Vendor: Microsoft

Exam Code: 70-660

Exam Name: TS: Windows Internals

Version: DEMO

1: You have a computer that runs Windows Server 2003. You notice that the total kernel-mode CPU time for the processor is 80 percent, and the total kernel-mode CPU time for all processes is 60 percent. You need to identify what is using the remaining 20 percent of the kernel-mode CPU time. Which two Perfmon counters should you use? (Each correct answer presents part of the solution. Choose two.)
A.Processor\% DPC Time
B.Processor\Interrupts/sec
C.Processor\% Interrupt Time
D.System\Context Switches
E.System\System Calls/sec
Correct Answers: A C

2: You install and run a new device driver. You receive the following error message.
Event ID: 2020
Source: Srv
Description: The server was unable to allocate from the system paged pool because the pool was empty.
You suspect that a device driver is causing kernel memory pool leaks. You find a kernel memory allocation tag named TAG1 that belongs to the leaked memory. You need to identify the device driver and the corresponding call stack that is causing the memory leak. What should you do?
A.Run Findstr.exe /m TAG1 *.sys.
B.Run Findstr.exe TAG1 pooltag.txt.
C.Use Driver Verifier and enable the Special Pool option.
D.Use WinDbg to issue the command ed nt!PoolHitTag '1GAT'.
Correct Answers: D

3: You have a computer that runs Windows Server 2008. The computer crashes weekly and creates a complete memory dump. You run the !analyze command from WinDbg and receive the following output:
Bad_Pool_Header 0x0000000019 (0x0000000020, 0xa34583b8, 0xa34584f0, 0x0a270001)
You need to identify the pool tag that is associated with the Bad_Pool_Header pool allocation. Which WinDbg command should you use?
A.!pool
B.!poolused
C.!vm
D.!xpoolmap
Correct Answers: A

4: You have a computer that runs Windows Vista. The computer intermittently performs slowly. When the computer performs slowly, you notice that the System process uses 90 percent of the CPU. You identify the System process thread that causes the high CPU usage. The thread has the start address ntkrnlpa.exe|ExpWorkerThread. You need to identify which functions the thread calls and how much CPU time each function uses. Which tool should you use?
A.Kernrate

B.Pstat
C.Qslice
D.Tlist
Correct Answers: A

5: You have a computer that runs Windows Server 2008. You notice that the LSASS process uses a majority of the CPU time. You generate a complete memory dump file on the computer. You need to view the kernel-mode and user-mode stacks of all threads in the LSASS process. Which WinDbg command should you use?
A.!locks
B.!process
C.!runaway
D.!vm
Correct Answers: B

6: You are debugging a Windows device driver. The device driver has an unexpectedly long delay. You locate the problem in the following synchronization mechanism.

```
kd> dt var_sema
Local var @ 0xf9dfbc48 Type _KSEMAPHORE
+0x000 Header : _DISPATCHER_HEADER
+0x010 Limit : 2
kd> dt nt!_DISPATCHER_HEADER f9dfbc48
+0x000 Type : 0x5 "
+0x001 Absolute : 0xe6 "
+0x002 Size : 0x5 "
+0x003 Inserted : 0xbb "
+0x004 SignalState : 0
+0x008 WaitListHead : _LIST_ENTRY [ 0x819ca438 - 0x819ca438 ]
kd> dt nt!_KWAIT_BLOCK 0x819ca438
+0x000 WaitListEntry : _LIST_ENTRY [ 0xf9dfbc50 - 0xf9dfbc50 ]
+0x008 Thread : 0x819ca3c8 _KTHREAD
+0x00c Object : 0xf9dfbc48
+0x010 NextWaitBlock : 0x819ca480 _KWAIT_BLOCK
+0x014 WaitKey : 0
+0x016 WaitType : 1
kd> dt nt!_KWAIT_BLOCK 0xf9dfbc50
+0x000 WaitListEntry : _LIST_ENTRY [ 0x819ca438 - 0x819ca438 ]
+0x008 Thread : 0x00000002 _KTHREAD
+0x00c Object : 0xfd050f80
+0x010 NextWaitBlock : 0xffffffff _KWAIT_BLOCK
+0x014 WaitKey : 0
+0x016 WaitType : 0
```

You need to identify the number of threads that the semaphore currently has waiting. How many threads does the semaphore currently have waiting?

A.0
B.1
C.2
D.5
Correct Answers: B

7: You start a computer that runs Windows Vista. You attach a hardware device to the computer. You need to debug the creation of the functional device object (FDO) for the hardware device. Which routine should you debug?
A.AddDevice()
B.DriverEntry()
C.DriverUnload()
D.StartIo()
Correct Answers: A

8: You create a new audio miniport driver. You need to test the driver by using the Driver Verifier tool. The tests must verify the following:
 Memory overruns
 Memory underruns
 Memory that is accessed after it is freed
Which option of Driver Verifier should you use to test the driver?
A.I/O verification
B.Low resources simulation
C.Pool tracking
D.Special pool
Correct Answers: D

9: You are designing an application. The application fails because of an access violation. The access violation is caused by a heap corruption. You need to identify the cause of the heap corruption. Which tool should you use?
A.Application Verifier
B.Process Viewer
C.Performance Monitor
D.Task Manager
Correct Answers: A

10: You plan to update a device driver on a Windows system. You download a copy of the device driver file from the Internet, but you are uncertain that the device driver is legitimate. You need to verify the device drivers digital signature. Which tool should you use?
A.Certmgr.exe
B.Certmgr.msc
C.Makecert.exe
D.Signtool.exe
Correct Answers: D

11: You have an application named MyApp that fails intermittently and displays the following exception code: 0xC0000005 The call stack shows that MyApp fails in various locations including ntdll.dll and MyApp.exe. The stack trace always includes the functions main and doRealWork. You review the source code for MyApp.exe and find the following code snippet:

```
#include <string.h>
#include <stdio.h>
extern void doRealWork(char *);
char * myfunc(char *);
void main(int argc,char *argv[])
{
        char * szLocalBuffer;
        szLocalBuffer = myfunc("Data Pay load");
        if (!szLocalBuffer)
        {
                printf("a failure has occured\r\n");
        }
        else
        {
                doRealWork(szLocalBuffer);
        }
}
char * myfunc(char *szData)
{
        char *szBuffer;
        szBuffer=(char*)malloc(10);
        if(szBuffer)
        {
                sprintf(szBuffer,"The data passed to this function was %s",szData);
                return szBuffer;
        }
        else
        {
                return NULL;
        }
}
```

You resolve the error in the above code. You notice that MyApp.exe continues to fail with the same call stacks. You need to identify what is causing the application to fail. What should you do?

A.Run Verifier.exe and enable the Special pool option.

B.Run Verifier.exe and enable the Pool tracking option.

C.Run Gflags.exe and enable the Enable page heap option.

D.Run Gflags.exe and enable the Enable heap tagging by DLL option.

Correct Answers: C

12: You develop a custom application. The application fails to run under Windows Vista when User Account Control (UAC) is enabled. You need to ensure that your application acquires elevated privileges when it is run on Windows Vista computers. What should you do?

A.Add the executable to the Software Restriction Policy.

B.Mark the executable for elevation in the manifest file.

C.Sign the executable by using a software publishing certificate.

D.Install the executable into the %SystemRoot%\System32 folder.

Correct Answers: B

13: You are designing an application that will write to a local transactional log. You need to ensure that each write operation is committed to the physical disk in chronological order, even in the event of a system failure. Which I/O method should your application use?

A.Buffered

B.Memory mapped

C.Write-combining

D.Write-through

Correct Answers: D

14: You are writing a user application that runs on Windows Server 2003. The design specification for the application requires user authentication. You need to ensure that users enter a local user name and password each time the application is started. Which routine should you use?

A.CredReadDomainCredentials()

B.CredUIParseUserName()

C.CredUIPromptForCredentials()

D.LsaRegisterLogonProcess()

Correct Answers: C

15: You plan to create a telecommunication application that reads from a communication device. You need to develop your application so that it reads the I/O synchronously. Which method should you use to initiate your I/O read operation?

A.Use the ReadFileEx function. Set an OVERLAPPED structure and a completion routine.

B.Use the ReadFileEx function. Set a callback function to be called when I/O completes.

C.Use the ReadFile function. Set a null value for the OVERLAPPED structure parameter.

D.Use the ReadFile function. Set a pointer to a properly initialized OVERLAPPED structure that contains a handle to an event object to signal when the operation completes.

Correct Answers: C

16: You are developing a user mode application that contains two processes. You need to allow the two processes to synchronize access to a shared data area. Which synchronization primitive should you use?

A.Critical Section

B.ERESOURCE

C.Mutex

D.Spinlock

Correct Answers: C

17: You are writing an I/O dispatch routine for a Windows device driver. The device driver supports buffered I/O. The dispatch routine transfers 1 KB of data to the user process. You need to retrieve the kernel address of the 1-KB buffer from the I/O request packet (IRP). Which field of the IRP contains the kernel address?

A.Irp->AssociatedIrp.SystemBuffer

B.Irp->Overlay.UserApcContext

C.Irp->Tail.Overlay.DriverContext[0]

D.Irp->UserBuffer

Correct Answers: A

18: You are developing an application. You need to ensure that the application can read from COM port 10 by using the CreateFile function. Which device name should you open?

A."COM10"

B."%COM10%"

C."\\COM10"

D."\\\\.\\COM10"

Correct Answers: D

19: You develop a device driver for Windows XP that runs on uniprocessor systems only. The driver creates a system thread and a deferred procedure call (DPC). The DPC is invoked by a repeating timer. The thread and the DPC must process entries from the same work queue. You need to ensure that the system thread and the DPC are synchronized. Which IRQ Level (IRQL) should you use?

A.APC_LEVEL

B.DISPATCH_LEVEL

C.LOW_LEVEL

D.PASSIVE_LEVEL

Correct Answers: B

20: You develop a Windows device driver for a hardware device. The hardware device uses a simple direct memory access (DMA) controller. The hardware device does not perform virtual address translation. You need to allocate a 64-KB buffer in Windows that accepts a DMA transfer of 64 KB from the hardware device. Which routine should you use?

A.AllocateHeap(655536)

B.ExAllocatePoolWithTag(PagePool, 65536, abcd)

C.ExAllocatePoolWithTag(NonPagePool, 65536, abcd)

D.MmAllocateContiguousMemory(65536, 0xFFFFFFFF)

Correct Answers: D