# DOWNLOAD PDF RESEARCH PAPER ON ETHICAL HACKING

## Chapter 1 : Ethical Computer Hacking - Research Paper

*This research completely concentrates on ethical hacking, problems that may occur while hacking process is in progress and various ethical hacking tools available for organizations. Information is the important source for any organizations while executing.*

As with most technological advances, there is also a dark side: With these concerns and others, the ethical hacker can help. This paper describes ethical hackers: The ethical hacking process is explained, along with many of the problems that the Global Security Analysis Lab has seen during its early years of ethical hacking for IBM clients. The term "hacker" has a dual usage in the computer industry today. Originally, the term was defined as: A person who enjoys learning the details of computer systems and how to stretch their capabilities--as opposed to most users of computers, who prefer to learn only the minimum amount necessary. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming. As computers became increasingly available at universities, user communities began to extend beyond researchers in engineering or computer science to other individuals who viewed the computer as a curiously flexible tool. Whether they programmed the computers to play games, draw pictures, or to help them with the more mundane aspects of their daily work, once computers were available for use, there was never a lack of individuals wanting to use them. Because of this increasing popularity of computers and their continued high cost, access to them was usually restricted. When refused access to the computers, some users would challenge the access controls that had been put in place. They would do these things in order to be able to run the programs of their choice, or just to change the limitations under which their programs were running. Initially these computer intrusions were fairly benign, with the most damage being the theft of computer time. Other times, these recreations would take the form of practical jokes. However, these intrusions did not stay benign for long. Occasionally the less talented, or less careful, intruders would accidentally bring down a system or damage its files, and the system administrators would have to restart it or make repairs. Other times, when these intruders were again denied access once their activities were discovered, they would react with purposefully destructive actions. When the number of these destructive computer intrusions became noticeable, due to the visibility of the system or the extent of the damage inflicted, it became "news" and the news media picked up on the story. Instead of using the more accurate term of "computer criminal," the media began using the term "hacker" to describe individuals who break into computers for fun, revenge, or profit. Since calling someone a "hacker" was originally meant as a compliment, computer security professionals prefer to use the term "cracker" or "intruder" for those hackers who turn to the dark side of hacking. For clarity, we will use the explicit terms "ethical hacker" and "criminal hacker" for the rest of this paper. What is ethical hacking? With the growth of the Internet, computer security has become a major concern for businesses and governments. They want to be able to take advantage of the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being "hacked. This scheme is similar to having independent auditors come into an organization to verify its bookkeeping records. In the case of computer security, these "tiger teams" or "ethical hackers"3 would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. This method of evaluating the security of a system has been in use from the early days of computers. They performed tests that were simple information-gathering exercises, as well as other tests that were outright attacks upon the system that might damage its integrity. Clearly, their audience wanted to know both results. There are several other now unclassified reports that describe ethical hacking activities within the U.

## Chapter 2 : Reliable Papers | Ethical Hacking | Reliable Papers

*Explain whether or not you believe ethical hackers have a negative connotation when it comes to their duties. Determine whether or not you believe there should be cause for concern when employing an ethical hacker based on the knowledge of hacking techniques that he / she possesses.*

Or maybe something a little bit more serious like your personal web page gets hi-jacked? Hacking can be ethical by providing the Internet world with a tightened sense of security by detecting and preventing security flaws before it is too late. There are a many types of hacks, and hackers in the cyber world. A hack can be any modification done to virtually anything, to make it do something better, or something completely different. Many hackers are hackers of electronic equipment, mostly computers, but even cell phones, routers, iPods, digital cameras, and even the Toyota Prius have been hacked to get better gas mileage with the hybrid-electric engine Rupley. But besides modifying computers themselves or gadgets, hackers play a significant role in the networking world. This type of crime is most likely the work of a script kiddie, or a "cracker", who is an inexperienced, unskilled "hacker" who attempts to infiltrate or disrupt computer systems by running pre-fabricated scripts designed to crack those systems Script Kiddie. These are the people setting the very negative example of computer literate people around the world. They know no morals, or ethical value behind what they do, but to compromise, and cause havoc upon the end user computing world. Hackers fall into two categories: Black Hat and White Hat Hackers. The term "hacker" can be explained as a person who enjoys learning the details of a computer system and how to stretch their capabilities beyond a person who learns the bare minimum to use a computer Palmer. By this definition, a hacker can be anyone who is willing to expand their knowledge with a computer to better benefit themselves, or more importantly, others. Many people disregard the ethical sense to hacking and believe all forms of hacking to be unjust, which is untrue, but hacking can be very beneficial. White Hat, or Ethical Hacking can be very useful by having security professionals attempt to break in to explore and try to exploiting systems to discover a loop-hole or security flaw in a network. This is similar to having independent auditors come into an organization to verify its bookkeeping records. These White Hat hackers are usually experts in their field and use the same tools and technology that Black Hat Hackers would use to infiltrate a system Palmer. By eliminating potential holes in a network, the initial data could then be out of harms reach, and close guarded by a secure network. This is a very important aspect to running a successful and safe network. One of the basic types of attacks done by hackers are Denial of Service Attacks, this is when a hacker infiltrates temporality disabled a major web sites such, such as eBay or Amazon, and it has a major effect on income and revenue for that particular company.

## Chapter 3 : Reliable Papers | EXPLAIN THE PURPOSE OF THE ETHICAL HACKING CONCEPT. | Reliab

*of breaching and lastly emphasis on why ethical www.nxgvision.com paper explores the ethics behind ethical hacking and whether there are. The paper also looks at ways in which future research could be looked www.nxgvision.coming highly qualified ethical hackers.*

Dave Sanjay Maheshwari rasiktdave gmail. University Indore Madhya Pradesh. Ethical Hacking - or, less colorfully, penetration test - involves simulating the attacks a malicious or illegal hacker could carry out on a network, so that protection can be tightened to prevent them. An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, looking for vulnerabilities that a malicious hacker could exploit. This work is ethical because it is performed to increase the protection of the computer systems, but only at the request of the company that owns the system and specially to prevent others from attacking it. With the increasing use of the internet, it has become an essential part of IT security industry today. The explosive growth of the Internet has brought many good things: As with most technological advances, there is also a dark side: This paper aims to analyze the role and work of ethical hackers in India with special reference to measures to safeguard the vulnerabilities that an hacker may exploit and damage. Introduction Ethical Hacking is having a good knowledge of computer and network. Hacking may be defined as an illegal act of breaking into a system or Internet. There are more types of hacking such as html hacking, password hacking. Recent news for hacking is hijacking face book account and using it for wrong purposes. Hacking may be defined as an illegal act of breaking into a system or internet. Hacker Hacking steals private information. For example stealing your mail user name and password etc. Three types of Hacking White hat: They are the unethical hackers who utilize their skill for their self-interest. Their activities harm other people. They are the people who are engaged in hacking telecommunication services or the public utility services. What is Ethical Hacking? Ethical Hacking is done by computer experts who use their programming capabilities to understand the system vulnerabilities. Ethical Hacking is performed by an individual who is termed as white hat or skilled expert with computers, who is given permission to use their programming skills which will help them detect any minor vulnerability in the system. The computer security community is strongly self-policing, given the importance of its work. Most ethical hackers, and many of the better computer and network security experts, did not set out to focus on these issues. Who are ethical hackers? The term "ethical hacker" has received criticism at times from people who say that there is no such thing as an "ethical" hacker. Hacking is hacking, no matter how you look at it and those who do the hacking are commonly referred to as computer criminals. However, the work that ethical hackers do for organizations has helped improve system security and can be said to be quite successful What do ethical hackers do? Illegal hackers penetrate your system and use your personal data for their own gain. Ethical Hacking on the other hand, protects your computer from illegal hacks. An anonymous computer hacker sends viruses that can crash your computer. Once your computer is at its weakest point, computer hackers steal your information and use it for their own means and gains. Evaluate vulnerabilities in IT infrastructure , Test human behavior , Find the leak etc. When the user requests an evaluation, there is quite a bit of discussion and paperwork that must be done up front. The discussion begins with the customers answers to questions similar to those posed: A surprising number of clients have difficulty precisely answering the first question: Such last-minute evaluations are of little use, since implementations of corrections for discovered security problems might take more time than is available and may introduce new system problems. What are white hat hackers and what are black hat hackers? White hat hackers are certified ethical hackers. They are allowed to penetrate computer systems to find out its kinks and make sure that these kinks are ironed out. They perform Ethical Hacking to ensure the safety of your computer system. Here is a list of benefits that you can derive from hiring white hat hackers: White hat hackers increase the security levels of computer systems. They help increase your protection against black hat hackers who are out to get your personal information. A white hat hacker prevents black hat hackers from entering your computer system. White hat hackers employ high level computer science to evaluate and increase the security of your computer system. White hat hackers perform Ethical Hacking to

improve the defense mechanism of your computer system. White hat hackers evaluate and assess the capability of your system to find out potential loopholes and cracks that black hat hackers can enter. They make sure that your system is protected from the sneaky techniques of black hat hackers. These are some of the benefits that white hat hackers can offer. If white hat hackers perform Ethical Hacking, black hat hackers are their antithesis. Black hat hackers are illegal hackers that want to steal your personal information. Black hat hackers are bad for your system. They wreck your system and prevent it from performing well. Black hat hackers leave your system in shambles. It is best to hire a white hat hacker to create a line of defense against black hat hackers. This is particularly vexing since the performance of the ethical hackers might mask those of the criminal hackers.. Several kinds of testing: The only information used is available through public sources on the Internet. This test represents the most commonly perceived threat. A well-defended system should not allow this kind of intruder to do anything. A well-defended system should only allow this kind of intruder to access his or her own account information. This tests whether or not insiders with some access can extend that access beyond what has been prescribed. A well-defended system should allow an insider to access only the areas and resources that the system administrator has assigned to the insider. An Ethical Hacker is someone who is Programming and networking skilled , Installation and maintenance skilled , System management skilled , Knowledgeable , Hardware and software , Completely trustworthy , Discrete , Patient, persistent and methodical , Certified Ethical Hacker etc. Information Security Challenges More particularly, the organization was attracted in ethical hacking as a response to shifting organizational network boundaries. This shift is the result of adoption of new technologies such as cloud computing and practices such as outsourcing. These technologies provide more robust information flow but also necessitate the ability to go beyond traditional technical controls. Prospects Today software companies whether government or private is dealing with hardcore security problems. Crackers and intruders enter databases and web servers for stealing, damaging and spreading of irrelevant programs. This brings in the need of ethical hackers and courses on ethical hacking. Ethical hacking in India is grabbing the market fast and is doing a brisk business. It is the job of ethical hackers to protect the networking infrastructure and corporate websites. Conclusions The ethical hackers would have an ongoing responsibility to ensure the safety of any information they retain, so in most cases all information related to the work is destroyed at the end of the contract. The idea of testing the security of a system by trying to break into it is not new. Whether an automobile company is crash-testing cars, or an individual is testing his or her skill at martial arts by sparring with a partner, evaluation by testing under attack from a real adversary is widely accepted as prudent. A single failure in any of these areas could very well expose an organization to cyber- vandalism, embarrassment, loss of revenue or mind share, or worse. Any new technology has its benefits and its risks. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place. Many companies are of the opinion that investing in Ethical Hacking is waste of time and money but reality is that is ignorance can cost company millions of Rupees.. Ethical hackers make sure that any of these vulnerabilities are fixed and problems plugged to protect data from fraudulent use.

# DOWNLOAD PDF RESEARCH PAPER ON ETHICAL HACKING

## Chapter 4 : Hacking - Research Paper

*ethical hacking is essential for the process of hacking. Sponsorship of the project is the most important step for ethical hacking process because one needs someone to protect.*

Ethical Hacking Ethical Hacking You will reference your text and one other scholarly reference in your response to this assignment. Make sure you use your spelling checker and grammar checker. A hacker is an individual with technical skills and creative savvy who is willing to push the limits of technology in order to discover the boundaries and weaknesses of a computer or networked system in order to gain unauthorized access to that system. The use of the term hacker often means that the individual is willing to cross ethical boundaries in order to test and gain access to a system. Ethical hackers use the same methods and techniques used by traditional hackers with one difference, the ethical hacker is someone who is trusted by the organization to discover vulnerabilities or weaknesses in a system and then report these issues back to the organization so that the issues can be fixed. For example, a bank might hire an ethical hacker to test the security of their banking system. If the ethical hacker discovers a method to steal money from the bank undetected, the ethical hacker will report this information and not use it to their advantage. Ten years ago, the term ethical hacker was viewed as an informal term used by management. It was used to describe individuals that were willing to cross traditional ethical boundaries in order to protect systems from those outside individuals that are not concerned with ethical issues. The primary concern is that an ethical hacker has to be willing to push the ethical boundary to match those conditions that would be used by a traditional hacker. Some security experts state that the term ethical hacker is a misnomer. An ethical hacker seems to imply the same contradiction that we might find in attempting to define an ethical thief. Respond to the following: Can the actions of a hacker be ethical and still be effective? Why or why not? What ethical issues does management need to consider when attempting to secure information systems? What are some possible benefits of hiring ethical hackers? What are some possible detriments to hiring ethical hackers? Should management hire ethical hackers to verify the security of their information systems? Give reasons and examples in support of your responses. Write your initial response in approximately words. Apply APA standards to citation of sources. Introduce new thoughts or ideas on this topic. Assignment 1 Grading Criteria Examined whether the actions of a hacker can be ethical and still be effective. You will reference your text and one other scholarly reference in your response to this assignment. Make sure you use your spelling checker and grammar checker prior to submitting your work. I look forward to your posts! Information is data that is framed in a specific context. In this sense, information is contextual data that has a level of inherent value. Data might be the binary 0s and 1s on a hard drive, but information is the combination of that binary data into a document, media file, or database. Therefore, information systems are methods of managing the value of different types of data. The value of the data might be in the personal records such as social security number, addresses, or shopping habits that are linked together to form an online shopping cart and on-click purchasing. The value of information provides for the potential for ethical, social, and political issues within an organization. An example of these ethical, social, and political issues can be found in the concept of privacy. What ethical, social, and political issues arise with the use of information systems? Which of these identified issues can have the most adverse effect on an organization if not managed properly? Assignment 2 Grading Criteria Maximum Points Listed and explained the ethical, social, and political issues that arise with the use of information systems giving an example for each issue.

## Chapter 5 : Ethical Hacking Research Papers - www.nxgvision.com

*Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This paper describes what is ethical hacking, what are the types of ethical hacking, impact of Hacking on.*

## Chapter 6 : Certified Ethical Hacking - Words - Essay | quintessay

# DOWNLOAD PDF RESEARCH PAPER ON ETHICAL HACKING

*This research completely concentrates on ethical hacking, problems that may occur while hacking process is in progress and various ethical hacking tools available for organizations. Information is the important source for any organizations while executing business operations.*