CS490 Windows Internals Labs

Oct 18th, 2013

1. Examining IRPs

In this experiment, you'll find an uncompleted IRP on the system, and you'll determine the IRP type, the device at which it's directed, the driver that manages the device, the thread that issued the IRP, and what process the thread belongs to. At any point in time, there are at least a few uncompleted IRPs on a system. This is because there are many devices to which applications can issue IRPs that a driver will only complete when a particular event occurs, such as data becoming available. One example is a blocking read from a network endpoint. You can see the outstanding IRPs on a system with the !irpfind kernel debugger command:

kd>!irpfind unable to get large pool allocationtable - either wrong symbols or pool tagging is disabled

Searching NonPaged pool (82502000 :8a502000) for Tag: Irp?

Irp [Thread] irpStack: (Mj,Mn) DevObj [Driver]

89695868 [00000000] Irp is complete (CurrentLocation4 >StackCount3) 0x43776f56

89712008 [8a29d7c0] irpStack: (e,9) 8a19e208 [\Driver\AFD]

89716008 [8a29d7c0] irpStack: (e,9) 8a19e208 [\Driver\AFD]

... 89cb3928 [8a3acbc0] irpStack: (3, 0) 8a09a030 [\Driver\Kbdclass]

89cb3c88 [89cb1da8]irpStack: (c,2) 8a436020 [\FileSystem\Ntfs]

89cb4640 [8a165498]irpStack: (e,9) 8a19e208 [\Driver\AFD]

The highlighted entry in the output describes an IRP that is directed at the Kbdclass driver, so it is likely the IRP that was issued by the Windows subsystem raw input thread that reads keyboard input. Next step is examining the IRP with the !irp command:

kd>!irp 8a1716f0

2. Looking at a Thread's Outstanding IRPs

When you use the !thread command, it prints any IRPs associated with the thread. Run the kernel debugger with live debugging, and locate the Service Control Manager process (Services.exe) in the output generated by the !process command:

lkd> !process 0 0

**** NT ACTIVE PROCESS DUMP****

...

PROCESS 8a238da8 SessionId:0 Cid: 02a8 Peb:7ffdf000 ParentCid:027c

DirBase:14fac000 ObjectTable:e1c3e008 HandleCount: 365.

Image:SERVICES.EXE

...

Then dump the threads for the process by executing the !process command on the process object. You should see many threads, with most of them having IRPs reported in the IRP List area of the threads:

```
kd>!process 8a238da8
PROCESS 8a238da8 SessionId:0 Cid: 02a8 Peb:7ffdf000 ParentCid:027c
   DirBase:14fac000 ObjectTable:e1c3e008 HandleCount: 365.
   Image:SERVICES.EXE
   VadRoot 8a1be328 Vads 88 Clone 0 Private 346. Modified 37. Locked 0.
   DeviceMape10087c0
…
THREAD 8a124870 Cid 02a8.0338 Teb:7ffd8000 Win32Thread:00000000 WAIT:
(WrQueue) UserModeNon-Alertable
      8a2dc620 Unknown
      8a124960 NotificationTimer
                                IRP List:    8a2c2c00: (0006,0094) Flags:00000900 Mdl: 00000000
      8a20f770: (0006,0094) Flags:00000900 Mdl:00000000
      8a437780: (0006,0094)Flags:00000900 Mdl:00000000
Choose an IRP, and examine it with the !irp command:
lkd>!irp 8a2c2c00
Irp is active with 1stacks1is current(= 0x8a2c2c70)
No Mdl Thread 8a124870: Irpstack trace.
cmd        flg      cl   Device     File   Completion-Context
  >[ 3, 0]   0          1  8a0e5680        8a26e4b8        00000000-00000000 pending
\Driver\Npfs     Args: 00000400 00000000 00000000 00000000
```

3. Dumping the Device Tree

A more detailed way to view the device tree than using Device Manager is to use the !devnode kernel debugger command. Specifying 0 1 as command options dumps the internal device tree devnode structures, indenting entries to show the hierarchy:

```
lkd>!devnode 01
Dumping IopRootDeviceNode (= 0x8a4b7ee8)
DevNode 0x8a4b7ee8 for PDO0x8a4b7020
   InstancePath is “HTREE\ROOT\0"
   State =DeviceNodeStarted(0x308)
   Previous State= DeviceNodeEnumerateCompletion(0x30d)
   DevNode0x8a4b7a50 for PDO 0x8a4b7b98
      InstancePathis “Root\ACPI_HAL\0000"
      State=DeviceNodeStarted(0x308)
      PreviousState =DeviceNodeEnumerateCompletion (0x30d)
      DevNode0x8a4af448 for PDO 0x8a4eb2c8
         InstancePath is “ACPI_HAL\PNP0C08\0"
         ServiceName is “ACPI"
         State= DeviceNodeStarted (0x308)
         Previous State=DeviceNodeEnumerateCompletion(0x30d)
         DevNode 0x8a4af198 for PDO 0x8a4b1350
            InstancePathis “ACPI\GenuineIntel_-_x86_Family_6_Model_9\_0"
```

ServiceNameis “gv3"
State =DeviceNodeStarted(0x308)
PreviousState= DeviceNodeEnumerateCompletion(0x30d)
DevNode 0x8a4e8008 for PDO 0x8a4a8950
InstancePathis “ACPI\ThermalZone\THM_"
State =DeviceNodeStarted(0x308)
PreviousState= DeviceNodeEnumerateCompletion(0x30d)
DevNode 0x8a4e82b8 for PDO 0x8a4eb640
InstancePathis “ACPI\ACPI0003\2&daba3ff&0"
ServiceNameis “CmBatt"