Windows Kernel Rootkit Techniques Preparation

Please familiarize yourself with the topics, data structures, debugger commands, and kernel APIs listed in this document to prepare yourself for the upcoming class. You should find a reasonable amount of information about these topics in the Windows Internals books and on the Internet. For any questions regarding this document please email codemachine@outlook.com.

Strings	
Topics	ASCII, widechar and Unicode strings
Data Structures	nt!_UNICODE_STRING
Debugger Commands	dS
Kernel APIs	RTL_CONSTANT_STRING() RtlInitUnicodeString() RtlDuplicateUnicodeString() RtlFreeUnicodeString() RtlEqualUnicodeString() FsRtlIsNameInExpression() RtlStringCbPrintfA()

Asynchronous Procedure Calls (APC)	
Topics	User mode APCs, alertable wait state, kernel mode APCs, critical regions, IRQL == APC_LEVEL, process attachment
Data Structures	nt!_KAPC
Debugger Commands	!apc
Kernel APIs	KeInitializeApc() KeInsertQueueApc() KeStackAttachProcess() KeUnstackDetachProcess()

Work Items	
Topics	Executive worker threads, work items, work queues, worker routines.
Data Structures	nt!_WORK_QUEUE_ITEM

Debugger Commands	!exquque (does not work on Windows 10)
Kernel APIs	ExInitializeWorkItem() ExQueueWorkItem()

Processes and Threads	
Topics	Process and Thread IDs, Process and Thread Handles
Data Structures	nt!_EPROCESS, nt!_KPROCESS, nt!_ETHREAD, nt!_KTHREAD
Debugger Commands	!process, !thread, .process, .thread
Kernel APIs	PsGetCurrentProcessId() PsGetCurrentThreadId() PsLookupThreadByThreadId() PsLookupProcessByProcessId() PsSuspendProcess() PsResumeProcess() PsGetProcessImageFileName() SeLocateProcessImageName()

I/O Manager Objects	
Topics	Driver Object, Device Object, File Object, Symbolic Link, Device Stacks, Filter Drivers, Object namespace for driver objects (\Driver) and device objects (\Device). Driver entry points - DriverEntry and DriverUnload.
Data Structures	nt!_DEVICE_OBJECT, nt!_DRIVER_OBJECT, nt!_FILE_OBJECT
Debugger Commands	!drvobj, !devobj, !devstack, !fileobj
Kernel APIs	IoCreateDevice() IoDeleteDevice() IoCreateSymbolicLink() IoDeleteSymbolicLink() IoAttachDevice() IoDetachDevice()

IRPs and I/O Stack Locations	
Topics	Dispatch Entry Points, Win32 I/O APIs to IRP major (IRP_MJ_xxx) function mapping. Device I/O Control, Buffering Methods - METHOD_BUFFERED, METHOD_IN_DIRECT_METHOD_OUT_DIRECT, METHOD_NEITHER
Data Structures	nt!_IRP, nt!_IO_STACK_LOCATION
Debugger Commands	!irp, !irpfind, !ioctldecode

Kernel APIs	IoGetCurrentIrpStackLocation() IoCopyCurrentIrpStackLocationToNext() IoSkipCurrentIrpStackLocation() IoSetCompletionRoutine() IoMarkIrpPending() IoCompleteRequest()

Objects	
Topics	Object Manager, Object Namespace, Objects and Handles, Object Header, Object Type, Object Reference Counting
Data Structures	nt!_OBJECT_HEADER, nt!_OBJECT_TYPE, nt!_HANDLE_TABLE_ENTRY
Debugger Commands	!object, !handle, !trueref
Kernel APIs	InitializeObjectAttributes() ObReferenceObjectByName() ObReferenceObjectByHandle() ObReferenceObject() ObDereferenceObject()

Memory Management and Pools	
Topics	Pool Types, NonPagedPool, Non Paged Pool Non-Executable, pool Tagging, Memory Descriptor Lists (MDL),
Data Structures	nt!_POOL_HEADER, nt!_MDL
Debugger Commands	!pool, !poolfind
Kernel APIs	ExAllocatePoolWithTag() ExFreePool() IoAllocateMdl() MmBuildMdlForNonPagedPool() MmGetMdlPfnArray() IoFreeMdl()

Doubly Linked Lists	
Topics	Doubly linked lists, list head and list nodes
Data Structures	nt!_LIST_ENTRY
Debugger Commands	dt -l, !list
Kernel APIs	InitializeListHead() InsertTailList() RemoveHeadList()

	RemoveEntryList() IsListEmpty()

Synchronization	
Topics	Event, Fast Mutexes, ERESOURCES, Spin Locks
Data Structures	nt!_KEVENT nt!_FAST_MUTEX nt!_ERESOURCE
Debugger Commands	!locks
Kernel APIs	KeInitializeEvent() KeClearEvent() KeSetEvent() ExInitializeResourceLite() ExEnterCriticalRegionAndAcquireResourceExclusive() ExReleaseResourceAndLeaveCriticalRegion() ExDeleteResourceLite() KeInitializeSpinLock() KeAcquireSpinLock() KeReleaseSpinLock() ExInitializeFastMutex() ExAcquireFastMutex() ExReleaseFastMutex()

Token	
Topics	Tokens, Privileges
Data Structures	nt!_TOKEN nt!_EX_FAST_REF nt!_SEP_TOKEN_PRIVILEGES
Debugger Commands	!token
Kernel APIs	SeCaptureSubjectContext() SeQuerySubjectContextToken() SeQueryInformationToken() SeTokenIsAdmin()

PE Files	
Topics	Static and Dynamically Linking of Kernel Functions, Loaded Module List,PE File Headers, Load Config Directory, Import Address Table, Export Table
Data Structures	nt!_IMAGE_DOS_HEADER, nt!_IMAGE_NT_HEADERS64, nt!_IMAGE_FILE_HEADER, nt!_IMAGE_OPTIONAL_HEADER64,

	nt!_IMAGE_RUNTIME_FUNCTION_ENTRY, nt!_KLDR_DATA_TABLE_ENTRY, nt!_IMAGE_DATA_DIRECTORY
Debugger Commands	!dh
Kernel APIs	RtlQueryModuleInformation() RtlImageNtHeader RtlImageDirectoryEntryToData() MmGetSystemRoutineAddress()

PnP Notifications	
Topics	Device Arrival and Removal Notifications, Device Instance IDs, Symbolic Links
Data Structures	DEVICE_INTERFACE_CHANGE_NOTIFICATION
Debugger Commands	!pnpevent
Kernel APIs	IoRegisterPlugPlayNotification() IoUnregisterPlugPlayNotificationEx()

In addition, please review the following articles at codemachine.com
Catalog of key Windows kernel data structures
X64 Deep Dive
Windows 7 Object Headers
NDIS 6 Net Buffer Lists and Net Buffers
Ten useful kernel APIs