

Tarea 1 - Reporte de L^AT_EX

Kathy Brenes Guerrero, Barnum Castillo Barquero

Maestría en Ciencias de la Computación, Introducción a la Investigación, ITCR

Abstract—One of the biggest issues that an operating system can experience is privilege escalation. Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. Understanding the weaknesses and flaws of a security level issue for the operating system can help implement better approaches and techniques to improve the software itself. Just because you have updated your computer to the latest update or patch, doesn't mean that it has been secured. Windows, for example, has a series of vulnerabilities that can affect the operating system and can't be solved by Microsoft because the updates can create incompatibilities with an older system or with some security protocols. The Privilege Escalation technique takes advantage of these vulnerabilities to gain privileges (access) within a remote system, in order to run applications and make commands on it. The focus of this paper is to list the vulnerabilities that have been demonstrated by third party systems in different operating system, and provide a technical point of view on what can be done to avoid these breaches (vulnerabilities or impacts). An Operation System breach can enable attackers to increase their level of control over target systems, such that they are free to access any data or make any configuration changes[4]. This study reveals the importance of the way in which current systems should be defended from this mechanism.

Index Terms—Operating System, Penetration Testing, Cyber-security, Internet of Things.

I. INTRODUCTION

To start talking about vulnerabilities, it might be easier to start with past operating systems, specifically MS-DOS and Windows 9x (95, 98 and Me), which were based on MS-DOS. All software running on an MS-DOS-based system was treated equally. Any program could, literally, do anything. Any program could play directly with the hardware, poke around in memory being used by other programs, or even modify the operating system itself on the fly.

It was not what we'd call 'secure' in any way. We suppose the only thing that prevented it from being a security nightmare is that today's ubiquitous connectivity didn't exist. Compared to what we take for granted today, it was at least cumbersome, and often outright difficult, to get data from one computer to another. Since the kernel can do anything, we refer to it as having more privilege than software running in user-mode. There are a number of different things that can be restricted based on privilege, but memory access is one of the clearer examples

A program running user-mode cannot read and write the memory of another program that happens to be running at the same time. Your web browser, for example, is not able to peek into the document you're currently editing in a word processor.

It's important to understand that this concept of privilege escalation matters. Hopefully, understanding the concept even at a high level and perhaps only partially will give you some idea that it's important, why it's important, and how it relates to the security of your computer.

Knowing that it's important, the single most important thing you can do to avoid issues and vulnerabilities that might be characterized as privilege escalation issues is to keep your system as up-to-date as possible. As with the recent CPU issue, operating system vendors are quickly putting out patches to avoid it, and it'll be important for you to have those patches when they come up.

The best way to do that is to keep whatever OS you run set to update automatically. Being always aware that keeping the operating system updated helps reduce the risk of these attacks but does not eradicate them 100

II. HISTORIA DEL L^AT_EX

Text here...

- 1) Interactive computing (time-sharing)
- 2) Hierarchical file systems
- 3) Fault tolerant structures
- 4) Interrupt systems
- 5) Automated overlays (virtual memory)
- 6) Multiprogramming
- 7) Modular programming
- 8) Controlled information sharing
- 9) Users

text here ...

III. USOS ACADÉMICOS, EXTENSIÓN, IMPORTANCIA

Text here ...

A. SubSection 1...

Text here..

- 1) Some Windows services are configured to run under the Local System user account. A vulnerability such as a buffer overflow (an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations) may be used to execute arbitrary code with privilege elevated to Local System. Alternatively, a system service that is impersonating a lesser user can elevate that user's privileges if errors are not handled correctly while the user is being impersonated (e.g. if the user has introduced a malicious error handler)[24].

- 2) Under some legacy versions of the Microsoft Windows operating system, the All Users screen saver runs under the Local System account any account that can replace the current screen saver binary in the file system or Registry can therefore elevate privileges [24].
- 3) In certain versions of the Linux kernel it was possible to write a program that would set its current directory to /etc/cron.d, request that a core dump be performed in case it crashes and then have itself killed by another process. The core dump file would have been placed at the program's current directory, that is, /etc/cron.d, and cron would have treated it as a text file instructing it to run programs on schedule. Because the contents of the file would be under attackers control, the attacker would be able to execute any program with root privileges [21].

Text Here

IV. ESTILOS DE DOCUMENTO

Text Here

A. Subsection 1

Example...

```
uname -a
cat /proc/version
cat /etc/issue
```

B. Subsection 2

Text here...

- 1) Check which processes are running

```
# Metasploit
ps
# Linux
ps aux
```

V. CÓMO HACER: PÁRRAFOS, EFECTOS DE LETRA, TILDES, TÍTULOS, SUBTÍTULOS, REFERENCIAS, MARCAS DE AGUA, HEADERS Y FOOTERS, MANEJO DE SALTOS DE PÁGINA, COLUMNAS DE LA PÁGINA, ETC.

A. Subsection 1

Text here..

VI. MANEJO DE TABLAS

A. Subsection 1

Text here..

VII. MANEJO DE FIGURAS Y GRÁFICOS

A. Subsection 1

Text here.

VIII. MANEJO DE FIGURAS AL LADO DE TABLAS (MINIPAGE)

A. Subsection 1

Text here.

IX. ECUACIONES MATEMÁTICAS

A. Subsection 1

Text here.

X. MANEJO DE COLORES

A. Subsection 1

Text here.

REFERENCES

- [1] A. Bryan (2013) *Vertical And Horizontal Privilege Escalation* [Blog post]. Retrieved from <https://bryanavery.co.uk/vertical-and-horizontal-privilege-escalation/>
- [2] A. Kurmus, N. Ioannou, M. Neugschwandtner, N. Papandreou & T. Parnell *From random block corruption to privilege escalation: A filesystem attack from rowhammer-like attacks* (Zurich, Switzerland, 2017).
- [3] M. Rangwala, P. Zhang, X. Zou & F. Li *A taxonomy of privilege escalation attacks in Android applications* (Indianapolis, USA, 2014).
- [4] Chandel, R. *4 Ways to get Linux Privilege Escalation*, November, 2016.
- [5] Stefano. *Dirty Cow: Story of a privilege escalation vulnerability*, June, 2016.
- [6] Lee, H., Kim, D., Park, M., Cho, S. (2016). *Protecting data on android platform against privilege escalation attack*. *International Journal Of Computer Mathematics*, 93(2), 401-414.
- [7] X. Jiang, *GingerMaster: First Android Malware Utilizing a Root Exploit on Android 2.3 (Gingerbread)*. Retrieved from <http://www.wisc.ncsu.edu/faculty/jiang/GingerMaster>.
- [8] H.-T. Lee, M. Park, and S.-J. Cho, *Detection and prevention of LeNa Malware on Android*, *J. Intern et Serv. Inf. Secur.* 3(3/4) (2013), pp. 6371.
- [9] M. Ongtang, S. McLaughlin, W. Enck, and P. McDaniel, *Semantically rich application-centric security in Android*, *Secur. Commun. Netw.* 5(6) (2009), pp. 658673.
- [10] Y. Park, C. Lee, C. Lee, J. Lim, S. Han, M. Park, and S.-j. Cho, *RGBDroid: A Novel Response-based Approach to Android Privilege Escalation Attacks*, *Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats (LEET12)*, San Jose, CA, April, 2012.
- [11] (2017) *What Is Privilege Escalation ?* [Blog post]. Retrieved from <https://affinity-it-security.com/what-is-privilege-escalation/>
- [12] (2017, November 27) *Privilege escalation vulnerability* Retrieved from <https://www.alibabacloud.com/help/faq-detail/37533.htm>
- [13] Nakamura, Y. & Yamauchi, T. *Proposal of a Method to Prevent Privilege Escalation Attacks for Linux Kernel* (September, 2015)
- [14] Piscitello, D (2015) *Qué es el escalonamiento de privilegios?* [Blog post]. Retrieved from <https://www.icann.org/news/blog/que-es-el-escalonamiento-de-privilegios>
- [15] (2018) *Privilege Escalation Linux* [Blog post]. Retrieved from https://chryzsh.gitbooks.io/pentestbook/privilege_escalation_-_linux.html
- [16] C. Long II, M *Attack and Defend: Linux Privilege Escalation Techniques of 2016* (January, 2016).
- [17] (2017) *Consigue instalar siempre con escalada de privilegios* [Blog post]. Retrieved from <http://www.enhacke.com/2017/02/28/escalada-de-privilegios/>.
- [18] Wilfahrt, N. *VulnerabilityDetails* (October, 2016).
- [19] Privilege Escalation, Coleman Kane, Coleman.Kane@ge.com, February 9, 2015.
- [20] Roch, Benjamin, "Monolithic kernel vs. Microkernel", 2004.
- [21] Feroze, R. (2018, February 22). A guide to Linux Privilege Escalation. Retrieved from <https://payatu.com/guide-linux-privilege-escalation/>.
- [22] iOS Hackers Handbook, Charlie Miller, Djon Blackakis, Dino Dai Xovi, Stefan Esser, Vincenzo Iozzo, Ralf-Phillip Weinmann, 2012.
- [23] B. (2013, December 19). *Vertical And Horizontal Privilege Escalation*. Retrieved from <https://bryanavery.co.uk/vertical-and-horizontal-privilege-escalation/>
- [24] Privilege Elevation - Microsoft Windows, Ivan Buetler, Compass Security, Q2/2007.
- [25] Denning, P. J. (2016). Fifty Years of Operating Systems. *Communications Of The ACM*, 59(3), 30-32. doi:10.1145/2880150
- [26] , *ETERNALBLUE Exploit Analysis and Port to Microsoft Windows 10* (June, 2017).
- [27] (2017, May 25). *7-Year-Old Samba Flaw Lets Hackers Access Thousands of Linux PCs Remotely*. Retrieved from <https://thehackernews.com/2017/05/samba-rce-exploit.html>