ACADEMICIA: An International Multidisciplinary Research Journal
ISSN: 2249-7137 Vol. 11, Issue 11, November 2021 SJIF 2021 = 7.492
A peer reviewed journal

A REVIEW PAPER ON HACKING BLIND

Chanchal Chawla*

* Teerthanker Mahaveer Institute of Management and Technology,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: chanchal.management@tmu.ac.in
DOI: 10.5958/2249-7137.2021.02484.8

ABSTRACT

The author demonstrate how to build remote stack buffer overflow attacks against services that resume after a crash without having a copy of the target binaries or source code. This enables the hacking of proprietary closed-binary services as well as open-source servers that have been manually built and installed from source and whose binary is unknown to the attacker. Traditional methods are typically used in conjunction with a certain binary and distribution where the hacker is aware of the location of relevant Return Oriented Programming gadgets (ROP). Instead, our Blind ROP (BROP) attack identifies enough ROP gadgets across the network to execute a write system call and transmit the vulnerable binary, after which an exploit may be carried out using existing methods. This is done by leaking a single piece of data depending on whether or not a process failed when given a certain input string. Stack vulnerability and a service that restarts after a crash are required for BROP to work. We used Braille, a fully automated exploit that yielded a shell in under 4,000 requests (20 minutes) against a current nginx vulnerability, yaSSL + MySQL, and a toy proprietary server written by a colleague, against a contemporary nginx vulnerability, yaSSL + MySQL, and a toy proprietary server written by a colleague. The attack uses address space layout randomization (ASLR), no-execute page protection (NX), and stack canaries to operate against current 64-bit Linux.

KEYWORDS: *ASLR, Attack, Blind, Hacking, ROP.*

REFERENCES

1. Bittau A, Belay A, Mashtizadeh A, Mazières D, Boneh D. Hacking blind. Proc. - IEEE Symp. Secur. Priv., 2014;227–242. doi: 10.1109/SP.2014.22.
2. Erickson J. Hacking: The Art of Exploitation, 2nd Edition. .
3. Jordan T. A Genealogy of Hacking. University of Sussex Word Count: 8,253 (9,554 with Bibliography included). 2017;253:1–34.
4. Cekerevac Z, Dvorak Z, Prigoda L, Cekerevac P. Hacking, protection and the consequences of hacking. Communications - Scientific Letters of the University of Zilina. 2018;18(4):129 – 133. doi: 10.26552/com.C.2018.2.83-87.
5. Jordan T. A genealogy of hacking. Convergence: The International Journal of Research into New Media Technologies, 2017;23(5):28-544. doi: 10.1177/1354856516640710.
6. Omoyiola BO. The Legality of Ethical Hacking. J. Comput. Eng., 2018;20(1):61-63.

7. Barros US, Barros MS. A Survey of Ethical Hacking process and Security. in International Conference on System Modeling & Advancement in Research Trends (SMART), 2015.

8. Billig J, Danilchenko Y, Frank CE. Evaluation of google hacking in Proceedings of the 5th Annual Conference on Information Security Curriculum Development, InfoSecCD '08, 2008, doi: 10.1145/1456625.1456634.

9. Lakshmi C, Basarkod PI. Basics Of Ethical Hacking. 2015.

10. Suresh Kumar VVN. Ethical Hacking and Penetration Testing Strategies. Int. J. Emerg. Technol. Comput. Sci. Electron., 2014;5(3):3389-3393.