CodeMachine Windows Kernel Rootkit Techniques

Course Pre-Requisite Knowledge Test

The following questions are meant to serve as a pre-requisite knowledge test for attendees of the CodeMachine Windows Kernel Rootkit Techniques training. We do not expect every attendee to have the answers to all of these questions at their fingertips. However, we do hope that attendees will research these answers and in the process, find, read, and learn relevant information and be better prepared for the class.

1. How much virtual memory does every process have access to on a x64 Windows system?
2. What is the layout of the kernel virtual address space on X64 systems?
3. What is the difference between copying and mapping memory?
4. Under what circumstances would you use PagedPool vs NonPagedPool ?
5. Where would you find the pointers to the ISR and DPC stacks?
6. What does the CPU's CR3 register contain? Which field of which kernel data structure is this register populated from, by the Windows kernel?
7. What is the equivalent of the Win32 API GetProcAddress() in kernel mode?
8. What is the underlying CPU exception that leads to access violation?
9. What is the difference between the Zw and Nt versions of the native APIs in kernel mode?
10. How do you tell Zw APIs to create a handle in the system handle table?
11. What is the difference between SSDT on 32-bit and 64-bit Windows systems?
12. Under what circumstances are user mode APCs delivered to a thread?
13. What is the use case of a mutex vs a spin lock in a Windows kernel module?
14. What is the relationship between objects and handles?
15. What is the purpose of the MaximumLength field of the UNICODE_STRING structure?
16. Why do drivers call IoCreateSymbolicLink() ?
17. Which data structure does the DRIVER_OBJECT.DriverSection point to?
18. Why should drivers not call IoCompleteRequest() with a spin lock held?
19. What would be the effect of p++, if 'p' is declared as PVOID p, PUCHAR p and PULONG p;
20. What is parameter homing space on X64 systems?
21. Why do 64-bit binaries have a .pdata section?
22. How does the LOCK prefix modify the behavior of an instruction?
23. Which CPU register points to the KPCR on X64 systems?
24. What impact does the Meltdown mitigation have on the virtual address space of the system?