

Forum:[Hack Forums](#)

Thread: [Remote CMD shell](#)

Kisame? - July 9, 2017, 11:30 am

Hello,

I'm coding my own RAT/shell, and so far it includes a real time keylogger, retrieve PC name and a command to retrieve all filenames from the desktop.

I now want to add another command, which would open a hidden CMD session on the clients side, to which I can send commands from the serverside.

I've tried some things and searched around, but the only thing I can find is how to send a single command to the clients CMD. I want to open a CMD Windows and view the input/output remotely.

I'm still kind of a noob @ C#, so I guess many will think something like 'find out yourself' or w/e. I understand that, and I'm not trying to beg here for someone to code it for me. But I'd like maybe some hints because I've no idea where to start to create this function.

Thanks in advance for any kind of help!

corexev - July 9, 2017, 12:35 pm

Use 'ConsoleAppLauncher' from the NuGet package manager:

You can create a class that stores the console output.

PHP Code

```
<?php
using SlavaGu.ConsoleAppLauncher;
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace MyApplication
{
    class RunConsoleApp
    {
        string Console = string.Empty;
        public string RunConsole(string executable, string arguments)
        {
            Console = Console + Environment.NewLine + ConsoleApp.Run(executable, arguments).
Output.Trim(); // Stores each run output
            return Console;
        }
    }
    public void Main()
    {
        RunConsoleApp rconsoleapp = new RunConsoleApp(); // Create object
```

```
        Console.WriteLine(rconsoleapp.RunConsole("cmd.exe", "ping 127.0.0.1"));
// Run and write to console
    }
}
```

Kisame? - July 9, 2017, 12:38 pm

(Jul 9, 2017 12:35 PM)corexev Wrote: [\[CITE\]](#) Use 'ConsoleAppLauncher' from the NuGet package manager:

You can create a class that stores the console output.

PHP Code

```
<?php
using SlavaGu.ConsoleAppLauncher;
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace MyApplication
{
    class RunConsoleApp
    {
        string Console = string.Empty;
        public string RunConsole(string executable, string arguments)
        {
            Console = Console + Environment.NewLine + ConsoleApp.Run(executable, arguments).
Output.Trim(); // Stores each run output
            return Console;
        }
    }
    public void Main()
    {
        RunConsoleApp rconsoleapp = new RunConsoleApp(); // Create object
        Console.WriteLine(rconsoleapp.RunConsole("cmd.exe", "ping 127.0.0.1"));
// Run and write to console
    }
}
```

I'm gonna give it a try. Thanks for your answer, anyway! Looks good :)

Is it possible to open this in a new window? So the custom shell (my program, not CMD) stays open aswell?

I can't seem to get it to work.

<http://prntscr.com/ftldye>

Any ideas?

corexev - July 9, 2017, 1:07 pm

(Jul 9, 2017 12:38 PM)Kisame? Wrote: [\[CITE\]](#) I'm gonna give it a try. Thanks for your answer, anyway! Looks good :)

Is it possible to open this in a new window? So the custom shell (my program, not CMD) stays open

aswell?

I can't seem to get it to work.

Any ideas? Use this as the class:

PHP Code

```
<?php
```

```
class RunConsoleApp
```

```
{
    string Console = string.Empty;
    public string RunConsole(string executable, string arguments)
    {
        Console = Console + Environment.NewLine + ConsoleApp.Run(executable, arguments).
Output.Trim(); // Stores each run output
        return Console;
    }
}
```

Add to the top with your other using statements;

PHP Code

```
<?php
```

```
using SlavaGu.ConsoleAppLauncher;
```

Make sure you have added ConsoleAppLauncher to your NuGet packages. (Right click project, 'Manage NuGet Packages...')

Here's an updated example for you:

PHP Code

```
<?php
```

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using SlavaGu.ConsoleAppLauncher;
```

```
namespace CAPP
```

```
{
    class Program
    {
        class RunConsoleApp
        {
            string Console = string.Empty;
            public string RunConsole(string executable, string arguments)
            {
                try {
                    Console += Environment.NewLine + ConsoleApp.Run(executable, arguments).Output.
Trim(); // Stores each run output
                } catch (Exception ex) { Console += ex.Message; }
                return Console;
            }
        }
        private static RunConsoleApp rconsoleapp = new RunConsoleApp(); // Create Object
        static void Main(string[] args)
        {
```

```
        Console.WriteLine(rconsoleapp.RunConsole(args[0], args[1]));  
    // Run args[0] with args[1] arguments and write to console  
    }  
}  
}
```

I'm not quite sure what you're asking about the 'open in a new window'. I added a try statement so your server doesn't close when using the class and appends the error to the console return variable.

Kisame? - July 9, 2017, 2:37 pm

Thanks for the help, I appreciate it!