****

**sIMATS ENGINEERING**

**SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES**

**CHENNAI-602105**

**CAPSTONE PROJECT**

**SOFTWARE ENGINEERING.**

**TITLE**: **DEVELOPING A PLATFORM FOR ETHICAL HACKING CHALLENGES AND LEARNING.**

**SUBMITTED BY:**

**ABHILAASH B (192365076)**

**CSA1087- SOFTWARE ENGINEERING FOR WEB DEVELOPMENT**

**UNDER SUPER VISION OF:- DR.R.GEETHA**

**Developing a platform for ethical hacking challenges and learning.**

**ETHICAL HACKING:-**

 Ethical hacking is the practice of using hacking techniques for legal and constructive purposes. Ethical hackers, often referred to as "white hat hackers," are cybersecurity professionals who test the security of computer systems, networks, or software to identify vulnerabilities. The goal is to help organizations strengthen their defenses against malicious hackers (black hat hackers). also known as penetration testing or "pen testing," is the act of deliberately probing computer systems, networks, or applications to find security vulnerabilities that could be exploited by malicious actors. Ethical hackers work proactively to identify and address weaknesses before attackers can exploit them.

**Key Points About Ethical Hacking:-**

1. **Authorized**: Ethical hackers work with permission from the system owner or organization.
2. **Preventive**: They simulate attacks to find and fix security weaknesses before real attackers can exploit them.
3. **Legal**: Ethical hacking is done under a legal framework and adheres to rules and regulations.
4. **Skills**: Ethical hackers use the same tools and techniques as malicious hackers but for good purposes.
5. **Certification**: Many ethical hackers hold certifications like CEH (Certified Ethical Hacker) or OSCP (Offensive Security Certified Professional) to demonstrate their expertise.

**Example:-**

Imagine a company hires an ethical hacker to test the security of its online banking system. The hacker might try to break into the system, find weak points, and report these to the company. The company can then fix the vulnerabilities to ensure its customers' data stays safe.

In essence, ethical hacking is like hiring a "friendly burglar" to test the locks and doors of a house to make it more secure!

**Advantage of Ethical Hacking :-**

* This helps to fight against cyber terrorism and to fight against national security breaches.
* This helps to take preventive action against hackers.
* This helps to build a system that prevents any kinds of penetration by hackers.
* This offers security to banking and financial establishments.
* This helps to identify and close the open holes in a computer system or network.

**Disadvantage of Ethical Hacking :-**

* This may corrupt the files or data of an organization.
* They might use information gained for malicious use. Subsequently, trustful programmers are expected to have achievement in this framework.
* By hiring such professionals will increase costs to the company.
* This technique can harm someone’s privacy.
* It hampers system operation

**Types of Ethical Hacking:-**

**Grey Hat Hacking**

**White Hat Hacking**

**Black Hat Hacking**

**WHITE HAT HACKER:-**

White hat hacker -- or [ethical hacker](https://www.techtarget.com/whatis/video/An-explanation-of-ethical-hackers) -- is an individual who uses hacking skills to identify security vulnerabilities in hardware, software or networks. However, unlike [black hat hackers](https://www.techtarget.com/searchsecurity/definition/black-hat) -- or malicious hackers -- white hat hackers respect the rule of law as it applies to hacking. Many white hat hackers are former black hat hackers. The terms come from old Western movies, where heroes often wore white hats and the bad guys wore black hats.

White hat hackers only seek vulnerabilities or exploits when they are legally permitted to do so. White hat hackers may do their research on open source software, as well as on software or systems they own or have been authorized to investigate, including products and services that operate [bug bounty programs](https://www.techtarget.com/whatis/definition/bug-bounty-program). These types of programs reward individuals with money for disclosing security flaws.

Unlike black or gray hat hackers, white hat hackers fully disclose all the vulnerabilities they find to the company or product owner who is responsible for fixing the flaws so the issues can be resolved before they are exploited by malicious hackers.

White hat hackers, especially those performing external penetration tests (pen tests), use the same hacking techniques and tools as black hat hackers. But white hat hackers do so with the intent of helping an organization improve its security posture.

Some white hat hackers used to be black hat hackers who became more ethically attuned as they matured; others were caught and then decided to take the ethical hacker path to pursue their interests without the threat of prosecution.

**BLACK HAT HACKER:-**

Black Hat Hackers refers to hackers with malicious intentions who gain unauthorized access to computer networks and systems. Black hat hackers aim to exploit security vulnerabilities in software or corporate systems. This is often to achieve financial gain by holding organizations to ransom or by selling data to third-party businesses and other cyber criminals. There are different types of black hat hackers, from those who act alone to those who operate within large, highly profitable cyber crime organizations. Many black hat hackers started out as so-called "script kiddies," who set out to exploit security vulnerabilities then evolved their techniques to make quick money. The upper levels of the black hat security world are skilled hackers working for sophisticated cyber crime organizations, which often work in the same way as legitimate businesses. These organizations have partners, resellers, and vendors with whom they buy and sell [**malware**](https://www.fortinet.com/resources/cyberglossary/malware) licenses for use by other criminal organizations around the world. Many Black Hat hackers started as novice "script kiddies" using purchased hacker tools to exploit security lapses. Some were trained to hack by bosses eager to make a fast buck. The upper echelon of Black Hats tends to be skilled hackers who work for sophisticated criminal organizations that sometimes provide collaboration tools for their workers and offer service agreements to customers, just like legitimate businesses.

**GREY HAT HACKER:-**

There are many [types of hackers](https://www.shiksha.com/online-courses/articles/types-of-hackers-to-be-aware-of/), each known by a different colour 'hat.' These colours indicate what they stand for and how they operate. For example, red hat hackers are about strong defence, and green hats are learners. The most commonly talked about are [black hat and white hat hackers](https://www.shiksha.com/online-courses/articles/difference-between-white-hat-vs-black-hat-hackers/). Black hats are the troublemakers, causing harm, breaking into systems, stealing data, or causing damage, often for their benefit. On the other hand, white hats are the good ones - they hack into systems, but only to find weaknesses, fix them, and work within the law. But there's a mix of these two: the grey hat hacker, a.k.a, gray hat hacker.

A grey hat hacker is an individual who engages in hacking activities without explicit owner's permission but with non-malicious intent. These individuals aim to identify and expose vulnerabilities in computer systems or networks to help organizations improve their security.

Grey hat hackers are often motivated by a combination of factors. Some may be driven by the thrill of breaking into secure systems and proving their skills. In contrast, others may aim to improve cybersecurity (a system's or network's security) by identifying vulnerabilities and reporting them to the appropriate parties.

Additionally, some grey hat hackers may receive compensation for their efforts, such as monetary rewards or job offers from companies looking to improve their security.

**Challenges Faced by Ethical Hacker:-**

 Rapidly Evolving Threat Landscape

* Cyber threats and hacking techniques evolve constantly, requiring ethical hackers to stay updated with the latest vulnerabilities, exploits, and defense mechanisms.
* Tools and frameworks used for penetration testing also need frequent updates to keep up with attackers.

**Lack of Proper Scope Definition**

* Clients may fail to define clear objectives or scope for penetration testing, which can lead to legal risks or missed vulnerabilities.
* Scope limitations might prevent ethical hackers from thoroughly testing all aspects of a system.

**Legal and Compliance Issues**

* Navigating legal frameworks can be challenging, especially when working internationally, where laws on penetration testing and cybersecurity vary.
* Ethical hackers must ensure they have proper authorization and comply with industry standards like GDPR, PCI DSS, or ISO 27001.

**Limited Access or Resources**

* Ethical hackers might be restricted by the tools, resources, or permissions provided by the client, limiting the effectiveness of their work.
* In some cases, organizations may underestimate the complexity of penetration testing and fail to allocate sufficient time or budget.