Survey on Hacking Analysis and Mitigation Techniques

Diogo Santos

Lusofona University of Porto, Portugal

a22005114@mso365.ulp.pt

Abstract. Nowadays we see a greater number of malware attacks and we see that it becomes increasingly difficult to combat and track this type of attacks. Malware is just a term that mean "malicious software" and there are many types of it.

In this project we will be looking at mitigation techniques, we will talk about the ones that are the most used and which are the best and offer more protection.

Mitigation techniques also involve detection, not only protection but also involves the prevention against these types of attacks, often this serves as a protection to them, preventing this kind of attacks it is always better than trying to solve them. As hacking gets more and more complex technology needs to evolve with it, we are going to go deeper into what technology gives us the best ability to counter hacking.

As time goes by, hacker techniques will evolve, and this technique will improve so that its detection will be more difficult for our devices. Networks are expanding day by day and the need of security is getting more and more important, ethical hacking is more used today to help and create security. In this paper we will go along of the hacking technique and some examples about it.

Keywords: Hacking, Mitigation, Malware, Ethical Hacking, Technology, Software, Vulnerability Analysis, Exploits

1 Introduction

Over the last few years, we have seen hacking rise in popularity due to advances in the technology field. Today many of our devices are connected to each other and connected to an internet network, this means that the same information is available between the various devices and with this there is an increased risk of attack by a stranger or even accessing our network and consecutively our personal information, our device and everything that is connected to it depending on the complexity of the attack that may occur. The connections between devices have been very advantageous for all of us, it makes our daily life much easier, in terms of work and leisure but it can also bring many risks to the security of all our information, this is a topic that many people are not aware or not paying attention, syncing devices to a cloud makes it easier and faster to switch devices but it also increases the risk of information leakage, whether personal or work data.

Many people continue with the idea that hacking is always bad, whenever the word is referred to, the idea arises that it is an illegal activity and that its purpose is to cause the cause. Although it can be used for this, nowadays we know that hacking is widely used for reasons of increased security in companies to protect their data, furthermore it has become a practically essential activity to increase the protection of companies, to find problems, weaknesses and therefore being able to correct them, to avoid hacker attacks with malicious intent and also expenses in recovering lost information, through this type of hacking companies are attacked with their permission and then a report is made about the areas that need to be reinforced and why, we are going to speak about this later in this paper, based in a journal, this is called ethical hacking[1] that, following the law simulate these kinds of attacks. We are talking about a lot of types of attacks (e.g., DOS, DDOS etc.) These types of attacks have varying levels of severity and damage to companies for example, I chose to speak about these specific attacks because they are the most used nowadays as they are the most difficult to defend, in this paper we will talk about the attacks are made and also explain the process behind launching an attack of this kind, it is important to remember that more and more attacks are difficult to prevent and consequently it is important to know how to protect all information and devices within the network, attacks within the network if they affect multiple devices, cause them to become zombie machines[2], devices that are compromised during an attack and then pose a threat to the rest of the network they are connected to, we are going to talk about this in depth later in the paper as well. All these attacks require Mitigation techniques, these are important to keep all the data safe in case of attack.

Furthermore, the present introduction section 1, the paper will have 6 more sections divided as follows:

Section 2 – Discusses the concept of "Hacking", why is it important, how hacking can help in companies protection.

Section 3 – We will go through the types of hackers that exist, explaining the purpose of each one and the situations that they act.

Section 4 – There are many types of attacks, in this section some of them will be presented.

Section 5 – As valuable as attacks, the techniques to avoid them will be presented in this section.

Section 6 – Presentation of a report that shows how an attack can cause more damage and panic than its taught.

Section 7 – Conclusion about the theme portrayed.

2 About Hacking

This activity started due to the curiosity of computer enthusiasts, these people are known for their skill in the field of technology (" He is a computer enthusiast and extremely proficient in programming languages, computer systems and networks.") [4]. These very skilled people are referred to as better programmers, programmers who don't follow normal programming methods, they have their own methodology and

program as their will, overcoming various barriers including discovering new ways to program by going deep in this area.

Many times, a hacker is considered to have good intentions which is not supposed to be, hackers are considered the (" safeguards of networks") [4], when exploiting breaches in the network and in the company.

We also have hackers with bad intentions, they attack without authorization and enter networks ("Malicious hacking is the unauthorized use of computer and network resources") [4]. This often ends up with information theft and with it ransom requests in the form of cash.

2.1 Hacking importance

Hacking nowadays is used by companies all the time, they need to be working for the better future of the company, doesn't matter in each area, they need to be always working for better, in terms of technology used and now it's more common for companies to invest in cyber security, so their data is safe and they can just keep their services online for longer, if their services are not online because of an attack this means that the company is losing a lot of money, at that point every minute counts, with this hacking becomes an important tool to help companies being more safe in their networks and services. We are speaking about ethical hacking of course, this type of hacking is all about an organized attack between the company and the ethical hacker, summing up the objective is to find vulnerabilities in the network system of the company by invading it, after this process the hacker is supposed to find ways to prevent the same attack he performed and other attacks that might get the company's data in danger, this whole process has distinct phases, like shown in the next figure.

Fig. 1. Hacking Phases [3]

Evidence about the" test attack" [3], must be erased and without a trace, in order not to leave breaching hints that were discovered by ethical hacking at the beginning of this process. This test attack, as it is called, is aimed at a more complete analysis of the entire network to help build a better structure to ensure maximum protection for the company that hired the ethical hacker, this is a paid job [3] and

everything is done in a controlled environment with full knowledge of company members. After the testing process, the security is certainly improved to avoid damage in an uncontrolled real situation, in case of attack.

3 Types of Hackers

In the realm of hacking (whether we talk about authorized and controlled hacking or hacking in the realm of crime) we have three main types of hackers that are important to know ("these have categories according to the shades or color of the "Hat".") [4] according to the hat color we have: White Hat Hackers, Gray Hat Hackers, Black Hat Hackers.
The color of each one's hat represents a different type of person, with different intentions in the same field, the lighter the color, the lower the malicious intention on the part of the hacker

Fig. 2. Different types of Hacking/Hackers [5]

3.1 White Hat Hackers

In the case of the white hat hacker, we need to know that, being the lightest color of the three that will be presented, they are certainly the ones with the best intentions regarding the act of hacking, this type of hacker is the so-called ethical hacker, it is about a paid professional to test the security of a company's network, report on that same test and also resolve network weaknesses, leaving the company better prepared in case of attack, either on the network or on its information.[5] (They are also known as "IT Technicians") [6].

3.2 Black Hat Hackers

Opposed to the white hat hackers the black hat hacker is known for his bad intentions in the act against the network and against its users, often causing damage to both, often the purpose of this type of hacker is theft of important information for the company and

a request for monetary redemption of the data, or even the destruction of information with the intention of causing great damage to its services, making it an impossible operation.

This type of hacker acts according to all your personal interests, the objective is not to test your skills, but to cause problems for your target, blocking the access of network users and only removing this block after the high payment they want. They know how important information and services are to these companies, hence these high-value redemption requests. [5][6]

3.3 Grey hat hackers

Gray hat hackers have an intermediate profile between white hat hackers and black hat hackers. These hackers have the same intention of infiltrating the network system and taking access by force. After the attack and after knowing how to access all the information that compromises the company in question, the gray hat hacker offers his services to company by making known the vulnerabilities they have, demanding a payment that you think is correct for it. This type of attack is much more thoughtful, as it is carried out so that it can be reversed, if the company accepts the payment to improve its security, the attack can be reversed and thus improve the security of the company in question. Although the company does not agree with the attack, it can accept his services [6].

4 Attacks

There are many types of hacking attacks that may happen in our everyday life, and without us noticing it, with this we are going to see some of the most important attacks in different scenarios like wired scenarios or wireless network scenarios.

In a public network, in a caffe, library, everywhere when a device is connected to the internet an attack may occur, every unprotected device is a target if it is in the wrong place at the wrong time depending on the hacker's intentions.

large companies or some type of service actively used by the population are usually targeted by Hackers these targets are the ones most likely to give hackers what they want as a ransom for data, money is usually what they ask for to give back the important data without any damage.

Table 1. Types of Hacking Attacks [10][8][11]

Type of Attack	Definition	Level of threat
DoS	"DoS" is a big attack base on throwing a lot of information(messages) at the same time for the same IP, overwhelming the all the traffic nodes throughout its passage, normally this type of attack is done to take down important servers for a few hours, all users connected to the server will suffer DoS as well	High
DDoS	In general, a DDoS attack aims to hindering the access of legitimate users to a target system or services by overwhelming the resources, this way the device cannot handle such amount of information and taking total or partial loss of services and files as well	High
Waterhole	Waterhole is done in websites with JavaScript or HTML code, this attack makes the user go in a website with a malware with will corrupt the device giving access of the whole user's network, this normally happens with the most used websites by the user	Medium
Fake WAP	Fake WAP is known to happen via wireless connections, this type of attack consists in getting a fake wireless access point to the network, as soon as a device is connected the user's data can be stolen by the hacker	Medium
Virus/Trojan	Trojan viruses are acquired by users by downloading programs with the virus, this gives the hacker access to the infected computer letting him know when the device is online and provides him with the ability of stealing users' information.	Medium
Phishing	There are 2 types of phishing, by link manipulation which is false URL's replacing sub domains different from the original sub domain so they can trick users to trust in links for example, or filter evasion which consists in using images instead of text, this makes anti- phishing filter useless when trying to detect it	High
Keylogger	This type of attack consists in a malware that is not visible at the normal view in the device, this records the keys that are pressed and write them in a log file which is usable by the hacker when login into a website the data is written, this way the hacker get access to all data about the user's accounts, personal information, passwords	Low

5 Mitigation Techniques

Mitigation techniques are all about keeping devices secured, servers and personal devices like computers, networks et. We know that today avoiding all these attacks is impossible, because there are always new ways to attack, despite of not being possible to defend your network from every single attack, it's possible to reduce the damage created by these attacks by avoiding some situations and using some tools to help you in the process. Some are simple than others but protection nowadays it's important, getting a secured network in your company decreases the risk of damage in case of attack [8][12] and with increasing security we don't waste money on recovering data, recovering data costs a lot of money. Many techniques are known but ignored by most of the population using devices all around the internet. Getting a strong password with numbers, capital letters and no names in it, most of the times this is ignored by normal users, and this might compromise their safety on the internet. Using VPN and avoiding downloads of cracked software's are some basic safety rules that are nor respected by many users.

For the attacks that we spoke about before, now we are going to tell you about the mitigation techniques to avoid those same attacks.

DoS/DDoS.

These attacks consist in sending a lot of information to the device at the same time making it to shut down. Nowadays this kind of attacks have been more frequently used as we can see from the graph under. This study was done by Google Pictures in the past year to show how popular these attacks since 2010 until the present time.[13]

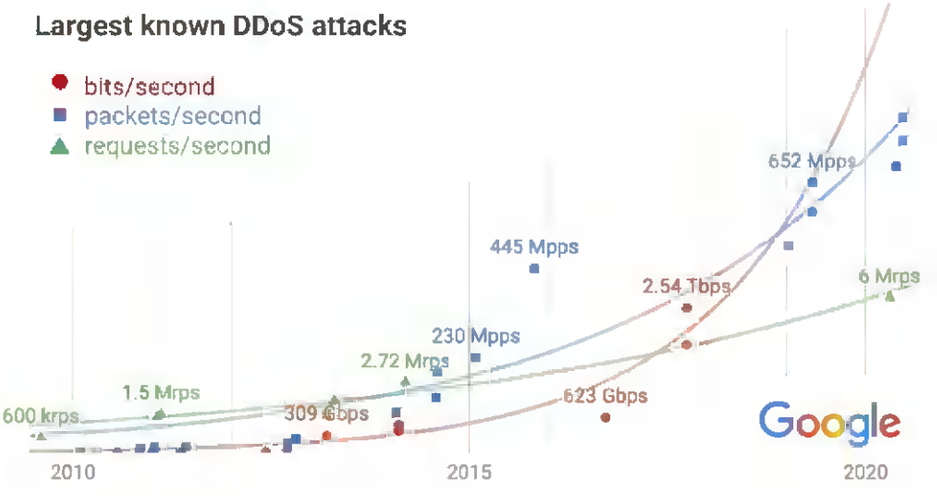

Fig. 3. Exponential growth in DDoS attack volumes [13]

("We need to factor in the exponential growth of the internet itself, which provides bandwidth and compute to defenders as well.") [13], comparing the growth of users with the growth of DDoS attacks we see that is a nice result, but it is important to use some counter measures to prevent these attacks. To prevent these attacks, we can use filters in our network, this only works if the hacker is not aware of this act, filtering lets your router analyze the information coming from outside the network and only letting into your device the clean information this prevents the overload of information. Using a secure overlay can be an option as well, this brings up a more trusted firewall that can only let go the clean information to the user's network. Honeypots is another way to protect your system from these attacks, it consists of miming your network, making the hacker attack a mimic network while your device and your network still intact.

Waterhole.
Protecting yourself from waterhole attacks u need to hide your online activity, you can use VPN for example this way your online activity gets encrypted, and it is more difficult for hacker to trace you.

Fake WAP.
To prevent this kind of attacks u should not connect your devices to unknown Wi-Fi's networks.

Trojan Virus.
Trojan virus are inside downloadable programs, first always avoid downloading software from unknown or not credited websites, most of these unknown downloads come with virus hidden in their installation launchers, making it unnoticeable to the user that is downloading apps, getting an anti-virus that can scan your pc from time to time also helps to clear any virus that got into your device by the user not noticing anything strange in downloads.

Phishing.
Avoiding Phishing is all about paying attention to emails that u might receive, some of them bring up messages that don't make sense with the user's reality, those are easy to spot. Getting a spam filter helps a lot in this manner and being informed and trained about some scenarios that appear when you get attacked by phishing.

Keylogger.
Defending versus a keylogger the user should get a 2-step verification, this always help to verify the usage of the website and may let you know if it's being used a keylogger or not, with this is important that the user is careful about his downloads, these malwares come on downloads from unknown sources as well.

6 Ciber attack on U.S. power grid could cost economy 1 trillion Dollars.

The report that we are going to see tell us about a study done by the university of Cambridge Center about the risk of a potential scenario that involves an electricity blackout in New York and Washington DC. The scenario created by Cambridge University is flagged as "technologically possible" to happen once in the next 200 years.

They speak of an episode for which it is necessary that the entities that ensure these electricity services are prepared for this possible threat.

The hypothetical attack created by this university, tells us about 93 million people with no electricity throughout New York and Washington DC. During this blackout the report shows an increase in the mortality of the population due to the lack of electricity in hospitals, which would cause the death of patients, including the non-operation of the hospital, security in all networks would also be a problem such as transport.

Since the US economy is directly linked to these types of services, it would be affected.

The estimated loss balance is also made, and we can draw our conclusions through this quote from the report ("The total impact to the US economy is estimated at $243 billion, rising to over $1 trillion in the most extreme version of the scenario") [14]

The extreme scenario speaks of the absence of support from 100 generators, which would lead to a loss of over 70 billion. These results are presented because of the evidence presented in 2014 in other major ("“Evidence of major attacks during 2014 suggests that attackers were often able to exploit vulnerabilities faster than advocates could remedy them,” said Tom Bolt, director of performance management at Lloyd's, in the report.[14]

7 Conclusion

Hacking is important because it helps companies in their own protection, to improve their services and make everything in a safer structure due to several known techniques.

We have several different types of hackers, and all have characteristics that can help in the evolution of security in this area.

Be they ethical hackers or malicious hackers, they all have the role of finding vulnerabilities and thus allowing for increased security.

We can observe that if security is not taken seriously, it can come to have great costs and an attack can come to affect great world powers at the economic level. These large-scale attacks can cause irreversible damage to companies.

Security must be taken seriously and more than protecting the network in real time, it must be taught how to avoid these same attacks, which part of the internet is secure and which part is suspicious through t these mitigation techniques. Attacks are more and more common which means that this area deserves much more attention from anyone thinking of connecting to the internet, now it is not just big companies that are the targets, but everyone can be targeted.

References

1. Regina D. Hartley Appalachian State University - Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack
2. Ms. Chandni M Patel*1, Asst. Prof. Viral H Borisagar #2 * C.S.E. Department, Government College of Engineering, Sector-28, Gandhinagar Gujarat Technology University, Gujarat, India. International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 9, November- 2012 ISSN: 2278-0181
3. Study Of Ethical Hacking Bhawana Sahare, Ankit Naik, Shashikala Khandey Research Scholar, Lecturer Department of Computer Science and Engineering, Kirodimal Institute of Technology, Raigarh Chhattisgarh – India - International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 2014
4. K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and InformationTechnologies,Vol.5(3),2014,3389-3393- http://ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503161.pdf last visited 2021/12/13
5. https://edgy.app/how-to-hack-for-the-greater-good-inside-ethical-hacking - photo by MatiasDelCarmine | shutterstock.com, last visited 2021/12/14
6. Palmer, C.C. (2001, April 13). Ethical Hacking. IBM Systems Journal Vol. 40 No.3 2001
7. Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack Regina D. Hartley Appalachian State University- https://scholarworks.lib.csusb.edu/jitim/, last visited 2021/12/14
8. A survey of distributed denial-of-service attack, prevention, and mitigation techniques Tasnuva Mahjabin1, Yang Xiao1, Guang Sun2 and Wangdong Jiang2 - https://journals.sagepub.com/doi/pdf/10.1177/1550147717741463, last visited 2021/12/14
9. Hacking Attacks, Methods, Techniques and Their Protection Measures Dr. Sunil Kumar1, Dilip Agarwal 2
10. Types of Hacking Attack and their Counter Measure Minakshi Bhardwaj and G.P. Singh
11. Survey of keylogger Technologies Yahye Abukar Ahmed, Mohd Aizaini Maarof, Fuad Mire Hassan and Mohamed Muse Abshir
12. Vulnerabilities and mitigation techniques toning in the cloud A cost and vulnerabilities coverage optimization approach using Cuckoo search algorithm with Levy flights Mhamed Zineddine MIS Department, ALHOSN University, Abu Dhabi, United Arab Emirates
13. https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks, last visited 2021/12/14
14. https://www.reuters.com/article/us-cyberattack-power-survey-idUSKCN0PI0XS20150708-, Reporting by Carolyn Cohn, editing by Louise Heavens, last visited 2021/12/17