The Windows Concept Journey — WRK (Windows Research Kernel)

2 min read · Dec 4, 2024

Shlomi Boutnaru, Ph.D. Follow

WRK (Windows Research Kernel) is a portion of the source code of "Windows XP"\"Windows 2003 Server" service pack 1 (2005 edition) — as shown in the screenshot below. The main usage of WRK was in universities\academies\scientific centers for investigating\researching the Windows NT kernel structure and working principles (https://betawiki.net/wiki/Windows_Research_Kernel). Using WRK we could extend the operating system for further research like implementing a new system call (https://osm.hpi.de/wrk/2007/07/howto-implementation-of-new-system-service-calls/).

Overall, using the WRK's guidelines we could build the kernel for x84/x64. However, the kernel is not enough but the rest of the Windows OS was not distributed with WRK (https://blog.adamfurmanek.pl/2018/07/21/windows-research-kernel-part-1/index.html). Also, WRK includes source for processes, threads, LPC, virtual memory, scheduler, object manager, I/O manager, synchronization, worker threads, kernel heap manager and other core NTOS functionality (https://www.academicresourcecenter.net/curriculum/pfv_ID_7366.html).

Lastly, WRK has been part of the “Windows Academic Program” which supplied universities with concert\code\projects for integrating Windows kernel technologies for teaching\researching. Beside WRK the program includes also CRK (Windows Curriculum Resource Kit) and ProjectOZ experimental environment — more on those in future writeups (https://web.archive.org/web/20130624215459/http://www.microsoft.com/education/facultyconnection/articles/articledetails.aspx?cid=2416&c1=en-us&c2=0).

See you in my next writeup ;-) You can follow me on twitter — @boutnaru (https://twitter.com/boutnaru). Also, you can read my other writeups on medium — https://medium.com/@boutnaru. You can find my free eBooks at https://TheLearningJourneyEbooks.com.

https://betawiki.net/wiki/Windows_Research_Kernel

Windows Security Technology Kernel Research

Follow

Written by Shlomi Boutnaru, Ph.D.

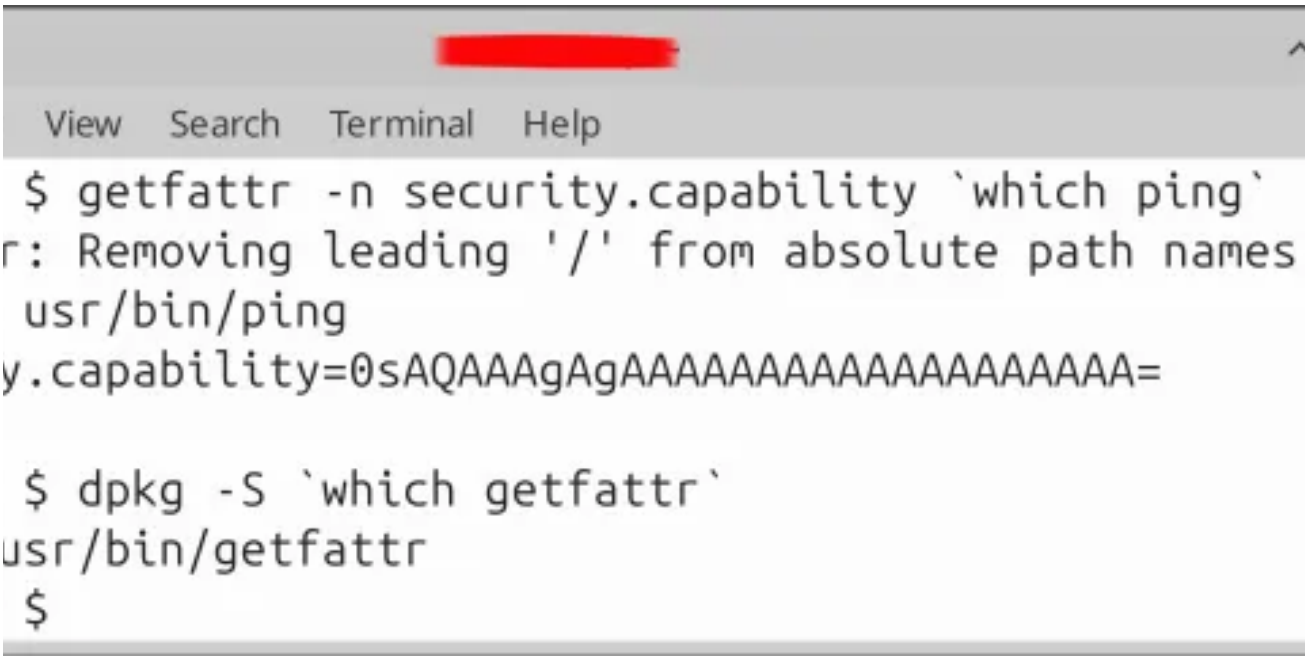
2.8K followers · 3 following

No responses yet

Write a response

What are your thoughts?

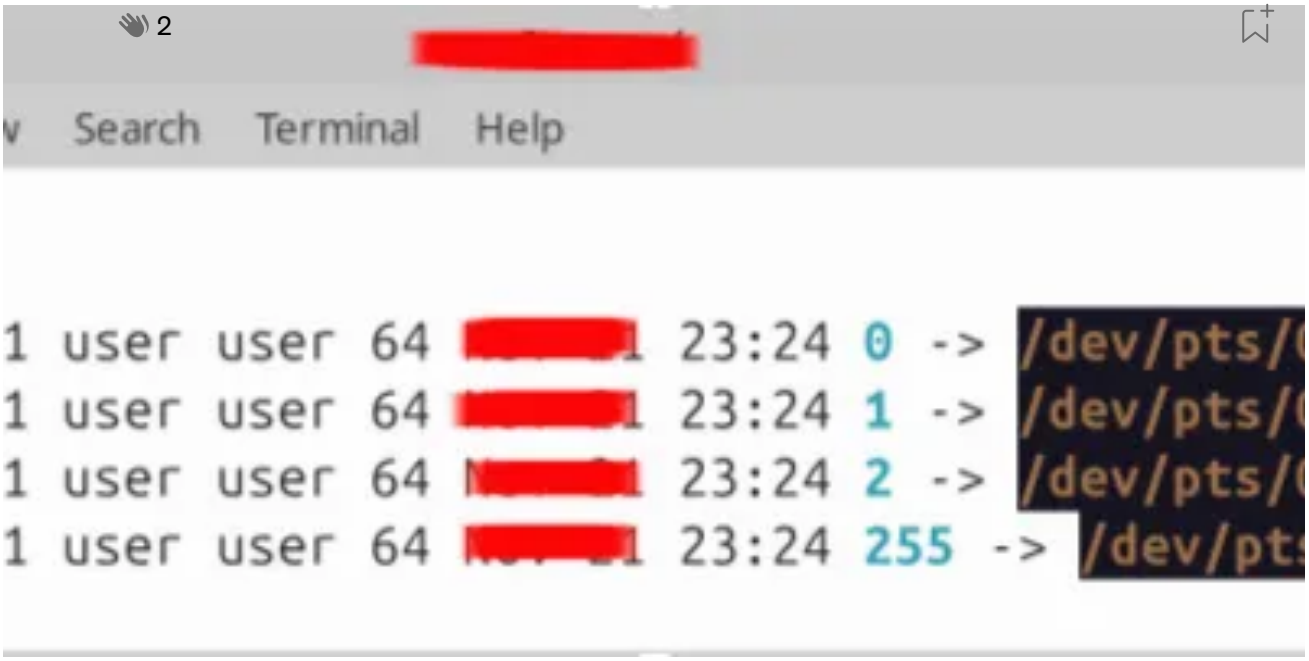
More from Shlomi Boutnaru, Ph.D.



Shlomi Boutnaru, Ph.D.

The Linux Concept Journey — Extended File Attributes (xattr)

Extended file attributes (xattrs) in Linux provide a mechanism for attaching permanent and non-standard metadata (in the form of...

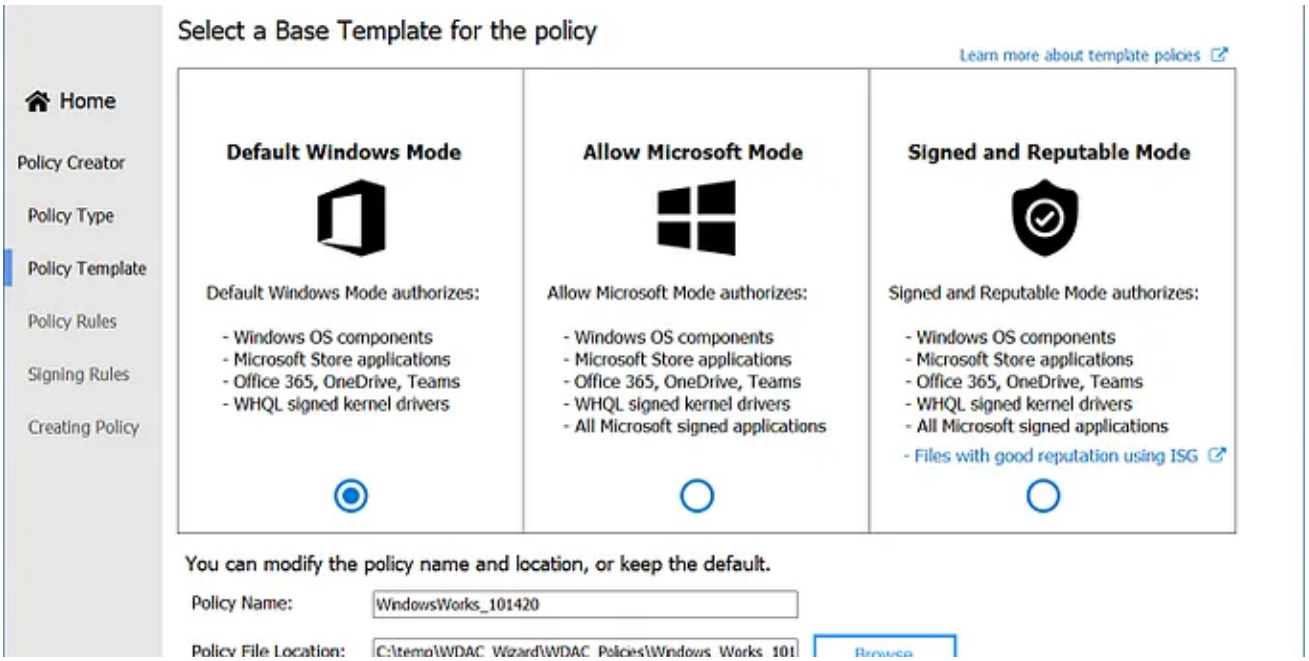


Shlomi Boutnaru, Ph.D.

The Linux Concept Journey — Everything is a File

The Unix\Linux concept that “everything is a file” means that diverse system resources (files\ devices\pipes\sockets\etc) are all treated...

Nov 24 2



Shlomi Boutnaru, Ph.D.

The Windows Security Journey — Differences between “WDAC” and “AppLocker”

In general, both AppLocker (https://medium.com/@boutnaru/the-windows-security-journey-applocker-application-locking-b9547fb9cbbd) and WDAC...

Sep 21, 2024 11

Shlomi Boutnaru, Ph.D.

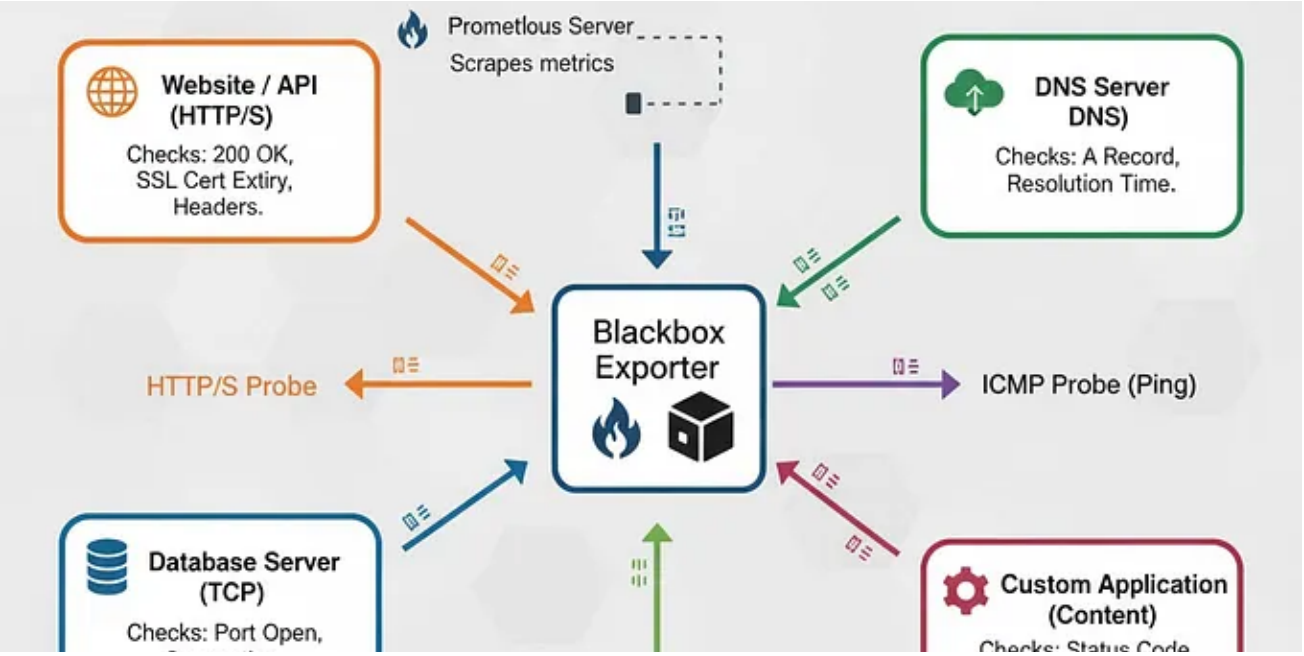
The Cryptography Concept Journey — Encryption

Encryption is a fundamental security process that transforms human readable data (aka “plaintext”) into an unreadable\scrambled format...

Dec 4 10

See all from Shlomi Boutnaru, Ph.D.

Recommended from Medium

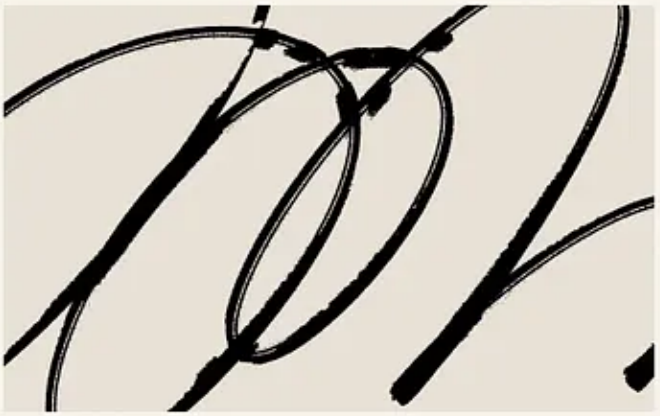


Sai Kiran Pikili

Don’t Just Monitor Your Containers, Monitor Your Customers: The Power of the Prometheus Blackbox...

Before you start reading this blog, I’d suggest checking out my previous blog to get a better understanding of observability, monitoring...

Nov 16 10

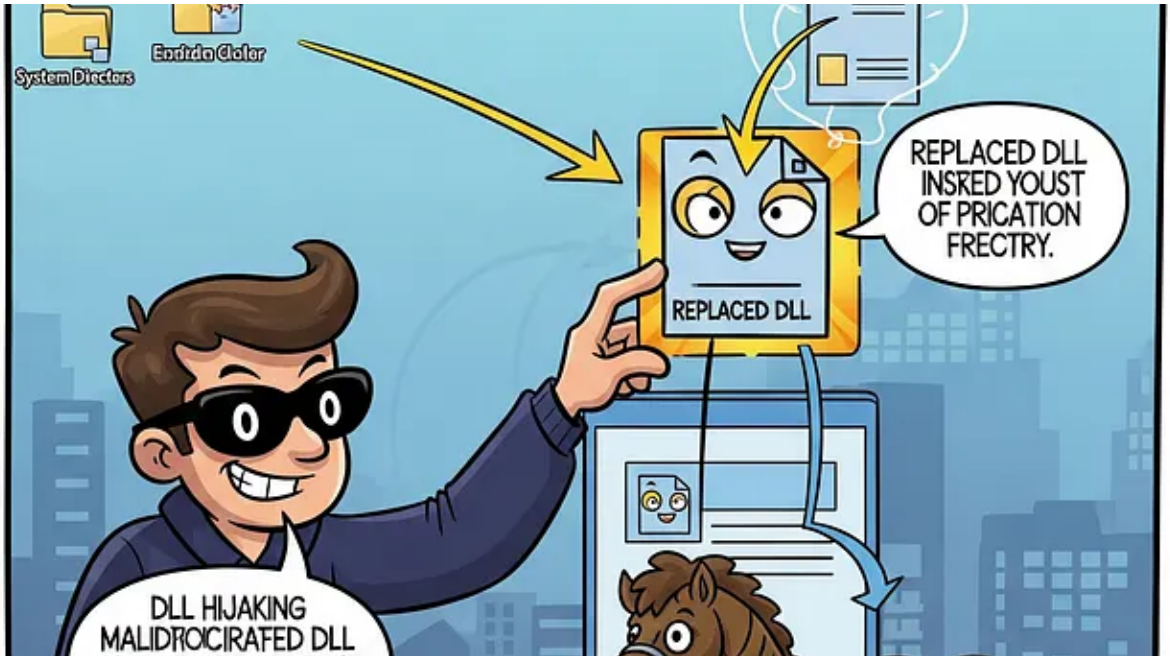


Linux Guide

Deep Dive into WireGuard Tuning on Linux Systems

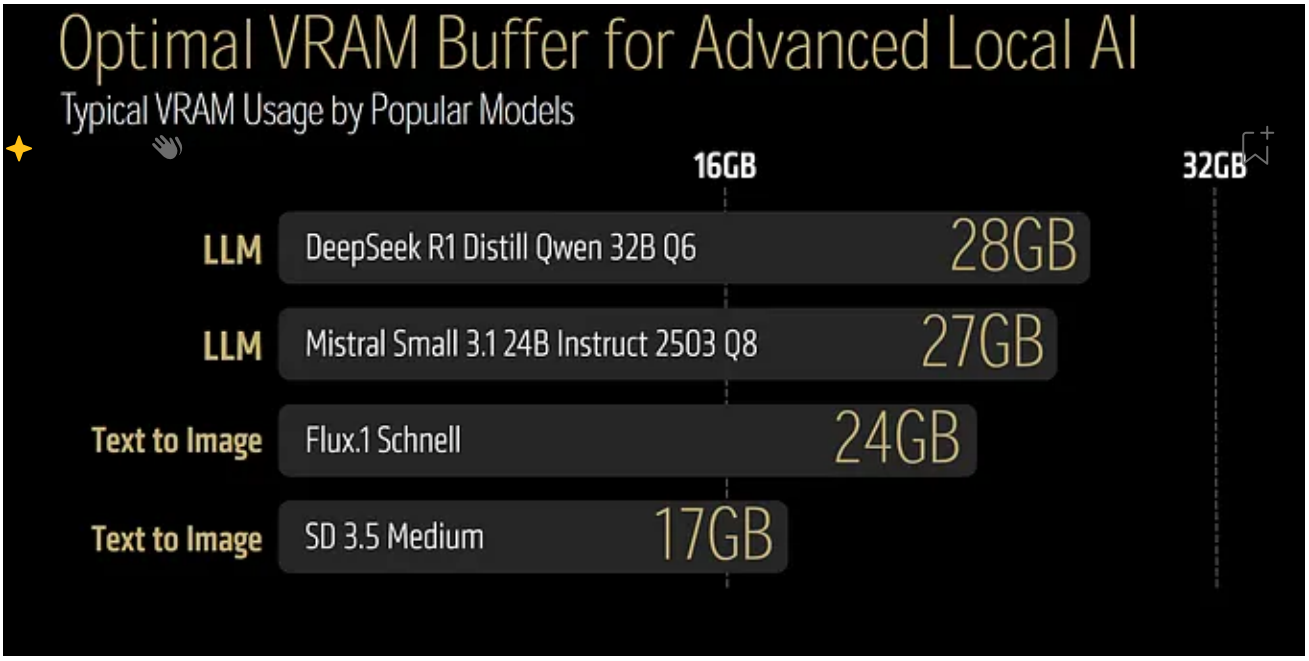
The efficient deployment and maintenance of secure overlay networks require deep introspection into kernel-level optimizations...

Dec 4 50



Ammar Ahmed

Privilege Escalation through DLL Hijacking (Windows Systems)

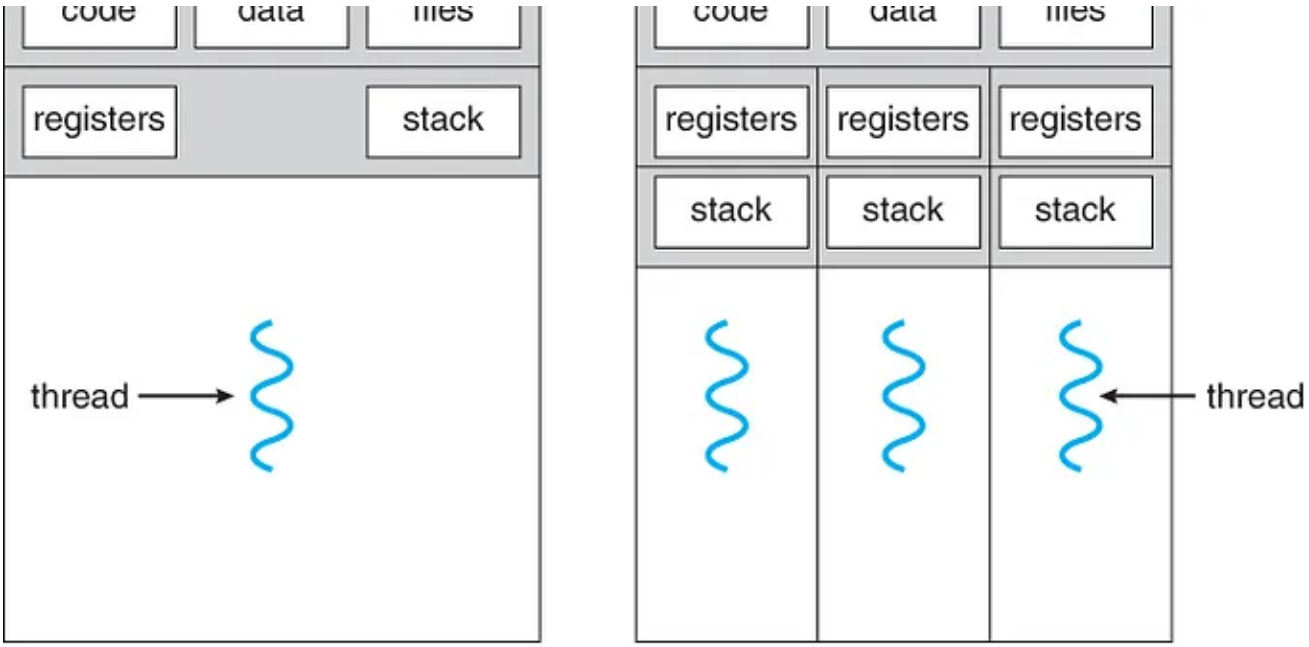


Shlomi Boutnaru, Ph.D.

The Artificial Intelligence Journey — VRAM (Video Random Access Memory)

Video Random Access Memory (VRAM) is a type of specialized and high-speed memory dedicated to a computer's GPUs (Graphics Processing...

3d ago 50

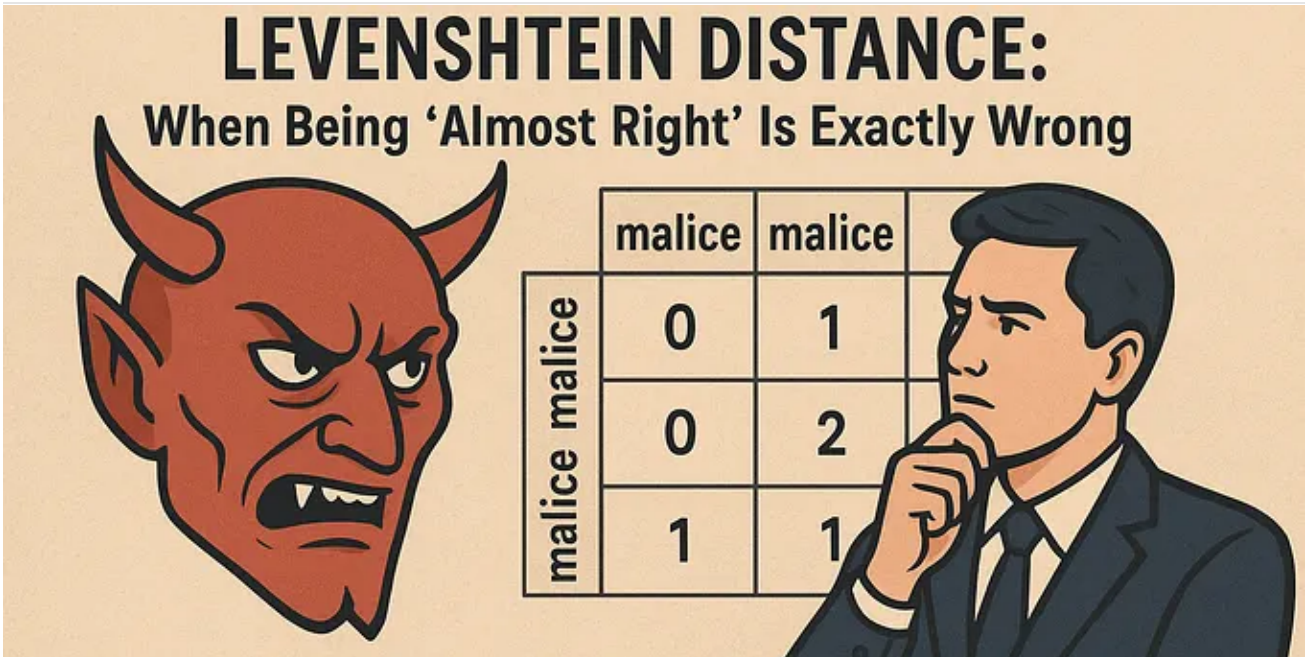


In WindowsInternalsBlogs by OS Dev

Windows Internals: Thread Management — Part 1

Thread Management on Windows. ETHREAD, KTHREAD and scheduling.

Jun 20 27



In Detect FYI by Koifsec

Measuring Malice: When Being 'Almost Right' Is Exactly Wrong

If you've spent any time writing detection rules for process masquerading, you know the game: an attacker uses scvhost.exe instead of...

3d ago 60

See more recommendations