Week 5 Quiz Question 16 Explanation

Devante Metoyer

University of Arizona

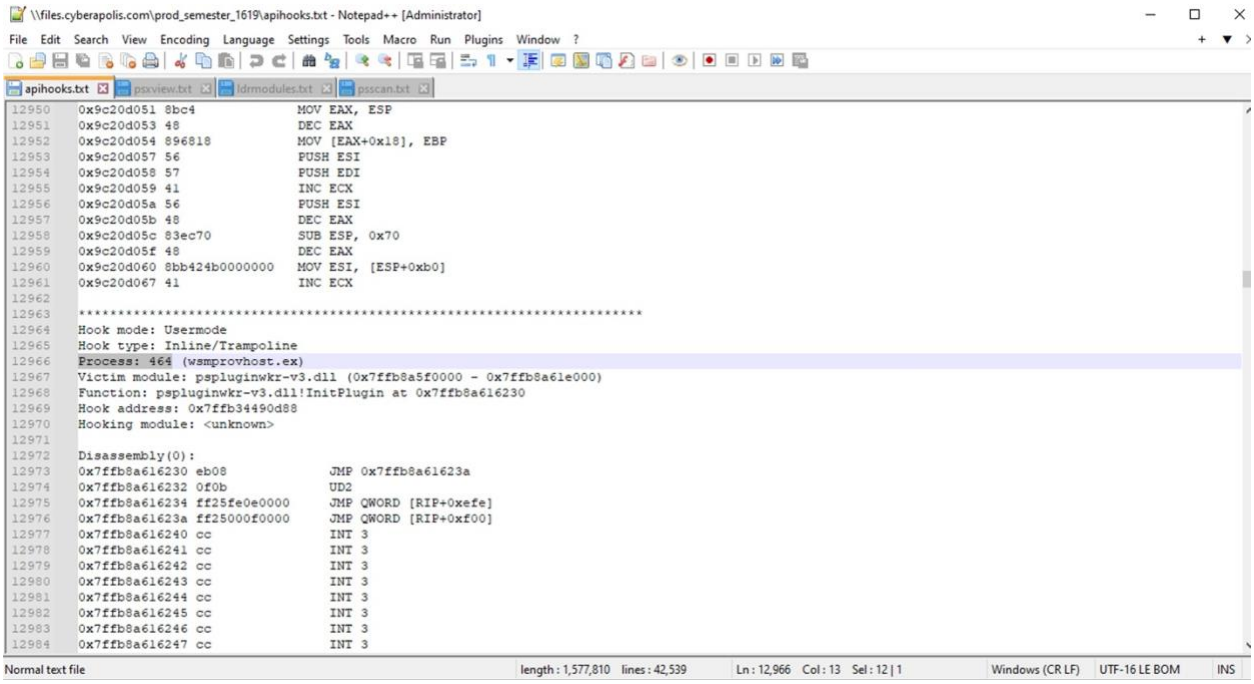
CYBV 400: Active Cyber Defense

Professor Thomas Jewkes

October 10th, 2024

API Module Detected Hooking Module: <unknown> in kernel mode

When analyzing hooks within cybersecurity, it's important to understand the difference between user mode and kernel mode. The quiz question 16, "The apihooks module detected Hooking module: <unknown> in kernelmode. True or False," hinges on this distinction. The correct response is False, and here's why.



The provided disassembly output reveals that the hook in question was operating in Usermode, not Kernelmode. This is crucial for determining the correct answer. In computing, user mode refers to an environment where regular applications operate with restricted access to system resources. Hooks in this mode only affect user-space processes, meaning they influence applications running on top of the operating system. In contrast, kernel mode refers to a more privileged state where code has unrestricted access to all system resources, including hardware and system memory.

From the disassembly file, the process wsmprovhost.exe is hooked in Usermode through an Inline/Trampoline technique. This type of hook modifies user-space processes to intercept function calls but does not affect kernel-level operations. As a result, stating that the hook was detected in kernel mode would be incorrect.

Conclusion

In summary, the correct answer is False because the hook was detected in Usermode, not Kernelmode. Understanding the distinction between the two modes is key to answering this question correctly. Since user mode operates within a limited scope, it does not have the same level of access as kernel mode, which governs core system operations. Thus, the hook's presence in user mode directly refutes the claim in the quiz question, confirming that the correct answer is False.