

Great job man :-)

Aku sendiri udah coba, tapi aku pake cara dan tools yang berbeda.  
Mungkin bisa membantu buat para newbie :-)

Tools :

- W32Dasm
- HEDt
- SoftICE ( optional )

Setelah nyoba sekali dan membaca nag screen yang muncul, aku Disassembly WinSolo dengan menggunakan W32Dasm. Setelah itu, aku pake fasilitas String Data References yang ada di W32Dasm.

Ini sebagian yang aku liat :

```
=====
String Resource ID=00002: "WinSolo"
"      (((((      "
" "
"* .exe"
" ."
"!ABS"
"\ "
"Boot"
"Browse for application"
"Explorer.exe"
"FYI. A more recent version of " ==>>> INI YANG MENARIK
"KERNEL32.DLL"
"MMTASK.TSK"
"MPREXE.EXE"
"MSGSRV32.EXE"
"PDT"
"Please close all MS-DOS sessions "
=====
```

Tulisan yang aku kasi' tanda di atas, adalah tulisan yang sama dengan apa yang tampil di nag screen.

Klik 2 kali di tulisan itu, dan pointer W32Dasm akan berpindah ke :

```
:0040114E 68B4104100      push 004110B4
```

Satu baris itu gak akan menolong, oleh karena itu, liat ke bagian atasnya dan kamu bakal melihat ini :

```
=====
:0040113D 83FAFC      cmp edx, FFFFFFFC
:00401140 7E05      jle 00401147      ( PETUNJUK 3)
:00401142 83FA78      cmp edx, 00000078
:00401145 7E14      jle 0040115B      ( PETUNJUK 4)
```

\* Referenced by a (U)nconditional or (C)onditional Jump at Address:  
|:00401140(C) ( PETUNJUK 2 )

```

|
:00401147 6A40          push 00000040

* Possible StringData Ref from Data Obj ->"WinSolo"
|
:00401149 6850114100    push 00411150

* Possible StringData Ref from Data Obj ->"FYI. A more recent version of "
->"this program MAYBE available from "
->"http://procode.com.au/. Otherwise "
->"the date setting on your computer "
->"is possibly wrong."
|
:0040114E 68B4104100    push 004110B4    ( PETUNJUK 1 )
:00401153 6A00          push 00000000

* Reference To: USER32.MessageBoxA, Ord:0195h
|
:00401155 FF1570644100    Call dword ptr [00416470]

```

---

Okeh kita bahas pelan - pelan :-)  
Perhatikan baris yang aku tandai dengan kata "PETUNJUK"

PETUNJUK 1 :  
Ini tempat menampilkan tulisan di dalam nag screen tersebut.  
Bagaimana aku tahu ???  
Perhatikan tulisan di atasnya, tulisan itu sama persis dengan apa yang muncul di nag screen....that's my clue ;-)

Sekarang kita telusuri ke belakang. Baca baris - baris di atasnya.

PETUNJUK 2 :  
"Referenced by a (U)nconditional or (C)onditional Jump at Address:"  
berarti menunjukkan lokasi tempat di mana nag screen itu dipanggil.  
Secara logika, kalo kita tau tempat dipanggilnya nag screen tersebut,  
kita tinggal merubah perintahnya supaya nag screen itu ngak pernah dipanggil.

PETUNJUK 3 :  
Alamat yang disebutkan di Petunjuk 2 mengarah ke petunjuk berikutnya.

```
:00401140 7E05          jle 00401147
```

Apa maksud perintah di atas ???  
Maksudnya, bahwa program akan melompat ke alamat 00401147 jika hasil perbandingan sebelumnya ( liat baris di atasnya ) bernilai "lebih kecil ato sama dengan".

Kita tau persis bahwa apapun hasil perbandingan di atas, program tidak boleh memanggil nag screen, oleh karena itu, perintah tersebut harus

dirubah. Salah satu contoh perubahan yang paling mudah adalah menggantinya dengan perintah NOP ( sudah diterangkan Teguh di tutsnya ). Dan karena perintah JLE itu sama dengan "7E 05" ( liat di kirinya ), maka kita harus menggantinya dengan "90 90"

Sudah selesai ???

Ternyata belon, setelah aku coba, nag screen masih tetap muncul. Untuk itu kita kembali ke listing program kita dan perhatikan petunjuk berikutnya.

PETUNJUK 4 :

```
:00401145 7E14          jle 0040115B
```

Ternyata masih ada Conditional Jump lainnya. Sama dengan perintah sebelumnya, perintah ini akan melompat berdasarkan hasil perbandingan sebelumnya ( perintah CMP ato Compare, di atasnya ).

Apabila hasilnya "lebih kecil ato sama dengan", maka nag screen tidak akan ditampilkan.

Lalu apa yang harus dilakukan ??? Apa harus dirubah dengan perintah NOP lagi ???

Tentu tidak, kita tidak boleh merubahnya menjadi NOP karena dengan demikian program akan tetap menjalankan perintah untuk menampilkan nag screen yang berada di bawahnya.

Kita harus membuat program untuk melompat ke 0040115B, tanpa memperdulikan hasil perbandingannya.

Untuk itu, kita tinggal merubah perintah "JLE" menjadi perintah "JMP" ato Jump, sebuah Unconditional Jump. Dengan perintah ini, program akan melompat ke alamat yang dituju tanpa memperdulikan hasil "CMP" di atasnya.

Testing....and cracked.....udah gitu ajah ;-)

Kode Hexa untuk perintah "JMP" bisa kamu liat dengan menggunakan SoftICE, sedangkan perubahan secara permanen bisa dilakukan dengan HEdit.

CHuPaCaBRa - [DCS]

The Only Crack Society - DeaD CRaX SoCieTY

<http://www.deadcrax.org>