Privilege Escalation:
Threats, Prevention, and a Case Study

Gencay Özdemir
Ahmet Yesevi University, Turkey

Gurkan Tuna
https://orcid.org/0000-0002-6466-4696
Trakya University, Turkey

EXECUTIVE SUMMARY

Considering we use technology in almost every area of our daily life, and the fact that the internet has become a part of our lives, the size of the risks and threats it brings has grown considerably. The expansion of the cyber environment day by day has transformed cyber attack methods into a system that updates itself day by day. Many methods continue to be developed to ensure information security in the cyberspace environment. The main objective of this chapter is to examine the vulnerabilities of privilege escalation used by cyber attackers and to explain what can be encountered in possible attack scenarios; measures that can be taken and methods that can be applied.

INTRODUCTION

Changes have come into play in many areas due to the Internet becoming an indispensable element of our daily lives. With the development of information technologies, the increasing use of the Internet has begun to be used as an indispensable tool in the personal, private sector and the public. For example, public institutions have transformed their services into e-services in order to make our daily life easier.

With the introduction of such services and factors such as facilitating access to information, continuation of the service regardless of distance, saving time, enable citizens to access all services in a fast and safe way. However, the existence of these services in cyberspace has brought certain risks.

In parallel with the advancements in technology, high technology products have been put into the service of humanity. Although high technology products make our lives easier, information security related threats and risks they bring continue to increase in complexity. The Internet emerged in the 1960s with the ARPANET, which was established to provide data communication for the US Department of Defense (Denning, 1989). Since the Internet is a structure that provides information exchange through certain protocols that connect billions of devices and millions of networks to each other, its use has become widespread all over the world. On the other hand, attacks on the Internet reveal how serious the situation has reached at the point of cyber security. It is clearly seen that taking institutional and individual measures to reduce risks with the spread of the Internet has become a part of our daily life (Aslay, 2017).

It is possible for both corporate users and individual users anywhere in the world to be exposed to cyber attacks, intentionally or unintentionally, at any time. Cyber attacks have more destructive effects on corprorate users. However, the systematic structure of cyber security is weak in most organizations and there is a lack of personnel with sufficient cyber security knowledge and experience (Li & Liu, 2021). Security measures taken to ensure the healthy survival of information systems, to ensure information security, and to prevent the services from being disrupted may become insufficient. Therefore, information systems sometimes are used to serve malicious purposes by using their vulnerabilities, and they are exposed to various types of threats (Thomas, 2020; Güler, 2018). The way how cyber attacks is realized has been changing continually and is turning into a structure that relies on less manpower and more machines and artificial intelligence. However, still human factor is one of the most critical vulnerabilities in security and even the weakest link (Hughes-Lartey et al., 2021), it becomes inevitable that user rights in corporate structures cause serious weaknesses.

Although the worldwide availability of information systems and the Internet offers freedom to users, the number of cyber threats has been rapidly increasing everyday. On the other hand, new techniques for countering intelligence have been emerging, and defense mechanisms developed with the benefits of cryptology science have begun to become useful tools in cyber wars. Nowadays, corporate information systems are faced with threats from both inside and outside. Therefore, a continuous and follow-up approach should be adopted by conducting periodical penetration tests of institutions and companies in order to discover possible