Zachary Nandapurkar

hw08

1. What worked was this VHDMP ZwDeleteFile Arbitrary File Deletion EoP, though I don’t know exactly what it did to a group of C# files that I imported.. “The VHDMP driver is used to mount VHD and ISO files so that they can be accessed as a normal mounted volume. There are numerous places where the driver calls ZwDeleteFile without specifying OBJ\_FORCE\_ACCESS\_CHECK. This can be abused to delete any arbitrary file or directory on the filesystem by abusing symbolic links to redirect the delete file name to an arbitrary location. Also due to the behaviour of ZwDeleteFile we also don’t need to play games with the DosDevices directory or anything like that, the system call opens the target file without specifying FILE\_DIRECTORY\_FILE or FILE\_NON\_DIRECTORY\_FILE flags, this means it’s possible to use a mount point even to redirect to a file due to the way reparsing works in the kernel.”