NAME

ntlm_auth - tool to allow external access to Winbind's NTLM authentication function

SYNOPSIS

ntlm_auth

DESCRIPTION

This tool is part of the **samba**(7) suite.

ntlm_auth is a helper utility that authenticates users using NT/LM authentication. It returns 0 if the users is authenticated successfully and 1 if access was denied. ntlm_auth uses winbind to access the user and authentication data for a domain. This utility is only intended to be used by other programs (currently Squid and mod_ntlm_winbind)

OPERATIONAL REQUIREMENTS

The **winbindd**(8) daemon must be operational for many of these commands to function.

Some of these commands also require access to the directory winbindd_privileged in $LOCKDIR. This should be done either by running this command as root or providing group access to the winbindd_privileged directory. For security reasons, this directory should not be world-accessable.

OPTIONS

--helper-protocol=PROTO

Operate as a stdio-based helper. Valid helper protocols are:

squid-2.4-basic

Server-side helper for use with Squid 2.4's basic (plaintext) authentication.

squid-2.5-basic

Server-side helper for use with Squid 2.5's basic (plaintext) authentication.

squid-2.5-ntlmssp

Server-side helper for use with Squid 2.5's NTLMSSP authentication.

Requires access to the directory winbindd_privileged in $LOCKDIR. The protocol used is described here: http://devel.squid-cache.org/ntlm/squid_helper_protocol.html. This protocol has been extended to allow the NTLMSSP Negotiate packet to be included as an argument to the YR command. (Thus avoiding loss of information in the protocol exchange).

ntlmssp-client-1

Client-side helper for use with arbitrary external programs that may wish to use Samba's NTLMSSP authentication knowledge.

This helper is a client, and as such may be run by any user. The protocol used is effectively the reverse of the previous protocol. A YR command (without any arguments) starts the authentication exchange.

gss-spnego
: Server-side helper that implements GSS-SPNEGO. This uses a protocol that is almost the same as squid-2.5-ntlmssp, but has some subtle differences that are undocumented outside the source at this stage.

  Requires access to the directory winbindd_privileged in $LOCKDIR.

gss-spnego-client
: Client-side helper that implements GSS-SPNEGO. This also uses a protocol similar to the above helpers, but is currently undocumented.

ntlm-server-1
: Server-side helper protocol, intended for use by a RADIUS server or the 'winbind' plugin for pppd, for the provision of MSCHAP and MSCHAPv2 authentication.

  This protocol consists of lines in the form: Parameter: value and Parameter:: Base64-encode value. The presence of a single period . indicates that one side has finished supplying data to the other. (Which in turn could cause the helper to authenticate the user).

  Currently implemented parameters from the external program to the helper are:

  Username
  : The username, expected to be in Samba's **unix charset**.

    Examples:

    Username: bob

    Username:: Ym9i

  NT-Domain
  : The user's domain, expected to be in Samba's **unix charset**.

    Examples:

NT-Domain: WORKGROUP

NT-Domain:: V09SS0dST1VQ

Full-Username
: The fully qualified username, expected to be in Samba's **unix charset** and qualified with the **winbind separator**.

Examples:

Full-Username: WORKGROUP\bob

Full-Username:: V09SS0dST1VQYm9i

LANMAN-Challenge
: The 8 byte LANMAN Challenge value, generated randomly by the server, or (in cases such as MSCHAPv2) generated in some way by both the server and the client.

Examples:

LANMAN-Challenge: 0102030405060708

LANMAN-Response
: The 24 byte LANMAN Response value, calculated from the user's password and the supplied LANMAN Challenge. Typically, this is provided over the network by a client wishing to authenticate.

Examples:

LANMAN-Response:
010203040506070809 0A0B0C0D0E0F101112131415161718

NT-Response
: The >= 24 byte NT Response calculated from the user's password and the supplied LANMAN Challenge. Typically, this is provided over the network by a client wishing to authenticate.

Examples:

NT-Response: 0102030405060708090A0B0C0D0E0F10111213141516171

Password
: The user's password. This would be provided by a network client, if the helper is being used in a legacy situation that exposes plaintext passwords in this way.

Examples:

Password: samba2

Password:: c2FtYmEy

Request-User-Session-Key

Upon successful authentication, return the user session key associated with the login.

Examples:

Request-User-Session-Key: Yes

Request-LanMan-Session-Key

Upon successful authentication, return the LANMAN session key associated with the login.

Examples:

Request-LanMan-Session-Key: Yes

Warning

Implementers should take care to base64 encode any data (such as usernames/passwords) that may contain malicious user data, such as a newline. They may also need to decode strings from the helper, which likewise may have been base64 encoded.

--username=USERNAME

Specify username of user to authenticate

--domain=DOMAIN

Specify domain of user to authenticate

--workstation=WORKSTATION

Specify the workstation the user authenticated from

--challenge=STRING

NTLM challenge (in HEXADECIMAL)

--lm-response=RESPONSE

LM Response to the challenge (in HEXADECIMAL)

--nt-response=RESPONSE

NT or NTLMv2 Response to the challenge (in HEXADECIMAL)

--password=PASSWORD
User’s plaintext password

If not specified on the command line, this is prompted for when required.

For the NTLMSSP based server roles, this parameter specifies the expected password, allowing testing without winbindd operational.

--request-lm-key
Retrieve LM session key

--request-nt-key
Request NT key

--diagnostics
Perform Diagnostics on the authentication chain. Uses the password from --password or prompts for one.

--require-membership-of={SID|Name}
Require that a user be a member of specified group (either name or SID) for authentication to succeed.

--pam-winbind-conf=FILENAME
Define the path to the pam_winbind.conf file.

--target-hostname=HOSTNAME
Define the target hostname.

--target-service=SERVICE
Define the target service.

--use-cached-creds
Whether to use credentials cached by winbindd.

--allow-mschapv2
Explicitly allow MSCHAPv2.

--offline-logon

Allow offline logons for plain text auth.

-?|--help
Print a summary of command line options.

--usage
Display brief usage message.

-d|--debuglevel=DEBUGLEVEL
level is an integer from 0 to 10. The default value if this parameter is not specified is 1 for client applications.

The higher this value, the more detail will be logged to the log files about the activities of the server. At level 0, only critical errors and serious warnings will be logged. Level 1 is a reasonable level for day-to-day running - it generates a small amount of information about operations carried out.

Levels above 1 will generate considerable amounts of log data, and should only be used when investigating a problem. Levels above 3 are designed for use only by developers and generate HUGE amounts of log data, most of which is extremely cryptic.

Note that specifying this parameter here will override the **log level** parameter in the smb.conf file.

--debug-stdout
This will redirect debug output to STDOUT. By default all clients are logging to STDERR.

--configfile=<configuration file>
The file specified contains the configuration details required by the client. The information in this file can be general for client and server or only provide client specific like options such as **client smb encrypt**. See smb.conf for more information. The default configuration file name is determined at compile time.

--option=<name>=<value>
Set the **smb.conf**(5) option "<name>" to value "<value>" from the command line. This overrides compiled-in defaults and options read from the configuration file. If a name or a value includes a space, wrap whole --option=name=value into quotes.

-V|--version
Prints the program version number.

EXAMPLE SETUP

To setup ntlm_auth for use by squid 2.5, with both basic and NTLMSSP authentication, the following should be placed in the squid.conf file.

```
auth_param ntlm program ntlm_auth --helper-protocol=squid-2.5-ntlmssp
auth_param basic program ntlm_auth --helper-protocol=squid-2.5-basic
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
```

Note

This example assumes that ntlm_auth has been installed into your path, and that the group permissions on winbindd_privileged are as described above.

To setup ntlm_auth for use by squid 2.5 with group limitation in addition to the above example, the following should be added to the squid.conf file.

```
auth_param ntlm program ntlm_auth --helper-protocol=squid-2.5-ntlmssp --require-membership-of='WORKGRO
auth_param basic program ntlm_auth --helper-protocol=squid-2.5-basic --require-membership-of='WORKGROU
```

TROUBLESHOOTING

If you're experiencing problems with authenticating Internet Explorer running under MS Windows 9X or Millennium Edition against ntlm_auth's NTLMSSP authentication helper (--helper-protocol=squid-2.5-ntlmssp), then please read the Microsoft Knowledge Base article #239869 and follow instructions described there.

VERSION

This man page is part of version 4.16.11 of the Samba suite.

AUTHOR

The original Samba software and related utilities were created by Andrew Tridgell. Samba is now developed by the Samba Team as an Open Source project similar to the way the Linux kernel is developed.

The ntlm_auth manpage was written by Jelmer Vernooij and Andrew Bartlett.