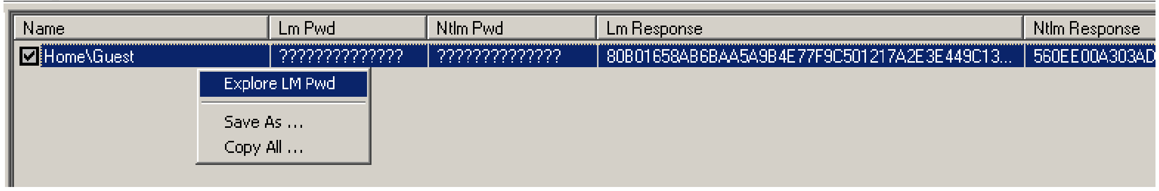
http://www.nsauditor.com

Nsasoft llc.

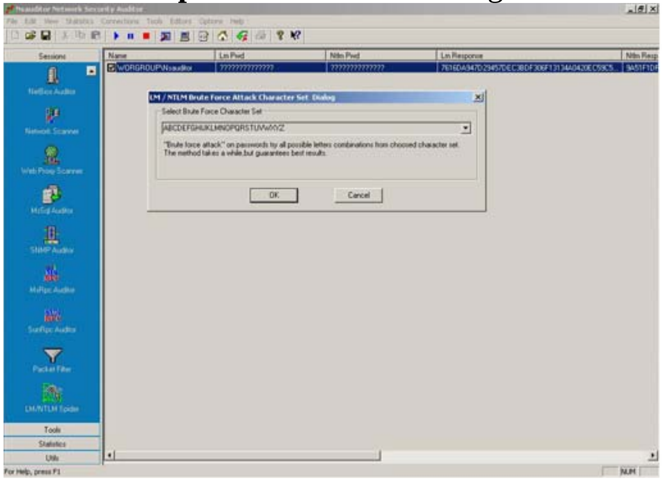
LM/NTLM Spider

LM/NTLM Spider is a password audit and recovery tool. Passwords are sources of vulnerabilities in different machines. This tool allows to identify and access password vulnerabilities. Auditing user password is one of the most important problems for network administrator. This is to know the strength of password the users are using. Week passwords represent vulnerability points for any organization.
Before using the tool you should select the Interface you want to use.
After the interface selection auditing is started. Nsauditor can capture the encrypted hashes from the challenge/response. That challenge is received when one machine is trying to connect and authenticate to another one over the network . All NTLMv1 authentication packets of SMB sessions (using commonly in Windows 95/98 and Windows NT 4.0 computers) will be captured and displayed in the SMB Packet Capture Output window.



Name	Lm Pwd	Ntlm Pwd	Lm Response	Ntlm Response
☑ Home\Guest	??????????????	??????????????	80B01658AB6BAA5A9B4E77F9C501217A2E3E449C13...	560EE00A303AD

The field **Name** contains the user name, the field **LM Pwd** contains the decrypted LM password., the field **NTLM Pwd** contains the decrypted NTLM password, **LM Response** is connected user’s password encrypted with **Challenge**(the encryption algorithm used in that case is DES), **NTLM Response** is connected user’s password encrypted with **Challenge**(NTLMv1 authentication uses MD4 cryptographic algorithm to encrypt NTLM hashes), the field **Started** contains the start and the field **Finished** contains the end time of capturing process.
After capturing SMB NTLMv1 authentication session packet or packets you can try to decrypt the received LM password hashes by right clicking on the window and selecting the button **Explore LM Pwd.** Clicking on the mentioned button will show the dialog:



Name	Lm Pwd	Ntlm Pwd	Lm Response	Ntlm Resp
☑ WORGROUP\Nsauditor	??????????????	??????????????	7616DA947D29457DEC38DF306F13134404206C59C5...	9A51F1D

LM / NTLM Brute Force Attack Character Set Dialog

Select Brute Force Character Set

ABCDEFGHIJKLMNOPQRSTUVWXYZ

"Brute force attack" on passwords try all possible letters combinations from choosed character set.
The method takes a while,but guarantees best results.

Select the character set you want to use for decrypting and click on the button **OK**. All combinations of the selected character set will be tryed. So this process can take a long time, depending on the character set length.
Note that as easy the password is decrypted as weak it is.

The NTLM audit is much more time consuming because the NTLM hash is based on a stronger algorithm, and is case sensitive, so in this version we will not support NTLM password recovering and SMB NTLMv2 (using commonly in Windows 2000/XP/2003 computers) packet capturing. Their support will be available in the next releases.