Cyberattack types - methods and technics for protection of communication resources

Zornitsa Terneva[1], Maria Nenova[2], Viktoria Terneva[3], Ivaylo Vladimirov[4] and Desislava Nikolova[5]

Abstract – **The paper is focused on analysis of the main types of cyberattacks and how this can help with ethical hacking. Instead of the analysis performed for some of those attacks will be proposed a technique and specifics of algorithms for protection against them. The paper will present how ethical hacking can be implemented as a part of test process for hardware or software. Also which of the malicious actions can be successfully used in smart homes. This is becoming increasingly relevant and important for the daily live of the ordinary people.**

Keywords – **cyberattacks, hackers, security, protection, vulnerabilities, penetration testing**

I. Introduction

In the age of digital technology, where even the youngest children have devices and learn how to use them, the functionality of each new development leads the market. Everyone wants to have the latest software, everyone wants it to be easy to use, but if the emphasis is more on new functionality and ease of use - security remains on the background. That is when the "Security Triangle" happens.

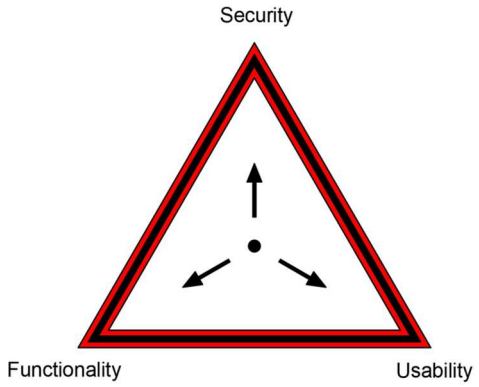

Figure 1: Security triangle

Figure 1 shows that the three elements of the triangle are mutually connected. But it often happens that the companies rely more on the ease of use of functionality and put product security in the background. This is why ethical / white hackers exist. They try to detect vulnerabilities in software and offer a solution to improve security. Despite significant investments in cybersecurity practice and research, the frequency and severity of security vulnerabilities in software is increasing [1].

II. The Problem

Nowadays, most attacks are aimed at smart devices. And this poses a huge risk to the security and privacy of the people themselves. Hackers seek to access sensitive information from their victims and use it against them. Smart devices make human life easier, but concerns about IoT security and privacy remain a major issue for IoT users and developers [2]. It is not uncommon for hackers to leave back doors so that they can access information again. The rear doors themselves are sometimes very difficult to detect even with special monitoring software.

In recent years malicious code injection attacks have been very common. For example, malicious SQL code can be "injected" into vulnerable applications [3]. But in addition to those mentioned, there are many other types of attacks. Other common malicious acts are: Eavesdropping on traffic; The man in the middle; Denial of Service (DOS), Social Engineering and many more.

Regardless of the type of the attacks, the main factor is the human being. Even if the hacker attacks are not clearly directed against him and the hacker remains in the shadows, there is a great risk to the security of information due to the users themselves. That is why in recent years, especially during the pandemic, the emphasis has been on social engineering attacks. One of the most popular types of attacks in social engineering is the phishing attack [4]. Upon it, the users receive fraudulent emails that are purposefully sent to the user in order to affect his psyche. Man is the weakest link. [5]

As an example, consider a web application that allows users to manage their bank accounts online. We live in a digital world and such actions happen all the time. Before allowing access to

[1]Zornitsa Terneva is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: zterneva@tu-sofia.bg

[2]Maria Nenova is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: mvn@tu-sofia.bg

[3]Viktoria Terneva is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: vterneva@tu-sofia.bg

[4]Ivaylo Vladimirov is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: ivladimirov@tu-sofia.bg.

[5]Desislava Nikolova is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria. E-mail: dnikolova@tu-sofia.bg

978-1-6654-8500-5/22/$31.00

an account, the application requires a username and personal identification number - PIN. There are many opportunities for various threats: gaining control over the bank's web server, creating a random account, accessing an account without a PIN code, etc. [6] And again here we can confirm that the human is the weakest link. Not all users are well informed about the threats of hacker attacks and what harm they can do. Another example is when using smart home devices, such as a smart camera. There are options for a person with unauthorized access to contact it and watch what is being broadcast on the camera.

So far, the article has discussed the vulnerabilities of the software and the user - victim, as a key factor for more successful attack. But there is something else that plays an important role in how big the threat could be. That would be the motivation of the hackers themselves and the reason why they want to carry out that malicious actions. Motivation clearly determines the type of hackers behind the attacks and the level of danger.

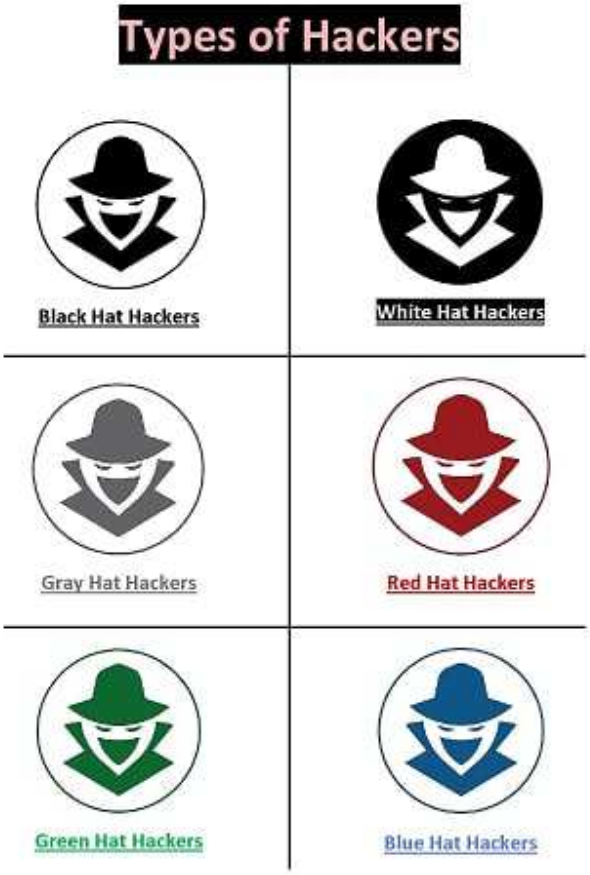

Fig 2. Types of hackers

Figure 2 shows that the main types of hackers are divided into 6 types:

- White hat hackers - these are ethical hackers. They test and look for vulnerabilities in software to offer solutions for better protection and security of information. Hackers with white hats use the same hacking methods as hackers with black hats. But they hack the system with the permission of the network owner. This makes the process legal. They perform penetration tests and vulnerability assessments and recommend solutions to correct them.

- Gray hat hackers - they do not care if their actions will harm someone. They accept the challenge if they can get something for themselves. They are a hybrid between black and white hackers. Gray hat hackers search for system vulnerabilities without the owner's permission, but generally not for malicious purposes. If they find problems, they inform the owner and can offer a solution for a fee. If the owner refuses, some gray hat hackers can publish the information online.

- Black hat hackers - they are only looking for profit. These hackers are computer hackers experts who use their skills to make profits illegally. Black hat hackers hack into systems without the permission of the owners. They are the bad participants. They distribute malware or aim to steal sensitive data. They may also alter or destroy data for ransom.

- Red Hat Hackers - Just like hackers in white hats, hackers in red hats want to save the world from bad hackers. But they choose extreme and sometimes illegal ways to achieve their goals. Red Hat Hackers are like Robin Hood in cybersecurity - they're going the wrong way to do the right thing. When they find a hacker with a black hat, they launch dangerous cyberattacks against him.

- Blue Hat Hackers - Two different definitions prevail in the field of cybersecurity and have almost nothing in common.

  - Blue Hat Hacker Definition 1: Revenge Seekers

  These hackers are not necessarily interested in money or fame. They hack to get revenge. These hackers use malicious software and deploy various cyber attacks on their enemies' servers / networks to damage their data, websites or devices.

  Sometimes they do docking and publish personal and confidential data of their enemies. In this way, they discredit their enemies.

  - Blue Hat Hacker Definition 2: External security professionals

  Blue hat hackers are security professionals who work outside the organization. Companies often invite them to test new software and find security vulnerabilities before releasing

it. Blue hat hackers perform penetration tests and use various cyber attacks without causing damage.

- Green Hat Hackers – They are new to hacking.

These are the "newcomers" in the world of hacking. Green hackers are not aware about the security mechanism and the internal workings of the network. These young hackers are fast learners and are motivated to rise in the hacking community. Although their intention is not extraordinary to cause harm, this can be done while trying out various software and attack techniques.

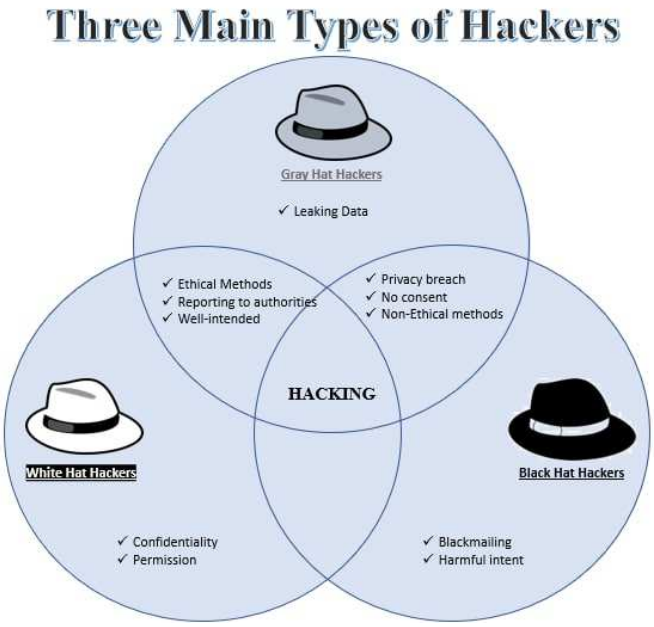

Figure 3: Main types of hackers

Despite the wide variety of hackers, Figure 3 shows the three main types of hackers: Black hat hackers, Gray hat hackers, and White hat hackers. They have different intentions and goals, but what they all have in common is that they all hack systems and use cyberattacks.

The huge number of network protocols and applications with their functionality are becoming a source of vulnerabilities in the IT infrastructure. Such vulnerabilities can be exploited by hackers or attackers who seek to benefit from access [7].

Although ethical hackers try to detect vulnerabilities in the system and help eliminate them, black hackers are often one step ahead. Attackers do not bother to do damage and the programs and devices that they use for their attacks are much more diverse. White hat hackers , on the other hand, are careful not to do harm and use more harmless programs. This restriction is in favor of black hat hackers . In addition, new attack programs are constantly being created, so protection methods need to be up to date.

III. The solution

This section will discuss the different methods of protection against malicious attacks and the evolution of technologies for protecting people's software and sensitive information .

For better protection, one should pay attention to the settings of the router and server. It is recommended to use strong encryption and appropriate protocols for data security in traffic, to install useful applications, etc.

The use of two-factor authentication is a good method nowadays to protect personal data from cyber attacks. Most online platforms offer two-factor protection, it only needs to be activated. It is triggered every time the system detects an attempt to gain unauthorized access to your account.

Routers should not be overlooked either. Another good and recommended method is to update the router's firmware. The router is the door between every computer and the world wide web. Much of the hacking attack on routers is due to the fact that their firmware has not been updated. The update occurs when you enter the router settings and press the refresh button.

The effectiveness of the firewall as well as the use of an antivirus program should not be underestimated. It is no coincidence that complex passwords are widely requested on the Internet. Passwords must have at least one special character, uppercase letter, lowercase letter, and number. It is recommended not to use mass words, birthdays, etc. They can be easily broken. It is recommended that each user monitors what sites they visit. When a site starts with the HTTP protocol, it means that it is not secure and hackers can easily access it. In order to be more secure on the Internet, it is important that the sites you visit have the HTTPS protocol.

Security engineers have developed software platforms and environments for testing various hacker attacks, which are very useful for cybersecurity [8]. There are also laboratories that perform various vulnerability tests. Due to the growing need for skilled professionals, an increasing number of commercial providers have developed online or virtual cybersecurity platforms [9]. They can be reached by students in the process of their education, as well as employees in various companies and organizations. For example, since May 2020, Virtual Hacking Laboratories [10] offer cards with different durations over time. The minimum access time is 1 week, and the longest period these virtual labs can be used is 1 year. Accordingly, their prices are different. In addition to the various laboratories, specialized courses are being set up to meet the quality and requirements of the CAE Cyber Operations Knowledge Units [11]. It is also very important to increase security when using mobile devices, because they are an even easier target than computers and contain more personal information. These courses are aimed in this direction. IoT devices are used in the

various courses [12]. In this way the quality of the curricula is improved and modern technologies are used.

Ethical hackers use different types of testing to try to find vulnerabilities. There are four typical types of penetration tests: external testing, in-house testing, blind testing and double-blind testing [13].

Different intrusion scenarios are being played out. After successful penetration, a report is written with detailed steps on what they have done, what they have managed to access and instructions for improving security.

Using appropriate programs is also very useful and is recommended. There are a variety of tools that can be used for penetration testing [14] or for protection. Some of them are open source and can be automated by users depending on their needs.

IoT devices have faced a number of cyber attacks [15]. It is necessary to identify the various malicious actions and to apply the specific measures according to the specific type of attack. It is essential that ordinary consumers are aware of the risks and minimize them for their safety.

IV. Conclusion

It is crucial to identify attacks in their early stages, not just when they are actually carried out, in order to protect our systems with effective security measures. With the advancement of technology and the entering into the digital world, the danger of cybercriminals is growing. New and better tools are being created to allow hackers to access sensitive information from their victims, but counteraction and protection methods are also improving. Various courses and laboratories are being set up to teach people how to protect themselves in the digital age.

Acknowledgement

This scientific paper is part of a research project.

References

[1] N. Munaiah, J. Pelletier, S. Su, J. Yang, A. Meneely, "A Cybersecurity Dataset Derived from the National Collegiate Penetration Testing Competition", Hawaii International Conference on System Sciences, January 2019;

[2] S. Hashemi, M. Zarei. "Internet of Things backdoors: resource management issues, security challenges, and detection methods", Transactions on Emerging Telecommunications Technologies, vol. 32, no. 2, pp. e4142, Wiley Online Library 2021.

[3] W. G. Halfond, J. Viegas, A. Orso, "A classification of SQL-injection attacks and countermeasures", In Proceedings of the IEEE international symposium on secure software engineering, vol. 1, pp. 13-15, IEEE, 2006.

[4] Z. Terneva, I. Vladimirov, D. Nikolova, "Accessing LinkedIn and Google E-mail Databases Using Kali Linux and TheHarvester,", 56th ICEST Conference, 2021;

[5] M. Velev, "Penetration testing and information security", Pragmatic lectures, 2019;

https://pragmatic.bg/all-courses/

[6] H. H. Thompson, "Application penetration testing," in IEEE Security & Privacy, vol. 3, no. 1, pp. 66-69, Jan.-Feb. 2005, doi: 10.1109/MSP.2005.3.J. Kizza, "Guide to Computer Network Security", Springer, 2017, ISBN 978-3-319-55605-5;

[7] J. Kizza, "Guide to Computer Network Security", Springer, 2017, ISBN 978-3-319-55605-5;

[8] L. Nikolov, V. Slavyanov, "Network Infrastructure For Sybersecurity Analysis", Proceedings of International Scientific Conference "Defense Technologies", Faculty of Artillery, Air Defense and Communication and Information Systems October 2018;

[9] A. -N. Moldovan, I. Ghergulescu, "Leveraging Virtual Labs for Personalised Group-based Assessment in a Postgraduate Network Security and Penetration Testing Module," 15th International Workshop on Semantic and Social Media Adaptation and Personalization (SMA, 2020;

[10] Virtual Hacking Labs, "IT Security Training Labs & Courses." April 2022, ; https://www.virtualhackinglabs.com/

[11] NSA, "Academic Requirements for Designation as a CAE in Cyber Operations Fundamental", 2020; https://www.nsa.gov/Resources/Students-Educators/centers-academic-excellence/cae-co-fundamental/requirements/

[12] T. OConnor, C. Stricklan, "Teaching a Hands-On Mobile and Wireless Cybersecurity Course", 56th ICEST Conference 2021;

[13] C. Weissman, "Security penetration testing guideline", Center for Secure Information Technology, Naval Research Laboratory (NRL), US, 1993;

[14] M. Denis, C. Zena and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies,", IEEE Long Island Systems, Applications and Technology Conference (LIS Proceedings of International Scientific Conference "Defense Technologies",

[15] Faculty of Artillery, Air Defense and Communication and Information Systems Proceedings of International Scientific Conference "Defense Technologies",

[16] Faculty of Artillery, Air Defense and Communication and Information SystemsAT), 2016;

[17] G. A. Abdalrahman and H. Varol, "Defending Against Cyber-Attacks on the Internet of Things," 7th International Symposium on Digital Forensics and Security (ISDFS), 2019;