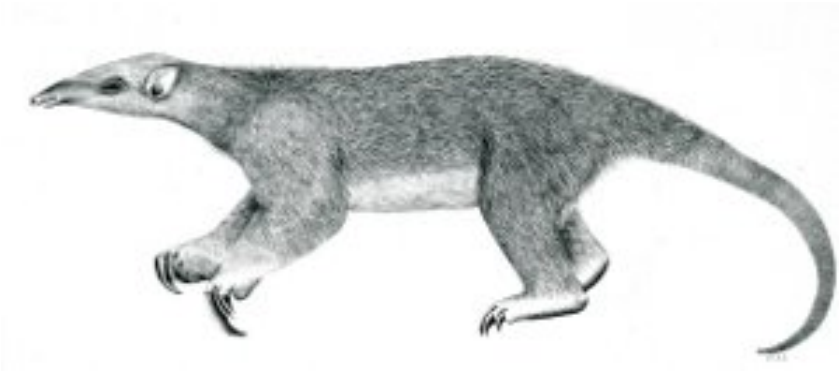
Tranalyzer2

smbDecode

SMB2



Tranalyzer Development Team

Contents

1 smbDecode

1.1 Description

The smbDecode plugin analyzes SMB2 traffic.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
SMB1_DECODE	0	Whether or not to decode SMB1 (beta)	
SMB_SECBLOB	0	Whether or not to decode security blob (beta)	
SMB_NUM_FNAME	5	number of unique filenames to store	
SMB2_NUM_DIALECT	3	number of SMB2 dialects to store	
SMB1_NUM_DIALECT	3	number of SMB1 dialects to store	SMB1_DECODE=1
SMB1_DIAL_MAXLEN	32	maximum length for SMB1 dialects	SMB1_DECODE=1
SMB2_NUM_STAT	18	number of unique SMB2 header status to store	
SMB1_SAVE_DATA	0	Whether or not to save files	SMB1_DECODE=1
SMB2_SAVE_DATA	0	Whether or not to save files	
SMB_SAVE_AUTH	0	Whether or not to save NTLM authentications	
SMB_NATIVE_NAME_LEN	64	Maximum length for names	
SMB_SAVE_DIR	"/tmp/TranSMB/"	Folder for saved data	SMB_SAVE_DATA=1
SMB_AUTH_FILE	"smb_auth.txt"	File where to store NTLM authentications	SMB_SAVE_AUTH=1
SMB_RM_DATADIR	1	Whether to remove SMB_SAVE_DIR before starting	SMB_SAVE_DATA=1
SMB_FNAME_LEN	512	Maximum length for filenames	

When saving files, the plugin uses a combination of the file ID and the flow index as name. The file ID can be replaced with the real filename by using the smbrename script and the SMB_GUID_MAP_FILE (*smb_filenames.txt*) file (See Section 1.5).

1.3 Flow File Output

The smbDecode plugin outputs the following columns:

Column	Type	Description	Flags
smbStat	H16	Status	
smb1NDialects	U32	Number of requested dialects (SMB1)	
smb1Dialects	RS	SMB1 requested dialects (client: supported, server: chosen)	
smb2NDialects	U32	Number of dialects (SMB2)	
smb2Dialects	RH16	SMB2 dialect revision (client: supported, server: chosen)	
smbNHdrStat	U32	Number of unique SMB2 header status values	

Column	Type	Description	Flags
smbHdrStat	RH32	SMB2 list of uniq header status	
smbOpcodes	H32	Opcodes	
smbNOpcodes	19x(U32)	Number of records per opcode	
smbPrevSessId	H64	SMB previous session ID	
smbNativeOS	S	SMB native OS	
smbNativeLanMan	S	SMB native LAN Manager	
smbPrimDom	S	SMB primary domain	
smbTargName	S	SMB target name	
smbDomName	S	SMB domain name	
smbUserName	S	SMB user name	
smbHostName	S	SMB host name	
smbNTLMServChallenge	S	SMB NTLM server challenge	
smbNTProofStr	S	SMB NT proof string	
smbSessionKey	S	SMB session key	
smbGUID	S	Client/Server GUID	
smbSessFlags_	H16_	Session flags,	
secM_	H8_	Security mode,	
caps	H32	Capabilities	
smbBootT	TS	Server start time	
smbMaxSizeT_R_W	U32_U32_U32	Max transaction/read/write size	
smbPath	S	Full share path name	
smbShareT	H8	Type of share being accessed	
smbShareFlags	H32_	Share flags,	
caps	H32_	Capabilities,	
acc	H32	Access mask	
smbNFiles	U32	Number of accessed files	
smbFiles	RS	Accessed files	

1.3.1 smbStat

The smbStat column is to be interpreted as follows:

smbStat	Description
0x0001	Flow is SMB
0x0002	SMB2 header status list truncated... increase SMB2_NUM_STAT
0x0004	Dialect name truncated... increase SMB1_DIAL_MAXLEN
0x0008	SMB1 dialect list truncated... increase SMB1_NUM_DIALECT
0x0010	SMB2 dialect list truncated... increase SMB_NUM_DIALECT
0x0020	List of accessed files truncated... increase SMB_NUM_FNAME
0x0040	Selected dialect index out of bound... increase SMB1_NUM_DIALECT
0x0080	Selected dialect index out of bound (error or reverse flow not found)
0x0100	Filename truncated... increase SMB_FNAME_LEN
0x1000	Authentication information extracted
0x8000	Malformed packets

1.3.2 smb2Dialects

The `smb2Dialects` column is to be interpreted as follows:

smb2Dialects	Description
0x0202	SMB 2.0.2
0x0210	SMB 2.1
0x0300	SMB 3
0x0302	SMB 3.0.2
0x0311	SMB 3.1.1
0x02ff	Wildcard revision number ($\geq$ 2.1)

1.3.3 smbHdrStat

The `smbHdrStat` column is to be interpreted as follows:

smbOpcodes	Description
0x00000000	STATUS_SUCCESS
0x00000103	STATUS_PENDING
0x0000010b	STATUS_NOTIFY_CLEANUP
0x0000010c	STATUS_NOTIFY_ENUM_DIR
0x80000005	STATUS_BUFFER_OVERFLOW
0x80000006	STATUS_NO_MORE_FILES
0xc0000003	STATUS_INVALID_INFO_CLASS
0xc000000d	STATUS_INVALID_PARAMETER
0xc000000f	STATUS_NO_SUCH_FILE
0xc0000010	STATUS_INVALID_DEVICE_REQUEST
0xc0000011	STATUS_END_OF_FILE
0xc0000016	STATUS_MORE_PROCESSING_REQUIRED
0xc0000022	STATUS_ACCESS_DENIED
0xc0000023	STATUS_BUFFER_TOO_SMALL
0xc0000034	STATUS_OBJECT_NAME_NOT_FOUND
0xc0000035	STATUS_OBJECT_NAME_COLLISION
0xc000003a	STATUS_OBJECT_PATH_SYNTAX_BAD
0xc0000043	STATUS_SHARING_VIOLATION
0xc0000061	STATUS_PRIVILEGE_NOT_HELD
0xc000006a	STATUS_WRONG_PASSWORD
0xc000006d	STATUS_LOGON_FAILURE
0xc0000071	STATUS_PASSWORD_EXPIRED
0xc00000ac	STATUS_PIPE_NOT_AVAILABLE
0xc00000ba	STATUS_FILE_IS_A_DIRECTORY
0xc00000bb	STATUS_NOT_SUPPORTED
0xc00000c9	STATUS_NETWORK_NAME_DELETED
0xc00000cc	STATUS_BAD_NETWORK_NAME
0xc0000101	STATUS_DIRECTORY_NOT_EMPTY
0xc0000120	STATUS_CANCELLED
0xc0000128	STATUS_FILE_CLOSED

smbOpcodes	Description
0xc000019c	STATUS_FS_DRIVER_REQUIRED
0xc0000203	STATUS_USER_SESSION_DELETED
0xc0000225	STATUS_NOT_FOUND
0xc0000234	STATUS_ACCOUNT_LOCKED_OUT
0xc0000257	STATUS_PATH_NOT_COVERED
0xc0000275	STATUS_NOT_A_REPARSE_POINT

For a comprehensive list of the possible status and more extensive description, refer to [MS-ERREF], Section 2.3.1.

1.3.4 smbOpcodes

The `smbOpcodes` column is to be interpreted as follows:

smbOpcodes	Description
2^0 (=0x00000001)	SMB2_NEGOTIATE
2^1 (=0x00000002)	SMB2_SESSION_SETUP
2^2 (=0x00000004)	SMB2_LOGOFF
2^3 (=0x00000008)	SMB2_TREE_CONNECT
2^4 (=0x00000010)	SMB2_TREE_DISCONNECT
2^5 (=0x00000020)	SMB2_CREATE
2^6 (=0x00000040)	SMB2_CLOSE
2^7 (=0x00000080)	SMB2_FLUSH
2^8 (=0x00000100)	SMB2_READ
2^9 (=0x00000200)	SMB2_WRITE
2^{10} (=0x00000400)	SMB2_LOCK
2^{11} (=0x00000800)	SMB2_IOCTL
2^{12} (=0x00001000)	SMB2_CANCEL
2^{13} (=0x00002000)	SMB2_ECHO
2^{14} (=0x00004000)	SMB2_QUERY_DIRECTORY
2^{15} (=0x00008000)	SMB2_CHANGE_NOTIFY
2^{16} (=0x00010000)	SMB2_QUERY_INFO
2^{17} (=0x00020000)	SMB2_SET_INFO
2^{18} (=0x00040000)	SMB2_OPLOCK_BREAK

1.3.5 smbNOpcodes

The `smbNOpcodes` column reports the number of records of each type separated by underscores.

smbNOpcodes	Description
1	Number of SMB2_NEGOTIATE records
2	Number of SMB2_SESSION_SETUP records
3	Number of SMB2_LOGOFF records
4	Number of SMB2_TREE_CONNECT records
5	Number of SMB2_TREE_DISCONNECT records

smbNOpcodes	Description
6	Number of SMB2_CREATE records
7	Number of SMB2_CLOSE records
8	Number of SMB2_FLUSH records
9	Number of SMB2_READ records
10	Number of SMB2_WRITE records
11	Number of SMB2_LOCK records
12	Number of SMB2_IOCTL records
13	Number of SMB2_CANCEL records
14	Number of SMB2_ECHO records
15	Number of SMB2_QUERY_DIRECTORY records
16	Number of SMB2_CHANGE_NOTIFY records
17	Number of SMB2_QUERY_INFO records
18	Number of SMB2_SET_INFO records
19	Number of SMB2_OPLOCK_BREAK records

1.3.6 smbSessFlags_secM_caps

The `smbSessFlags_secM_caps` column is to be interpreted as follows:

smbSessFlags	Description
0x01	Client authenticated as guest user
0x02	Client authenticated as anonymous user
0x04	Server requires encryption of messages on this session (SMB 3.x)

smbSecM	Description
0x01	Security signatures enabled on the server
0x02	Security signatures required by the server

smbCaps	Description
0x01	Server supports the Distributed File System (DFS)
0x02	Server supports leasing
0x04	Server supports multi-credit operation (Large MTU)
0x08	Server supports establishing multiple channels for a single session
0x10	Server supports persistent handles
0x20	Server supports directory leasing
0x40	Server supports encryption

1.3.7 smbShareT

The `smbShareT` column is to be interpreted as follows:

smbShareT	Description
0x01	Physical disk share
0x02	Named pipe share
0x03	Printer share

1.3.8 smbShareFlags_caps_acc

The smbShareFlags_caps_acc column is to be interpreted as follows:

smbShareFlags	Description
0x00000001	Specified share is present in a Distributed File System (DFS) tree structure
0x00000002	Specified share is present in a DFS tree structure (DFS root)
	If none of the following three bits is set, then the caching policy is "manual"
0x00000010	Auto caching
0x00000020	VDO Caching
0x00000030	Offline caching MUST NOT occur
0x00000100	Restrict exclusive opens
0x00000200	Force shared delete
0x00000400	Allow namespace caching
0x00000800	Server will filter directory entries based on access permissions of the client
0x00001000	Server will not issue exclusive caching rights on this share
0x00002000	Enable hash V1
0x00004000	Enable hash V2
0x00008000	Encrypt data required

smbShareCaps	Description
0x00000008	Specified share is present in a DFS tree structure
0x00000010	Continuous availability
0x00000020	Scaleout
0x00000040	Cluster
0x00000080	Asymmetric

smbShareAcc	Description
0x00000001	Read access
0x00000002	Write access
0x00000004	Append access
0x00000008	Read extended attributes access
0x00000010	Write extended attributes access
0x00000020	Execute access
0x00000040	Delete child access

smbShareAcc	Description
0x00000080	Read attributes access
0x00000100	Write attributes access
0x00010000	Delete access
0x00020000	Read access to owner, group and ACL of the SID
0x00040000	Owner may write the DAC
0x00080000	Can write owner (take ownership)
0x00100000	Can wait on handle to synchronise on completion of I/O
0x01000000	System security is NOT set
0x02000000	Maximum allowed is NOT set
0x10000000	Generic all is NOT set
0x20000000	Generic execute is NOT set
0x40000000	Generic write is NOT set
0x80000000	Generic read is NOT set

1.4 Plugin Report Output

The number of SMB, SMB2 and SMB3 records is reported. In addition, if SMB_SAVE_AUTH=1, the number of NetNTLMv2 hashes extracted is reported.

1.5 Post-Processing

1.5.1 smbrename

The **smbrename** script can be used to rename and organise the files extracted by the plugin. It must be run from within the SMB_SAVE_DIR folder (where the file *smb_filenames.txt* is located). By default, it will replace the file ID with the real filename and organise the files into folders according to their mimetype. Either operation can be performed or not. Try 'smbrename -help' for more information.

1.5.2 SMB Authentications

When SMB1_DECODE=1, SMB_SECBLOB=1 and SMB_SAVE_AUTH=1, the plugin produces a file with suffix SMB_AUTH_FILE containing all the NetNTLMv2 hashes extracted from the traffic. The hashes can then be reversed using JohnTheRipper[1] or Hashcat[2] as follows:

```
john --wordlist=password.lst -format=netntlmv2 FILE_smb_auth.txt
        hashcat -m 5600 FILE_smb_auth.txt wordlist.txt
```

1.6 References

- [MS-CIFS]: Common Internet File System (CIFS) Protocol
- [MS-SMB]: Server Message Block (SMB) Protocol
- [MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3
- [MS-ERREF]: Windows Error Codes

[1] https://github.com/magnumripper/JohnTheRipper
[2] https://hashcat.net

- [MS-SPNG]: Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Extension
- [MS-AUTHSOD]: Authentication Services Protocols Overview
- [MS-DTYP]: Windows Data Types
- [RFC4178]: The Simple and Protected Generic Security Service Application Program Interface (GSS-API) Negotiation Mechanism