Case Study On: ETHICAL HACKING

ABSTRACT:

Today more and more softwares are developing and people are getting more and more options in their present softwares. But many are not aware that they are being hacked without their knowledge. One reaction to this state of affairs is a behaviour termed “Ethical Hacking" which attempts to pro-actively increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. A good ethical hacker should know the methodology chosen by the hacker like reconnaissance, host or target scanning, gaining access, maintaining access and clearing tracks. For ethical hacking we should know about the various tools and methods that can be used by a black hat hacker apart from the methodology used by him. From the point of view of the user one should know at least some of these because some hackers make use of those who are not aware of the various hacking methods to hack into a system. Also when thinking from the point of view of the developer, he also should be aware of these since he should be able to close holes in his software even with the usage of the various tools. With the advent of new tools, the hackers may make new tactics. But at least the software will be resistant to some of the tools.

INTRODUCTION:

Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal. Ethical hacking is performed with the target’s permission. The intent of ethical hacking is to discover vulnerabilities from a hacker’s viewpoint so systems can be better secured. It’s part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors’ claims about the security of their products are legitimate.

Security:

Security is the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. In the case of networks, the security is also called the information security. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction

Need for Security:

Computer security is required because most organizations can be damaged by hostile software or intruders. There may be several forms of damage which are obviously interrelated which are produced by the intruders.

These include:

1. lose of confidential data
2. 2. Damage or destruction of data
3. 3. Damage or destruction of computer system

4. Loss of reputation of a company

Hacking:

Eric Raymond, compiler of "The New Hacker's Dictionary", defines a hacker as a clever programmer. A "good hack" is a clever solution to a programming problem and "hacking" is the act of doing it. Raymond lists five possible characteristics that qualify one as a hacker, which we paraphrase here:

A person who enjoys learning details of a programming language or system
A person who enjoys actually doing the programming rather than just theorizing about it
A person capable of appreciating someone else's hacking
A person who picks up programming quickly
A person who is an expert at a particular programming language or system

Types of Hackers:

Hackers can be broadly classified on the basis of why they are hacking system or why they are indulging hacking. There are mainly three types of hacker on this basis

Black-Hat Hacker

A black hat hackers or crackers are individuals with extraordinary computing skills, resorting to malicious or destructive activities. That is black hat hackers use their knowledge and skill for their own personal gains probably by hurting others.

White-Hat Hacker

White hat hackers are those individuals professing hacker skills and using them for defensive purposes. This means that the white hat hackers use their knowledge and skill for the good of others and for the common good.

Grey-Hat Hackers

These are individuals who work both offensively and defensively at various times. We cannot predict their behaviour. Sometimes they use their skills for the common good while in some other times he uses them for their personal gains.

ETHICAL HACKING:

Ethical hacking – defined as "a methodology adopted by ethical hackers to discover the vulnerabilities existing in information systems' operating environments."

With the growth of the Internet, computer security has become a major concern for businesses and governments.

In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems.

What do an Ethical Hacker do?

An ethical hacker is a person doing ethical hacking that is he is a security personal who tries to penetrate in to a network to find if there is some vulnerability in the system. An ethical hacker will always have the permission to enter into the target network. An ethical hacker will first think with a mind-set of a hacker who tries to get in to the system. He will first find out what an intruder can see or what others can see. Finding these an ethical hacker will try to get into the system with that information in whatever method he can. If he succeeds in penetrating into the system, then he will report to the company with a detailed report about the particular vulnerability exploiting which he got in to the system. He may also sometimes make patches for that particular vulnerability or he may suggest some methods to prevent the vulnerability.

Required Skills of an Ethical Hacker:

Microsoft: skills in operation, configuration and management.
Linux: knowledge of Linux/Unix; security setting, configuration, and services
Firewalls: configurations, and operation of intrusion detection systems.
Routers: knowledge of routers, routing protocols, and access control lists
Network Protocols: TCP/IP; how they function and can be manipulated.
Project Management: leading, planning, organizing, and controlling a penetration testing team.

Advantages and disadvantages:

Ethical hacking nowadays is the backbone of network security. Each day its relevance is increasing, the major pros & cons of ethical hacking are given below.

Advantages:

"To catch a thief you have to think like a thief"
Helps in closing the open holes in the system network
Provides security to banking and financial establishments
Prevents website defacements
An evolving technique

Disadvantages:

All depends upon the trustworthiness of the ethical hacker
Hiring professionals is expensive.

Future enhancements:

As it an evolving branch the scope of enhancement in technology is immense. No ethical hacker can ensure the system security by using the same technique repeatedly. He would have to improve, develop and explore new avenues repeatedly.
More enhanced softwares should be used for optimum protection. Tools used, need to be updated regularly and more efficient ones need to be developed.

Speech by Brand Ambassador of Digital India Project

Mangaluru: "For the sake of a secure online future of many citizens all over the country, ethical hacking must be learnt for safety purposes and not for misuse", said brand ambassador for Prime Minister's "Digital India" Project Ankit Fadia in Sahyadri College of Engineering and Management in Adyar.

On his visit to Mangaluru, he dropped into Sahyadri College on Friday, October 28 to disseminate his knowledge by conducting a workshop on "Ethical Hacking". Speaking to the gathering at the event he opined that ethical hacking was important for national security but at the same time it could be a bane if misused by the ones who learnt it.

Pertaining to the topic of misuse of ethical hacking Ankit went on to say, "It is indeed true that hacking in an ethical manner can save a lot of cybercrime from happening and keep many e-accounts of people safe from online sharks. It is also true that this skill can be misused for illegal purposes but at the same time it is hard to reject it totally because of its better implications in the online world."

"Officers of the law should learn the skill of ethical hacking since most cybercrime divisions of the police department do not have hackers. The IPS officers from Hyderabad, Kerala and Karnataka say that they have undergone cybercrime training but they often seek help of ethical hackers to crack cases", he said while stressing on the point that police department must have active ethical hackers.

Concluding his address to the gathering, Ankit said that after the advent of hacking from computers to mobile phones, the future of hacking will proceed to electronic home appliances using various codes and disrupting effective working of the appliances. "Common knowledge of ethical hacking should be learnt by everyone to be safe in the digital world", he concluded.

Conclusion:

This report looked at the, good and bad things about ethical hacking where you have white hat hackers, they are known as ethical hackers. Then you have blackhat hackers, who are the criminal s of the internet. You also have the activists, who break into websites and deface them by changing the content of the website. I also discussed the advantages of ethical hacking, where they protect company's data, and some of the disadvantages where ethical hackers have ended up in jail for hacking into Facebook. With the future of technology changing so fast, the ethical hacker has to keep up with the criminals.

(TE EXTC Student)
Rubini Pulliadi