Exploiting Bugs to Take Advantage of Vulnerabilities on the Operating System

Ing. Kathy Brenes Guerrero, Student, ITCR, Ing. Sleyter Angulo, Student, ITCR, and Ing. Roberto Hernández, Student, ITCR,

Abstract—One of the biggest issues that an operating system can suffer through is the 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 application or user. Understanding weaknesses and flaws of a security level issue for the operating system can help to implement better approaches and techniques to improve the software itself. Having the latest update and patches of the operating system doesnt mean it is completely secure. Windows, for example, has a series of vulnerabilities that can affect the operating system and cant be solved by Microsoft because the updates can create incompatibilities with an older system or with some security network protocols. Privilege Escalation technique takes advantage of these vulnerabilities to gain privileges within a remote system, run applications and commands on it. The main focus on this paper is to list the vulnerabilities that have been demonstrated by third party systems in different operating systems and provide a technical point of views on what could be done to avoid vulnerabilities or impacts. Successful privilege escalation attacks 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 required to ensure freedom of operation and persistent access to the target system (Williams, 2016). It brings the study importance of the way in which current systems are defended from this mechanism.

Index Terms—Computer Society, IEEE, IEEEtran, journal, LaTeX, paper, template.

1 Introduction

This demo file is intended to serve as a "starter file" for IEEE Computer Society journal papers produced under LaTeX using IEEEtran.cls version 1.8b and later. I wish you the best of success.

mds
August 26, 2015

1.1 Subsection Heading Here

Subsection text here.

1.1.1 Subsubsection Heading Here

Subsubsection text here.

2 Conclusion

The conclusion goes here.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

Appendix two text goes here.

- *M. Shell was with the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332. E-mail: see http://www.michaelshell.org/contact.html*
- *J. Doe and J. Doe are with Anonymous University.*

Manuscript received April 19, 2005; revised August 26, 2015.

Acknowledgments

The authors would like to thank...

References

[1] H. Kopka & P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.

[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] (2017) *What Is Privilege Escalation ?* [Blog post]. Retrieved from https://affinity-it-security.com/what-is-privilege-escalation/

[7] (2017, November 27) *Privilege escalation vulnerability* Retrieved from https://www.alibabacloud.com/help/faq-detail/37533.htm

[8] Nakamura, Y. & Yamauchi, T. *Proposal of a Method to Prevent Privilege Escalation Attacks for Linux Kernel* (September, 2015)

[9] Piscitello, D (2015) *Qu es el escalonamiento de privilegios?* [Blog post]. Retrieved from https://www.icann.org/news/blog/que-es-el-escalonamiento-de-privilegios

[10] C. Long II, M *Attack and Defend: Linux Privilege Escalation Techniques of 2016* (January, 2016)

[11] (2017) *Consigue instalar siempre con escalada de privilegios* [Blog post]. Retrieved from http://www.enhacke.com/2017/02/28/escalada-de-privilegios/

[12] Wilfahrt, N. *VulnerabilityDetails* (October, 2016)

Michael Shell Biography text here.

John Doe Biography text here.

Jane Doe Biography text here.