Tranalyzer2

ntlmsspDecode

NT LAN Manager (NTLM) Security Support Provider (NTLMSSP)

Tranalyzer Development Team

Contents

Copyright © 2008–2024 by Tranalyzer Development Team

1 ntlmsspDecode

1.1 Description

The ntlmsspDecode plugin analyzes the NT LAN Manager (NTLM) Security Support Provider (NTLMSSP) protocol.

1.2 Configuration Flags

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

Name	Default	Description	Flags
NTLMSSP_CLI_CHALL	0	Output client challenge	
NTLMSSP_DNS	1	Output DNS computer/domain/tree name	
NTLMSSP_NETBIOS	1	Output NetBIOS computer/domain name	
NTLMSSP_VERSION	2	Output format for the version: 0: do not output the version 1: output the version as string 2: major_minor_build_revision	
NTLMSSP_NAME_LEN	64	Max length for string output	
NTLMSSP_SAVE_AUTH_V1	1	Extract NetNTLMv1 hashes	
NTLMSSP_SAVE_AUTH_V2	1	Extract NetNTLMv2 hashes	

NTLMSSP_SAVE_INFO	0	Add flow information in the hashes files	NTLMSSP_SAVE_AUTH_V1=1||
			NTLMSSP_SAVE_AUTH_V2=1

The suffix used for the NetNTLMv[12] hashes files is controlled by:

- NTLMSSP_AUTH_V1_FILE (default to "_NetNTLMv1.txt") for NetNTLMv1
- NTLMSSP_AUTH_V2_FILE (default to "_NetNTLMv2.txt") for NetNTLMv2

1.2.1 Environment Variable Configuration Flags

The following configuration flags can also be configured with environment variables (ENVCNTRL>0):

- NTLMSSP_AUTH_V1_FILE
- NTLMSSP_AUTH_V2_FILE

1.3 Flow File Output

The ntlmsspDecode plugin outputs the following columns:

Column	Type	Description	Flags
ntlmsspStat	H8	Status	
ntlmsspTarget	STRC	Target name	
ntlmsspDomain	STRC	Domain name	
ntlmsspUser	STRC	Username	
ntlmsspHost	STRC	Host/workstation	

Copyright © 2008–2024 by Tranalyzer Development Team

Column	Type	Description	Flags
ntlmsspNegotiateFlags	H32	Negotiate Flags	
ntlmsspServChallenge	STRC	Server challenge	
ntlmsspNTProofStr	STRC	NT proof string	
ntlmsspCliChallenge	STRC	Client challenge	NTLMSSP_CLI_CHALL=1
ntlmsspSessKey	STRC	Session key	
ntlmsspVersion	STR	Version	NTLMSSP_VERSION=1
ntlmsspVersionMajor_	U8_	Major Version,	NTLMSSP_VERSION=2
Minor_	U8_	Minor Version,	
Build_	U16_	Build Number and	
Rev	U8	NTLM Current Revision)	
ntlmsspNbComputer	STRC	NetBIOS computer name	NTLMSSP_NETBIOS=1
ntlmsspNbDomain	STRC	NetBIOS domain name	NTLMSSP_NETBIOS=1
ntlmsspDnsComputer	STRC	DNS computer name	NTLMSSP_DNS=1
ntlmsspDnsDomain	STRC	DNS domain name	NTLMSSP_DNS=1
ntlmsspDnsTree	STRC	DNS tree name	NTLMSSP_DNS=1
ntlmsspAttrTarget	STRC	Attribute Target Name	
ntlmsspTimestamp	U64.U32/S	Timestamp	

1.3.1 ntlmsspStat

The ntlmsspStat column is to be interpreted as follows:

ntlmsspStat	Description
0x01	Flow is NTLMSSP
0x02	Flow contains Negotiate messages
0x04	Flow contains Challenge messages
0x08	Flow contains Authenticate messages
0x10	NetNTLMv1 hash was extracted for this flow
0x20	NetNTLMv2 hash was extracted for this flow
0x40	String output was truncated... increase NTLMSSP_NAME_LEN
0x80	Decoding error, invalid message type, ...

1.3.2 ntlmsspNegotiateFlags

The ntlmsspNegotiateFlags column is to be interpreted as follows:

ntlmsspNegotiateFlags	Description
2^0 (=0x00000001)	NTLMSSP_NEGOTIATE_UNICODE
2^1 (=0x00000002)	NTLMSSP_NEGOTIATE_OEM
2^2 (=0x00000004)	NTLMSSP_REQUEST_TARGET
2^3 (=0x00000008)	NTLMSSP_NEGOTIATE_00000008 (Reserved, MUST be 0)
2^4 (=0x00000010)	NTLMSSP_NEGOTIATE_SIGN

Copyright © 2008–2024 by Tranalyzer Development Team

ntlmsspNegotiateFlags	**Description**
2^{5} (=0x00000020)	NTLMSSP_NEGOTIATE_SEAL
2^{6} (=0x00000040)	NTLMSSP_NEGOTIATE_DATAGRAM
2^{7} (=0x00000080)	NTLMSSP_NEGOTIATE_LM_KEY
2^{8} (=0x00000100)	NTLMSSP_NEGOTIATE_00000100 (Reserved, MUST be 0)
2^{9} (=0x00000200)	NTLMSSP_NEGOTIATE_NTLM
2^{10} (=0x00000400)	NTLMSSP_NEGOTIATE_NT_ONLY (Reserved, MUST be 0?)
2^{11} (=0x00000800)	NTLMSSP_NEGOTIATE_ANONYMOUS
2^{12} (=0x00001000)	NTLMSSP_NEGOTIATE_OEM_DOMAIN_SUPPLIED
2^{13} (=0x00002000)	NTLMSSP_NEGOTIATE_OEM_WORKSTATION_SUPPLIED
2^{14} (=0x00004000)	NTLMSSP_NEGOTIATE_00004000 (Reserved, MUST be 0)
2^{15} (=0x00008000)	NTLMSSP_NEGOTIATE_ALWAYS_SIGN
2^{16} (=0x00010000)	NTLMSSP_TARGET_TYPE_DOMAIN
2^{17} (=0x00020000)	NTLMSSP_TARGET_TYPE_SERVER
2^{18} (=0x00040000)	NTLMSSP_TARGET_TYPE_SHARE (Reserved, MUST be 0?)
2^{19} (=0x00080000)	NTLMSSP_NEGOTIATE_EXTENDED_SESSIONSECURITY
2^{20} (=0x00100000)	NTLMSSP_NEGOTIATE_IDENTIFY
2^{21} (=0x00200000)	NTLMSSP_NEGOTIATE_00200000 (Reserved, MUST be 0)
2^{22} (=0x00400000)	NTLMSSP_REQUEST_NON_NT_SESSION_KEY
2^{23} (=0x00800000)	NTLMSSP_NEGOTIATE_TARGET_INFO
2^{24} (=0x01000000)	NTLMSSP_NEGOTIATE_01000000 (Reserved, MUST be 0)
2^{25} (=0x02000000)	NTLMSSP_NEGOTIATE_VERSION
2^{26} (=0x04000000)	NTLMSSP_NEGOTIATE_04000000 (Reserved, MUST be 0)
2^{27} (=0x08000000)	NTLMSSP_NEGOTIATE_08000000 (Reserved, MUST be 0)
2^{28} (=0x10000000)	NTLMSSP_NEGOTIATE_10000000 (Reserved, MUST be 0)
2^{29} (=0x20000000)	NTLMSSP_NEGOTIATE_128
2^{30} (=0x40000000)	NTLMSSP_NEGOTIATE_KEY_EXCH
2^{31} (=0x80000000)	NTLMSSP_NEGOTIATE_56

1.4 Plugin Report Output

The following information is reported:

- Aggregated ntlmsspStat
- Number of NTLMSSP packets
- Number of NetNTLMv1 hashes extracted (NTLMSSP_SAVE_AUTH_V1=1)
- Number of NetNTLMv2 hashes extracted (NTLMSSP_SAVE_AUTH_V2=1)

Copyright © 2008–2024 by Tranalyzer Development Team

1.5 Additional Output

The following non-standard files are produced:

- `PREFIX_NetNTLMv1.txt`: NetNTLMv1 hashes (`NTLMSSP_SAVE_AUTH_V1=1`)
- `PREFIX_NetNTLMv2.txt`: NetNTLMv2 hashes (`NTLMSSP_SAVE_AUTH_V2=1`)

Copyright © 2008–2024 by Tranalyzer Development Team

1.6 Post-Processing

1.6.1 NTLMSSP Authentications

When `NTLMSSP_SAVE_AUTH_V1=1` or `NTLMSSP_SAVE_AUTH_V1=1`, the plugin produces file(s) with suffix defined by `NTLMSSP_AUTH_V1_FILE` and `NTLMSSP_AUTH_V2_FILE` containing all the NetNTLMv1 and NetNTLMv2 hashes extracted from the traffic. The hashes can then be reversed using JohnTheRipper[1] or Hashcat[2] as follows:

- NetNTLMv1:
  - `john --wordlist=password.lst -format=netntlm FILE_NetNTLMv1.txt`
  - `hashcat -m 5500 FILE_NetNTLMv1.txt wordlist.txt --show`
- NetNTLMv2:
  - `john --wordlist=password.lst -format=netntlmv2 FILE_NetNTLMv2.txt`
  - `hashcat -m 5600 FILE_NetNTLMv2.txt wordlist.txt --show`

1.7 References

- [MS-NLMP]: NT LAN Manager (NTLM) Authentication Protocol

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

Copyright © 2008–2024 by Tranalyzer Development Team