**Abstract (I)**

Major Points:

1. What is Black/Grey/White Hacking

2. What is the ethical impact? (The difference between theft and protection)

3. Should it be taught? (CyberSec Majors)

4. MAIN QUESTION: Is Gray Hat Hacking Ethical? (Situations where it is/isn't and why it is/isn't)

**Methods (II)**

**Results (III)**

**Main Idea 1 – What are White/Black/Gray-Hat hackers?**

**What is Ethical Hacking? White Hat Hackers Explained.**

**Abstract:** Ethical hackers, on the other hand, are quite often employed by cyber security companies, or within the security departments of larger organizations. Large companies, particularly tech firms like Facebook, Microsoft, and Google, offer a reward to researchers or hackers who discover security holes within their networks or services. [...]bug bounty programmers can provide incredibly generous payouts for discovering major flaws – the current record-holder for the highest-value bug bounty is Google's $112,500 payment to a Chinese researcher who discovered a remote exploit vulnerability in Android.

**Notes:** What is White-Hat hacking? In essence, it is an ethical form of hacking, as opposed to Black-Hat hacking. White-Hat hackers include cyber security analysts and researchers who attempt to break through a systems defense for the purpose of enforcing it. This includes bug detection software. A White-Hat hackers’ job is to find the weakness in software and exploit it to later fix it. This is radically different than Black-Hat hackers who exploit weaknesses for monetary gain in the form of theft. A good example is from *What is Ethical Hacking? White Hat Hackers Explained*[1]. In it, it describes Charlie Miller, a prolific computer whizz and ethical hacker. He used his expertise to uncover major bugs in Apple’s MacBook Air that could have caused some serious issues for the computing firm. He would later find show weaknesses also in Apple’s Safari. These discoveries would earn him $15,000 total.

So, lets compare this Black-Hat hacking. Black-Hat hackers have one goal, to exploit weaknesses for selfish gain. In essence, it is remarkably similar to White-Hat hacking, in that exploitations are used for monetary gain. However, the difference is in how Black-Hat hackers are hack for self-serving reasons such as financial gain, revenge or simply, to wreak havoc. The main way Black-Hat hackers gain their money is through theft, fraud, and extortion[1]. This is a polar opposite to the White-Hat hacker’s methods and ideals for monetary accumulation. Black-Hat hacking is also illegal.

Finally, we have Gray-Hat hackers. This type of hacker falls in between Black and White-Hat hackers. Gray-Hats are as quick to protect a company as they are to hack in and commit theft from that same company. Gray-Hats often conduct slightly more morally questionable operations such as hacking groups that they are ideologically opposed to or launching hacktivist protests[1]. These kinds of hackers are primarily driven by curiosity, desire to make the world private and, of course, money. Only Gray-Hat and White-Hat hackers are considered to be ‘ethical’ hackers, as state in *What is Ethical Hacking? White Hat Hackers Explained*[1].

**NOTE: ALL ETHICS DISCUSSED IN *Discussion* SECTION**

**THIS SECTION IS PURELY RESEARCH (*Results*)**

**Main Idea 2 – What is their ethical impact and how do we discern from right and wrong?**

**White Hat, Gray Hat, Black Hat. (Main Idea 2)**

**Abstract:** "Part of the hard thing in government is that you're not really meant to question how things work," he said, adding the same goes for large companies. "You're expected to take orders and do things...[but] that's what [hackers] are here for, to question."

**Notes:** Now that we have discussed what these hackers are, lets discuss how they affect the world around them. In the beginning, most computer network crackers hacked a system simply because it was there. In today’s world, that is no longer the case. In the past several years, Black-Hat hackers have changed from script kiddies who deface web sites to spread worms to earn glory, to real sociopaths intent on doing more devious things, as stated by Dragos Ruiu in *White hat, Gray hat, Black hat* [2]. In fact, hackers secure their computers better than the rest of the computing community and Government agencies and industry could learn from their hacking and protection techniques to improve technology security. The government can learn from two groups as well, the White-Hats and Gray-Hats, who he says research vulnerabilities to protect employers’ and customers’ and who alert user to vulnerabilities. In fact, the government is already using hacker methods such as penetration testing , a search for security holes in a computer system, says Steven Manzuik [2]. This has also led to a multitude of good practices such as the issuing of information security regulations based in part on consultations with hackers, said Mark Loveless, a senior security analyst and BindView and a hacker of 25 years.

This proves that hackers’ importance as teachers is increasing. As software insecurity remains the norm, the number of targets increases and the stakes involved in losing control of financial and confidential data rises, experts say [2]. "Everything you forget, they will find," Roesch said. "It's like the proverbial millions of monkeys typing on typewriters. They have infinite resources and infinite time to find weaknesses in your system." Hackers’ impact on the world of computing is profound, and in some cases, not all that bad.

**NOTE: ALL ETHICS DISCUSSED IN *Discussion* SECTION**

**THIS SECTION IS PURELY RESEARCH (*Results*)**

<https://www.eff.org/pages/grey-hat-guide>

<https://ethics.acm.org/integrity-project/ask-an-ethicist/ask-an-ethicist-grey-hat-hacking/>

             Grey hat hacking occurs when a researcher in the computer science field unintentionally discovers a problem with a company’s  security but does not have permission from the company to find an error in the first place. If the researcher tells the company about the problem, he might be charged with illegally obtaining access into company information. If he does not tell the company, the company could be at risk for hackers with malicious intent to cause problems by revealing private customer information, or causing a breach in security, or initiating a virus.

Which direction should the researcher choose to take? Potentially face criminal charges for inadvertently finding flaws in a company’s system? Or not speak up, but leave the company exposed to future hacking, which could harm the company and its clients? Until there are clear and concise laws which govern and protect the researcher, it is best for them to seek permission from the company before delving into a secure area they do not have permission to be in.

Should Ethical (Grey Hat) Hacking be Taught?

Despite their intentions being good, grey hat hacking can have unsettling social consequences. Even the smallest non-threatening “attack” can be recreated by any “black hat” hacker and turned into something malicious. There are many arguments against teaching hacking but there are equally as many benefits to teaching hacking. Most hackers don’t begin hacking to cause harm to others or for financial gain. “After interviewing six black hat hackers, Xu, Hu, and Zhang (2013) discovered that the pursuit of hacking often starts off with innocent motives, such as simply wanting to know more about computers, or being able to modify school computers to allow playing games even though it was against school policy.” [3] (**Will reformat quote).** Since they began hacking with the intent to do no harm, it was instilled in them that it was okay to hack as long as no harm was done to others.

**Against:** Teaching students how to hack when they are young gives them the tools and knowledge to access secure networks. Having that much knowledge may cause them to take part in “black hat” hacking and cause them to get into some serious trouble. “For example, in April 2014, a Western University student was caught after hacking into the Canada Revenue Agency (the Canadian equivalent of the U.S. Internal Revenue Service). Although he was a very bright student, his ethical reasoning was influenced by a previously established moral value, his lawyer argued. At 14, the student had hacked into his school board’s computer systems and had not been punished for it, sending him the message that it was “OK to hack”” [3] **(Will reformat quote).**

Another problem is that students may think of hacking as a game or a way to easily achieve personal benefits even though the impact hacking can cause is huge. A student may hack into a rival school’s system or even to change their grades and other students’ grades. There are certain examples that show that younger students may not be mature or ethical enough to be trusted with access to certain resources and knowledge that goes along with being taught how to hack.

**Benefits:** As the internet expands and technology becomes increasingly embedded into the daily lives of people, the threat of being hacked also increases. “As hackers “develop sophisticated methods to penetrate security efforts, the threats of cybersecurity breaches [will] continue to have a large prominence in the minds of management teams across all types of businesses”” [3] **(Will reformat quote).** This poses a concern for organizations on how they will be able to protect themselves if their staff only knows very little about hacking.

Programs focusing on teaching ethical hacking are starting to appear everywhere. For these programs to work, there have been many factors set in place. Some factors include “modeling ethical behaviors, cultivating social interactions and relationships with white hat interest groups and law professionals, engaging in competitions where ethical reasoning must play a role, ensuring that successful individual and team efforts receive recognition, and providing ongoing skills development for hackers” [3]. Some educators have even proposed specific principles and methods to help with the integration and development of ethical reasoning skills.

Even if hacking skills aren’t taught at school, there will still be hackers. If the skills needed for hacking or cybersecurity are not taught in schools, all hackers will be self-taught and will be less willing to devote the same amount time to understating the ethical reasoning and context of cybersecurity. If hacking were to become part of the curriculum, the schools and universities that teach it will also be able to teach students how to be ethical hackers and lowering the possibility of students using their knowledge and skills to me malicious hackers.

**Discussion (IV)**

**Ethics:** So ethically, where do they all fall? To explain this, we will use Act Utilitarianism and Virtue Ethics to describe all three viewpoints. Starting with Black-Hat hacking we attempt to as the question of: are Black-Hat hackers ethical? According to Act Utilitarianism, this could be true or false. For example, a scenario where a Black-Hat hacker steals money from a wealthy man. In that situation, the hacker’s happiness could outweigh the wealthy man’s unhappiness, yielding a sum greater than zero, making that action ethical by Act Utilitarianism. Another scenario could be a hacker commits fraud on a homeless person. The hacker would be upset because he did not gain anything from it and the homeless person could be happy due to them acquiring a legal claim and allowing them to gain some form of currency. This situation’s sum would be greater than zero, making it ethical. Now, a situation where a hacker commits fraud on a middle-class homeowner. The hacker would gain a moderate amount of money at the homeowner’s expense. The hacker’s happiness would increase a moderate amount, but the homeowner’s happiness would decrease drastically. This action would be unethical.

**Conclusion (V)**

**Extra:** Now that we know of Black-Hat hacking and White-Hat hacking, where does that leave us? In the middle, there is an ethically gray area, Gray-Hat hacking. This is where ethics become more malleable and what is considered morally right and wrong come into question. Gray-Hat hackers fall somewhere between Black and White-hat hackers, such that they use methods of both for the gain of both. For example, White-Hat hackers find exploits to reinforce security measures as well as for money. [1]. A Gray-Hat hacker would do these things, but their sense of right and wrong is not as acute as the White-Hat hackers. A true White-Hat should never hack for revenge or because of their ideals. This is where the Black-Hat’s ideals come into play. A Gray-Hat would hack for their ideals, revenge, money, and anything really. The motivations of both sides are equally appealing to a Gray-Hat hacker. In *White Hat, Gray Hat, Black Hat*[2], Matthew Gray says that hackers will always follow the path of least resistance. However, Gray Hats pose no real risk to computer security because they do not act maliciously.