Protection of computer systems and networks from attacks

Dr.sc. Marijan Mijatović, Dr.sc. Marko Mijatović, Dr.sc. Srećko Stanković

photo.by.mile@gmail.com, marko.mijatovic@hercegovina.edu.ba, srecko2403965@gmail.com

Nezavisni Univerzitet Banja Luka, Veljka Mlađenovića 12e, 78000 Banja Luka, Republika Srpska

Sveučilište Hercegovina, Fakultet društvenih znanosti doktora Milenka Brkića, Kraljice Mira 3A, 88266 Bijakovići, FBiH

Abstract

Technological development emphasizes faster and more dynamic development of new services and products, while security aspects have generally had very little impact on the widespread adoption of new technologies. Users typically have minimal knowledge of the technology they use, especially its applications, making it very difficult to assess the security features of most commercial products regarding the protection of users' data. Modern enterprises are deeply embedded with communication and information technology. People are connected through various technologies for transmitting text, images, sound, etc. The creation of the internet has established a sovereign cyber space composed not only of the aforementioned infrastructure but also of an ever-growing amount of available data and users who increasingly communicate with each other. Nowadays, individuals are more exposed in cyber space, which in turn increases their vulnerability to attacks. Additionally, there is a growing need for the protection of electronic data, known as cyber security.

Keywords: Cybersecurity, Attacks, Systems, Protection, Hackers

Introduction

Cybersecurity and hacking are becoming key parts of today's business processes. Once, the security of digital operating systems was often just an overlooked afterthought. Nowadays, this is no longer the case. With the increasing public awareness of private, health-related, sensitive, and personal data, there is growing pressure on data managers. It is essential to ensure very strict and documented processes for handling, processing, and storing sensitive information.

Cybersecurity involves the thorough monitoring, analysis, and testing of systems, during which existing vulnerabilities in the systems are identified, documented, and repaired. This process can be divided into multiple levels and sub-levels, involving members of the entire project team. The fundamental concepts of cybersecurity are explained, different classifications of attacks and attackers are described, the concept of hackers is defined, and all stages of system testing and attacks on them are presented. Cybersecurity is presented from the perspective of organizational risk management.

Vulnerabilities and their impacts, methods for identifying, analyzing, and managing risks are outlined. The practical part consists of demonstrating hacking principles on a selected operating system. The system consists of a simple web application or website and a Linux server on which it is hosted. The methods demonstrated provide unauthorized access to the system for monitoring web media content on the site, as well as unlimited, unauthorized access and control over the entire server.

1. Basic concepts of cybersecurity

Security engineers must be familiar with both the basic and advanced concepts of cybersecurity to operate effectively. Each of the fundamental principles is crucial for a specific aspect of information security and maintaining trust in the system. The main concepts that need to be understood are:

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation

Confidentiality of data refers to ensuring that information is kept confidential by clearly defining access rights for each piece of information we possess. It encompasses all the measures necessary to provide access to data only to individuals who have been granted the appropriate access rights. It also means that data should not be accessible to individuals who do not have authorization to handle it. One method of achieving data confidentiality is through data encryption. Such data can only be accessed by individuals who know the encryption method, key, and decryption process. Another potential way to ensure confidentiality is by implementing access control systems. An example of such a system is Microsoft Active Directory.
Ensuring data security and integrity does not mean much if the data that must be handled is not available. Availability encompasses all procedures and measures that ensure a system, network, or data is accessible to authorized individuals attempting to access them. Attacks on availability generally fall into the category of attacks known as Denial-of-Service (DoS). The goal of this type of attack is to overload the system with data requests, thereby preventing legitimate users from accessing it. If the system is constantly serving the attacker, it will not have enough resources to process legitimate data requests. DoS attacks vary greatly in terms of technical complexity. They range from highly sophisticated and complex attacks to simple actions such as turning off the power to a component critical to the system's operation.

1.1. Motivation for attacking systems

The reasons for cyber-attacks encompass a wide range of motivations, from simple individual curiosity to coordinated and sponsored attacks by state or terrorist organizations. Nowadays, awareness and understanding of threats provide a significant advantage for any organization's operations, which is why it is necessary to invest substantial resources in the continuous development of security systems.
Political attacks aim to spread propaganda, disable the online presence and infrastructure of political opponents, and coordinate and finance crimes in both the cyber and real domains. One of the more well-known examples, also characterized as the first internet war, is the conflict that began in 1998 over control of Kosovo. Hackers on both sides of the conflict disrupted access to state computers and disabled government

organization websites. The internet was also used as a tool to share content such as text, images, and videos that were not available through other media.
Economic cyber-attacks aim to secure financial resources, personal or corporate gain. The most well-known are the so-called Ransomware attacks. Attackers gain access to a protected system, encrypt all available data, and demand a ransom from the owner for access to the decryption keys. Even if the data owners decide to pay the ransom, there is no guarantee that they will regain access to the original data. These attacks are particularly dangerous for critical systems, such as those in hospitals, where the uninterrupted operation is crucial for many human lives. The best way to defend against this type of attack is to ensure multiple copies of critical data.

1.2. Classifying cyber attackers

Attacker profiles can primarily be divided into two groups: internal and external attackers. Internal attackers pose the greatest threat to an organization because they already have a certain level of access. Dissatisfied employees and recently terminated employees can cause significant damage to an organization if their accounts are not immediately deactivated upon termination of employment. Thorough checks are necessary when hiring new staff. An attacker may apply for an open position to gain access to the system and later use their position to harm the organization from within.
In addition to malicious attackers, accidental damage to an organization is also possible. Every employee should study the organization's guidelines for properly handling data, passwords, and programs in their daily work environment at the beginning of their employment. Continuous education is also crucial for the organization's security. Staff should attend a security seminar every four to six months. It is particularly important to educate staff about the dangers of social engineering. Attackers often use email to try to obtain sensitive data from the organization. Every system is only as secure as its weakest point. Nowadays, the weakest point in a system is often the people who use it and have access to its data.

2. Ethical hacking

2.1. Hackers and their classification

A hacker is a person with strong skills and interest in computers, software, hardware, computer networks, and similar areas, with a particular emphasis on a pronounced desire to experiment, analyze, and test systems. They are especially characterized by their motivation to find security vulnerabilities in systems. In modern times, the term hacker carries negative connotations and is increasingly used to describe individuals involved in illegal activities aimed at causing harm, whether to specific individuals or companies. The security community opposes this specific definition and prefers to use the term "cracker" or "attacker" to describe individuals who act in an unethical and dishonest manner.
In addition to the division into ethical hackers (or simply hackers) and unethical hackers, or crackers, a highly visual classification using hat colors is also used. This terminology has its roots in American popular culture from Western films, where protagonists typically wore light-colored hats, while antagonists often wore completely black hats. The security community adopted this concept, and ethical hackers are often referred to as hackers wearing white hats, while crackers are called hackers wearing black hats.

Unlike the two previously mentioned groups, crackers pay no attention to the morality and ethics of their actions. They will take ownership of any system and cause damage if they are able to do so. They often act alone, but it is also possible to encounter organizations interested in engaging in illegal activities in cyberspace. One of the most well-known crackers is Kevin Mitnick, who attacked more than forty major corporations worldwide.

2.2. The levels of system testing implementation

There are five different levels when conducting each security test of a system. These levels do not necessarily have to be sequential, as there can sometimes be some overlap or skipping of steps. Hackers will not waste time on recon of the entire system if they immediately spot an easy opportunity to gain access.

The first level of testing involves gathering publicly available information about a potential target (Reconnaissance). During this step, hackers use passive attack methods: they assess the state of physical security, visit the target's websites, and collect relevant information that may later be useful. They also study job advertisements for the organization they intend to attack, as these ads may reveal which technologies and hardware are used internally. At this level, they may also study the movement of personnel, record their schedules, determine the number of employees working in the organization, and identify their shifts, etc.

3. Cybersecurity

Cybersecurity is a very broad term that spans many branches of information technology. Cybersecurity is defined as applied information security concerning all electronic information. In other words, information security also includes concepts outside the domains of networks, applications, the internet, and the cyber (digital) space.

Maintaining security in today's world must be a priority for every serious organization. What sets the best organizations apart from others is their approach to the principles of implementing security procedures. Organizations that treat security as an integral part of their business processes throughout their existence face fewer breaches and incidents, and their response time to critical situations is reduced. A company with developed security risk control methods has the following characteristics:

- The company's board recognizes the importance of security and sees investment in security as a positive addition to the business.
- Senior management is actively involved in implementing security methodologies.
- Security risks are effectively monitored, and sufficient human and financial capital is provided to support security.
- Industry standards and methodologies are followed during the construction, implementation, and monitoring of security.
- Security strategies are continuously aligned and analyzed to ensure they are in line with business objectives.
- Performance of existing security methods is monitored and reported in comparison with international recommendations.
- Security priorities and activities are optimized and adjusted according to existing threats and the company's needs.

3.1. Vulnerabilities and their impact

Vulnerabilities are an integral part of an organization's assets. The term assets does not only refer to the data and information an organization stores on its infrastructure. Assets have a broader meaning and encompass hardware, software, information about physical locations, the organization's infrastructure, and more. It is important to note that a threat and a vulnerability do not have the same meaning. A threat is a term used to describe an attacker who must possess three characteristics to achieve their goal:

- Motive
- Means
- Method

Conclusion

The protection of computer systems and networks from attacks is a crucial aspect of security in the digital age. Various types of threats, such as malware, phishing, DDoS attacks, and unauthorized access, require the implementation of advanced security measures. The use of encryption, firewalls, antivirus programs, security policies, and regular system updates helps prevent attacks and protect sensitive data.
In addition to technical measures, it is extremely important to educate users about security threats and best practices for data protection. Organizations and individuals should continuously monitor new security threats and adjust their defensive strategies to stay one step ahead of cyber attackers.
In conclusion, effective protection of computer systems and networks requires a combination of technological solutions, continuous monitoring, and user education. Only an integrated approach can ensure a high level of security and reduce the risk of cyberattacks.

References

- B. Reinheimer, L. Aldag, P. Mayer, M. Mossano, R. Duezguen, B. Lofthouse, T. v. Landesberger i M. Volkamer, (2020). »An investigation of phishing awareness and education over time: When and how to best remind users,« u Proceedings of the Sixteenth Symposium on Usable Privacy and Security, Redmond Washington USA.
- D. Antonucci, (2017). The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities, Hoboken, New Jersey.: John Wiley & Sons.
- D. Sutton, (2017). Cyber Security: A Practitioner's Guide, Swindon, UK: BCS Learning & Development Ltd.
- J. Arquilla i D. Ronfeldt, (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy, Santa Monica, California: National Security Research Division Corporation.
- K. Poulsen, R. McMillan i M. Evans, (2021). »A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death,« The Wall Street Journal,. [Mrežno]. Dostupno na: https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116.
- Kaspersky, »Black hat, White hat, and Gray hat hackers – Definition and Explanation,« AO Kaspersky Lab, [Mrežno]. Dostupno na: https://www.kaspersky.com/resource-center/definitions/hacker-hat-types. [Pokušaj pristupa 24. kolovoza 2022.].
- M. Sohaib, (2022). Ethical Hacker's Certification Guide (CEHv11)—A Comprehensive Guide on Penetration Testing Including Network Hacking, Social Engineering, and Vulnerability Assessment, Noida, India: BPB Publications.
- R. Lehtinen, D. Russel i G. T. Gangemi Sr., (2011). Computer security basics, Sebastopol, California: O'Reilly Media.
- S. Jelen, (2021). »Hacker vs Cracker: Main Differences Explained,« SecurityTrails, [Mrežno]. Dostupno na: https://securitytrails.com/blog/hacker-vs-cracker. [Pokušaj pristupa 24. kolovoza 2022.].