Determination of User's Logon Status

Dustin Hurlbut

For more information contact: info@syntricate.com

I have seen questions on the various list serves with a recurring theme; can we determine a user's level of privilege in a Windows system forensically, without booting the system? I used to answer; "no, not that I know of". However, while doing research on carving out deleted V values from the SAM file, I discovered an investigator can tell what level of access a user had by viewing binary data in the SAM registry file.

To locate the information, navigate to the following path in the SAM file:

HKLM\SAM\SAM\domains\account\users\<userRID> / V

The V value contains information regarding the assigned user's name, full name, comment, and other information including the encrypted hash of the user's password. It is actually like a mini file system with pointers to the variable length data sets stored there.

The pointers are in 12-byte values. For example, the second set of 12 bytes (offsets 12-23) point to the user's name. The first four bytes are the offset where the data set begins, plus 204. The second four bytes show the value's size and the last four don't appear to be used. See Figure 1 below.

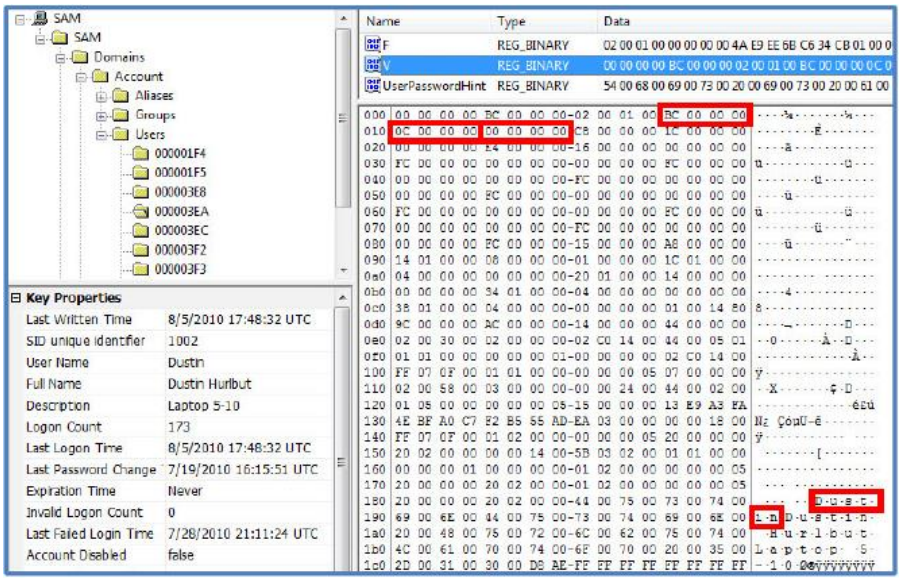

Figure 1 – Locating a User's Name in the V Value

SYNTRICATE

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. Syntricate makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, LAB, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of the AccessData Group, Inc. in the United States and/or other countries. Other trademarks referenced are property of their respective owners.

Dustin Hurlbut

For more information contact: info@syntricate.com

In Figure 1, the first four bytes of the second 12-byte set (offsets 12-23) are 0x BC 00 00 00. Converted to little endian and then decimal, this value is 188. Add 188 plus 204 and the beginning of the user AccessData Registry Determination of a User's Logon Status Page 2 name is at offset 392. The second set of 4 bytes in this 12-byte set indicates the value is decimal 12 which is the six byte Unicode equivalent of the user's name.

Other 12-byte values that act as pointers in this system include:

User Name: Offset 12-23
Full Name: Offset 24-35
Comment: Offset 36-47
LAN Hash: Offset 156-167
NT Hash: Offset 168-179

The first 12 bytes data set doesn't appear to be used as a pointer. However, I noticed when trying to determine a unique header for the V value for carving purposes, there were three distinctly different values in the second four bytes of the 12-byte set;

0x BC 00 00 00 ADMINISTRATIVE USER
0x D4 00 00 00 USER ONLY PRIVILEGE LEVEL
0x B0 00 00 00 GUEST ACCOUNT

Figure 2 – Headers that show Logon Privilege Levels

At offset 4, if the designation is 0x BC, the user has administrative privilege. The signature of 0x D4 denotes a limited user privilege and the 0x B0 is a Microsoft designation for the Guest account.

The values shown in Figure 2 work for Windows 2000, XP, Vista, and Windows 7 operating systems including the server versions that are running in a standalone environment.

If a user is set as a limited user (by default using the Manage Utility and by default a "standard user" in Control Panel using Windows 7) that user will be designated a 0x D4 00 00 00 at offsets 4-7. If that user is changed to an administrative user, the designation will change to 0x BC 00 00 00. Figure 3 shows an example of the V values in a Windows Vista (Ultimate build) system with all three privilege types in the SAM file.

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. Syntricate makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, LAB, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of the AccessData Group, Inc. in the United States and/or other countries. Other trademarks referenced are property of their respective owners.

F

RID	Twelve Byte Header	Account Type
000001F4	0x 00 00 00 00 bc 00 00 00 02 00 01 00 - Administrator	Default Admin Account
000001F5	0x 00 00 00 00 b0 00 00 00 02 00 01 00 - Guest	Default Guest Account
000003E8	0x 00 00 00 00 bc 00 00 00 02 00 01 00 - Wes Mantooth	Custom Admin Account
000003EA	0x 00 00 00 00 d4 00 00 00 02 00 01 00 - Count Dracula	Custom Limited Account
000003EB	0x 00 00 00 00 d4 00 00 00 02 00 01 00 - Laurent	Custom Limited Account

Figure 3 – Example of User Types in Windows Vista Ultimate build

I have tested this observation on over 200 machines and found this behavior to be consistent. Please let me know if you find any different results.

Some topics and items in this class syllabus are subject to change. This document is for information purposes only. Syntricate makes no warranties, express or implied, in this document. AccessData, AccessData Certified Examiner, ACE, Distributed Network Attack, DNA, Forensic Toolkit, FTK, LAB, Password Recovery Toolkit, PRTK, Registry Viewer, and Ultimate Toolkit are registered trademarks of the AccessData Group, Inc. in the United States and/or other countries. Other trademarks referenced are property of their respective owners.