International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Review on Ethical Hacking

M. Subaa Shree[1]*, C. P. Kanishka Varshini*[2]

[1,2]*Sri Krishna College of Arts and Science,Coimbatore,Tamil Nadu*

ABSTRACT

Ethical hacking is the process of attempting to gain unauthorized access to digital systems or networks with the purpose of finding and patching security vulnerabilities. An ethical hacker is an individual who is authorized to test the security of a system in order to discover any potential weaknesses or vulnerabilities. The goal of ethical hacking is to assess the security posture of a system or network and to identify any potential risks or threats. Ethical hackers use a variety of tools and techniques to identify weaknesses in a system or network and to assess the security posture. These tools and techniques include port scanning, vulnerability scanning, password cracking, social engineering, and malware analysis. Once any potential threats have been identified, the ethical hacker will work with the system owners to implement countermeasures and mitigate any risks or threats. Ethical hacking is an important part of the overall security posture of any system or network. By identifying and patching security vulnerabilities, the risk of unauthorized access or exploitation can be significantly reduced.

Keywords: Authorized–to give someone official permission to do something, assess–Risk management process us for identity, Malware – Group of virus helps to hack the computer, Mitigate – To make something less serious, exploitation – To threat somebody

1. Introduction

In this article, ethical hacking is reviewed. Assessing and locating the holes that a hostile hacker may exploit in a digital system is part of the practise of ethical hacking. These flaws give the malevolent hacker an easy path to get access and damage the victim's system or reputation. So, a trained ethical hacker would strengthen the current security measures while identifying any potential vulnerabilities. In order to protect people, businesses, or governments from the possibility of hostile hacking and security breaches, hackers must uphold ethical standards. Additionally, ethical hacking is carried out with the concerned clients' approval to increase the security of their internet presence.

Online CEH training is a great approach to comprehend, apply, and learn how to execute ethical hacking properly. You may acquire a variety of skills from these training classes, as well as how to use them and protect sensitive information online.

This useful essay will provide you a thorough overview of ethical hacking so you can comprehend the essential ideas involved. Additionally, it will provide a thorough distinction between harmful and ethical hackers.

Consist of

HACKERS

WHITE HACKERS

BLACK HACKERS

GREY HACKERS

1.1 HACKERS

Hackers (H-Hide IP, A- Aim Victim, C-Crack Encrypt, K- Kill Firewall, E- Enter System, and R- Return Anonymous). Many people wrongly think that a "hacker" is a self-taught genius or rogue programmer skilled at changing computer hardware or software so that it may be used in ways different from how the original creators intended. However, this is a constrained viewpoint that falls well short of addressing the vast array of reasons why someone could decide to hack. To learn about the many motives that various types of hackers may hold, read Under the hoodie: why money, power, and ego drive hackers to cybercrime. There are three different types of hackers.

- WHITE HACKERS
- BLACK HACKERS
- GREY HACKERS

1.1.1. WHITE HACKERS

In simple terms, a white chapeau hacker is a hacker who's fairly hired by an association or person to hack their information architectures to find possible sins. While these people designedly transgress security systems, they're pacing with authorization, which distinguishes them from other hackers, including hacktivists.

The term “ white chapeau ” refers to old Western pictures The good guys would generally wear white headdresses while the bad guys would wear black. In the realm of computer hacking, numerous white headdresses are former black chapeau hackers who moved on to legal and ethical hacking for one reason or another.

Unlike other cybercriminals, white headdresses help associations perform vulnerability assessments and notify the companies responsible for creating patches of any sins. rather of playing for information and particular or political gain, white chapeau hackers break into systems to increase safety and reduce vicious attacks.

1.1.1.1. Techniques used by White hackers:-

a) Social engineering

b) Penetration Testing

c) Reconnaissance and Research

1.1.1.2. SOCIAL ENGINEERING

Since the dawn of time, social engineering and confidence tactics have been a human culture component. Although the scheme has been modified to include technology, the principle remains the same: exploiting natural human behavior is simpler than pushing your way in. Social engineering, in ethical hacking, has become a common (and extremely effective) method of determining how accessible an organization’s employees are. Cybersecurity certificate programs cover this technique and related strategies in detail.

Social engineering can help you uncover gaps and effectively handle employee security concerns when applied ethically. A social engineering mandate also aims to establish methods to enhance the international degree of confidentiality, integrity, and accessibility of your company’s data.

1.1.1.2. PENETRATION TEST

A penetration test (pen test) mimics an online attack on your computer in order to identify weak spots. In the field of online application security, penetration testing is widely employed as an addition to a web application firewall. (WAF). In order to uncover flaws, such as unsanitized inputs that are vulnerable to code injection attacks, pen testing involves attempting to break into various application systems (such as APIs, frontend/backend servers). You may use the penetration tester's findings to enhance your WAF security protocols and fix any vulnerabilities that were found.

1.1.1.3. RECONNAISSANCE AND RESEARCH

An important step in ethical hacking is collecting intelligence and knowing the target machine. Reconnaissance is a collection of processes and methods (such as footprinting, scanning, and enumeration) used to uncover and gather knowledge of the target device secretly.

1.1.2. BLACK HACKERS

Black hat hackers are crooks that penetrate computer networks bypassing security measures. Their main objective is to gain money, although they occasionally engage in corporate espionage or activism as well. They frequently strive to change or delete data in addition to stealing it, depending on their objectives. Any age, gender, or race may be a member of this group. Although many cybercriminals are novices, some of them may be computer geniuses. Of course, not everyone is capable of creating intricate exploit chains, but certain assaults don't need to be highly sophisticated in their design. They are adept at social engineering as well. Although they may appear to be hoodie-clad loner types who spend their days in front of a screen, they are actually highly skilled at persuasion the victims of the files

Techniques used by Black hat hackers:-

a) Malware creation

b) Unavailability of services

c) Perform social engineering scams

d) Steal confidential information

e) Phishing attacks

f) Exploit security flaws

g) Installing spyware

1.1.2.1. MALWARE

Black hat creates and distribute malware in order to weaken the security posture of a system or device. Trojan horses are a common type of malware. Some types malwares are (fig1.1)

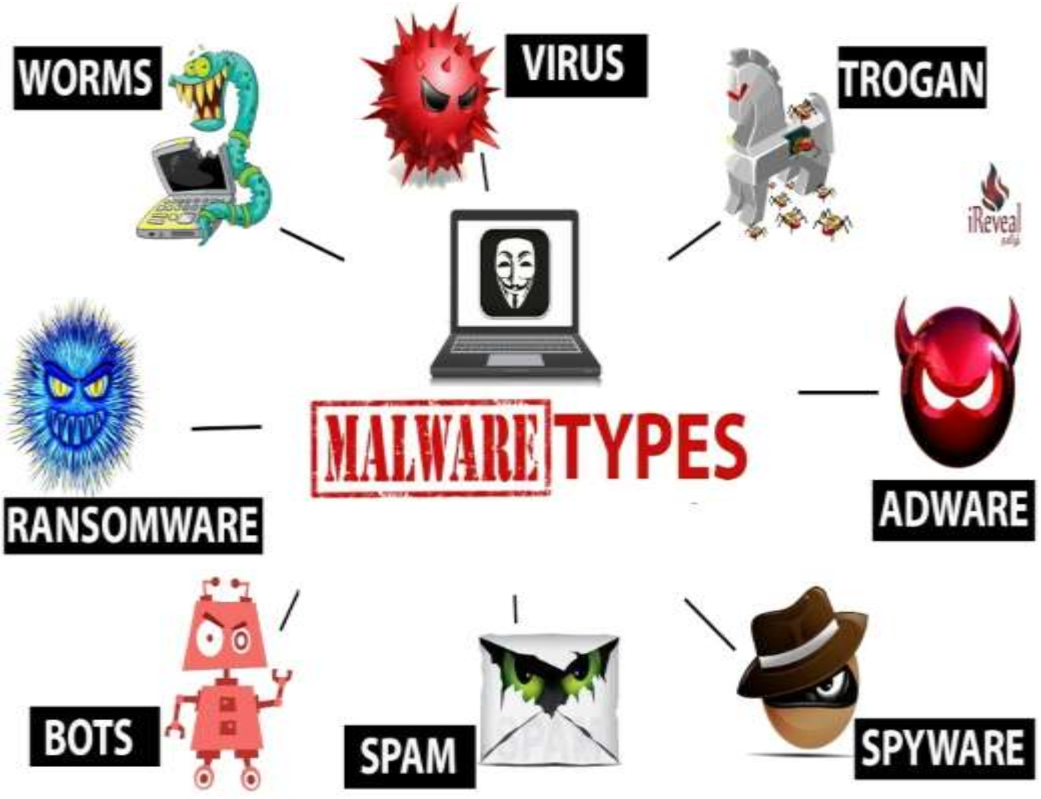


Fig 1.1

1.1.2.2. UNAVAILABILITY OF SERVICES:-

Black hat hackers perform DDoS assaults on government websites and servers to obstruct business, create unrest, and wreck havoc.

1.1.2.3. PERFORM SOCIAL ENGINEERING SCAMS:-

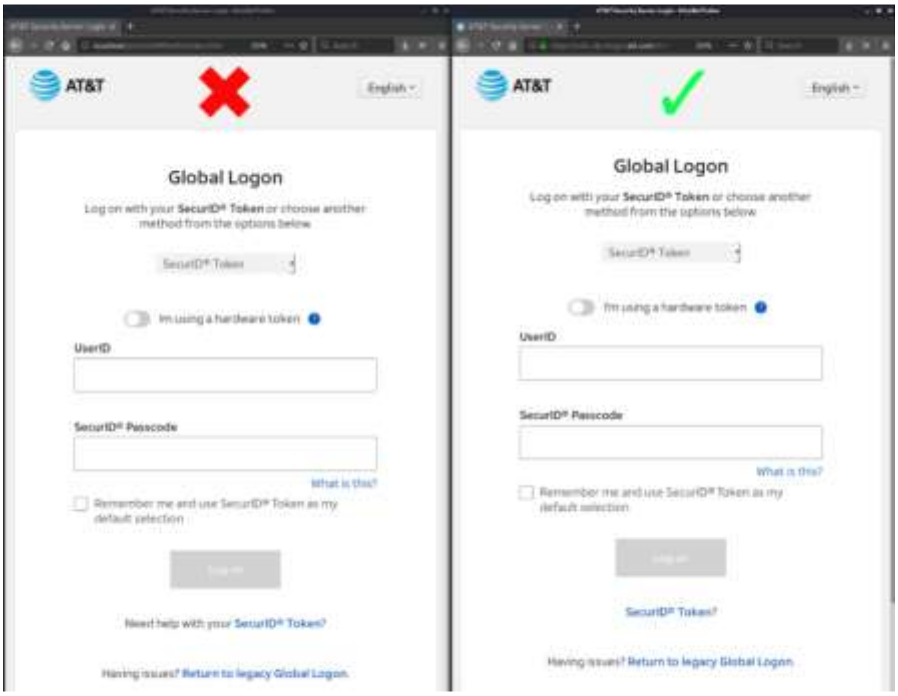
In order to trick you into providing private or financial information that they may exploit fraudulently, black hat hackers construct fictitious social media profiles of individuals you trust. Black hat hackers could potentially guess your login information and get around security safeguards using the information you publish online.

1.1.2.4. STEAL CONFIDENTIAL INFORMATION:-

These hackers steal user information like credit card numbers, aadhar numbers, pan card numbers, etc. by breaking into databases that have security flaws

1.1.2.5. USE PHISHING ATTACKS:-

Black hat hackers use a range of social engineering methods to persuade individuals into doing things they shouldn't in order to distribute malware or scam people. Phising page and original page contrasted. Example:-Fig 1.2



Global Logon

Log on with your **SecurID® Token** or choose another method from the options below

SecurID® Token

I'm using a hardware token

UserID

SecurID® Passcode

What is this?

□ Remember me and use SecurID® Token as my default selection

Need help with your SecurID® Token?

Having issues? Return to legacy Global Logon.

Global Logon

Log on with your **SecurID® Token** or choose another method from the options below

SecurID® Token

I'm using a hardware token

UserID

SecurID® Passcode

What is this?

□ Remember me and use SecurID® Token as my default selection

SecurID® Token?

Having issues? Return to legacy Global Logon.

Fig 1.2

1.1.2.6. Utilize security holes

Black hat hackers are continuously searching for weaknesses to discover methods to take advantage of them for their own gain. As a result, black hat hackers find it simple to exploit users of outdated OS versions, software, plug-ins, applications, etc.

1.1.2.7. Installation of spyware:

Black hat hackers extort their victims by installing malware on their computers. They might follow the whereabouts of their targets using such malware. This kind of virus can take screenshots of users' activities or provide the hacker direct access to the displays of their devices. The black hat hacker may decide to frighten victims if they refuse to pay the ransom after entering the system.

1.3 GREY HACKERS

The term "gray hat hacker" (sometimes spelt "grey hat hacker") refers to someone who may transgress moral or ethical guidelines without having the harmful intent associated with black hat hackers. Gray hat hackers may participate in actions that don't appear entirely legal, yet they frequently work for the greater benefit.

The Techniques Grey Hackers Use:-

1)Social Engineering

2)Testing For Penetration

3)Reconnaissance and research

4)Programming

5)Using a variety of digital and physical tools

1) Social Engineering:-

Social engineering, sometimes known as "people hacking," is a typical tactic used by white hat hackers to identify gaps in an organisation's "human" defences.The goal of social engineering is to manipulate and deceive victims into acting inappropriately. (making wire transfers, sharing login credentials, and so on).

2) Testing For Penetration:-

Penetration testing seeks to identify endpoint and defence vulnerabilities and weaknesses so that they may be fixed.

3) Reconnaissance and research:-

This entails investigating the company to find weaknesses in the IT and physical infrastructure. The goal is to gather enough knowledge to find lawful ways to get around security measures and controls without causing harm or breaking anything.

4) Programming:-

White hat hackers build honeypots that work as ruses to entice online criminals, divert them, or assist the white hats in learning crucial details about the attackers.

5) Using a variety of digital and physical tools:-

This comprises the tools and equipment that enable the penetration testers to access the servers or network and install malware such as bots.

References

1. https://www.sciencedirect.com/topics/computer-science/black-hat-hacker
2. https://www.saintleo.edu/about/stories/blog/ethical-hacking-do-you-have-what-it-takes
3. https://www.avast.com/c-hacker-types
4. https://www.synopsys.com/glossary/what-is-ethical-hacking.html#:~:text=Ethical%20hacking%20involves%20an%20authorized,and%20actions%20of%20malicious%20attackers
5. https://techjury.net/blog/what-is-a-black-hat-hacker/#gref