WFA HowTo: Track User Login activity in a Windows Image

Windows systems record a great deal of user activity, and much of this information is recorded and maintained automatically, without any user interaction (though some specifics steps may be taken to prevent the data from being recorded). This data can be extremely valuable to a forensic analyst pursuing an investigation.

One aspect of user activity that a forensic examiner may need to establish a timeline for may be when the user was logged into a system. Fortunately, there are a number of locations that provide an examiner with timestamp information with regards to user login activities.

SAM

User account information is maintained on a Windows system in the Security Accounts Manager (SAM) database; essentially, the SAM Registry hive file located in the %WinDir%\system32\config directory. This file can be easily extracted from within a system image and parsed using tools such as SAMParse.pl. For example, SAMParse.pl extracted the following information from about the Administrator account from the SAM database of a Windows XP system:

```
Key LastWrite Time = Tue Aug 17 20:31:47
   2004 (UTC)
Last Login        = Never
Login Count       = 0
Pwd Reset Date    = Tue Aug 17 20:31:47 2004
   (UTC)
Pwd Failure Date  = Never
```

This information shows us that the Registry key containing the user information was last modified on 17 Aug 2004 (i.e., the "Key LastWrite Time"). The Administrator's last login is "Never" and the login count is 0, indicating that the user account was never used to log into this system. This information is corroborated by a lack of an Administrator user profile. Finally, the password reset date (i.e., the date that the password was last changed) is the same date as the key's LastWrite time.

The following was extracted for another user account within the same SAM database, also using SAMParse.pl:

```
Key LastWrite Time = Mon Sep 26 23:37:51
   2005 (UTC)
Last Login        = Mon Sep 26 23:37:51 2005
   (UTC)
Login Count       = 35
Pwd Reset Date    = Wed Aug 18 00:49:42 2004
   (UTC)
Pwd Failure Date  = Mon Sep 26 23:37:47 2005
   (UTC)
```

At the time that the image was acquired from the system, the above user account was used to log into the system a total of 35 times, the last time being on 26 Sep 2005.

UserAssist Keys

Another location in the Registry that can provide quite a bit more detail regarding timeframes for user activity on a system is the UserAssist key located within the user's NTUSER.DAT file.

> The forensic value of the contents of the UserAssist keys is covered in a separate article.

The UserAssist keys record artifacts of the user's activity with the system via the Windows Explorer shell, such as navigating the Program Menu, clicking on Windows shortcut files, and double-clicking application EXE files. Many of the values within the UserAssist keys contain

timestamps (i.e., FILETIME[1] objects) as part of their data. This information is recorded based on activity specific to the user account used to log into the system, and may therefore be used to establish a timeline of user activity.

The following is an extract of the output of the UAssist.pl Perl script:

```
Mon Sep 26 23:33:06 2005 (UTC)
UEME_RUNPATH:C:\WINDOWS\system32\notepad.exe;10

Mon Sep 26 23:26:43 2005 (UTC)
UEME_RUNPATH:Z:\WINNT\system32\sol.exe;6

Mon Sep 26 23:22:30 2005 (UTC)
UEME_RUNPATH:Downloads.lnk;6

Mon Sep 26 23:16:26 2005 (UTC)
UEME_RUNPATH:C:\Program Files\Morpheus\Morpheus.exe;6

Mon Sep 26 23:16:25 2005 (UTC)
UEME_RUNPATH:Morpheus.lnk;6
```

The UAssist.pl Perl script is used to extract the contents of the UserAssist keys, decrypting the value names (ROT-13 "encrypted") and parsing the data. The value names describing the user activity are then sorted based on the timestamps within the data. Entries are added to the UserAssist keys based on actions taken by the user, such as clicking on shortcuts on the Program Menu, double-clicking an application EXE file, etc. For example, the previous extract indicates that the user clicked on the Morpheus[2] shortcut in the Program Menu, and that almost immediately afterward, clicking on the shortcut caused the shell to execute the application EXE file. Following that, the user launched the Solitaire and Notepad applications.

Other Registry keys, such as those that maintain most recently used (MRU) lists, may also be used to establish that a particular user account had been used to log into a system. In order to access a file, for example (Excel spreadsheet, Word document, movie file, iTunes music file, etc.) that user account would have to be used to log into the system. Access to files may be recorded in multiple locations within the user account's NTUSER.DAT Registry hive file.

Event Logs

If properly configured, the Windows Security Event Log will provide information regarding user login activity. Within an image, the analyst will need to extract the necessary information from the Security Registry hive file (located by default in the %WinDir%\system32\config directory on Windows 2000, XP, and 2003 systems). Specifically, the analyst will need to extract and parse the contents of the Default value from the following Registry key:

HKLM\Security\Policy\PolAdtEv[3]

The contents of this value will tell the examiner if (a) auditing was enabled and (b) if either successful or failed (or both or neither) logon/logoff events were being audited. This Registry value can be easily parsed using tools such as SECParse.pl to display the audit configuration, such as the following example from a Windows XP system:

```
LastWrite: Fri Sep  9 01:11:43 2005 (UTC)
Auditing was enabled.
There are 9 audit categories.

Privilege Use                 None
Object Access                 None
Account Logon Events          Both
System Events                 Both
Policy Change                 Both
Logon Events                  Both
Account Management            Both
Directory Service Access      None
Process Tracking              None
```

[1] http://support.microsoft.com/kb/188768
[2] http://morpheus.com/
[3] http://support.microsoft.com/default.aspx?scid=kb;EN-US;q246120

The examiner should then parse the Security Event Log using tools such as EvtUI (as illustrated in figure 1).

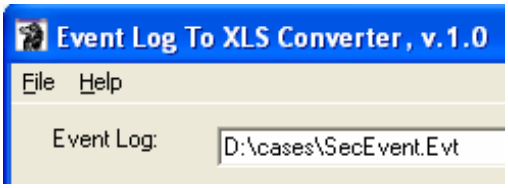

Figure 1

EvtUI bypasses the MS API when parsing Event Logs (note that Windows Event Logs from Vista systems are in an XML, rather than binary, format and therefore require other tools), and writes the event records to an Excel binary-compatible spreadsheet. In addition, EvtUI produces a report file that contains, among other things, a frequency report for event records based on sources and event IDs. For example, an extract from a Security Event Log report file contains the following information specific to logons:

528,2	7
528,5	35
529,2	7
538,2	5
538,3	8
540,3	12

Event ID 528[4] refers to successful logons, with type 2 logons being interactive logons at the console. Event ID 540[5] indicates a successful network logon. Event ID 538 indicates a successful logoff from the system.

However, this method of tracking user login activity is dependent upon the configuration of the Event Log files themselves. For example, the number of event records written and the date ranges that the records span depend largely on the audit configuration, the size of the Security Event Log file (i.e., configuration setting), and the volume of activity on the system.

EvtUI also displays, as part of its report, the date ranges of the event records parsed from the Event Log file. For example:

Date Range of event records, in UTC
Fri Sep 9 01:11:25 2005 to
Tue Sep 27 00:38:58 2005

Other events recorded within the Event Log will give indications of when the system was booted[6], although not necessarily provide indications of actual user activity.

File System

When a user account is created on a system, an entry is made in the Security Accounts Manager (SAM) database; however, the user's profile is not created until the first time that the user logs into the system. Therefore, the creation date for the user's profile folder, as well as the creation date on the user's Registry hive file (NTUSER.DAT) should correspond to the date that the user first logged into the system. When a user logs out of the system, the NTUSER.DAT file is updated, and the last modification time of the file should correspond to that time.

Summary

When a user logs into a system, there may be a number of useful artifacts available that a skilled forensic analyst can use to establish a timeline of activity associated with that user account. Indications of activity such as the times that the user account was used to log into the system can be observed in the Registry as well as within the file system.

[4] http://support.microsoft.com/kb/140714
[5] http://support.microsoft.com/kb/299475
[6] http://support.microsoft.com/kb/196452/EN-US/

Resources

- *Tracking Logon and Logoff Activity in Windows 2000*[7]
- Eric Fitzgerald's description of event IDs 528 and 540 - http://blogs.msdn.com/ericfitz/archive/2004/12/09/279282.aspx

Harlan is a forensic analyst located in the metro DC area, and is the author of three books related to live response and forensic analysis of Windows systems. He also presents at conferences and provides training on those same topics, as well. He can be reached at keydet89@yahoo.com.

[7] http://technet.microsoft.com/en-us/library/bb742436.aspx