**A**

**Technical Seminar Report on**

**GRAY HAT HACKING**

**Submitted to the Dept. of Information Technology, SNIST**

**in the partial fulfillment of the academic requirements for the award of**

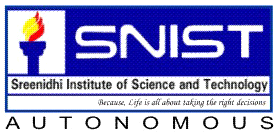
**B.Tech (Information Technology)**

**under JNTUH**

**by**

**RAHUL TEJA B**

**18311A12J8**



**Department of Information Technology**

**School of Computer Science and Informatics**

**SreeNidhi Institute of Science and Technology (An Autonomous Institution)**

**Yamnampet, Ghatkesar Mandal, R. R. Dist., Hyderabad – 501301**

**affiliated to**

**Jawaharlal Nehru Technological University Hyderabad**

**Hyderabad – 500 085**

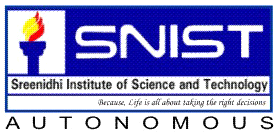
**2020–2021**

**Department of Information Technology**

**School of Computer Science and Informatics**

**SreeNidhi Institute of Science and Technology (An Autonomous Institution)**

**Yamnampet, Ghatkesar Mandal, R. R. Dist., Hyderabad – 501301**



**Certificate**

**This is to certify that the Technical Seminar report on “GRAY HAT HACKING” is a bonafide work carried out by RAHUL TEJA B Roll No 18311A12J8 in the partial fulfillment for the award of B.Tech degree in Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, affiliated to Jawaharlal Nehru Technological University Hyderabad (JNTUH), Hyderabad under our guidance and supervison.**

**The results embodied in the Technical seminar have not been submitted to any other university or Institute for the award of any degree or diploma.**

**Internal Guide Head of the department Ch.Vijaya Bhaskar Dr.V. V. S. S. S. Balaram**

**CONTENTS**

|  |  |
| --- | --- |
| Abstract |  |
| 1.Introduction |  |
| 2.Types of hackers |  |
| 3.Gray hat hacking |  |
| 4.Types of hacking |  |
| 5.Advantages |  |
| 6.Disdvantages |  |
| 7.Prevention  8.Applications |  |
| 9.Conclusion |  |
| 7.References |  |

**1.Introduction:**

The dictionary of Cambridge University Press defines hacking as ‘the activity of using a computer to access information stored on another computer system without permission of the owner, or to spread computer virus.’ Hacking refers to using one’s expertise in Networking and Computer skills to manipulate the normal behavior of a particular system and other systems connected or associated with it. It is an attempt to gain access to a computer’s network security systems which, as mentioned, may or may not be with a prior permission. Hacking also refers to finding loopholes in any system to break into that particular system or to control the access. Having one’s computer system hacked can have serious consequences if not dealt with in a sensible manner. The consequences may include stealing, deletion or manipulation of data and even locking out of authorized users. The concept of hats which is quite famous in communicating about the ethical inclination behind hacking prevails in the Cyber Security field. It refers to the classification of different types of ‘Hacking’.

**2.Types of hackers**

There are typically four key drivers that lead to bad actors hacking websites or systems: (1) financial gain through the theft of credit card details or by defrauding financial services, (2) corporate espionage, (3) to gain notoriety or respect for their hacking talents, and (4) state-sponsored hacking that aims to steal business information and national intelligence. On top of that, there are politically motivated hackers—or hacktivists—who aim to raise public attention by leaking sensitive information, such as Anonymous, LulzSec, and WikiLeaks.A few of the most common types of hackers that carry out these activities involve:

### Black Hat Hackers

Black hat hackers are the "bad guys" of the hacking scene. They go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage, or as part of a nation-state hacking campaign. These individuals’ actions can inflict serious damage on both computer users and the organizations they work for. They can steal sensitive personal information, compromise computer and financial systems, and alter or take down the functionality of websites and critical networks.

### White Hat Hackers

White hat hackers can be seen as the “good guys” who attempt to prevent the success of black hat hackers through [proactive hacking](https://www.fortinet.com/blog/industry-trends/proactive-hacking-to-build-better-security). They use their technical skills to break into systems to assess and test the level of network security, also known as ethical hacking. This helps expose vulnerabilities in systems before black hat hackers can detect and exploit them. The techniques white hat hackers use are similar to or even identical to those of black hat hackers, but these individuals are hired by organizations to test and discover potential holes in their security defenses.

### Grey Hat Hackers

Grey hat hackers sit somewhere between the good and the bad guys. Unlike black hat hackers, they attempt to violate standards and principles but without intending to do harm or gain financially. Their actions are typically carried out for the common good. For example, they may exploit a vulnerability to raise awareness that it exists, but unlike white hat hackers, they do so publicly. This alerts malicious actors to the existence of the vulnerability.

**3.Gray hat hacking**

Hackers who are considered worthy of a second chance by authorities are employed by ‘Bluescreen’, a cyber-security company in Plymouth. They work with the police against other hackers who they earlier used to see as their fellow brothers. Jack, employed there, was just 16 when the police raided his house as he had stolen information of 1000 people. Though for him, it was just an intellectual exercise and he had no intentions of putting that information.

**4.Types of hacking**

A resource (both physical or logical), called an [asset](https://en.wikipedia.org/wiki/Asset_(computing)), can have one or more [vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_(computing)) that can be [exploited](https://en.wikipedia.org/wiki/Exploit_(computer_security)) by a [threat](https://en.wikipedia.org/wiki/Threat_(computer)) agent in a threat action. As a result, the [confidentiality](https://en.wikipedia.org/wiki/Confidentiality), [integrity](https://en.wikipedia.org/wiki/Integrity) or [availability](https://en.wikipedia.org/wiki/Availability) of resources may be compromised. Potentially, the damage may extend to resources in addition to the one initially identified as vulnerable, including further resources of the organization, and the resources of other involved parties (customers, suppliers).The so-called [CIA triad](https://en.wikipedia.org/wiki/CIA_triad) is the basis of [information security](https://en.wikipedia.org/wiki/Information_security).The attack can be *active* when it attempts to alter system resources or affect their operation: so it compromises integrity or availability. A "*passive attack*" attempts to learn or make use of information from the system but does not affect system resources: so it compromises confidentiality.A threat is a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "accidental" (e.g., the possibility of a computer malfunctioning, or the possibility of an "act of God" such as an earthquake, a fire, or a tornado).A set of policies concerned with information security management, the [information security management systems](https://en.wikipedia.org/wiki/Information_security_management_system) (ISMS), has been developed to manage, according to [risk management](https://en.wikipedia.org/wiki/Risk_management) principles, the [countermeasures](https://en.wikipedia.org/wiki/Countermeasure_(computer)) in order to accomplish to a security strategy set up following rules and regulations applicable in a country.

**5.Advantages and Disadvantages**

There are always two sides to a coin. Educating an individual with the ins and outs of hacking with the objective to not maliciously use his skill can always turn out helpful but it also poses potential danger and threat of teaching the same skills to enable a hacker to hack with the wrong intent.System technology keeps developing and changing over time proceeding to a more elevated level. Operating frameworks need to keep up with the changes in the systems and adapt accordingly. Hacking needs to be approached and taught with keeping an ethical principle in mind. Those who want to educate themselves can do so through other means of learning which can exist .

**7.Prevention**

According to one definition of a grey-hat hacker, when they discover a vulnerability, instead of telling the vendor how the exploit works, they may offer to repair it for a small fee. When one successfully gains illegal access to a system or network, they may suggest to the system administrator that one of their friends be hired to fix the problem; however, this practice has been declining due to the increasing willingness of businesses to prosecute. Another definition of Grey hat maintains that Grey hat hackers only arguably violate the law in an effort to research and improve security: legality being set according to the particular ramifications of any hacks they participate in.[[](https://en.wikipedia.org/wiki/Grey_hat#cite_note-Cybercrime:_investigating_high-technology_computer_crime-5)

**8.Conclusion**

Taking into account what people with different opinions have to say, it is difficult to judge till what extent Grey-hat-hacking is acceptable and how it should be regulated. The argument about being harsh on the Grey-hat hackers is detrimental to company’s growth is completely reasonable. But also, if the law remains lenient, the magnitude of damage caused is huge, not only to the company but to every person, even to the one most distantly connected. Therefore, in the want of fast and free growth we cannot ignore the harsh consequences some unfortunate incidents can bring. Thus, the utilitarian argument fails here as social good and bad are equally possible by the act. Also, keeping in mind the Deontology theory and Aristotle’s theory, Greyhat-hacking cannot be acceptable. Breaking into a system sans permission cannot be acceptable and therefore Grey-hat-hacking cannot be legalized. Thus, Grey-hat-hacking, even if done with constructive intentions, doesn’t qualify to be legalized.

**9.Applications**

•Web application hacking will be booming with time

•As the complexity of software increases with time , there are chances of presence of presence of vulnerability in the software system

•So it is highly unlikely that the web application hacking will be facing any pity falls In the coming years

•Block unwanted traffic and protect

•Anti bot solution

**7.References:**

•<http://pages.cs.wisc.edu/~ace/media/gray-hat-hacking.pdf>

•<https://www.arsdcollege.ac.in/wp-content/uploads/2020/04/GE-4-1.pdf>

•Key loggers: <https://www.ijitee.org/wp-content/uploads/papers/v9i3/C8817019320.pdf>

•DOS: <https://www.youtube.com/watch?v=OWLGUgiz_eE>

•Phishing attack: <https://www.ripublication.com/ijaer19/ijaerv14n9_15.pdf>