

## **Week 5 Quiz Question 16 Explanation**

Devante Metoyer

University of Arizona

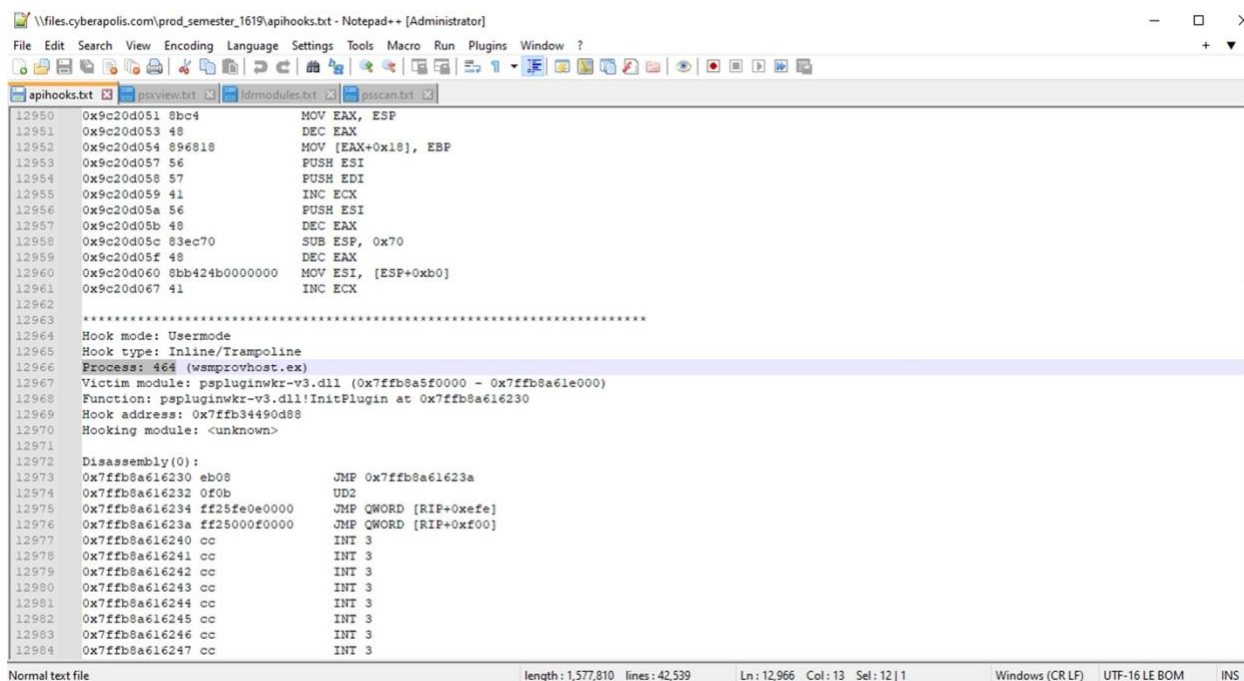
CYBV 400: Active Cyber Defense

Professor Thomas Jewkes

October 10<sup>th</sup>, 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.



```

\\files.cyberpolis.com\prod_semester_1619\apihooks.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
apihooks.txt psscan.txt idmodules.txt
12950 0x9c20d051 8bc4 MOV EAX, ESP
12951 0x9c20d053 48 DEC EAX
12952 0x9c20d054 896818 MOV [EAX+0x18], EBP
12953 0x9c20d057 56 FUSH ESI
12954 0x9c20d058 57 FUSH EDI
12955 0x9c20d059 41 INC ECX
12956 0x9c20d05a 56 FUSH ESI
12957 0x9c20d05b 48 DEC EAX
12958 0x9c20d05c 83ec70 SUB ESP, 0x70
12959 0x9c20d05f 48 DEC EAX
12960 0x9c20d060 8bb424b0000000 MOV ESI, [ESP+0xb0]
12961 0x9c20d067 41 INC ECX
12962 *****
12963 Hook mode: Usermode
12964 Hook type: Inline/Trampoline
12965 Process: 464 (wsmpvhost.exe)
12966 Victim module: pspluginwkr-v3.dll (0x7ffb8a5f0000 - 0x7ffb8a61e000)
12967 Function: pspluginwkr-v3.dll!InitPlugin at 0x7ffb8a616230
12968 Hook address: 0x7ffb34490d88
12969 Hooking module: <unknown>
12970
12971 Disassembly(0):
12972 0x7ffb8a616230 eb08 JMP 0x7ffb8a61623a
12973 0x7ffb8a616232 0f0b UD2
12974 0x7ffb8a616234 ff25fe0e0000 JMP QWORD [RIP+0xefe]
12975 0x7ffb8a61623a ff25000f0000 JMP QWORD [RIP+0xf00]
12976 0x7ffb8a616240 cc INT 3
12977 0x7ffb8a616241 cc INT 3
12978 0x7ffb8a616242 cc INT 3
12979 0x7ffb8a616243 cc INT 3
12980 0x7ffb8a616244 cc INT 3
12981 0x7ffb8a616245 cc INT 3
12982 0x7ffb8a616246 cc INT 3
12983 0x7ffb8a616247 cc INT 3
12984
Normal text file length: 1,577,810 lines: 42,539 Ln: 12,966 Col: 13 Sel: 12 | 1 Windows (CR LF) UTF-16 LE BOM INS

```

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.