountancy records. In the case of pc security, these tiger groups or moral hackers would use an equivalent tools and techniques because the intruders, but they would neither damage the target systems nor steal information. Instead, they might appraise the target systems' security and report back to the homeowners with the vulnerabilities they found and directions for the way to remedy them.

Ethical Hacking ≈ Hacking   Ethical Hacking ≠ Cracking

2. Importance of Ethical Hacking

Government agencies and business organisation nowadays ar in constant would like of moral hackers to combat the growing threat to that security. A lot of government agencies, professional and corporations now understand that if you want to protect a system, you cannot do it by just locking your doors. New worms, malware, viruses, and ransom ware are multiplying every day and is creating a need for ethical hacking services to safeguard the networks of businesses, government agencies or defence.

The Code of Conduct of an Ethical Hacker: -

- **Identifying and determining the confidentiality and privacy of the data of any organization before**

- **The intensions of an ethical hacker must be very clear, that not to harm the client or organization.**

- **Working within the limits set by the client or the organization, do not go beyond them.**

- **After the hacking do not disclose the private or confidential findings during the hacking with others.**

- Identifying and determining the confidentiality and privacy of the data of any organisation before hacking and should not violate any rule and regulations.
- Before and after the hacking maintaining the transparency with the client or owner of the organisation.
- The intension of an ethical hacker must be very clear, that not harm the client or organisation.
- Working within the limits set by the client or the organisation, do not go beyond them.
- After the hacking do not disclose the private or confidential findings during the hacking with others.

Need of Ethical hacking in Industry:

As every organisation has its own confidential information which may be hacked by the malicious hackers or can be broken by them thus so as to guard that information the organisations heir moral hackers and permit them to hack their own systems ethically any find flaws or loopholes in their systems and proper them before any hacker hacks it.

3. Techniques of Ethical Hacking

- Information Gathering
- Vulnerability scanning
- Exploitation
- Test Analysis
- Information Gathering

In this step, the testers collect as much information about the web application as possible and gain understanding of its logic. The information gathered will be used to create a knowledge base to act upon in later steps. The testers should gather all information even if it seems useless and unrelated since no one knows at the outset what bits of information are needed. This step can be carried out in many different ways: by using public tools such as search engines; using scanners; sending simple HTTP requests etc.

- Vulnerability Analysis

Using the knowledge collected from the information gathering step, the testers then scan the vulnerabilities that exist in the web application. The testers can conduct testing on configuration management, business logic in this step, web server vulnerabilities, authentication mechanism vulnerabilities, input-based vulnerabilities and function-specific vulnerabilities are examined.

- Exploitation

After the vulnerability analysis, the testers should have a idea of the areas that will be targeted for exploits. With the list of vulnerabilities on hand, the two applications were then exploited.

- Test Analysis

It is the interface of the result, the testers and the target entity. It is important that the target entity is aware of attacker modus techniques and tools on which attackers rely on.

4. Footprinting

Footprinting is the art of finding/gathering information relating to the target to be attacked. For example, if someone wants to rob a bank that is done first is the bank's office is located, where the cashier used to save money, bank routes to escape preparation and various matters related to the target. This information is beneficial to a hacker who is trying to crack a whole system. The purpose is to accumulate as much information as possible, including the target's platform, application software technology, backend database version, configurations, and possibly even the network architecture/ topology.

Here are some key pieces of information that a security expert usually gathers about a website:

1. Related domains and subdomains

2. Technology and programming languages being used

3. Cached pages

4. Website history

5. Publically indexed files on search engines

6. Default pages and login forms

7. Related IP addresses

8. Other services running on those IP addresses

9. The version of the services/software being used

10. Publicly disclosed vulnerabilities in the software being used

11. Default users

12. Default passwords

13. Valid email address and usernames

5. Phishing Technique

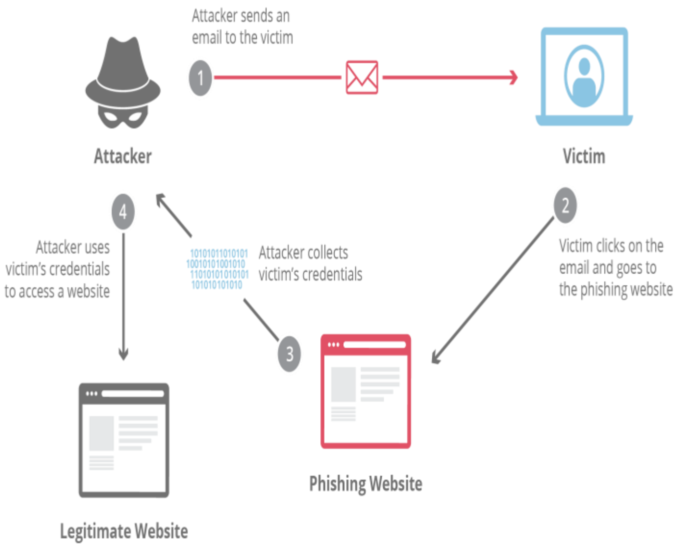
Phishing is a type of internet fraud that uses false or deceptive content to trick users and extract information from them. Phishing historically used e-mails as a medium to reach its target, but soon spread to other forms of communication like websites, SMS's

THE REASON WHY PHISHING PREVAILS?

1. Lack of computer system knowledge
2. Lack of knowledge of security indicators
3. Lack of understanding of the verification process

E-MAIL PHISHING

Phishing emails are messages designed to fool the recipient into handing over personal information, such as login names, passwords, credit card numbers, account credentials, social security numbers, etc. Fraudulent emails harm their victims through the loss of funds and identity theft. They also hurt Internet business, because people lose their trust in Internet transactions for fear that they will become victims of fraud.


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

How Phishing works.

Phishing attacks typically rely on social networking techniques applied to email or other electronic communication methods, including direct messages sent over social networks, SMS text messages and other instant messaging modes.

- z-shadow tool

What is Z-Shadow?

Z-Shadow is a website specially designed for hacking Facebook or other social site. like Facebook, gmail and many more. You just need to create an account on that website and have to copy the URL of the site which your victim uses. For example if you want to hack Facebook, then you just need to copy the URL of the fake Facebook page. Don't worry no account get bans or suspended because z-shadow is specially created for hacking. Now send this URL to your target, and when they click it, it opens up a new page which requires them to add

their ID and password. This page is backed by your Z-Shadow profile and when they their credentials to enter, they get hacked and you can get the results. Results will be available in your z-shadow account. Now you can easily use that ID and password for whatever you want to do.

- Anti-phishing and countermeasure

There are several methods to protect users from phishing attacks. But prevention is not enough. We need detection measures to get early warning signals when a phishing attack is being planned or is in progress.

The attacker needs to setup a look-alike site. First, a domain name is registered. Many times attackers register a domain which sounds similar to the original. If they are targeting www.abcbank.com attackers might register www.abccbank.com.

There is also a website www.phishtank.com where you can check by putting the site which you already have and phishtank will check throughout their database if such a website is marked as a phishing website. If you already know that the website is a phishing site you can also put up on phishtank and mark that website as phishing website.

6. Conclusions

The whole world is moving towards the enhancement of technology, and more, with this the risk of security increases.

This paper described about the hackers and ethical hackers who tried to illegally break into the security. In the ADPS, hacking plays a significant role because it deals with either side of being smart or unhealthy. Then in the next section it describe the importance and the techniques of ethical hacking. Further, this paper tells about how hackers enter into the system called as footprinting. It also describe about phishing which tells what is phishing, how does phishing works. In conclusion, it must be said that ethical hacking is a tool which can help in better understanding of the system and improving the security techniques as well.

REFERENCES

[1] https://www.researchgate.net/publication/271079090_ETHICAL_HACKING_Tools_Techniques_and_Approaches

[2] Bansal, A., & Arora, M. (2012). Ethical Hacking and Social Security. Radix International Journal of Research in Social Science, 1(11), 1-16

[3] https://www.researchgate.net/publication/316431977_Ethical_Hacking_and_Hacking_Attacks

[4] Study of Ethical Hacking a paper by (Bhawana Sahare, Ankit Naik, Shashikala Khandey) http://www.ijecs.in/issue/v4-i4/68%20ijecs.pdf

[5] *"FootPrinting-First Step of Ethical Hacking"*.