

Re: more details

Source:

<http://www.tech-archive.net/Archive/WindowsCE/microsoft.public.windowsce.platbuilder/2005-05/msg00899.html>

- *From:* "Joseph Garibaldi" <jsph_garibaldi@xxxxxxxx>
 - *Date:* Wed, 25 May 2005 03:00:25 +0530
-

ok, i just went through it again...

I changed my "AdapterList"="mac1"(which was the case till now and not "mac1;" as wrongly mentioned in the initial post) to "AdapterList"="mac1;" and now, before accessing remoteadmn, if i try to access \\box from my host m/c, i get a Access denied dialog box. And all i need to do with remoteadmn is to set the initial password and then i can access \\box ==> i don't require to select the Adapter to use through remoteadmn now.

I don't know how this is creating any difference as PB help does given an example like

```
[HKEY_LOCAL_MACHINE\Services\SMBServer]
"AdapterList"="PCI\RTL81392;VMINI1"
```

where VMINI1 is not followed by a ;

But the main thing is that i tried to reproduce the "Folder not responding" from the host side, problem again...now, i don't even need to go "up" and "down" the shared folder...even getting into the shared folder and stepping into another folder inside is sometimes enough to get my host site to "folder not responding" status (as indicated by the task manager).

The following is the detailed log from SMB Server messages. I have indicated my steps at the host side by introducing a line of ===== followed by my step at the host side. The rest of the messages is the response of the SMB server as output through KITL. check out the part near the placeholder

<<<<PROBLEM STARTS HERE I GUESS >>>> for the part of messages where things start failing.

Please refer to my first post for my current registry settings. the \profiles folder shared has a structure like \profiles -> default -> some files. So, on the host side it should appear as \\box\root\default*.

Would be glad if somebody is able to make out something out of this and helps me out. I am sorry for this long (even after some tailoring) post.

Re: more details

130816 PID:c786682a TID:c7321fc2 0x87324800: SECUR32: Locating package 'Negotiate' ...
130816 PID:c786682a TID:c7321fc2 0x87324800: found (0x0004D3E0).
130816 PID:c786682a TID:c7321fc2 0x87324800:
SPNEGO:NegAcquireCredentialsHandle: Get a Negotiate CredHandle:
130816 PID:c786682a TID:c7321fc2 0x87324800: SECUR32: Locating package 'KERBEROS' ...
130816 PID:c786682a TID:c7321fc2 0x87324800: Package NOT found.
130816 PID:c786682a TID:c7321fc2 0x87324800: SECUR32: Locating package 'NTLM' ...
130816 PID:c786682a TID:c7321fc2 0x87324800: found (0x0004D3C0).
130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO:NegPackageLoad called for fLoad 1, dwPackageID 10, Name 343204, fCapabilities 0x83f,

dwRPCID 10, TokenSize 1904

130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO:package N is being loaded
130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO:package N is NOW loaded
130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO:Loaded package NTLM
130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO:Assigned package OID: 1.3.6.1.4.1.311.2.2.10.
130816 PID:c786682a TID:c7321fc2 0x87324800: SECUR32: Locating package 'NTLM' ...
130816 PID:c786682a TID:c7321fc2 0x87324800: found (0x0004D3C0).
130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO: Added 00053CB0:00000004, NTLM
130816 PID:c786682a TID:c7321fc2 0x87324800:
SPNEGO:NegAcquireCredentialsHandle: returned 0x0
130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO:AcceptLsaModeContext(53f80, 0)
130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO:Gathering up server name for hint
130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO:Deleting context 54000
130816 PID:c786682a TID:c7321fc2 0x87324800: SPNEGO:Releasing credentials 00053F80
130816 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: SUCCESS! --- cracked by PC_NETWORK_PROGRAM_1.0
130816 PID:c786682a TID:c7321fc2 back from cracker Current Status of 1: 29 ms
130816 PID:c786682a TID:c7321fc2

130816 PID:c786682a TID:c7321fc2 Queuing send Current Status of 1: 30 ms
130816 PID:c786682a TID:c7321fc2 SMBSRV-TCP --- sending response for packet: 1 on socket 15
130816 PID:c786682a TID:c7321fc2 SMB_SRV: TCP transport --- needed to block on overlapped WSASend()
130816 PID:c786682a TID:c7321fc2 SMB(0x 72 --- SMBnegprot) packet 1 --- took 36 to process!

Re: more details

Re: more details

130816 PID:c786682a
TID:c7321fc2 -----
130816 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes
130816 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 206
bytes
130816 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (206
bytes---id 2)
130816 PID:c786682a TID:872e1a32 Going to cracker Current Status of 2: 3
ms
130816 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: Processing CMD: 0x73 ---
SMBsesssetupX
130816 PID:c786682a TID:872e1a32 SMB_SRV: Creating new connection to active
list
130816 PID:c786682a TID:872e1a32 0x8734ecd0: SECUR32: Locating package
'Negotiate' ...
130816 PID:c786682a TID:872e1a32 0x8734ecd0: found (0x0004D3E0).
130816 PID:c786682a TID:872e1a32 0x8734ecd0:
SPNEGO:NegAcquireCredentialsHandle: Get a Negotiate CredHandle:
130816 PID:c786682a TID:872e1a32 0x8734ecd0: SECUR32: Locating package
'NTLM' ...
130862 PID:c786682a TID:872e1a32 0x8734ecd0: found (0x0004D3C0).
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO: Added
00054360:00000004, NTLM
130862 PID:c786682a TID:872e1a32 0x8734ecd0:
SPNEGO:NegAcquireCredentialsHandle: returned 0x0
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SECUR32: Locating package
'Negotiate' ...
130862 PID:c786682a TID:872e1a32 0x8734ecd0: found (0x0004D3E0).
130862 PID:c786682a TID:872e1a32 SMBSRV: ASC Handle: 0x540c4 Connection:
131057 MID: 47232 PID: 65279
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:AcceptLsaModeContext(
543a0, 0)
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:buf 0E2FF0B9
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:bufsize 49
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Token size (post der) 6
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:buf 0E2FF0BC
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:bufsize 46
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:header 1
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:OidLength 8
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:OidPtr 0E2FF0BA
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Incoming Mechanism:
1.3.6.1.4.1.311.2.2.10.
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Comparing to Mechanism:
1.3.6.1.4.1.311.2.2.10.
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Common Package is NTLM
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Adding mech list for
00054F70
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Desired Package match
with token!
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:WLSaAcceptContext(

Re: more details

Re: more details

NTLM) returned 90312
130862 PID:c786682a TID:872e1a32 SMBSRV Security: need continue --- sending back that in response!!
130862 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: FAILURE! --- sending error message
130862 PID:c786682a TID:872e1a32 back from cracker Current Status of 2: 28 ms
130862 PID:c786682a TID:872e1a32

130862 PID:c786682a TID:872e1a32 Queuing send Current Status of 2: 29 ms
130862 PID:c786682a TID:872e1a32 SMBSRV-TCP --- sending response for packet: 2 on socket 15
130862 PID:c786682a TID:872e1a32 SMB_SRV: TCP transport --- needed to block on overlapped WSASend()
130862 PID:c786682a TID:872e1a32 SMB(0x 73 --- SMBsesssetupX) packet 2 --- took 33 to process!
130862 PID:c786682a
TID:872e1a32 -----
130862 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4 bytes
130862 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 278 bytes
130862 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (278 bytes---id 3)
130862 PID:c786682a TID:872e1a32 Going to cracker Current Status of 3: 3 ms
130862 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: Processing CMD: 0x73 --- SMBsesssetupX
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SECUR32: Locating package 'Negotiate' ...
130862 PID:c786682a TID:872e1a32 0x8734ecd0: found (0x0004D3E0).
130862 PID:c786682a TID:872e1a32 SMBSRV: ASC Handle: 0x540c4 Connection: 131057 MID: 47296 PID: 65279
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:AcceptLsaModeContext(543a0, 54f70)
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Failed to decode data: -1011
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:WLsaAcceptContext(NTLM) returned 0
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Freeing mech list for 00054F70
130862 PID:c786682a TID:872e1a32 SMBSRV Security: verified user with NTLM (doesnt mean they have permission.. but they are who they say they are!!
130862 PID:c786682a TID:872e1a32 --- User: ADMIN verified
130862 PID:c786682a TID:872e1a32 SMB_SRV: Setting username to ADMIN
130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Releasing credentials

Re: more details

Re: more details

000543A0

130862 PID:c786682a TID:872e1a32 0x8734ecd0: SPNEGO:Deleting context 54f70
130862 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: SUCCESS! --- cracked by
PC_NETWORK_PROGRAM_1.0
130862 PID:c786682a TID:872e1a32 back from cracker Current Status of 3:
14 ms
130906 PID:c786682a TID:872e1a32

130906 PID:c786682a TID:872e1a32 Queuing send Current Status of 3: 15 ms
130906 PID:c786682a TID:872e1a32 SMBSRV-TCP --- sending response for packet:
3 on socket 15
130906 PID:c786682a TID:872e1a32 SMB_SRV: TCP transport --- needed to block
on overlapped WSASend()
130906 PID:c786682a TID:872e1a32 SMB(0x 73 --- SMBsesssetupX) packet 3 ---
took 23 to process!
130906 PID:c786682a
TID:872e1a32 -----
130906 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes
130906 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 82
bytes
130906 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (82
bytes---id 4)
130921 PID:c786682a TID:c7321fc2 Going to cracker Current Status of 4: 4
ms
130921 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: Processing CMD: 0x75 ---
SMBtconX
130921 PID:c786682a TID:c7321fc2 SMBSRV SMB_Com_Tree_Connect: Searching for
share (IPC\$) in TreeConnect!!
130921 PID:c786682a TID:c7321fc2 SMBSRV SMB_Com_Tree_Connect: Using TID
65521 for Share:!!!
130921 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: SUCCESS! --- cracked by
PC_NETWORK_PROGRAM_1.0
130921 PID:c786682a TID:c7321fc2 back from cracker Current Status of 4:
8 ms
130921 PID:c786682a TID:c7321fc2

130921 PID:c786682a TID:c7321fc2 Queuing send Current Status of 4: 10 ms
130921 PID:c786682a TID:c7321fc2 SMBSRV-TCP --- sending response for packet:
4 on socket 15
130921 PID:c786682a TID:c7321fc2 SMB_SRV: TCP transport --- needed to block
on overlapped WSASend()
130921 PID:c786682a TID:c7321fc2 SMB(0x 75 --- SMBtconX) packet 4 --- took
14 to process!
130921 PID:c786682a

Re: more details

Re: more details

TID:c7321fc2 -----
130921 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4 bytes
130921 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 100 bytes
130939 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (100 bytes---id 5)
130941 PID:c786682a TID:c7321fc2 Going to cracker Current Status of 5: 3 ms
130941 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: Processing CMD: 0xa2 --- Unknown
130941 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: SMB_NT_Create request
130941 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: ANDX command in chain failed, stop processing
130941 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: FAILURE! --- sending error message
130941 PID:c786682a TID:c7321fc2 back from cracker Current Status of 5: 7 ms
130941 PID:c786682a TID:c7321fc2

130941 PID:c786682a TID:c7321fc2 Queuing send Current Status of 5: 8 ms
130941 PID:c786682a TID:c7321fc2 SMBSRV-TCP --- sending response for packet: 5 on socket 15
130941 PID:c786682a TID:c7321fc2 SMB_SRV: TCP transport --- needed to block on overlapped WSASend()
130941 PID:c786682a TID:c7321fc2 SMB(0xfffffa2 --- Unknown) packet 5 --- took 14 to process!
130941 PID:c786682a
TID:c7321fc2 -----
130941 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4 bytes
130941 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 111 bytes
130957 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (111 bytes---id 6)
130957 PID:c786682a TID:872e1a32 Going to cracker Current Status of 6: 3 ms
130957 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: Processing CMD: 0x25 --- SMBtrans
130957 PID:c786682a TID:872e1a32 Processing TransACT-SMB. API:(63)
130957 PID:c786682a TID:872e1a32 ...processing API_WNetWkstaGetInfo
130957 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: SUCCESS! --- cracked by PC_NETWORK_PROGRAM_1.0
130963 PID:c786682a TID:872e1a32 back from cracker Current Status of 6: 7 ms
130963 PID:c786682a TID:872e1a32

Re: more details

Re: more details

130963 PID:c786682a TID:872e1a32 Queuing send Current Status of 6: 9 ms
130963 PID:c786682a TID:872e1a32 SMBSRV-TCP --- sending response for packet:
6 on socket 15
130963 PID:c786682a TID:872e1a32 SMB_SRV: TCP transport --- needed to block
on overlapped WSA Send()
130963 PID:c786682a TID:872e1a32 SMB(0x 25 --- SMBtrans) packet 6 --- took
12 to process!
130963 PID:c786682a
TID:872e1a32 -----
130963 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes
130963 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 100
bytes
130963 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (100
bytes---id 7)
130963 PID:c786682a TID:872e1a32 Going to cracker Current Status of 7: 2
ms
130963 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: Processing CMD: 0xa2 ---
Unknown
130963 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: SMB_NT_Create request
130963 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: ANDX command in chain
failed, stop processing
130963 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: FAILURE! --- sending error
message
130963 PID:c786682a TID:872e1a32 back from cracker Current Status of 7:
6 ms
130963 PID:c786682a TID:872e1a32

<===== SIMILAR MESSAGE REPEATS
=====>

132624 PID:c786682a TID:c7321fc2 Queuing send Current Status of 49: 13
ms
132624 PID:c786682a TID:c7321fc2 SMBSRV-TCP --- sending response for packet:
49 on socket 15
132624 PID:c786682a TID:c7321fc2 SMB_SRV: TCP transport --- needed to block
on overlapped WSA Send()
132624 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes
132624 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 100
bytes
132624 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (100
bytes---id 50)
132624 PID:c786682a TID:872e1a32 Going to cracker Current Status of 50:
2 ms

Re: more details

Re: more details

132624 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: Processing CMD: 0xa2 ---
Unknown
132624 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: SMB_NT_Create request
132624 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: ANDX command in chain
failed, stop processing
132624 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: FAILURE! --- sending error
message
132624 PID:c786682a TID:872e1a32 back from cracker Current Status of 50:
5 ms
132624 PID:c786682a TID:872e1a32

132624 PID:c786682a TID:872e1a32 Queuing send Current Status of 50: 6 ms
132808 PID:c786682a TID:c7321fc2 SMB(0x 25 --- SMBtrans) packet 49 --- took
182 to process!
132808 PID:c786682a
TID:c7321fc2 -----
132808 PID:c786682a TID:872e1a32 SMBSRV-TCP --- sending response for packet:
50 on socket 15
132808 PID:c786682a TID:872e1a32 SMB_SRV: TCP transport --- needed to block
on overlapped WSASend()
132826 PID:c786682a TID:872e1a32 SMB(0xfffffa2 --- Unknown) packet 50 ---
took 172 to process!
132826 PID:c786682a
TID:872e1a32 -----
132826 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes
132826 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 111
bytes
132826 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (111
bytes---id 51)
132826 PID:c786682a TID:87d39a2a Going to cracker Current Status of 51:
3 ms
132826 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: Processing CMD: 0x25 ---
SMBtrans
132826 PID:c786682a TID:87d39a2a Processing TransACT-SMB. API:(13)
132826 PID:c786682a TID:87d39a2a ...processing API_WNetWkstaGetInfo
132826 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: SUCCESS! --- cracked by
PC_NETWORK_PROGRAM_1.0
132826 PID:c786682a TID:87d39a2a back from cracker Current Status of 51:
6 ms
132826 PID:c786682a TID:87d39a2a

132826 PID:c786682a TID:87d39a2a Queuing send Current Status of 51: 7 ms
132826 PID:c786682a TID:87d39a2a SMBSRV-TCP --- sending response for packet:
51 on socket 15

Re: more details

Re: more details

132826 PID:c786682a TID:87d39a2a SMB_SRV: TCP transport --- needed to block on overlapped WSASend()
132826 PID:c786682a TID:87d39a2a SMB(0x 25 --- SMBtrans) packet 51 --- took 14 to process!
132826 PID:c786682a
TID:87d39a2a -----
132826 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4 bytes
132826 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 100 bytes
132826 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (100 bytes---id 52)
132826 PID:c786682a TID:872e1a32 Going to cracker Current Status of 52:
3 ms
132826 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: Processing CMD: 0xa2 --- Unknown
132826 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: SMB_NT_Create request
132826 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: ANDX command in chain failed, stop processing
132826 PID:c786682a TID:872e1a32 SMBSRV-CRACKER: FAILURE! --- sending error message
132826 PID:c786682a TID:872e1a32 back from cracker Current Status of 52:
6 ms
132826 PID:c786682a TID:872e1a32

132826 PID:c786682a TID:872e1a32 Queuing send Current Status of 52: 8 ms
132826 PID:c786682a TID:872e1a32 SMBSRV-TCP --- sending response for packet: 52 on socket 15
132826 PID:c786682a TID:872e1a32 SMB_SRV: TCP transport --- needed to block on overlapped WSASend()
133033 PID:c786682a TID:872e1a32 SMB(0xfffffa2 --- Unknown) packet 52 --- took 189 to process!
133033 PID:c786682a
TID:872e1a32 -----
=====

STEP INTO THE FOLDER root (which is the shared folder \profiles at the target m/c)

202618 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4 bytes
202618 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 218 bytes
202618 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (218 bytes---id 71)
202618 PID:c786682a TID:87d39a2a Going to cracker Current Status of 71:
3 ms

Re: more details

Re: more details

202618 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: Processing CMD: 0x73 ---
SMBsesssetupX
202618 PID:c786682a TID:87d39a2a SMB_SRV: Creating new connection to active
list
202618 PID:c786682a TID:87d39a2a 0x87324cd0: SECUR32: Locating package
'Negotiate' ...
202618 PID:c786682a TID:87d39a2a 0x87324cd0: found (0x0004D3E0).
202618 PID:c786682a TID:87d39a2a 0x87324cd0:
SPNEGO:NegAcquireCredentialsHandle: Get a Negotiate CredHandle:
202618 PID:c786682a TID:87d39a2a 0x87324cd0: SECUR32: Locating package
'NTLM' ...
202618 PID:c786682a TID:87d39a2a 0x87324cd0: found (0x0004D3C0).
202618 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO: Added
000526B0:00000004, NTLM
202618 PID:c786682a TID:87d39a2a 0x87324cd0:
SPNEGO:NegAcquireCredentialsHandle: returned 0x0
202618 PID:c786682a TID:87d39a2a 0x87324cd0: SECUR32: Locating package
'Negotiate' ...
202618 PID:c786682a TID:87d39a2a 0x87324cd0: found (0x0004D3E0).
202618 PID:c786682a TID:87d39a2a SMBSRV: ASC Handle: 0x52584 Connection:
131057 MID: 51648 PID: 65279
202618 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:AcceptLsaModeContext(
52b40, 0)
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:buf 0E30F0B9
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:bufsize 56
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Token size (post der) 6
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:buf 0E30F0BC
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:bufsize 53
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:header 1
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:OidLength 8
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:OidPtr 0E30F0BA
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Incoming Mechanism:
1.3.6.1.4.1.311.2.2.10.
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Comparing to Mechanism:
1.3.6.1.4.1.311.2.2.10.
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Common Package is NTLM
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Adding mech list for
000550C0
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Desired Package match
with token!
202673 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:WLsaAcceptContext(
NTLM) returned 90312
202673 PID:c786682a TID:87d39a2a SMBSRV Security: need continue --- sending
back that in response!!
202686 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: FAILURE! --- sending error
message
202686 PID:c786682a TID:87d39a2a back from cracker Current Status of 71:
27 ms
202686 PID:c786682a TID:87d39a2a

Re: more details

202686 PID:c786682a TID:87d39a2a Queuing send Current Status of 71: 28
ms
202686 PID:c786682a TID:87d39a2a SMBSRV-TCP --- sending response for packet:
71 on socket 15
202686 PID:c786682a TID:87d39a2a SMB_SRV: TCP transport --- needed to block
on overlapped WSASend()
202686 PID:c786682a TID:87d39a2a SMB(0x 73 --- SMBsesssetupX) packet 71 ---
took 32 to process!
202686 PID:c786682a
TID:87d39a2a -----
202686 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes
202686 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 218
bytes
202686 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (218
bytes---id 72)
202686 PID:c786682a TID:87d39a2a Going to cracker Current Status of 72:
3 ms
202686 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: Processing CMD: 0x73 ---
SMBsesssetupX
202686 PID:c786682a TID:87d39a2a 0x87324cd0: SECUR32: Locating package
'Negotiate' ...
202686 PID:c786682a TID:87d39a2a 0x87324cd0: found (0x0004D3E0).
202686 PID:c786682a TID:87d39a2a SMBSRV: ASC Handle: 0x52584 Connection:
131057 MID: 51712 PID: 65279
202686 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:AcceptLsaModeContext(
52b40, 550c0)
202686 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Failed to decode
data: -1011
202686 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:WLsaAcceptContext(
NTLM) returned 0
202686 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Freeing mech list for
000550C0
202686 PID:c786682a TID:87d39a2a SMBSRV Security: verified user with NTLM
(doesnt mean they have permission.. but they are who they say they

are!!
202686 PID:c786682a TID:87d39a2a --- Authed Guest (NULL Session)
202709 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Releasing credentials
00052B40
202709 PID:c786682a TID:87d39a2a 0x87324cd0: SPNEGO:Deleting context 550c0
202709 PID:c786682a TID:87d39a2a --- User: REJECTED
202709 PID:c786682a TID:87d39a2a SMB_SRV: Killing specific connection on
transport connection: 0x1fff1
202709 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: ANDX command in chain
failed, stop processing
202713 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: FAILURE! --- sending error
message
202713 PID:c786682a TID:87d39a2a back from cracker Current Status of 72:

Re: more details

Re: more details

18 ms

202713 PID:c786682a TID:87d39a2a

202713 PID:c786682a TID:87d39a2a Queuing send Current Status of 72: 19

ms

202713 PID:c786682a TID:87d39a2a SMBSRV-TCP --- sending response for packet:
72 on socket 15

202713 PID:c786682a TID:87d39a2a SMB_SRV: TCP transport --- needed to block
on overlapped WSASend()

202713 PID:c786682a TID:87d39a2a SMB(0x 73 --- SMBsesssetupX) packet 72 ---
took 23 to process!

202713 PID:c786682a

TID:87d39a2a

202713 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes

202713 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 39
bytes

202713 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (39
bytes---id 73)

202713 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes

202713 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 100
bytes

202713 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (100
bytes---id 74)

202713 PID:c786682a TID:87d39a2a Going to cracker Current Status of 73:

5 ms

202713 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: Processing CMD: 0x74 ---
SMBulogoffX

202713 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: SUCCESS! --- cracked by
PC_NETWORK_PROGRAM_1.0

202713 PID:c786682a TID:87d39a2a back from cracker Current Status of 73:

7 ms

202713 PID:c786682a TID:87d39a2a

202713 PID:c786682a TID:87d39a2a Queuing send Current Status of 73: 9 ms

202713 PID:c786682a TID:87d39a2a SMBSRV-TCP --- sending response for packet:
73 on socket 15

202713 PID:c786682a TID:87d39a2a SMB_SRV: TCP transport --- needed to block
on overlapped WSASend()

202739 PID:c786682a TID:c7321fc2 Going to cracker Current Status of 74:

11 ms

202739 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: Processing CMD: 0xa2 ---
Unknown

202739 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: SMB_NT_Create request

Re: more details

Re: more details

202739 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: ANDX command in chain failed, stop processing
202739 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: FAILURE! --- sending error message
202739 PID:c786682a TID:c7321fc2 back from cracker Current Status of 74: 15 ms
202739 PID:c786682a TID:c7321fc2

<===== SIMILAR MESSAGE REPEATS
=====>

203279 PID:c786682a TID:87d39a2a Queuing send Current Status of 84: 8 ms
203279 PID:c786682a TID:87d39a2a SMBSRV-TCP --- sending response for packet: 84 on socket 15
203279 PID:c786682a TID:87d39a2a SMB_SRV: TCP transport --- needed to block on overlapped WSASend()
203279 PID:c786682a TID:87d39a2a SMB(0x 25 --- SMBtrans) packet 84 --- took 13 to process!
203279 PID:c786682a
TID:87d39a2a -----
203279 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4 bytes
203279 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 82 bytes
203279 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (82 bytes--id 85)
203279 PID:c786682a TID:c7321fc2 Going to cracker Current Status of 85: 3 ms
203279 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: Processing CMD: 0x75 --- SMBtconX
203279 PID:c786682a TID:c7321fc2 SMBSRV SMB_Com_Tree_Connect: Searching for share (ROOT) in TreeConnect!!
203279 PID:c786682a TID:c7321fc2 SMBSRV SMB_Com_Tree_Connect: Using TID 65522 for Share:R!!
203279 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: SUCCESS! --- cracked by PC_NETWORK_PROGRAM_1.0
203279 PID:c786682a TID:c7321fc2 back from cracker Current Status of 85: 7 ms
203279 PID:c786682a TID:c7321fc2

<===== SIMILAR MESSAGE REPEATS
=====>

203279 PID:c786682a TID:87d39a2a Queuing send Current Status of 84: 8 ms
203279 PID:c786682a TID:87d39a2a SMBSRV-TCP --- sending response for packet: 84 on socket 15
203279 PID:c786682a TID:87d39a2a SMB_SRV: TCP transport --- needed to block on overlapped WSASend()

Re: more details

Re: more details

203279 PID:c786682a TID:87d39a2a SMB(0x 25 --- SMBtrans) packet 84 --- took 13 to process!

203279 PID:c786682a

TID:87d39a2a -----

203279 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4 bytes

203279 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 82 bytes

203279 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (82 bytes--id 85)

203279 PID:c786682a TID:c7321fc2 Going to cracker Current Status of 85: 3 ms

203279 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: Processing CMD: 0x75 --- SMBtconX

203279 PID:c786682a TID:c7321fc2 SMBSRV SMB_Com_Tree_Connect: Searching for share (ROOT) in TreeConnect!!

203279 PID:c786682a TID:c7321fc2 SMBSRV SMB_Com_Tree_Connect: Using TID 65522 for Share:R!!

203279 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: SUCCESS! --- cracked by PC_NETWORK_PROGRAM_1.0

203279 PID:c786682a TID:c7321fc2 back from cracker Current Status of 85: 7 ms

203279 PID:c786682a TID:c7321fc2

203847 PID:c786682a TID:c7321fc2 Queuing send Current Status of 100: 9 ms

203847 PID:c786682a TID:c7321fc2 SMBSRV-TCP --- sending response for packet: 100 on socket 15

203847 PID:c786682a TID:c7321fc2 SMB_SRV: TCP transport --- needed to block on overlapped WSASend()

203847 PID:c786682a TID:c7321fc2 SMB(0x 25 --- SMBtrans) packet 100 --- took 13 to process!

203847 PID:c786682a

TID:c7321fc2 -----

203847 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4 bytes

203847 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 100 bytes

203847 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (100 bytes--id 101)

203847 PID:c786682a TID:87d39a2a Going to cracker Current Status of 101: 2 ms

203847 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: Processing CMD: 0xa2 --- Unknown

203847 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: SMB_NT_Create request

203847 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: ANDX command in chain failed, stop processing

203847 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: FAILURE! --- sending error message

Re: more details

Re: more details

203847 PID:c786682a TID:87d39a2a back from cracker Current Status of
101: 6 ms
203847 PID:c786682a TID:87d39a2a

203847 PID:c786682a TID:87d39a2a Queuing send Current Status of 101: 7
ms
203847 PID:c786682a TID:87d39a2a SMBSRV-TCP --- sending response for packet:
101 on socket 15
203847 PID:c786682a TID:87d39a2a SMB_SRV: TCP transport --- needed to block
on overlapped WSASend()
203847 PID:c786682a TID:87d39a2a SMB(0xfffffa2 --- Unknown) packet
101 --- took 12 to process!
203847 PID:c786682a
TID:87d39a2a

203847 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes
203847 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 111
bytes
203847 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (111
bytes---id 102)
203847 PID:c786682a TID:c7321fc2 Going to cracker Current Status of 102:
4 ms
203847 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: Processing CMD: 0x25 ---
SMBtrans
203847 PID:c786682a TID:c7321fc2 Processing TransACT-SMB. API:(63)
203847 PID:c786682a TID:c7321fc2 ...processing API_WNetWkstaGetInfo
203847 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: SUCCESS! --- cracked by
PC_NETWORK_PROGRAM_1.0
203847 PID:c786682a TID:c7321fc2 back from cracker Current Status of
102: 7 ms
203847 PID:c786682a TID:c7321fc2

203847 PID:c786682a TID:c7321fc2 Queuing send Current Status of 102: 9
ms
203847 PID:c786682a TID:c7321fc2 SMBSRV-TCP --- sending response for packet:
102 on socket 15
203847 PID:c786682a TID:c7321fc2 SMB_SRV: TCP transport --- needed to block
on overlapped WSASend()
203885 PID:c786682a TID:c7321fc2 SMB(0x 25 --- SMBtrans) packet 102 ---
took 31 to process!
203885 PID:c786682a
TID:c7321fc2

203906 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 4
bytes
203906 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport --- just recv'ed 70

Re: more details

Re: more details

bytes

203906 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (70 bytes--id 103)

203906 PID:c786682a TID:87d39a2a Going to cracker Current Status of 103:
2 ms

203906 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: Processing CMD: 0x32 --
SMBtrans2

203906 PID:c786682a TID:87d39a2a SMBSRV-CRACKER: SUCCESS! -- cracked by
PC_NETWORK_PROGRAM_1.0

203906 PID:c786682a TID:87d39a2a back from cracker Current Status of
103: 5 ms

203906 PID:c786682a TID:87d39a2a

203906 PID:c786682a TID:87d39a2a Queuing send Current Status of 103: 6
ms

203906 PID:c786682a TID:87d39a2a SMBSRV-TCP -- sending response for packet:
103 on socket 15

203906 PID:c786682a TID:87d39a2a SMB_SRV: TCP transport -- needed to block
on overlapped WSASend()

203925 PID:c786682a TID:87d39a2a SMB(0x 32 -- SMBtrans2) packet 103 --
took 43 to process!

203925 PID:c786682a

TID:87d39a2a

203925 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport -- just recv'ed 4
bytes

203925 PID:c786682a TID:8759cf02 SMB_SRV: TCP transport -- just recv'ed 70
bytes

203925 PID:c786682a TID:8759cf02 SMBSRV-TCPRECV:Got a TCP packet! (70
bytes--id 104)

203925 PID:c786682a TID:c7321fc2 Going to cracker Current Status of 104:
3 ms

203925 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: Processing CMD: 0x32 --
SMBtrans2

203925 PID:c786682a TID:c7321fc2 SMBSRV-CRACKER: SUCCESS! -- cracked by
PC_NETWORK_PROGRAM_1.0

203925 PID:c786682a TID:c7321fc2 back from cracker Current Status of
104: 5 ms

203925 PID:c786682a TID:c7321fc2

203925 PID:c786682a TID:c7321fc2 Queuing send Current Status of 104: 7
ms

203925 PID:c786682a TID:c7321fc2 SMBSRV-TCP -- sending response for packet:
104 on socket 15

203925 PID:c786682a TID:c7321fc2 SMB_SRV: TCP transport -- needed to block
on overlapped WSASend()

Re: more details

Re: more details

204106 PID:c786682a TID:c7321fc2 SMB(0x 32 --- SMBtrans2) packet 104 ---
took 164 to process!
204106 PID:c786682a
TID:c7321fc2 -----

=====
===== >>

rest in the next message.

• **References:**

- ◆ **File Sharing in 5.0**
 - ◇ From: joseph garibaldi
 - ◆ **more details**
 - ◇ From: joseph garibaldi
 - ◆ **RE: more details**
 - ◇ From: wrx03ppp
 - ◆ **Re: more details**
 - ◇ From: Joseph Garibaldi
 - ◆ **Re: more details**
 - ◇ From: wrx03ppp
 - ◆ **Re: more details**
 - ◇ From: Joseph Garibaldi
 - ◆ **Re: more details**
 - ◇ From: wrx03ppp
- Prev by Date: **Re: Want EBOOT..for Intel 82559 Ehternet...**
 - Next by Date: **Debug messages**
 - Previous by thread: **Re: more details**
 - Next by thread: **Debug messages**
 - Index(es):
 - ◆ **Date**
 - ◆ **Thread**