UNIVERSIDAD FRANCISCO DE VITORIA

ESCUELA POLITECNICA SUPERIOR

Fundamentals of Computer Engineering

Practical work I

ETHICAL HACKING

GROUP NUMBER 1

Table of contents

Abstract

In the world of technology and computers, hacking is a widespread practice that we cannot forget. Besides being one of the main disciplines of computer engineering, sometimes, it can be used in malicious ways. Hacking is used to commit crimes, whether for economic, military, or political purposes. As with other tools, there are people who make the decision to use it to do evil. This is why we should know what ethical hacking is and how we should apply it.

Ethical hacking is a professional outlet or practice within the field of computer science that tries to solve or defend against hacker attacks. The same functions and tools are used, but with an opposite intention to this bad practice. Different types of ethical hacking are crackers and Black hat, White hat or Grey hat hackers.

Many high-level companies are hiring cybersecurity professionals to apply ethical hacking. These are dedicated to detecting and resolving vulnerability problems that can be found in computer systems or programs with the objective that no one can access the information, much less manipulate it. It is usually carried out mainly in large companies, organizations, or governments.

This could be solved by providing more education on morals and ethics when training computer scientists in universities or schools. It is something of global interest since hacker attacks affect us all and should be eradicated.

Resumen

En el mundo de la tecnología y los ordenadores, el hacking es una práctica muy llevada a cabo que no podemos olvidar. Además de ser una de las disciplinas principales de la ingeniería informática, a veces, puede ser de forma negativas o malintencionadas. Se utiliza el hacking para cometer delitos, ya sea con fines económicos, militares o políticos. Al igual que con otras herramientas, hay gente que toma la decisión de utilizarla para hacer el mal. Por esto debemos saber en qué consiste el hacking ético y cómo debemos aplicarlo.

El hacking ético es una salida profesional o práctica dentro del campo de la informática que trata de solucionar o defenderse de ataques de hackers. Se utilizan las mismas funciones y herramientas, pero con una intención opuesta a esta mala práctica. Algunos tipos de hacking ético son: crackers and Black hat, White hat and Grey hat hackers.

Muchas empresas de muy alto nivel están contratando profesionales en ciberseguridad para aplicar el hacking ético. Estos se dedican a detectar y resolver los problemas de vulnerabilidad que se pueden encontrar en los sistemas o programas informáticos con el objetivo de que nadie pueda acceder a la información y mucho menos manipularla. Se suele llevar a cabo sobre todo en grandes empresas, organizaciones, o gobiernos.

Esto se podría solucionar dando una mayor educación sobre la moral y la ética a la hora de formar a informáticos en los centros como universidades o escuelas. Es algo de interés global ya que los ataques de los hackers nos afectan a todos y deberían erradicarse.

1 Introduction

1.1 Motivation

Our motivation to start this research article finds its foundations on primarily two menaces:

First, the alarming low awareness of the average internet user leaves them exposed to innumerable potential dangers while surfing the web. The risks we, as web surfers, unknowingly assume are wide and if not taken in account may be extremely harmful to our economics, reputation, or optimal device performance to name a few.

On the other hand, even if some of the biggest companies are well aware of the existence of these risks, the malicious population of hackers is constantly improving and looking for holes in the security systems of such businesses which enhance the idea of hiring experienced ethical hackers to regularly test and update their security. More so when taken into account the unimaginable value of the data certain organizations have in custody and the catastrophic consequences of them falling in wrong hands.

As these two menaces which attempt to exploit our carelessness are created by hackers and dealt by their more ethic counterpart – ethical hackers – we have concluded that their awareness should further be extended by the use of our work.

1.2 Objectives

Nowadays, we know that there is a risk of our information being compromised by computer attacks. That is why the main purpose of this project is to try to identify and prevent these security problems by increasing awareness of this issue. Another objective of the project is to discuss hacking from an ethical view, trying to discern when these types of practices are right or wrong.

Therefore, the objective of our work is to capture these security problems to which our computers could be exposed and to understand how hackers use their tools to solve this lack of security.

1.3 Practical work outline

2 Name of the topic

The domain of ethical hacking spreads across a variety of areas of the world, particularly to the computer industries. They are an essential for any large or small organization to protect the data they have in custody from malicious hands.

2.1 Description of the technology/topic

Ethical hacking is, with the user's authorization, identifying the security problems to which data, an application, a computer system or network is exposed, analysing the problem, and solving these vulnerabilities through a legal and ethical use of hacking. In this way, ethical hackers look for possible attack vectors by imitating the behaviour of an attacker[1]. Ethical hackers exist because, in contrast, there are malicious hackers. They are the ones who are responsible for violating the privacy of individuals and accessing information, computer systems or networks in an unauthorized way to gain access to private data such as personal or financial information, damage the system or introduce a virus.

In order to fight against these attacks, these are some technologies or practices ethical hacking typically uses:

- Ettercap. This host and network analysis application allows you to sniff an SSH (Secure Socket Shell) connection, as well as enter a few characters on the client's server or network.
- Netsparker. This is a web application scanner that detects vulnerabilities in its security.
- Burp suite, which allows the execution of penetration tests in order to evaluate the security of diverse applications.
- John the Ripper. It is a practice used to crack and evaluate the security of passwords.
- Nmap. This practice is mostly used to detect malware, local hosts, network audits and network mapping.
- Acunetix. It is a completely automatic hacking practice that prevents any intruder. It is capable of scanning variants such as SQL or XSS injection.[2]

In our current technological environment, ethical hacking plays an important role in helping companies to keep their information secure and prevent cyber threats.

2.2 Types of hackers and hacking methods

In the cybersecurity world, different groups of hackers can be identified depending on the use of their knowledge, mastery level and motivation:

- Black Hat Hackers: these can be commonly referred to as malicious hackers which perform illegal activities to steal money, data, or other valuable assets for their personal gain.

- White Hat Hackers: this group of hackers, also known as ethical hackers, are the cybersecurity experts who use their skills to protect systems and networks. They also try to hack into these systems and networks with permission of the owner in order to discover vulnerabilities and be able to patch them so they can prevent malicious hackers from exploiting them, helping organizations increase their digital security.

- Grey Hat Hackers: which are a combination of black and white hackers. This means they discover vulnerabilities without authorisation and may decide either to report it to the company or either exploit them. This decision may depend on a balance between the hacker's ethnicity or personal gain.

- Hacktivists: hacktivists are hackers that use their skill to promote a political ideology or a social cause. They carry out cyber attacks in order to spread these ideals. Some hacktivist examples are Anonymous, LulzSec and Russian-Ukrainian groups of hackers.

So, having established the intentions for each, how do ethical hackers discover vulnerabilities and what tools and methods do they use to accomplish this?

The most frequent type of ethical hacker tries to discover security flaws in an organization with their previous authorization. This gives the security expert a lot more knowledge about their clients' presence in the digital world and access permissions to them; this also includes legal permission to perform emulated attacks in order to discover the hidden vulnerabilities.

Some important tests performed by the experts include Denial of Service (DoS) where they try to overflow networks or systems with requests in order for the servers to collapse and stop responding. The security challenge here is to try to find bot patterns and categorize fake petitions from real ones, responding only to real users lowering the stress created by the heavy traffic.

Another ethical hacking technique is cross site scripting, where the hacker tries to insert any kind of virus or script in a web page trying to integrate it so end-users receive it when displaying the web page. If this kind of vulnerability is discovered, it must be reported and worked on in order to patch it.

Black hat hackers' intentions aren't only bound to inserting any kinds of malwares such as spyware, adware, or ransomware; they also try to steal any kind of sensitive data from the organization's databases. This includes bank accounts, passwords, medical data, user browsing information, personal Identification, and many others.

Specifically for passwords, hackers may use either brute force by continuously testing password combinations bypassing the servers control that only allows a certain amount of attempts or through the use of keyloggers inserted either through malware into the user’s computer or by redirecting them to exact replicas of the organization's web pages.

When an ethical hacker realizes false copies of their original web page roam the internet with phishing intentions and identity theft, it is his duty to alert the authorities which range from Internet server providers, their national cybercrime department and the different search engines, in order to take them down.

2.3 The future of the technology

Hackers often perform activities with intentions to do evil and with a significant impact in society, governments, in the economic sphere... These activities cause problems in computer systems and steal private information that may even be sensitive or very confidential. However, there is a profession called ethical hacking, in which some individuals or even a team of several, take advantage of all these skills and knowledge used by hackers for the greater good. Ethical hackers are doing increasingly important work in our society and in the technological world, bringing about a new future in the field of cybersecurity and changing the world for the better.

Cyber-attacks are constantly evolving. Hackers are continually changing their methods, tools, tactics and procedures (TTPs) to get past the defences of targeted networks. Despite trying to not be identified, they do not want to be charged with crimes, even though these network attacks are criminal and punishable, even with jail. If the attackers are at a more advanced level, better professionals are needed to defend systems and companies, and to catch and identify them.

Ethical hacking is a growing profession. If hacking techniques evolve and change or improve, ethical hacking will also increase. Therefore, it is a profession that not only has a future and will not end or disappear in the short term, but it will increase exponentially in the era in which we live.

Companies struggle to find cybersecurity professionals with the expertise to help them in this area. It would help if schools actually taught computer science students how to hack into systems or programs, to be prepared to deal with malicious hackers they learned by doing and defend their companies from these attacks. This is why there are more and more of these jobs, and it is a career with a lot of future, there are not enough qualified people to fill all the gaps in the labour market where there would be a need for workers of this type.

All organizations are always in danger of becoming the next target of a major cyber-attack, ethical hackers will continue to get work. As companies move all their information and data to the cloud, they will also need greater protection of this as there is greater exposure and vulnerability, especially for systems that are not on-premises and therefore may not be as protected and guarded as fixed devices or servers in their offices. In addition, industry experts predict and comment that the value of the global market in this area will reach $4.1 billion by 2027, which paints a bright future, very well remunerated and full of opportunities for ethical hackers.

- Some trends for the next few years of ethical hacking are:

- In the social engineering and phishing ambit, the goal is to obtain personal information from a victim. Emails are the most common means used by this method to steal personal data. They are sent by making the person believe they are someone they know very well and asking for certain sensitive or private information.
- In the malware-injected devices ambit, cyber attackers install camouflaged malicious software on your device. With a USB, they can easily plug into your computer and access the data. Although now they have started to do it telematically without the need to connect a USB or physical cable to the computer. They install it through files called Trojans that serve to introduce and install a camouflaged malicious program on your computer. This is done to be able to subsequently control it from another computer from anywhere. To get rid of this type of attack, companies prefer to hire ethical hackers who are trained to avoid this type of situation.
- There will also be a lot related with password cracking remotely or with artificial intelligence.

In conclusion, this career has a lot of future and possibilities as ethical hackers are everyday more needed by every company for protecting crucial and private information. And every day the number of companies that have all their information about accounting or customers in the cloud. This fact produces vulnerabilities with respect to hackers while ethical ones are going to increase exponentially.

2.4 The ethical view, advantages and disadvantages

Ethical hackers sell their knowledge and skills to organizations in order to grant their cybersecurity as they help patch the holes which may lead to a breach in their digital security system, however these same skills could be used in a malicious manner with devastating consequences. Therefore, the moral of a hacker, the purpose with which he employs his skills, is what draws the line between an ethical hacker and a criminal. As the name suggests, the ethics of ethical hackers are as important if not more than their actual skills in this particular profession.

The thin line that separates hackers from ethical hackers is usually given by the companies and is denominated limited scope. This is the area in which they are allowed to attack, however it is not out of discussion to suggest an out-of-scope attack to the company as this may be crucial to deliver the service as promised and grant total cybersecurity.

According to the cybercrime magazine [4], 8 trillion USD is the amount estimated to be lost by the end of 2023 to cyberattacks. The average salary of an ethical hacker ($106,934 according to salary.com) looks like pocket money in comparison and makes ethical hackers objectively a great asset for companies if they perform as expected. The consequences of unethical hacking have proven to be extremely devastating for companies and individuals.

“With great power comes great responsibilities”, an ethical hacker possesses both, while a hacker only uses his knowledge for personal benefit; ethical hackers, instead, pledge to fight temptations and choose to offer a highly valued service to organizations as a form of living.
The morals of white hats should therefore serve as a guide for them not to take advantage of others nor to employ their skills to cause any harm to anyone but on the contrary help improve system security.

From an ethical view - as well as from an economic perspective - the role of an ethical hacker, serving as a white-hatted digital guardian to the storage of data of, for example, a healthcare company is mandatory. Saying otherwise would be betraying the client’s trust in their service – and even more important, their contract, as when you provide confidential data, there. more often than not, is a policy involved - letting leaks of their private information out. The potential consequences of a breach are severe[5], ranging from compromised patient privacy to the disruption of medical services. Ethical hackers, with their specialized skills, can help identify and rectify these vulnerabilities before malicious actors can exploit them.

Even in the shadow, there is a darkness darker than others, in this case we are talking about the hacking of medical devices and prosthetics such as pacemakers or infusion pumps whose malfunction may lead to unrepairable outcomes. Therefore, it is no exaggeration to say that patients trust ethical hackers (no doubt about doctors too of course) with their life, a statement as powerful as it gets. Which means that on the other side there are people who have the capabilities to end someone’s life remotely, if it where not for our white hatted angels service. The statement says more about how unethical hacking is and the vitality of white hats than rather than the ethical view on ethical hackers.

In cyber-security, in contrast with real life, there are no such limitation when fighting back a malicious hacker. This comes so as cyber counterattacks are aimed to disable the tools of a hacker to protect the data of the rightful owner.

The advantages they offer are closer to rights than to benefits, therefore, there is no doubt about the imperative of their presence on the totality of digital services which involve the usage of personal or valuable data.

Other, while very view, may consider the use of an ethical hacking to be too risky as the difference between them and a hacker is their word not to surpass certain limits. They usually are capable of accomplishing most of the security themselves, for the rest of the population there is almost no other choice than to have faith in their good intentions.

3 conclusions

To sum up, the presence of white hats is no longer a question as it is an imperative for any data/digital related business. They serve as a reaction to malicious hackers who try to illegally exploit software systems in their own benefit disrupting the order established, white hats are thus the protectors of order and servants of law inside the digital realm. They may not seem too big of a deal today, but with the rise of technology, the demand to their labour is more than granted, sadly, as this is a consequence of high skilled people with bad intentions trying to take advantage of others. Not only is their intervention assured, but we also speculate their role will be, even more than to the date, of great prestige in a similar way to the police or military of the real world in a way but being able to operate from home and with higher salaries as their demand will be immense. Then, even with all the dangers the digital realm hides, and all the filthy thieves who will try to harm others in their benefit, we will still be able to make use of the digital services – fortunately as they are a necessity now a days – thanks to those who keep vigil of us in that realm, hope is not yet lost and the technology has still much to unveil. It is because of these hero-like people that mankind can continue enjoying software facilities to life. Nevertheless, we should not be overconfident and always try to be aware of the risks and act responsibly in consequence.

References

[1]*What is ethical hacking and how does it work? | Synopsys*. (n. d.).
https://www.synopsys.com/glossary/what-is-ethical-hacking.html
[2] *Ethical hacking Techniques, tools and types*. (12/10/2023).
https://www.knowledgehut.com/blog/security/ethical-hacking-techniques

https://snyk.io/blog/ethical-hacking-techniques/
https://www.youtube.com/watch?v=XLvPpirlmEs
https://hackingbharat.com/blog/ethical-hacking-for-healthcare-best-practices/#Use_non-intrusive_methods

[3] *Ethics in Hacking.*
https://www.pluralsight.com/blog/software-development/ethic-in-hacking

[4] Cybercrime To Cost The World 8 Trillion Annually In 2023

https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[5] C*yberattack cripples Spanish drug giant Alliance Healthcare*

https://cybernews.com/news/cyberattack-alliance-healthcare/