

Slacker How-to 101

Version 1.0.1

© 3/31/2011

By Dr. J. Burton Browning
www.jbbrowning.com

How to hide files in slack file space with Slacker.exe

In this lab you will learn how to hide data in the slack space of a file (space that is not being used, but is “associated” with a valid file on a computers file system).

By learning how to secretly store data with this particular tool, you will better understand where to look for data when performing forensics or other auditing operations on a system.

This lab assumes you have a basic understanding of:

Downloading files

File systems

DOS or prompt-driven operation of a computer

Basic interest in security

Concept of data with regards to block size, capacity, devices (e.g. HDD, floppy, etc)

Time to complete: 1 hour

Required software/hardware:

Windows 2000 or higher, PC with Internet access. Rights on system similar to administrator (or enough to access local C:\ root drive).

Thompson and Monroe create slacker.exe to hide data in slack file space on Windows NTFS partitions.

Steps:

1) Download *slacker.exe* from:
<http://www.jbbrowning.com/sandbox/security.html>

Note other interesting information on the site.

2) Save the file to the root of your c:\ drive or a location you can easily get to via a command prompt.

3) Shell out to your command prompt by typing CMD and pressing ok once you click Start, run. This will work on winnt, win2k, and XP, Vista will have the icon for this under the Accessories folder.

- 4) Change directories to where you saved slacker.exe. Ask a local expert if you do not know DOS commands. (this will be your c:\root if you followed step 2 above.
- 5) To see the options for slacker, execute it by typing slacker (Enter) from the command prompt.
- 6) Create a secret file we want to hide in slack space. For this lab, use notepad to create a file called foo.txt with some special or secret message in the body of the file. Save the file to the root of the c:\ drive.
- 7) Create a folder off the c: called pics and put several jpg files in it.
- 8) To run slacker and hide the file foo.txt we just made, try the following after you download a graphics file from the Internet with a.jpg extension and renaming it to *nicksn.jpg*

```
C:\>slacker -s foo.txt c:\pics 1 c:\nicksn.jpg password -d -n
Mode: store
File: foo.txt
Path: c:\pics
Levels: 1
Meta: c:\nicksn.jpg
Pass: password
Tech: 1
Hide: 1
File being hidden: foo.txt
Filename length: 8
File size: 35
Xor Key: 0
Number of victim files used: 1

File index: 0
Filename: c:\pics\nicksn1.jpg
Filename length: 20
Last known file size: 29068
Used sectors: 1

C:\>_
```

Where slacker is the executable program.
-s tells it to store a file in slack space.
C:\foo.txt is the file to hide.
C:\nicksn.jpg is used for data storage info
Password is the password to retrieve file with.
C:\pics holds jpg files used for slack storage space.

You could now delete your foo.txt file since it is hidden. But keep the jpg files though of course!

How to get your file back:

Type in the following noting similar options to when you stored your file in slack space:

```
C:\>slacker -r c:\nicksm.jpg password -o myfoo.txt
Mode: restore
Meta: c:\nicksm.jpg
Pass: password
Out: myfoo.txt
C:\>
```

This will create a new file named myfoo.txt which is actually the file you were hiding in slack file space!

Extend your learning

Document and try other options that slacker offers and examine the following:

<http://synfulpacket.blogspot.com/2008/11/metasploit-anti-forensics-project-mafia.html>

<http://www.thetrainingco.com/pdf/Tuesday/Tuesday%20Keynote%20-%20Anti-Forensics%20-%20Henry.pdf>

<http://www.forensickb.com/2007/10/enscript-to-detect-use-of-slackerexe.html>

<http://www.forensicfocus.com/index.php?name=Content&pid=66&page=1>
