GitHub Gist Search... All gists Back to GitHub Sign in Sign up

Instantly share code, notes, and snippets.

nasbench / DumpMinitool.md

Created last year

Star 0 Fork 0

Code Revisions 1 Embed <script src="https:// Download ZIP

DumpMinitool LOLBIN

DumpMinitool.md Raw

DumpMinitool.exe LOLBIN

This binary can be used as a LOLBIN as described here

Addtional Info

- The arguments flags are meaningless only the order is important. This means as long as you provide exactly 6 flags and their value the binary will still work. Here are the exact positions for reference:

```
// Usage: --file <fullyResolvedPath> --processId <processId> --dumpType <dumpType>

args[0] // --file
args[1] // <fullyResolvedPath>
args[2] // --processId
args[3] // <processId>
args[4] // --dumpType
args[5] //<dumpType>
```

- The `processId` argument must be an intereger as it's type casted before storage

```
int processId = int.Parse(args[3], (IFormatProvider) CultureInfo.InvariantCulture);
```

- There are three types of dump type options:

```
internal enum MiniDumpTypeOption
{
  Full,
  WithHeap,
  Mini,
}
```

- The dump type value are case sensitive since they are used in a switch case for comparaison

```
switch (type)
{
  case MiniDumpTypeOption.Full:
    // Code
  case MiniDumpTypeOption.WithHeap:
    // Code
  case MiniDumpTypeOption.Mini:
    // Code
  default:
    // Code
}
```

- The binary is using `MiniDumpWriteDump` from `Dbghelp.dll`.

- If a dump type other than the ones specified in the ENUM is provided. It will default to using the `MiniDumpNormal` - https://learn.microsoft.com/en-us/windows/win32/api/minidumpapiset/ne-minidumpapiset-minidump_type

```
switch (type)
{
  case MiniDumpTypeOption.Full:
    minidumpType = MiniDumpWriteDump.NativeMethods.MinidumpType.MiniDumpWithDataSegs | MiniDumpWriteDump.NativeM
    break;
  case MiniDumpTypeOption.WithHeap:
    minidumpType = MiniDumpWriteDump.NativeMethods.MinidumpType.MiniDumpWithDataSegs | MiniDumpWriteDump.NativeM
    break;
  case MiniDumpTypeOption.Mini:
    minidumpType = MiniDumpWriteDump.NativeMethods.MinidumpType.MiniDumpWithThreadInfo;
    break;
  default:
    minidumpType = MiniDumpWriteDump.NativeMethods.MinidumpType.MiniDumpNormal;
    break;
}
...
...
...
[Flags]
      public enum MinidumpType : uint
      {
        MiniDumpNormal = 0,
        MiniDumpWithDataSegs = 1,
        MiniDumpWithFullMemory = 2,
...
...
...
```

- The dump is performed by calling `MiniDumpWriteDump` https://learn.microsoft.com/en-us/windows/win32/api/minidumpapiset/nf-minidumpapiset-minidumpwritedump

```
for (int index = 0; index < 5 && !MiniDumpWriteDump.NativeMethods.MiniDumpWriteDump(process.Handle, (uint) proce
{
  int forLastWin32Error = Marshal.GetHRForLastWin32Error();
  if (forLastWin32Error != -2147024597)
    Marshal.ThrowExceptionForHR(forLastWin32Error);
}
```