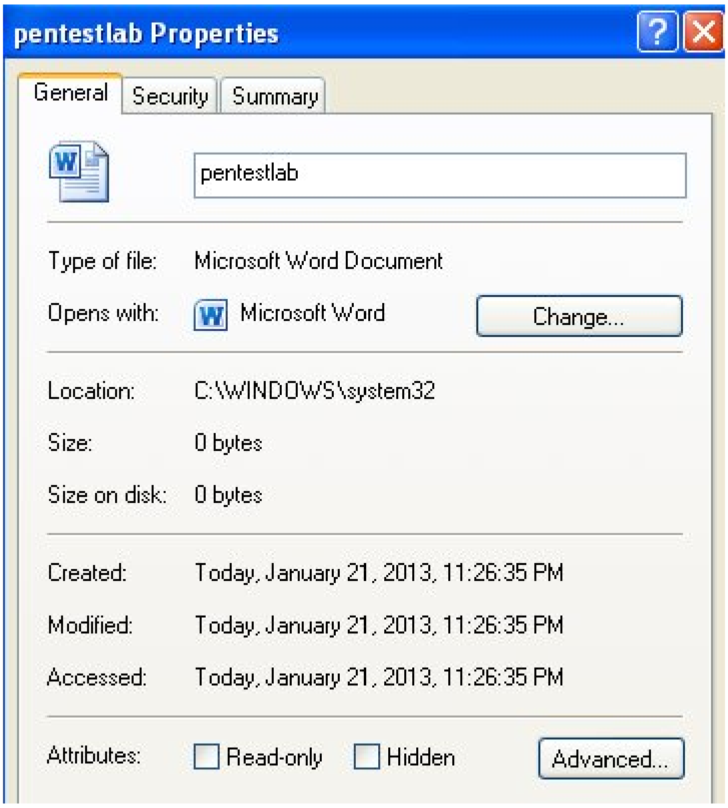
Using Timestomp To Change The MACE Values Of A File

January 22, 2013

Often in post exploitation activities penetration testers are trying to access files in order to read their contents.However this means that immediately the MACE (Modified-Accessed-Created-Entry) attributes of the file are changing and this is an indication for the administrator or the file owners that someone has read or modified the information that is stored on the file.Metasploit framework provides us with a module that we can change these values in case that we don't want to leave any marks behind.

Let's say that we have already obtained a meterpreter session and we have a .doc file with the following attributes:

As we can see the files has created,modified and accessed on January 21 at 11:26:35.In the meterpreter session we can use the timestomp -h in order to see the available options and how to use the timestomp properly.



pentestlab Properties

pentestlab

Type of file: Microsoft Word Document

Opens with: Microsoft Word

Location: C:\WINDOWS\system32

Size: 0 bytes

Size on disk: 0 bytes

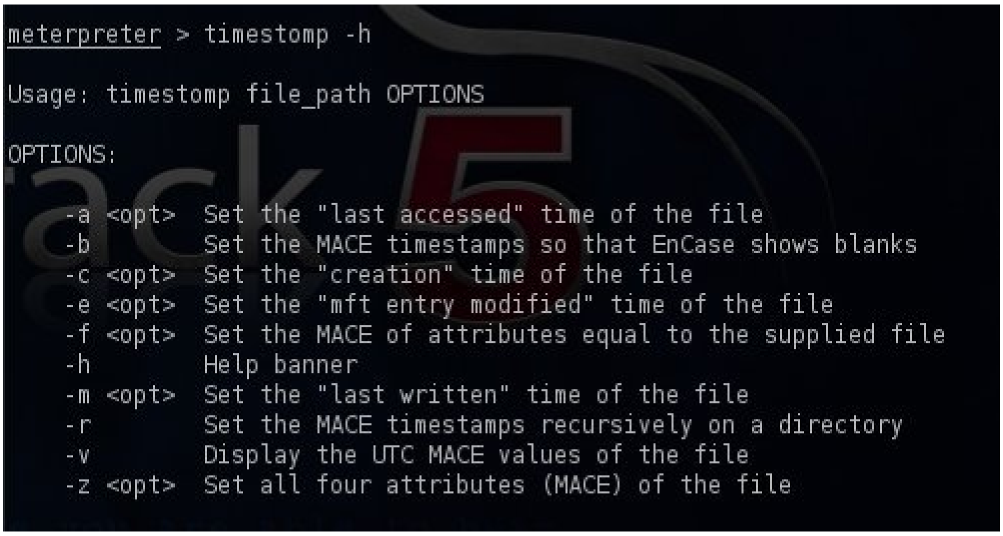
Created: Today, January 21, 2013, 11:26:35 PM

Modified: Today, January 21, 2013, 11:26:35 PM

Accessed: Today, January 21, 2013, 11:26:35 PM

Attributes: □ Read-only □ Hidden

MACE Attributes – Doc

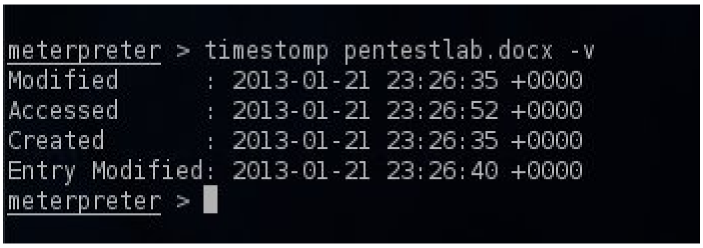


```
meterpreter > timestomp -h

Usage: timestomp file_path OPTIONS

OPTIONS:

    -a <opt>  Set the "last accessed" time of the file
    -b        Set the MACE timestamps so that EnCase shows blanks
    -c <opt>  Set the "creation" time of the file
    -e <opt>  Set the "mft entry modified" time of the file
    -f <opt>  Set the MACE of attributes equal to the supplied file
    -h        Help banner
    -m <opt>  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 <opt>  Set all four attributes (MACE) of the file
```

timestomp – help banner

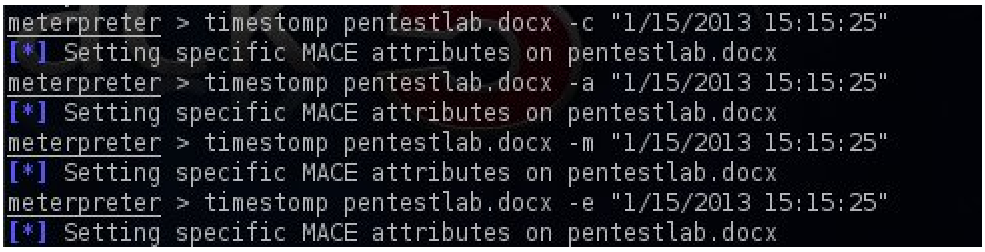
The -v option is used to display the MACE values of the file.So we will run the following command:

Now we can run the same command 4 times with the following arguments -a -m -e and -c each time along with the date and time of our desire.



```
meterpreter > timestomp pentestlab.docx -v
Modified      : 2013-01-21 23:26:35 +0000
Accessed      : 2013-01-21 23:26:52 +0000
Created       : 2013-01-21 23:26:35 +0000
Entry Modified: 2013-01-21 23:26:40 +0000
meterpreter >
```

Display MACE values

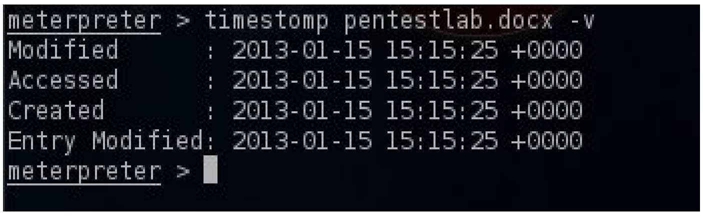


```
meterpreter > timestomp pentestlab.docx -c "1/15/2013 15:15:25"
[*] Setting specific MACE attributes on pentestlab.docx
meterpreter > timestomp pentestlab.docx -a "1/15/2013 15:15:25"
[*] Setting specific MACE attributes on pentestlab.docx
meterpreter > timestomp pentestlab.docx -m "1/15/2013 15:15:25"
[*] Setting specific MACE attributes on pentestlab.docx
meterpreter > timestomp pentestlab.docx -e "1/15/2013 15:15:25"
[*] Setting specific MACE attributes on pentestlab.docx
```

Changing the MACE values

We can verify that the file attributes has changed with the -v operator again.

As we can see from the above image we have successfully change the MACE attributes of the .doc file pentestlab.Alternatively we can use the -z option which it will assign the same values to all attributes.However this shall be avoided as realistically a file cannot be created,accessed and modified at the same time.



```
meterpreter > timestomp pentestlab.docx -v
Modified      : 2013-01-15 15:15:25 +0000
Accessed      : 2013-01-15 15:15:25 +0000
Created       : 2013-01-15 15:15:25 +0000
Entry Modified: 2013-01-15 15:15:25 +0000
meterpreter >
```

Verify the MACE changes