European Journal of Business Transformation and Analytics

White Hacking: its importance in today's Cyber world

Mohammed Al-sebai, Amro Helal, Taher ALL Abbas, Hasan Abdulaal, Riyaz Ahmad Khan

1. Department of management, College of Business Administration, Imam abdulraman Bin Faisal University, Dammam, Saudi Arabia

2150010974@iau.edu.sa, 2150010975@iau.edu.sa, 2140001232@iau.edu.sa , 2130002282@iaue.du.sa,

Abstract: "Hacker." What are your thoughts when you hear that word? A few teenagers or a man in his early 20's that lives in the basement of his parents' house, trying to do something he should not be doing? A criminal…a random stranger that you don't know but they are getting to know you because they are stealing your identity? Or a single person or group of people that have a political agenda of some kind? The image portrayed by the media is not pretty. For those that believe mainstream media, whether it's by reading the newspaper or watching the news, hackers should be feared. They are people that are committing crimes and need to be stopped. There are several types of hackers and various levels of hacking. The most common types of hackers are known as Black Hat, Gray Hat, and White hat hackers. How are they different?

1. Introduction

Let's start with black hat hackers. These are the criminals. They use their skills for personal gain. They steal information, blackmail individuals as well as companies. They are capable of destroying lives of people, reputations of companies, and costing those companies lots of money. They do it because they can. They do it for fun. They do it because they don't think they will get caught. And sometimes this is true.

Next is the gray hat hacker. They are not necessarily criminals, but are ethical hackers. They are very intelligent people that use their ability to challenge themselves or others. Often, they use their skills to send a specific message to a specific person, such as a public official that is working AGAINST the people instead of FOR the people.

The white hat hacker does not hack for personal gain, or criminal reasons. They possess the skills of any hacker, has the ability to hack systems and networks with the same style and tools used by other hackers. So, what makes the White hat hacker different? They use their skills for a greater good. For example, if a Black hat hacker were able to access the system used by a company, not only could they steal millions of dollars but they also pose a risk to employees, business associates and clients by leaking their personal information. White hat hackers are often employed by companies to test their systems to keep this from happening. White hat hackers are ethical hackers. They believe in human rights and equality for all humanity. When rights are being violated and laws are being broken, those involved are often exposed by White hat hackers. We send emails, shop, pay bills, manage bank accounts and health records and so much more…it's all online. Yes, there are programs that protect our information but there are people (Black hat hackers) that will make it their mission to bypass security systems for their benefit. And as long as the criminals and corrupt public officials and human rights violations exist, White hat hackers will be there to protect the people and expose the corruption.

Citation: Sebai M.A.; Helal, A.; Abbass, T.A. White Hacking: its importance in today's Cyber world. *Int. J. European Journal of Business Transformation and Analytics* **2022**,

Received: 17-10-2021
Accepted: 17-12-2021
Published: 30-01-2022

When you are in school and your teacher asks what you want to be when you grow up, no one says "I want to be a hacker." However, as you get older and become aware of the world it becomes a question. "How do I become a hacker?" The answer to that is another question. "What kind of hacker do you want to be? A White Hat (ethical) or a Black Hat (unethical). An education in Computer Science or Information Technology is a good start.

2. Compensation

Hackers break into systems, obtaining email addresses and passwords to steal credit card information, and any other info they can sell for profit. High-tech hackers were brought in by the Pentagon in an attempt to breach DOD (department of defense) websites. They were successful in finding 138 different security vulnerabilities. The Pentagon says 1,410 hackers took part in the challenge and the first vulnerability was identified just 13 minutes after the hunt began. Overall, they found 1,189 vulnerabilities, but a review by the Pentagon found that only 138 were valid and unique. The experiment cost $150,000. Of that, about half was paid out to the hackers as bounties, including one who received the greatest prize of $15,000 for submitting several security vulnerabilities. Others received varying amounts, to as low as $100. (1)

Instead of taking these people and putting them in jail, governments should develop their talent and use it to benefit the country. Offer them employment so they can put their skills to beneficial use for themselves as well.

Such things are applied by some governments, antivirus companies and privet companies like (Microsoft, google, apple…), in general, western countries are interested in cyber security this leads to more ethical hackers there, on the other hand in the Middle East most of the countries are not interested in cyber security and developing information systems this caused too many cyber-attacks which is this lead to a lot of hackers are behaved in a wrong way, and that's force ethical hackers to travel out of the Middle East borders to find better opportunities.

3. Education

'The Philosopher's Stone ': Is a legendary material that is believed to convert cheap metals (such as mercury or lead) into gold or silver (2). In the same way, education transforms the poor into rich and terrible things into wonderful things that contribute to the development of the world. the education help to harness and direct the hackers in the right way, as anything in the life the method of use creates an enormous difference such as when use the knife for cooking or killing.

Today there is Certified Ethical Hacking (3) it gives to people who have enough skills and professionals to understand how to find vulnerabilities or flaws in systems and use the same knowledge tools as a malicious hacker, but in a legal way.

The adoption of these certificates will create many Job title such as Senior Web Security Engineer deal with malware and Lead Information Security Analyst Etc.

In recent years, the Kingdom has made a lot of efforts in combating cybercrime and establishing sanctions to reduce it like The Anti-Cyber Crime Law was issued under the Council of Ministers Decision 10 years ago You can view it through a website of Communications and Information Technology Commission (4).

So, we hope that all the countries will put all its exertion, to complete the same way and embrace teaching programs that contribute to the prevention of hacker damage and direct emerging talent to use their skill properly.

4. Raising Awareness

After stealing copyrights of a software, identities, thousands of dollars, and launching some of the most destructive computer viruses, a black hat might find themselves behind bars — or behind a desk in a swanky office.

Black hats are the "bad hackers," the people who poke vulnerabilities and create worms and take what does not belong to them. White hats are the good guys. They are the security experts who try to protect the Internet from those black hats other cyber-attacks.

But sometimes after a black hat gets caught, in some cases they find themselves suddenly on the white hat side with the opportunity to help government agencies or start a security company, one of many examples that support my idea is, Robert Tappan Morris:

Morris is known as that guy behind the first computer virus, appropriately known as the Morris Worm. This worm didn't steal information as many do today; it caused computers to crash — accidentally. Morris didn't intend for the

virus to be malicious. Instead, he was using it to measure the size of the Internet itself, to see just how far the virus could reach. Morris released the virus from MIT so as to not associate it with his graduate studies at Cornell.

However, once the worm was on a computer, it started taking up space and memory. It wasn't smart enough to determine if a computer was previously infected, so it would reinstall itself everywhere. Eventually, this caused systems to crash from heavy processing demands, causing financial damage for the owner.

Morris was arrested and was the first to be tried under the Computer Fraud and Abuse Act (CFAA). He received a $10,000 fine and 400 hours of community service.

Today, the CFAA is a controversial law that many say has led to overly harsh punishments for "computer crimes." The recent death of Aaron Swartz, a civil rights activist who siphoned off five million JSTOR articles using MIT's computer network, spurred this conversation. Swartz is believed to have committed suicide while facing dozens of years in jail and a $1 million fine for his actions.

Morris currently works for MIT in the electrical engineering and computer science department. He also helped found the well-known Silicon Valley tech incubator Y Combinatory. (5)

As we can see from previous example that I provided, it's not necessary that all hackers want to abuse others, some of them do it by mistake like Morris, also some of them do it by purpose and harm people, but there is a good person inside of them, so if they get the right treatment from the authority they will turn to the right side and help society to move forward, because they are talented, intelligent, and they deserve the better.

To conclude, while electronic revolution is expanding in 21th century, there is continues development in systems which is lead to more vulnerabilities, so because our Armed defense systems, transportations, Electronic Government Transactions, social media, and E-learning systems are associated with cybersecurity, it's not going to be easy to keep all these systems secured without protect it from cyberattacks, so we should develop our networks and systems security regularly through Security Information Centers which are basically rely on some specialists in information security which is basically contained of white hat hackers.

That's why we should contain hackers, and develop their skills to encourage them to choose the right path, and educate them by establishing educational centers for cybersecurity.

References

1. http://www.militarytimes.com/story/military/tech/2016/06/17/white-hat-hackers-find-security-vulnerabilitys-pentagon-websites/86057008/

2. https://en.oxforddictionaries.com/definition/philosopher%27s_stone

3. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

4. http://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Documents/LA_004_%20E_%2 0Anti-Cyber%20Crime%20Law.pdf

5. https://venturebeat.com/2013/11/08/black-to-white-hat/