עבודה סמינריונית

תכנות מערכות דפנסיבי

סמינר: תכנות מערכות דפנסיבי 20928

מגיש: עמית סידס

בהנחיית: פרופ' לאוניד ברנבוים

תעודת זהות: 206768780

תאריך:

תוכן עניינים

מבוא

שפת C++

מבנה ותחביר השפה

מחלקות, אובייקטים וירושה

פולימורפיזם

מודל הזיכרון

איומי אבטחה

חולשת Stack Buffer Overflow
[1]

מתקפת Return-oriented Programming

דריסת משתנים וטבלאות וירטואליות
[2]

[3]

מנגנוני אבטחה

שפת Python

מבנה ותחביר השפה

דינאמיות השפה

מחלקות, אובייקטים וירושה

איומי אבטחה

חולשות ב-Deserialization

[4]

טעינת קובץ זדוני

[5]

חילוץ קבצים זדוניים

[6]

[7]

[8]

שימוש בפונקציות מסוכנות

מנגנוני אבטחה

תקשורת

אבטחה בתקשורת

פרוטוקולי הצפנה ואימות

אלגוריתם Diffie–Hellman
[9]

הצפנת RSA

פרוטוקול SSL

פרוטוקול TLS

מתקפות שונות על פרוטוקולי תקשורת

[10]

מתקפת POODLE

מתקפת BEAST

מתקפת CRIME

מתקפת Heartbleed

מתקפה על מנגנון האימות של TLS
[11]

[12]

אבטחת מערכת

מתקפות MiTM

מתקפת ARP Poisoning

[13]

[14]

מתקפת DNS Poisoning

[15]

מתקפות מניעת שירות

[16]

מתקפת DOS

מתקפת DDOS

מתקפת DRDOS

ביבליוגרפיה

[1] P. LACROIX and J. DESHARNAIS, "Buffer Overflow Vulnerabilities in C and C++," 7 August 2008. [Online]. Available: http://www2.ift.ulaval.ca/~desharnais/Recherche/RR/DIUL-RR-0803.pdf.

[2] "Exploiting C++ VTABLES: Instance Replacement," 11 May 2013. [Online]. Available: https://defuse.ca/exploiting-cpp-vtables.htm.

[3] C. Zhang, C. Song, K. Z. Chen and Z. Chen, "VTint: Protecting Virtual Function Tables' Integrity," February 2015. [Online]. Available: https://www.researchgate.net/profile/Chengyu_Song/publication/281784405_VTint_Protecting_Virtual_Function_Tables'_Integrity/links/55f8743d08ae07629dd5e648/VTint-Protecting-Virtual-Function-Tables-Integrity.pdf.

[4] K. Tanaka and T. Saito, "Python Deserialization Denial of Services," in *Computational Science/Intelligence & Applied Informatics*, 2018, pp. 15-25.

[5] A. Shaw, "10 common security gotchas in Python and how to avoid them," 16 June 2018. [Online]. Available: https://hackernoon.com/10-common-security-gotchas-in-python-and-how-to-avoid-them-e19fbe265e03.

[6] A. Abraham, "Exploiting insecure file extraction in Python for code execution," 28 September 2017. [Online]. Available: https://ajinabraham.com/blog/exploiting-insecure-file-extraction-in-python-for-code-execution.

[7] MITRE, "CVE-2019-9674 - denial of service via a ZIP bomb," 4 February 2020. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-9674.

[8] MITRE, "CVE-2019-20907 - TAR archive leading to an infinite loop," 13 July 2020. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-20907.

[9] Wikipedia, "Diffie–Hellman key exchange," [Online]. Available: https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange.

[10] A. Prodromou, "TLS Security 6: Examples of TLS Vulnerabilities and Attacks," 31 March 2019. [Online]. Available: https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/.

[11] D. Wagner and B. Schneier, "Analysis of the SSL 3.0 Protocol," November 1996. [Online]. Available: https://www.usenix.org/legacy/publications/library/proceedings/ec96/full_papers/wagner/wagner.pdf.

[12] N. Mavrogiannopoulos, F. Vercauteren, V. Velichkov and B. Preneel, "A cross-protocol attack on the TLS protocol," October 2012. [Online]. Available: https://www.researchgate.net/publication/262208728_A_cross-protocol_attack_on_the_TLS_protocol.

[13] B. Fleck and J. Dimov, "Wireless Access Points and ARP Poisoning," December 2013. [Online]. Available: https://digilander.libero.it/SNHYPER/files/arppoison.pdf.

[14] C. Nachreiner, "Anatomy of an ARP Poisoning Attack," 18 November 2012. [Online]. Available: http://csci6433.org/Papers/Anatomy%20of%20an%20ARP%20Poisoning%20Attack%20_%20WatchGuard.pdf.

[15] S. Son and V. Shmatikov, "The Hitchhiker's Guide to DNS Cache Poisoning," in *Security and Privacy in Communication Networks*, The University of Texas, Austin, 2010, pp. 466-483.

[16] Prolexic, "An Analysis Of DrDoS DNS Reflection Attacks," [Online]. Available: http://vertassets.blob.core.windows.net/download/74db6f36/74db6f36-56e7-4f4f-a6b4-a1880089f28a/analysis_of_drdos_dns_reflection_attacks_white_paper_us_031513.pdf.